T H Ø G E R B A N G

T A L T E O R I

Foraaret 1977

KAPITEL I: Indledning.

Vort Emne skal fremfor alt være den naturlige Talrække, altsaa Strukturen $(\mathbb{N},+,\cdot,<)$.

Kronecker (1823-91) skrev: "Die ganzen Zahlen hat der liebe Gott geschaffen, alles anderes ist Menschenwerk." Fra det indledende Algebrakursus er det bekendt at man kan gaa dybere, idet Peano (1858-1932) og andre gav en aksiomatisk Opbygning af Talrækken udfra Tallet 1 ved Hjælp af Processen "at lægge 1 til", eller - løsere udtrykt - "Talrækken er en stadigt fortsættelig Række en, to, tre,... uden Gentagelser". Ved denne Fremstilling faar man ogsaa umiddelbart den naturlige Ordning af Mængden, altsaa Strukturen $(\mathbb{N},<)$.

Det er ogsaa bekendt hvorledes Talrækken kan organiseres som ordnet Halvgruppe paa to Maader, ved "Addition" og "Multiplikation", og at disse Regningsarter yderligere opfylder de sædvanlige Betingelser (de kommutative og distributive Love).

Halvgruppen med $+$ kan udvides til en Gruppe, og derved opnaar man det ordnede Integritetsomraade $(\mathbb{Z},+,\cdot,<)$ som en Udvidelse af Strukturen $(\mathbb{N},+,\cdot,<)$.

Desuden har som bekendt $(\mathbb{Z},+,\cdot,<)$ Egenskaben: Enhver nedad/opad begrænset Talmængde har et minimalt/maximalt Element.

Specielt har $(\mathbb{N},<)$ den "nedstigende Kædes Egenskab": Enhver aftagende (i svag Forstand) Følge er sluttelig stationær.

Denne sidste Egenskab er især fremhævet og benyttet til Umulighedsbeviser af Pierre de Fermat (1601-65) i Metoden "descente infinie":

Hvis $M \subseteq \mathbb{N}$, og $a \in M \Rightarrow \exists b: b < a \wedge b \in M$, saa er $M = \emptyset$.

Eksempler (den endnu ikke omtalte men velkendte entydige Primopløsning af hele Tal benyttes):

1) Tallet $\sqrt{2}$ er irrationalt. Thi antages $\sqrt{2} = p/q$, $p,q \in \mathbb{N}$, faas $p^2 = 2q^2$ hvoraf følger at p er lige, $p = 2r$, og indsættes dette faas $q^2 = 2r^2$, saa at $\sqrt{2} = q/r$; endvidere er aabenbart $p > q$. Lad nu M være Mængden af mulige Tællere for $\sqrt{2}$, saa vil M med p ogsaa indeholde det mindre Tal q, hvoraf følger at M er tom og $\sqrt{2}$ er irrational.

2) Polynomiet $x^3 + (2x+3)^3 + 1 = 9x^3 + 36x^2 + 54x + 28$ har ingen rational Rod og er altsaa irreducibelt over $\mathbb{Q}$.

Bevis: Prøver vi med $x = p/q$ ($p \in \mathbb{Z}$, $q \in \mathbb{N}$) og indsætter faas

(A) $$\underbrace{9p^3 + 36p^2q + 54pq^2}_{\text{deleligt med 3,}} + 28q^3 = 0 \qquad \text{altsaa } q = 3q_1 \text{ ;}$$

indsættes dette faas (ved at dividere med 9)

$$p^3 + \underbrace{12p^2q_1 + 54pq_1^2 + 84q_1^3}_{\text{deleligt med 3,}} = 0 \qquad \text{altsaa } p = 3p_1 \text{ ;}$$

indsættes dette faas igen Ligningen (A), men nu med p_1 og q_1 i St.f. p og q (ikke overraskende, da den er homogen i p og q). Hvis M er Mængden af mulige Nævnere ($\in \mathbb{N}$) for x vil M med q altsaa indeholde $q_1 < q$, hvoraf følger at M er tom. (Man bemærker, at Polynomiets Irreducibilitet ikke kan bevises med det fra Algebraen bekendte "Eisensteins Kriterium").

Lad os uddybe den i det foregaaende behandlede Induktion med følgende Sætning, som vi for at gøre den mere umiddelbart forstaaelig vil formulere grafteoretisk:

Ramsey's Sætning (R. 1903-1930): Lad der være givet en Graf bestaaende af uendelig mange Punkter og deres Forbindelseslinier (netop én Forbindelseslinie mellem hvert Punktpar), og enhver af disse er enten rød eller grøn. Da er det muligt at udtage en uendelig Delgraf, i hvilken samtlige Forbindelseslinier har samme Farve.

Bevis: Lad Punktmængden hedde M. For $a \in M$ sætter vi R_a lig Mængden af de Punkter i M som med rød Linie er forbundet med a, og G_a lig Mængden af de Punkter aom med grøn Linie er forbundet med a; $R_a + G_a = M \setminus \{a\}$.

Dersom nu

$$(Z) \qquad \forall A \subseteq M, A \text{ uendelig } \exists a \in A: A \cap R_a \text{ uendelig}$$

gaar det at udtage en uendelig "rød" Delgraf:

Vi vælger $a_1 \in A_o = M$ saaledes at $A_1 = A_o \cap R_{a_1}$ uendelig

... $a_2 \in A_1$ ... $A_2 = A_1 \cap R_{a_2}$ ...

... $a_3 \in A_2$ ... $A_3 = A_2 \cap R_{a_3}$ ...

o.s.v.;

da $a_n \in A_{n-1} = \bigcap_{j=1}^{n-1} R_{a_j}$ vil enhver Forbindelseslinie mellem a_n og a_j være rød (for $j < n$), saa $\{a_n\}$ giver en rød Graf.

Dersom (Z) svigter gælder Negationen

$$\exists A_o \subsetneq M,\ A_o \text{ uendelig } \forall a \in A_o: A_o \cap R_a \text{ endelig}$$

og dermed

$$\forall A \subseteq A_o,\ A \text{ uendelig } \forall a \in A: A \cap R_a \text{ endelig.}$$

Men da $A \cap R_a$ endelig medfører $A \cap G_a$ uendelig ses, at vi er kommet tilbage til Situationen fra (Z), blot med "grøn" i St.f. "rød" og med A_o i St.f. M; vi kan altsaa i dette Tilfælde udtage en uendelig grøn Delgraf. □

Kommentarer:

1) Der er naturligvis intet i Vejen for at der kan være Tilfælde, hvor det er muligt at udtage baade en uendelig rød og en uendelig grøn Delgraf.

2) Sætningen kan umiddelbart generaliseres til et endeligt Antal Farver, h Stk., idet man først udtager en rød Delgraf eller en som kun indeholder de øvrige h-1 Farver; i det sidste Tilfælde udtager man dernæst enten en grøn Delgraf eller en som kun indeholder de øvrige h-2 Farver, o.s.v.

3) Beviset benytter aabenbart Udvalgsaxiomet, men dersom den givne Graf bestaar af eller indeholder en Punktfølge kan det gøres konstruktivt, idet man ved hvert Valg af a_j blot tager det første Punkt som opfylder de ønskede Krav.

4) Det er rimeligt - og ogsaa vist af Ramsey - at der gælder "endelige Tilnærmelser" til Sætningen af Typen: Hvis man har en flerfarvet Graf med et stort Antal Punkter, da kan man udtage en ensfarvet Graf med et ret stort Antal Punkter. Men numeriske Vurderinger af de indgaaende Antal fører til voldsomme Vanskeligheder, som trods stort Arbejde langtfra er løst.

Eksempler:

1) Hvis der er givet uendelig mange Punkter i et euklidisk Rum er det muligt muligt at udtage enten en uendelig Delmængde hvori alle Distancer er rationale, eller en uendelig Delmængde hvori alle Distancer er irrationale.

2) Af en vilkaarlig Følge af Elementer $x_1, x_2, \ldots$ i en totalt ordnet Mængde kan man udtage enten en strengt monoton Delfølge eller en konstant Delfølge (man lader blot for $i < j$ tre Farver svare til hhv. $x_i < x_j$, $x_i = x_j$ og $x_i > x_j$). Man bemærker, at i $(\mathbb{R}, <)$ kan dette Resultat let ses direkte, men derved benyttes limsup og liminf i denne Struktur (!).

3) Matematiske Værker har hyppigt mange Referencer til (tidligere udkomne) matematiske Værker. Af et uendeligt (eller meget stort) matematisk Bibliotek er det muligt at udtage et uendeligt(eller ret stort) Delbibliotek D, enten saa ingen Bog i D refererer til nogen anden Bog i D, eller saa enhver Bog i D refererer til samtlige ældre Bøger i D.

Det er bekendt at den induktivt definerede Talrække kan benyttes til Angivelse af Antal, altsaa som Kardinaltal, der paa denne Maade bliver et afledt Begreb, medens Ordinaltallene er det primære (det sker, idet man jo er i Stand til at bevise den ofte empirisk konstaterede Kendsgerning, at hvis man fx. har en Stabel Nummersedler med 1,2,3,... og sætter én fast paa Ryggen af hver af Deltagerne i et Cykelløb, saa vil man altid komme lige langt ned i Bunken hvordan man end fordeler Sedlerne paa Cykelrytterne, og Tallet paa den sidst benyttede siges saa at angive Antallet). I Forbindelse hermed har man Sætningerne (idet vi lader $|A|$ betegne Antallet Elementer i Mængden A): Hvis en Afbildning $A \to B$ er injektiv saa er $|A| \leqq |B|$, hvis den er surjektiv saa er $|A| \geqq |B|$, og hvis den er bijektiv saa er $|A| = |B|$. Disse Sætninger og deres umiddelbare Konsekvenser er Indholdet af de saakaldte Skuffeprincipper (tysk: Schubfachpr., eng.: pigeonhole-pr.) som er fremhævet og med stor Succes anvendt af Lejeune Dirichlet (tysk, 1805-1859). Lad os nævne et Par: "Hvis man har flere Skuffer end Ting i dem, saa er nogle af Skufferne tomme" og "hvis uendelig mange Ting er fordelt i endelig mange Skuffer, saa vil mindst en af Skufferne indeholde uendelig mange Ting".

Eksempler:

1) (Variant af klassisk Opgave) Der findes i hvert Fald 3 Mennesker i København som har det samme Antal Haar paa Hovedet.

Bevis: Persontallet er $>$ 500.000 (hvorledes det end udregnes) og Antallet Haar paa et Hoved er $<$ 200.000 (50.000 angiver som "normalt", 120.000 som exceptionelt stort), og putter 500.000 Mennesker i 200.000 Skuffer vil mindst en af dem indeholde mindst 3 Personer.

2) For at kunne skelne mellem n Tilfælde maa der være mindst n forskellige Muligheder i Informationsmaterialet:

a) Givet n Mønter, af hvilke en falsk med (lidt) afvigende Vægt. Uden Lodder skal man ved højst p Vejninger paa en ligearmet Skaalvægt finde den falske og bestemme om den er for let eller for tung. Enhver Vejning kan give 3 Resultater: Ligevægt eller højre Skaal tungest eller venstre Skaal tungest. Altsaa

$$2n < 3^p.$$

(NB: Det er uden Betydning at Fremgangsmaaden ved de senere Vejninger vil afhænge af Resultaterne af de foregaaende. Endvidere ses, at Betingelsen kun er nødvendig; for $n = 2$ er Opgaven uløselig).

b) Et Personnummer bestaar af 10 Cifre

a	b	/	c	d	/	e	f	-	g	h	i	j
Da			Må			År						

De 4 første Cifre angiver en Dato, og der er altsaa ca. 360 Muligheder for dem; de sidste 6 Cifre giver 10^6 Muligheder, men det samlede Antal Muligheder bliver kun ca. 33.000.000, da der i Nummeret er indbygget en Kontrolregel (Tallet $4a+3b+2c+7d+6e+5f+4g+3h+2i+j$ skal være delelig med 11; bemærk at dette fx sikrer mod Ombytning af to Nabocifre). Man ser at der er et vist Overskud i Fh.t. Danmarks Befolkning, men dels skal Systemet jo ogsaa kunne identificere (nylig) afdøde og endnu ufødte Personer og dels er med den givne

Aldersfordeling visse Fødselsaar hyppigere end andre (or bl.a. af Hensyn til de hundredeaarige benyttes $g \geq 5$ ved Fødselsaar 18.., hvilket væsentligt nedsætter Ant 11et), og endelig skal der jo ogsaa være Plads til statistiske Svingninger; at j lige benyttes for Kvinder og j ulige for Mænd betyder ikke noget væsentligt Tab, da der er nogenlunde lige mange.

3) Ethvert naturligt Tal har et positivt Multiplum, som i Titalssystemet skrives med kun Cifrene 0 og 1 (russisk Olympiadeopgave).

Bevis: Ved sædvanlig Division med n er der kun Mulighed for n forskellige Divisionsrester. Blandt Tallene 1, 11, 111,... vil der derfor være to som giver samme Rest ved Division med Tallet, og deres Differens har Egenskaben.

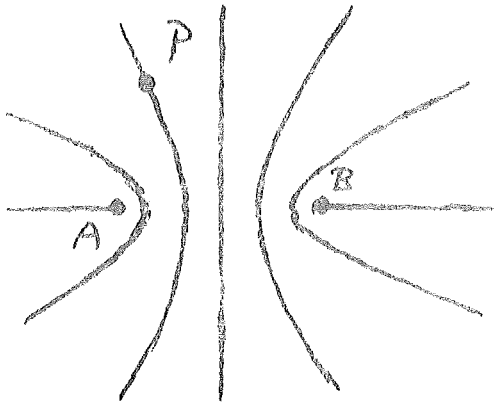
4) Hvis man blandt Tallene 1, 2,..., 2n udtager n+1 Stk., vil der blandt dem findes to a og b, hvor a gaar op i b (det er aabenbart ikke tilstrækkeligt at udtage n Stk., idet Sættet n+1, n+2,..., 2n ikke har Egenskaben).

Bevis: Ethvert naturligt Tal kan skrives paa Formen $2^h \cdot u$, hvor u er ulige. Her kan u antage de n Værdier 1, 3, 5,..., 2n-1 og vi putter nu Tal med samme u i samme Skuffe; der vil være mindst en Skuffe med flere Tal, og to af disse har Egenskaben.

5) Hvis man har 9 Punkter i det 3-dimensionale Heltalsgitter $\mathbb{Z}^3$, da vil mindst et af Liniestykkerne imellem dem indeholde et Gitterpunkt i sit indre (aabenbart er 8 Punkter ikke nok, hvilket ses af Hjørnerne i en Enhedsterning).

Bevis: Punkterne falder i 8 Klasser af Type (lige,lige,lige), (lige,lige,ulige),..., altsaa mindst en Klasse med to Punkter. Deres Koordinatdifferenser er lige, og Forbindelsesliniestykkets Midtpunkt er derfor et Gitterpunkt.

6) Hvis der er givet uendelig mange Punkter i en euklidisk Plan og samtlige Distancer er heltallige, saa vil Punkterne ligge paa ret Linie.



Bevis: Lad A og B være to af Punkterne. For et tredie Punkt P er $|PA - PB|$ hel og $\leqq AB$, og P vil derfor ligge paa en af endelig mange Hyperbelgrene med Brændpunkter i A og B eller evt. paa Midtnormalen eller en af Halvlinierne udfra A eller B. Gøres det samme med PA i St.f. AB faas igen et endeligt Hyperbelsystem, og de to Systemer har ialt kun endeligt mange Fællespunkter (to Hyperbler har højst 4 Fællespunkter, da et Keglesnit er bestemt ved 5 Punkter), medmindre P ligger paa Linien AB, i hvilket Tilfælde Halvlinierne tildels vil falde sammen. Men naar Punktmængden er uendelig maa det sidste Tilfælde indtræffe, og Mængden er lineær.
Beviset skyldes P.Erdös,(1913 -).

Lad os videreføre Skuffeprincippet med en mere generel Afbildningssætning, som løst udtrykt siger at "det er muligt at anbringe Ting i Skuffer paa ønsket Maade medmindre det er aabenlyst umuligt".

Ligesom tidligere skal $|A|$ betegne Elementtallet i Mængden A. At en Afbildning f af en Mængde A er injektiv kan aabenbart udtrykkes ved at det for enhver endelig Delmængde $D \subseteqq A$ gælder at $|f(D)| = |D|$.

Idet M og K er endelige Mængder vil vi betragte Afbildninger $f: M \to \{\text{Delmængder af } K\}$. For $a \in M$ har vi altsaa $f(a) \subseteqq K$, og for en Delmængde $D \in M$ sættes (som sædvanlig) $f(D) = \bigcup_{a \in D} f(a)$.

Man bemærker at $f(D \cup E) = f(D) \cup f(E)$ og at $f(D \cap E) \subseteqq f(D) \cap f(E)$. Idet $|f(a)|$ betegner Antallet af Elementer (i K) ses, at en Afbildning $M \to K$ kan opfattes som en Afbildning af ovennævnte Art hvori $|f(a)| = 1$ for alle a.

For Afbildningerne indfører vi en partiel Ordning idet vi sætter $f_1 \succ f_2$ dersom $f_1(a) \supseteqq f_2(a)$ for alle $a \in M$. Man ser at $f_1 \succ f_2$ medfører at $|f_1(D)| \geqq |f_2(D)|$ for alle $D \subseteqq M$.

König's Sætning (D.König, 18 -19): Nødvendigt og tilstrækkeligt for at f majoriserer en injektiv Afbildning af M ind i K er det at $|D| \leqq |f(D)|$ for alle $D \subseteqq M$.

En Variant af Sætningen er senere fremsat af Philip Hall, og den gaar derfor undertiden under hans Navn.

Bevis: At Betingelsen er nødvendig er klart, thi som bemærket gælder for en Injektion f at $|D| = |f(D)|$ for alle $D \subseteqq M$.

Vi skal vise Tilstrækkeligheden.

Lad F være Mængden af de f for hvilke $|D| \leqq |f(D)|$ for alle $D \subsetneqq M$. Saa er Problemet aabenbart at vise, at ethvert Element i F som er minimalt ved $\prec$ er en injektiv Afbildning $M \to K$, thi da F er endelig vil ethvert f majorisere et Minimalelement.

For et $f \in F$ gælder $|D| = |f(D)|$ for visse (evt. ingen) $D \subseteqq M$, og dersom det gælder for D_1 og D_2 saa gælder det ogsaa for $D_1 \cap D_2$ (og iøvrigt ogsaa for $D_1 \cup D_2$), idet

$$|D_1| + |D_2| = |D_1 \cup D_2| + |D_1 \cap D_2| \leqq |f(D_1 \cup D_2)| + |f(D_1 \cap D_2)|$$
$$\leqq |f(D_1) \cup f(D_2)| + |f(D_1) \cap f(D_2)| = |f(D_1)| + |f(D_2)|$$

som igen er lig $|D_1| + |D_2|$, saa der maa gælde Lighedstegn i Uligheden her. Endvidere ses at for et $f \in F$ kan $f(a)$ ikke være tom, da jo $|f(a)| \geq |\{a\}| = 1$.

At f er minimal i F betyder, at hvorledes der end fjernes et Element c fra et $f(a)$, saa vil der være en Ulighed $|D| \leq |f(D)|$ som brister.

Heraf ses for det første, at for ethvert a maa der findes et $D \ni a$ for hvilket $|D| = |f(D)|$, thi hvis vi altid havde $|D| < |f(D)|$ kunde i værste Fald Ulighedstegnet blive ændret til et Lighedstegn; endvidere ses at Ulighedens Bristen sker ved at det paagældende c ikke ligger i noget $f(a')$, $a' \in D$, $a' \neq a$ (for hvis det gjorde det, vilde det jo stadig tilhøre $f(D)$).

Blandt de $D \ni a$, hvor $|D| = |f(D)|$ vil der ifølge ☞ være et mindste, nemlig D_a = Fællesmængden for dem, og det paagældende c tilhører altsaa ikke noget $f(a')$ med $a' \in D_a$, $a' \neq a$. Vi noterer, at $|D_a| = |f(D_a)|$.

Nu var c et vilkaarligt Element af $f(a)$, og vi har derfor $f(D_a \setminus \{a\}) = f(D_a) \setminus f(a)$ og dermed $|f(D_a \setminus \{a\})| = |f(D_a)| - |f(a)|$ $= |D_a| - |f(a)|$ og da $f \in F$ er dette $\geq |D_a \setminus \{a\}| = |D_a| - 1$, saa at $|f(a)| \leq 1$.

Dermed er vist, at ethvert $|f(a)| = 1$, saa f er en Afbildning $M \to K$, og da $f \in F$ saa $|D| \leq |f(D)|$ er det en Injektion. □

Eksempler:

1) Lokalefordeling paa H.C.Ørstedinstituttet til et vist Tidspunkt. Et Studenterhold a kan p.G.a. sin Størrelse, Krav til Tavleplads og Installationer o.s.v. kun benytte en vis Delmængde $f(a)$ af den samlede Mængde K af Auditorier. Hvis en Fordeling af Mængden M af Studenterhold skal være mulig

(og injektiv, idet man ikke ønsker to Hold i samme Rum), er det klart, at for en vilkaarlig Samling af $|D|$ Stk. Hold skal der kunne komme mindst ligesaa mange Auditorier paa Tale, men Sætningen viser saa, at denne nødvendige Betingelse ogsaa er tilstrækkelig.

2) En Samling M af Raad a med tildels de samme Medlemmer f(a) skal hver sende en Repræsentant til et nyt Raad; i dette kan ingen Deltager optræde som Repræsentant for mere end et af de gamle Raad. For at dette kan gøres er det klart nødvendigt, men altsaa ogsaa tilstrækkeligt, at et vilkaarligt Sæt D af Raadene skal have ialt mindst $|D|$ forskellige Medlemmer.

3) "Ægteskabsproblemet": Man har to Mængder D og P med lige mange Elementer. Der findes en Del (venligtsindede og gensidige) Bekendtskaber mellem Elementer fra D og P. Dersom blot enhver Delmængde af D tilsammen kender mindst ligesaa mange Elementer fra P, saa er det muligt at foretage en Bijektion mellem Mængderne, saaledes at hvert $d \in D$ forbindes med en ham bekendt $p \in P$. Heraf følger det (paa Forhaand langtfra indlysende), at enhver Delmængde af P maa ogsaa tilsammen have kendt mindst ligesaa mange Elementer af D.

Fra tidligere Algebrakurser er det bekendt at det ordnede Integritetsomraade $(\mathbb{Z}, +, \cdot, <)$ kan udvides til sit Brøklegeme $(\mathbb{Q}, +, \cdot, <)$, som vi ogsaa lejlighedsvis skal betragte. De videre Strukturer $\mathbb{R}$ og $\mathbb{C}$ og Funktionslæren paa dem skal vi kun benytte som Hjælpemidler, men ikke for deres egen Skyld (dog vil de bl.a. indgaa i fx Sætninger om Vurderinger af Talmængder).

I Integritetsomraadet $(\mathbb{Z},+,\cdot)$ kendes alle Idealer, idet det netop er Hovedidealerne (n), hvor $n \in \mathbb{N}_0$ (og der gælder det specielle, at enhver Undergruppe i den additive Gruppe er et Ideal). De ikke-trivielle Homomorfier er derfor Afbildningerne af Typen $(\mathbb{Z},+,\cdot) \to (\mathbb{Z},+,\cdot)/(n) = (\mathbb{Z}_n,+,\cdot)$, hvor Billedet er Restklasseringen modulo n. Den tilsvarende Ækvivalensrelation kaldes Kongruens modulo n og betegnes $\equiv \pmod{n}$. Den er indført af Gauss (1777-1855) som det første Eksempel paa en Ækvivalensrelation harmonerende med Kompositioner.
$(\mathbb{Z},+,\cdot)$ er altsaa en Hovedidealring, dens invertible Elementer er $\{\pm 1\}$ og en Klasse associerede er $\{\pm a\}$, og af enhver Klasse associerede kan vælges netop én Repræsentant $\in \mathbb{N}$ (og Multiplikation af saadanne Repræsentanter fører igen til Repræsentanter i $\mathbb{N}$).
For de ikke-invertible Elementer af $\mathbb{N}$ gælder at $ab = c \Rightarrow 1 < a,b < c$, hvoraf ses at der findes irreducible Elementer, nemlig i hvert Fald det mindste ikke-invertible Element (altsaa Tallet 2). De irreducible Elementer indenfor $\mathbb{N}$ betegnes "Primtal" og kan opstilles ordnet 2,3,5,... .
Hovedidealet frembragt af et Primtal p er et Maximalideal, hvoraf følger at den tilsvarende Restklassering $(\mathbb{Z}_p,+,\cdot)$ er et Legeme. Da et Maximalideal ogsaa er et Primideal vil $p \mid ab \Rightarrow p \mid a \vee p \mid b$.
Da $(\mathbb{Z},+,\cdot)$ er en Hovedidealring gælder for Idealerne den "opstigende Kædes Egenskab", som medfører at ethvert naturligt Tal kan skrives som Produkt af Primtal. Endvidere gælder "Fællesmaalsegenskaben", som medfører at den nævnte Primopløsning er entydig.
Medens Primopløsningens Mulighed er ret triviel - den mindste Divisor større end 1 i et Tal vil altid være Primtal - saa er

dens Entydighed ikke indlysende (omend ret let beviselig, fx ved Induktion), hvilket fx Euklid (365-275 (?) f.Chr.) ikke var klar over. "Euklids Algoritme" benyttede han til Bestemmelse af største fælles Divisor for to Tal, men ikke til at vise Primopløsningens Entydighed, den forudsatte han blot stillíende. Entydigheden blev første Gang omtalt og bevist af Gauss i "Disquisitiones Arithmeticæ" 1801.

At Primopløsningen er entydig kan ogsaa udtrykkes: Strukturen $(\mathbb{N}, \cdot)$ er en fri Halvgruppe med Primtallene som Frembringerelementer, hvor Glosen "fri" gaar paa at der ikke findes nogen Identiteter $p_1^{\alpha_1} \dots p_r^{\alpha_r} = q_1^{\beta_1} \dots q_s^{\beta_s}$ mellem dens Elementer; Halvgruppen er abelsk.

Funktionen $[x]$.

Den paagældende Funktion er en Afbildning $\mathbb{R} \to \mathbb{Z}$, som til ethvert x lader svare det største hele Tal mindre end eller lig x.

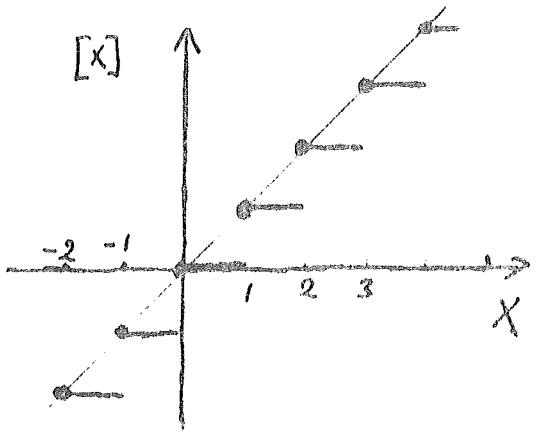
Betegnelse: $[x]$ = "den hele Del af x" (ent x bruges ogsåa).

Eksempler: $[1] = 1$

$[\sqrt{2}] = 1$

$[-\sqrt{2}] = -2$

$[\pi] = 3$



For $a \in \mathbb{Z}$ er $[x+a] = [x] + a$.

Endvidere

$$x - 1 < [x] \leqq x < [x] + 1.$$

Eksempel: $[x + \frac{1}{2}]$ = det hele Tal som ligger nærmest ved x, dog det største hvis x ligger midt imellem to hele Tal, thi $[x + \frac{1}{2}] = n \Leftrightarrow n - \frac{1}{2} \leqq x < n + \frac{1}{2}$. Ønskes det hele Tal nærmest x, dog det mindste hvis x ligger midt imellem to hele Tal, kan man bruge $-[-x+\frac{1}{2}]$.

Eksempel: $$[x] = \left[\frac{x}{n}\right] + \left[\frac{x+1}{n}\right] + \ldots + \left[\frac{x+n-1}{n}\right].$$

Rigtigheden fremgaar fx af at begge Sider er voksende Trappefunktioner af x, kontinuerte fra højre, og de har begge de samme Spring, nemlig +1, naar x voksende passerer et helt Tal, idet da netop ét af Leddene paa højre Side springer; og for $x = 0$ gælder Formlen, $0 = 0$. Man ser, at den foranomtalte Funktion $[x+\frac{1}{2}]$ ogsaa kan skrives $[2x] - [x]$.

Ved en Divisionsligning med Rest forstaas en Ligning, hvor der til given Dividend $D \in \mathbb{Z}$ og Divisor $d \in \mathbb{N}$ er taget en heltallig Kvotient q og en Rest r, saa $D = d \cdot q + r$.
Den principale Divisionsligning er den hvor $q = \left[\frac{D}{d}\right]$, hvilket ses at være ensbetydende med at $0 \leqq r < d$.

Positionssystemet.

Vi bruger 10-Talssystemet; Babylonerne brugte 60-Talssystemet (Reminiscenser i Minut-og Sekundinddelingen af Tid og Vinkler), og andre - tildels blandede - Systemer har været brugt, hvoraf der findes Reminiscenser i forskellige Sprog.
Ideen er som bekendt, at man vælger et Grundtal $g \in \mathbb{N} \setminus \{1\}$, og saa gælder Sætningen:
Ethvert Tal $n \in \mathbb{N}$ kan paa netop én Maade skrives paa Formen

$$n = a_0 + a_1 g + \ldots + a_r g^r,$$

hvor for alle j gælder $0 \leqq a_j < g$, og endvidere $a_r > 0$. Og omvendt vil ethvert Udtryk af denne Art fremstille et $n \in \mathbb{N}$.

Den sidste Paastand er indlysende, og det første ses let ved Induktion efter n, idet det aabenbart gælder for $n \leqq g$, og for $n > g$ har man $a_0 = n - \left[\frac{n}{g}\right] g$, hvor $\left[\frac{n}{g}\right]$ er naturligt Tal $< n$.

Som Skrivemaade for Tallet n benyttes saa det ordnede Sæt $a_r a_{r-1} \ldots a_1 a_0$.

Velkendte Sætninger fra 10-Talssystemet ses at have tilsvarende i g-Talssystemet, fx Ved Division med $g-1$ vil et Tal give samme Rest som dets Tværsum $a_r + \ldots + a_1 + a_0$.

Thi Homomorfien $(\mathbb{Z},+,\cdot) \to (\mathbb{Z}_{g-1},+,\cdot)$ fører g over i Etelementet, hvoraf Sætningen ses.

Denne Homomorfi kan som bekendt benyttes til en simpel Kontrol, i 10-Talssystemet kaldet "Ni-Prøve", paa Regningers Rigtighed, fx

	i 10-Talssystemet	modulo 9
	23·38	5·2
	+ 114	+ 6
faas til	874+114=988	≡ 7 ≡ 16.

Decimalbrøkslæren kan ogsaa umiddelbart overføres til vilkaarligt Grundtal g: For $0 < \delta < 1$ sættes $b_1 = [g\delta]$, $\delta_1 = g\delta - [g\delta]$

$b_2 = [g\delta_1]$, o.s.v.

og saa skrives δ som $0,b_1 b_2 \ldots$

Der gælder Sætninger som: Hvis q gaar op i en Potens af g, saa vil $\frac{p}{q}$ faa en endelig Udvikling; hvis q er primisk med g bliver $\frac{p}{q}$ rent periodisk; o.s.v.

Den konsekvente Brug af Decimalbrøker blev indført af Simon Stevin (nederlandsk, 1548-1620); iøvrigt kan man sige, at allerede Babylonerne brugte "flydende Komma" i deres Tabeller.

De i Skolen indlærte Regneskemaer kan ogsaa umiddelbart anvendes i g-Talssystemet, fx viser hosstaaende et Divisionsskema udført efter de sædvanlige Vedtægter (tvetydigt paa

				e	d
a	b	⌈ c	d	e	f
		c	c	d	
			e	d	f
			e	a	e
					d

et enkelt Punkt, nemlig hvorvidt den sidste Rest, d, har lov til at være 0). Det er et Eksempel paa en velkendt Opgavetype, idet det er en Division i g-Talssystemet hvori hvert Ciffer er erstattet med et Bogstav, og forskellige Bogstaver betegner forskellige Cifre; Opgaven er saa at finde Bogstavernes Cifferværdi og Grundtallet g (Vink til Løsning: find først Egenskaber ved d,e og g).

Saadanne Opgaver kan være morsomme, at de ikke behøver at være det kan ses af

$$\text{TWO} \cdot \text{ZERO} = \text{NOTHING},$$

som staar for en Multiplikation i 10-Talssystemet, og er en god Opgave forsaavidt som den har netop én Løsning, men det er næppe muligt uden Brug af en større Elektronregnemaskine at eliminere alle Mulighederne undtagen den ene rigtige, som er $867 \cdot 2057 = 1783419$.

Endnu et Eksempel: 11111 i g-Talssystemet er et Kvadrattal = K; g søges. Idet $(g^2+\frac{1}{2}g)^2 < g^4+g^3+g^2+g+1 = K < (g^2+\frac{1}{2}g+1)^2$ ses at $K = (g^2+\frac{1}{2}g+\frac{1}{2})^2$ er den eneste Mulighed, og indsætter man dette faas en Andengradsligning med Rødderne 3 og -1, saa g maa være 3. Indsættes dette ser man at det stemmer, idet $3^4+3^3+3^2+3+1 = 121 = 11^2$.

Stort g medfører, at Tallene n kan skrives kortere, men til Gengæld faar man Brug for flere Ciffertegn, og - hvad der er værre - man skal kunne den "lille Additionstabel" og den "lille Multiplikationstabel" udenad, altsaa alle a+b og a·b med $0 < a,b < g$. Der findes dog exceptionelle Regnekunstnere som regner i 100-Talssystemet, hvilket tydeligt ses idet Facits Cifre (i 10-Talssyst.) bliver opskrevet parvis (men de Præstationer man almindeligvis ser paa Dyrehavsbakken o.l.St. er ret ordinære).

Selve det at opskrive Resultatet af en Multiplikation uden Hel-

Ialmresultater kan gøres efter Diagonalmetoden uden at stille egentlige hukommelsesmæssige krav:

Fx

$$\begin{array}{r} 217 \\ \cdot\ 4328 \\ \hline 939176 \end{array}$$

$\boxed{.}$ er Facits Cifre bagfra

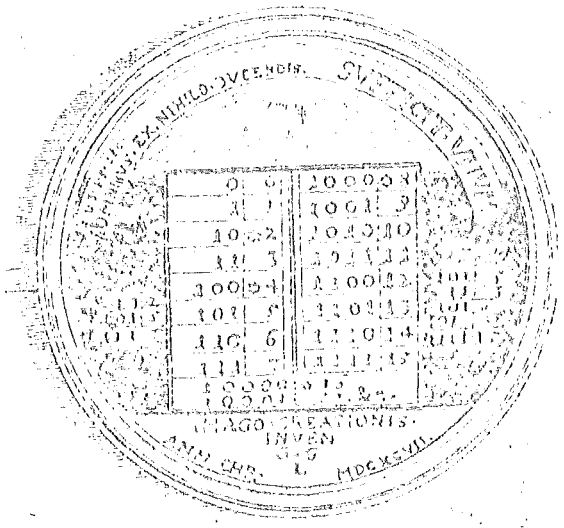
$7 \cdot 8 = 5\ \boxed{6}$

$5 + 1 \cdot 8 + 7 \cdot 2 = 2\ \boxed{7}$

$2 + 2 \cdot 8 + 1 \cdot 2 + 7 \cdot 3 = 4\ \boxed{1}$

o.s.v.

Den anden Yderlighed er $g = 2$. Der findes kun to Cifre, nemlig 0 og 1, og den"lille Tabel"er indskrænket til: $1 \cdot 1 = 1$.



Leibniz (1646-1716) benyttede Dualsystemet, og da han hørte at franske Jesuitermissionærer i Peking var stødt paa ældgamle Figurer, der maatte fortolkes som Tal i Dualsystemet foreslog han at man lavede en Medaille som hosstaaende, der paa en Gang giver Dualsystemet og kunde benyttes i Missionen som Billede paa Verdens Skabelse. I Midten er en Omsætningstabel, t.h. og t.v. (utydeligt) ses 2+5=7 og 5·3=15 udført i Dualsystemet; foroven staar:"Til at frembringe alt (2,3,4,5etc.) af intet (: 0) er Ét (: 1) tilstrækkeligt", forneden:"Billede paa Skabelsen" og hans (latiniserede) Initialer og Aaret 1697.

Dualsystemets moderne Anvendelser er velkendte og skal ikke beskrives her. Det indgaar ogsaa i talrige Spil og lignende.

Eksempel: "Talkunst":
"Sig i hvilke Rækker det af dig valgte Tal staar, og jeg skal sige dig hvad Tallet er."

1	3	5	7	9	11	13	15
2	3	6	7	10	11	14	15
4	5	6	7	12	13	14	15
8	9	10	11	12	13	14	15

Facit: Summen af Rækkernes Begyndelsestal(!)
(hvorfor ?)

I alt det følgende bruges vort sædvanlige 10-Talssystem.

KAPITEL II: Om Primopløsning og Primtallenes Fordeling.

Vi betragter Halvgruppen $(\mathbb{N},\cdot)$. I den findes entydig og altid mulig Primopløsning

$$a = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r},$$

hvor alle p_j er Primtal og alle $\alpha_j \in \mathbb{N}$ (i en Del Forbindelser kan det dog være praktisk at tillade Eksponenter $\alpha_j = 0$; om man vil kan man jo ogsaa tænke sig at Primtallene er opstillet ordnet og at Eksponenterne α_j saa er en Følge af Tal $\in \mathbb{N}_0$, men hvori kun endelig mange Led er positive).

Vi har "Gaa-op-Relationen", skrevet med Tegnet $|$, defineret ved at $a \mid b \Leftrightarrow \exists\, c\colon b = ac$. Dens Negation betegnes med $\nmid$. (Disse Relationer og Betegnelserne kan naturligvis bruges i enhver multiplikativ Struktur).

Gaa-op-Relationen er

reflexiv, da $a \mid a$
transitiv, da $a \mid b \wedge b \mid c \Rightarrow a \mid c$
asymmetrisk, da $a \mid b \wedge a \neq b \Rightarrow b \nmid a$,

det er altsaa en reflexiv Ordningsrelation paa $\mathbb{N}$; den er kun partiel, ikke total, da $2 \nmid 3 \wedge 3 \nmid 2$. Man ser ogsaa, at den er stærkere end Størrelsesordningsrelationen $\leq$, idet $a \mid b \Rightarrow a \leq b$.

Af Primopløsningerne

$$a = p_1^{\alpha_1}\cdot\ldots\cdot p_r^{\alpha_r}$$
$$b = p_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}$$

følger umiddelbart, at $a \mid b \Leftrightarrow$ alle $\alpha_j \leq \beta_j$.

Heraf følger igen, at der eksisterer en <u>største fælles Divisor for a og b</u>, nemlig $(a,b) = \prod_j p_j^{\alpha_j \wedge \beta_j}$ og et <u>mindste fælles</u>

Multiplum for a og b, nemlig m.f.Mult.$\{a,b\} = \{a,b\} = \prod_j p_j^{\alpha_j \vee \beta_j}$. Vi benytter her Betegnelsen $\alpha \wedge \beta$ til at angive det mindste af Tallene α og β, og $\alpha \vee \beta$ til at angive det største af dem; den afkortede Betegnelse $\{a,b\}$ er en ad hoc Betegnelse kun til Brug i dette Kapitel, den rummer en - dog næppe alvorlig - Risiko for Forveksling med Mængdesymbolet, og som det straks vil fremgaa kan den hyppigt undværes; endelig minder vi om at Betegnelsen (a,b) jo ogsaa benyttes om det af a og b frembragte Ideal indenfor $\mathbb{Z}$, men da det netop er frembragt af deres største fælles Divisor kan det næppe medføre uheldige Konsekvenser.

Idet $(\alpha \wedge \beta) + (\alpha \vee \beta) = \alpha + \beta$ ses, at $(a,b) \cdot \{a,b\} = ab$, saa $\{a,b\} = \frac{a \cdot b}{(a,b)}$.

De nævnte Resultater viser, at naar vi benytter $|$ som Ordningsrelation, saa gælder at en endelig Mængde har ved Gaa-op-Relationen en nedre Grænse og en øvre Grænse (d: Mængden af deres fælles Minoranter har et største Element, nemlig største fælles Divisor for Mængdens Elementer, og Mængden af deres fælles Majoranter har et mindste Element, nemlig Elementernes mindste fælles Multiplum).

Primtallene er netop Minimalelementerne i $\mathbb{N} \setminus \{1\}$ ved Gaa-op-Relationen.

Operationerne $(\ ,\ )$ og $\{\ ,\ \}$ kan opfattes som Kompositioner indenfor $\mathbb{N}$. Naar vi regner med dem kan vi enten direkte bruge deres begrebsmæssige Definition eller vi kan regne med Exponenterne α_j i Primopløsningen for Tal a.

Kompositionerne $(\ ,\ )$ og $\{\ ,\ \}$ er idempotente, altsaa $(a,a) = a$ og $\{a,a\} = a$. De er kommutative, altsaa $(a,b) = (b,a)$ og

$\{a,b\} = \{b,a\}$. De er associative, saa Udtrykkene (a,b,c) og $\{a,b,c\}$ o.s.v. har en Mening.

De første Paastande er evidente, og det sidste ogsaa idet baade $((a,b),c)$ og $(a,(b,c))$ ses at angive den største fælles Divisor for a,b og c, og analogt med $\{a,b,c\}$.

Endvidere ser man at $(a,b) = a \Leftrightarrow \{a,b\} = b$.

Sætningerne understreget viser at $(\mathbb{N}, (\ ,\ ), \{\ ,\ \})$ er en algebraisk Struktur af den Art som kaldes "lattice" ("Verband"), endda kommutativ.

Begge Kompositioner er distributive m.H.t. sig selv. Det følger af de nævnte Egenskaber, idet fx $(a,(b,c)) = ((a,b),(a,c))$ fordi begge Sider er lig (a,b,c).

Enhver af Kompositionerne er distributiv m.H.t. den anden, altsaa $(a,\{b,c\}) = \{(a,b),(a,c)\}$ og $\{a,(b,c)\} = (\{a,b\},\{a,c\})$. Dette er begrebsmæssigt sværere at indse, men følger let hvis man betragter Exponenterne til p_j, idet $\alpha \wedge (\beta \vee \gamma) = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$ (rigtigt, thi p.G.a. Symmetrien mellem β og γ kan vi antage $\beta \leqq \gamma$, og saa er begge Sider lig $\alpha \wedge \gamma$), og den tilsvarende med $\wedge$ og $\vee$ ombyttet.

Man kan altsaa "gange Parenteser ud", saa fx

$$\{(a,b),(c,d)\} = (\{a,c\},\{a,d\},\{b,c\},\{b,d\}).$$

Taleksempel:

$$(\{12,8\},\{9,42\}) \overset{?}{=} \{(12,9),(12,42),(8,9),(8,42)\}$$

$$(24\ ,\ 126)\ \Big|\ \{3\ ,\ 6\ ,\ 1\ ,\ 2\}$$

$$6 \qquad\qquad 6$$

Gaa-op-Relationen harmonerer med $(\ ,\ )$ og $\{\ ,\ \}$, saa at $a \mid b \wedge c \mid d \Rightarrow (a,c) \mid (b,d)$ og $\Rightarrow \{a,c\} \mid \{b,d\}$. Begrebsmæssigt er det klart, og med Exponenter er det blot at $(\alpha \leqq \beta) \wedge (\gamma \leqq \delta)$ medfører $(\alpha \wedge \gamma) \leqq (\beta \wedge \delta)$ og analogt med $\vee$.

Multiplikationen er ogsaa en Komposition paa $\mathbb{N}$, og med de benyttede Betegnelser vil Produktet ab faa Exponenterne $\alpha_j+\beta_j$.

Multiplikationen er kommutativ og associativ og Gaa-op-Relationen harmonerer med den, altsaa $(a|b)\wedge(c|d) \Rightarrow ac|bd$.

Bevis for det sidste: Begrebsmæssigt er det klart, og med Exponenter følger det af $(\alpha \leqq \beta) \wedge (\gamma \leqq \delta) \Rightarrow (\alpha+\gamma) \leqq (\beta+\delta)$.

Multiplikationen er distributiv m.H.t. baade $(\ ,\ )$ og $\{\ ,\ \}$, altsaa $a\cdot(b,c) = (ab,ac)$ og $a\cdot\{b,c\} = \{ab,ac\}$, og endvidere gælder $b|c \iff ab|ac$.

Med Exponenter følger det af at $\alpha+(\beta\wedge\gamma) = (\alpha+\beta)\wedge(\alpha+\gamma)$ og den analoge med $\vee$, og det sidste af at $\beta \leqq \gamma \iff \alpha+\beta \leqq \alpha+\gamma$.

Derimod er ingen af de tre Kompositioner distributive m.H.t. Multiplikation:

$$2\cdot(2\cdot2) \neq (2\cdot2)\cdot(2\cdot2),$$
$$(2,2\cdot2) \neq (2,2)\cdot(2,2),$$
$$\{2,1\cdot2\} \neq \{2,1\}\cdot\{2,2\}$$

(Addition er jo heller ikke distributiv m.H.t. Multiplikation, fx $2+(2\cdot2) \neq (2+2)\cdot(2+2)$, og man kunde tro det svært at finde en Komposition $*$ som paa $\mathbb{R}_+$ er distributiv m.H.t. Multiplikation, altsaa $a*(b\cdot c) = (a*b)\cdot(a*c)$; en triviel Løsning er $x*y = 1$ for alle x,y, men der findes ogsaa ikke-trivielle Løsninger, fx $x*y = e^{\log x \,\cdot\, \log y}$, thi saa er $(\mathbb{R}_+,\cdot,*)$ blot isomorft Billede ved Exponentialfunktionen af $(\mathbb{R},+,\cdot)$, og her er $\cdot$ distributiv m.H.t. $+$).

Som tidligere nævnt er de tre Kompositioner koblet ved

$$(a,b)\cdot\{a,b\} = a\cdot b$$

og det er derfor muligt at undvære Tegnet $\{\ ,\ \}$, omend det sommetider kan give upraktiske Udtryk.

Eksempel:

Vi har $\{a,b,c\} = \dfrac{\{a,b\}\cdot c}{(\{a,b\},c)}$ som vi enten kan omskrive til

$$\frac{\frac{ab}{(a,b)}\cdot c}{\{(a,c),(b,c)\}} = \frac{\frac{ab}{(a,b)}\cdot c}{\frac{(a,c)\cdot(b,c)}{(a,c,b,c)}} = \underline{\frac{abc\cdot(a,b,c)}{(a,b)\cdot(a,c)\cdot(b,c)}},$$

eller vi kan omskrive det til

$$\frac{\frac{ab}{(a,b)}\cdot c}{(\frac{ab}{(a,b)}, c)} = \frac{abc}{(ab,(a,b)\cdot c)} = \underline{\frac{abc}{(ab,ac,bc)}}.$$

Med Exponenter har vi altsaa Identiteterne

$$\alpha \vee \beta \vee \gamma = \alpha + \beta + \gamma + (\alpha \wedge \beta \wedge \gamma) - [(\alpha \wedge \beta) + (\alpha \wedge \gamma) + (\beta \wedge \gamma)]$$

hhv. $$\alpha \vee \beta \vee \gamma = \alpha + \beta + \gamma - [(\alpha + \beta) \wedge (\alpha + \gamma) \wedge (\beta + \gamma)]$$

(da der er Symmetri mellem α, β og γ kan man antage $\alpha \leqq \beta \leqq \gamma$, og saa er et direkte Bevis for Identiteterne ret let).

Lad os angive et Par mere konkrete Konsekvenser af den entydige Faktorisering:

1) For $n,m \in \mathbb{N}$ er $\sqrt[n]{m}$ hel eller irrational.

Thi antages $\sqrt[n]{m} = a/b$ (uforkortelig), faas $a^n = m \cdot b^n$, altsaa $b \mid a^n$, men da $(a,b) = 1$ maa b være 1, saa a/b hel.

2) Hvis g ikke er en Potens, altsaa $g = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$, hvor $(\gamma_1, \ldots, \gamma_r) = 1$, saa er for $n \in \mathbb{N}$

$$\log_g n = \log n / \log g \text{ hel eller irrational.}$$

(Altsaa: Tallene i en sædvanlig Logaritmetabel er irrationale)

Thi antages $\log n/\log g = a/b$ (uforkortelig), faas $n^b = g^a$, saa at b gaar op i alle Exponenterne $\gamma_1 a, \ldots, \gamma_r a$ i Primopløsningen for g^a, men da $(a,b) = 1$ maa b være 1, saa a/b hel.

Alt det hidtil omtalte er kun Konsekvenser af den entydige Primopløsning, og er altsaa egentlig kun en Undersøgelse af en fri Halvgruppes Struktur.

Disse af Multiplikationen udledte Kompositioner er saa koblet med Additionen ved den distributive Lov mellem $+$ og $\cdot$, og som en Konsekvens af denne har man at

$$(a,b) \mid a - b$$

der som bekendt er Grundlaget for Euklids Algoritme.

Eksempel:

Af Hensyn til en senere Anvendelse vil vi vise at

$$\frac{n!}{k!\,(n-k-1)!} \mid \{n,n-1,n-2,\ldots,n-k\}, \qquad n > k \geq 0.$$

Tallet paa venstre Side kan ogsaa skrives $n\cdot\binom{n-1}{k}$, og er altsaa et helt Tal. Vi vil føre Beviset ved Induktion efter k, og for $k = 0$ staar der blot $n \mid n$, hvilket stemmer (som altid er $0!=1$); for $k=1$ staar der $\frac{n!}{1!\,(n-2)!} \mid \{n,n-1\}$ hvilket ogsaa stemmer (idet n og $n-1$ er primiske, saa $\{n,n-1\}$ er lig deres Produkt). Vi antager nu Paastanden gyldig for $k-1$ og alle n, og vil vise Relationen som den staar med k og n. Med $k-1$ og n har vi

$$\frac{n!}{(k-1)!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k)!}\cdot n \mid \{n,n-1,\ldots,n-k+1\}$$

og med $k-1$ og $n-1$ har vi

$$\frac{(n-1)!}{(k-1)!(n-k-1)!} = \text{- do. -} \cdot (n-k) \mid \{n-1,\ldots,n-k+1,n-k\}$$

og vi benytter nu Reglen om at $(a\mid b)\wedge(c\mid d) \Rightarrow \{a,c\}\mid\{b,d\}$ og endvidere at en fælles Faktor for a og c kan trækkes udenfor $\{\ ,\ \}$-Tegnet; dermed faas

$$\frac{(n-1)!}{(k-1)!(n-k)!}\cdot\{n,n-k\}\mid\{n,n-1,\ldots,n-k\}$$

hvor Højresiden netop er den ønskede. Nu er $\{n,n-k\}$ lig $n(n-k)/(n,n-k)$ og $(n,n-k)$ vil gaa op i k, saa $\{n,n-k\}$ er et Multiplum af $\frac{n(n-k)}{k}$ og indsættes dette kan det trækkes sammen med den foranstaaende Brøk og det ønskede er vist. □

Eksempel:

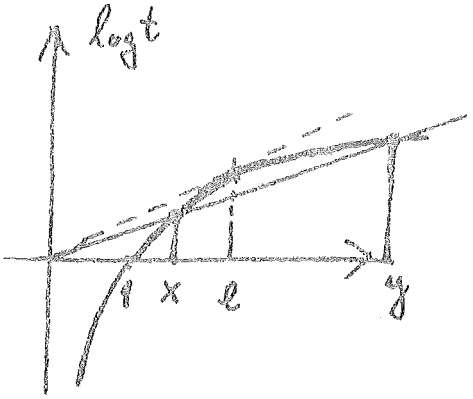
Som et Eksempel der ikke benytter meget andet end den entydige Primopløsning kan vi ogsaa betragte Opgaven:

$$\text{Løs} \quad x^y = y^x \,, \quad \text{hvor} \quad x,y \in \mathbb{Q}^+$$

Som trivielle Løsninger har vi aabenbart $x = y$ = vilkaarligt positivt rationalt Tal, Problemet er at finde eventuelle andre Løsninger, og da der er Symmætri mellem x og y kan vi gerne antage at $x < y$. Jøvrigt bemærker man, at $x=2, y=4$ er Løsning, da $2^4 = 16 = 4^2$. Ved at tage Logaritmer ser man at Ligningen ogsaa kan skrives

$$\frac{\log x}{x} = \frac{\log y}{y}$$

og ved at betragte Logaritmefunktionens Graf ses, at for eventuelle Løsninger har man $1 < x < e < y$.



Vi sætter nu $y = x\cdot(1+\frac{1}{z})$, og saa er Opgaven ensbetydende med at finde $x,z \in \mathbb{Q}^+$ saaledes at

$$x^{x(1+\frac{1}{z})} = (x(1+\frac{1}{z}))^x \,;$$

eller

$$x^{\frac{x}{z}} = (1+\frac{1}{z})^x$$

hvoraf faas

$$x = (1+\frac{1}{z})^z .$$

Hvis nu z skrives som uforkortelig Brøk $\frac{a}{b}$ skal altsaa baade

$$1+\frac{1}{z} = \frac{a+b}{a} \qquad \text{og} \quad x = (\frac{a+b}{a})^{\frac{a}{b}}$$

tilhøre $\mathbb{Q}^+$; opløftes den første til k' Potens og den anden til h' Potens, $h,k \in \mathbb{Z}$, skal Produktet af dem være rationalt, og det ses at være $(\frac{a+b}{a})$ opløftet til Potensen $\frac{ha+kb}{b}$; her

kaa ha + kb gennemløbe det af a og b frembragte Ideal (a,b), og altsaa antage Værdien 1, saa at $(\frac{a+b}{a})$ opløftet med Exponenten $\frac{1}{b}$ er rational eller med andre Ord: den uforkortelige Brøk $\frac{a+b}{a}$ maa være en b'te Potens, af Form $\frac{(n+d)^b}{n^b}$, idet Tælleren aabenbart er større end Nævneren.. Da nu $a+b = (n+d)^b$ og $a = n^b$ kan vi udvikle efter Binomialformlen og faar $b = (n+d)^b - n^b = b \cdot n^{b-1} \cdot d + \ldots$ med ialt b Led; da alle Bogstaverne er naturlige Tal ses at det kun er muligt med $b = 1$ (og $d = 1$), saa at z er et helt Tal.

Indsættes dette ser man at x og y virkelig bliver rationale, og vi har dermed fundet samtlige ikke-trivielle Løsninger med $x < y$, nemlig den numerable Følge

$$x = (1 + \frac{1}{z})^z \quad , \quad y = (1 + \frac{1}{z})^{z+1}$$

idet z gennemløber $\mathbb{N}$. Man ser, at Løsningerne konvergerer mod e fra højre og venstre.

Nogle Definitioner og Betegnelser.

1) Foran er indført $|A|$ som Betegnelse for Antallet af Elementer i en Mængde A.
2) Vi har ogsaa indført $a \wedge b$ og $a \vee b$ som Betegnelse for hhv. min a,b og max a,b. Ds vi ogsaa benytter Tegnene $\wedge$ og $\vee$ med den sædvanlige Betydning fra Logikken kan der opstaa tvetydige Situationer, som man kan værge sig imod med de fornødne Parenteser; fx kan $a = b \wedge c < d$ forstaas paa to Maader, evt. kan lidt større Mellemrum klargøre Meningen.
3) Hvis (a,b) = 1 siger vi at a og b er primiske. For mere end to Tal a,b,c,... kan det være sikrere at sige at de er "uden fælles Divisor" naar man mener at (a,b,c,...) = 1,

idet man ellers kan forvekle det med Situationen hvor a,b,c... er parvis primiske, altsaa at (a,b) = (a,c) = (b,c) = ... = 1.

4) Foruden Gaa-op-Relationen vil vi indføre en Relation betegnet med $\|$, idet $a\|b$ skal betyde at der findes et c saa $b = ac \wedge (a,c) = 1$. Man ser, at dersom specielt a er en Primtalspotens p^{α}, saa: $p^{\alpha}\|b \Leftrightarrow p^{\alpha} \mid b \wedge p^{\alpha+1} \nmid b$; Taleksempel $2^3\|24$. At $a\|b$ betyder at a er Produkt af visse af Primpotenserne fra b's Primopløsning; heraf ses at Relationen er transitiv, men den vil ikke som Gaa-op-Relationen give Anledning til en lattice-Struktur.

5) At a er kvadratfri betyder at a ikke er delelig med noget Kvadrattal større end 1, eller med andre Ord at a er Produkt af lutter forskellige Primtal (0,1 eller flere). Hvis $a = p_1^{\alpha_1}\cdot\ldots\cdot p_r^{\alpha_r}$ hvor alle $\alpha_j > 0$, kan man evt. betegne $p_1\cdot\ldots\cdot p_r$ som den "kvadratfri Kerne" af a.

6) Summationsindices (og Indices ved Produktdannelse) løber altid indenfor $\mathbb{N}$, (medmindre andet udtrykkeligt er bemærket), og saa med de yderligere Krav som maatte være anført. At man hyppigt møder Summer som formelt er uendelige, men hvor Leddene er 0 fra et vist Trin saa de de facto er endelige, kan ikke genere (det er en unødigt komplicerende Uvane at mange Forfattere under et $\sum$-Tegn føler sig forpligtet til at anføre de Indices for hvilke Leddene er $\neq 0$).

7) Ved Angivelse af Variationsintervaller vil vi hyppigt benytte den praktiske Intervalskrivemaade med $[\ ,\ ]$ o.s.v uden at der deri skal ligge nogen Antydning af at vi arbejder indenfor $\mathbb{R}$. Eksempel: Ved Division med n vil den principale Divisionsrest ligge i $[0,n[$.

8) Binomialkoefficienter $\binom{a}{b}$ hvor $a,b \in \mathbb{Z}$, er lig 0 saafremt $a < 0$ eller $b < 0$ eller $b > a$. Denne Definition vil aldrig give Vanskeligheder, og det er det som man naturligt faar, hvis de indgaaende Fakulteter erstattes med Γ-Funktioner. Eksempel til 6) og 8): For $n \in \mathbb{N}$ er

$$\sum_j \binom{n}{j} = 2^n - 1.$$

Om Primtallenes Fordeling.

Sættes $\mathbb{N} \setminus \{1\} = \mathbb{N}'$, saa er $\mathbb{N}'^2 = \{\text{sammensatte Tal}\}$, og Mængden $\mathbb{P}$ af Primtal kan saa bestemmes ved Formlen $\mathbb{P} = \mathbb{N}' - \mathbb{N}'^2$ (idet vi benytter den sædvanlige Skrivemaade $AB = \{ab: a \in A, b \in B\}$).

Fra Oldtiden har man en induktiv Bestemmelse af Primtallene, nemlig Eratostenes' Si (E. 276-194 f.Chr.), Der bestaar i at opskrive $\mathbb{N}'$, understrege det første Tal og fjerne alle Multipla af det, understrege det første ikke fjernede, fjerne alle Multipla af det, understrege det første ikke fjernede, o.s.v.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ ..

og de understregede Tal er saa Mængden af Primtal. Man ser, at dette er en induktiv Bestemmelse af $\mathbb{P}$ ved Formlen $\mathbb{P} = \mathbb{N}' - \mathbb{P}\mathbb{N}'$ hvorved altsaa er benyttet at $\mathbb{P}\mathbb{N}' = \mathbb{N}'^2$, hvilket jo ogsaa er i fuld Overensstemmelse med at $\mathbb{N}' = \mathbb{P} \cup \mathbb{P}^2 \cup \mathbb{P}^3 \cup \ldots$.

Vi har: Hvis n ikke er delelig med noget Primtal $\leq \sqrt{n}$, saa er n et Primtal; Beviser for det er velkendte, og man ser, at det er i fuld Overensstemmelse med de ovenfor angivne Bestemmelser af $\mathbb{P}$.

Ved Hjælp heraf kan man bestemme Primtallene saa langt frem som man ønsker, og der findes trykte Tabeller over Primtallene op til (ihvertfald) 14.000.000 og paa Magnetbaand har man Tabeller over dem op til Størrelsesordenen 10^9.

Euklid viste: Der findes uendelig mange Primtal.

Bevis: Vi konstruerer en voksende Følge $a_1, a_2, \ldots$ af indbyrdes parvis primiske Tal. Ethvert af dem maa saa have sine egne Primdivisorer, og der maa derfor være uendelig mange Primtal.

Vi sætter

$$\begin{aligned} a_1 &= 2 \\ a_2 &= a_1 + 1 \\ a_3 &= a_1 a_2 + 1 \\ &\cdots\cdots\cdots \\ a_n &= a_1 a_2 \ldots a_{n-1} + 1 \\ &\cdots\cdots\cdots \end{aligned}$$

Man ser, at hvis $d \mid a_m$, saa vil vi for $n > m$ faa Resten 1 hvis vi dividerer d op i a_n, og følgelig er $(a_m, a_n) = 1$. □

Iøvrigt giver Beviset mere, thi da $a_n = (a_{n-1}-1)\cdot a_{n-1} + 1 < a_{n-1}^2$ slutter vi ved Induktion at $a_n < 2^{2^n}$ (det gælder for $n = 1$ da $a_1 = 2 < 2^2$, og vi har $\left(2^{2^{n-1}}\right)^2 = 2^{2^n}$). Følgelig maa der findes mindst n forskellige Primtal mindre end 2^{2^n}, men vi skal om lidt udlede langt stærkere Resultater.

Der findes vilkaarligt lange primtalfri Stykker i Talrækken, fx er

$$n!+2, \quad n!+3, \quad \ldots\ldots \quad n!+n$$

delelige med hhv. $2, \quad 3, \quad \ldots\ldots \quad n,$

men Primtallene kommer til at ligge mere og mere spredt jo længere man gaar ud i Talrækken, og i Virkeligheden er Længden af det primtalfri Interval $]n!+1, n!+n[$ "under Middel" fordi $n!$ er et meget stort Tal.

Til Gengæld synes det at fremgaa af Tabellerne at der findes Par af paa hinanden følgende ulige Tal som er Primtal, saakaldte

"Primtaltvillinger", saa langt ud som det skal være, omend de bliver temmelig sjældne,

Eksempler: 3-5 .. 11-13 .. 41-43 .. 2309-2311 ..10016957-10016959.

Man er ikke i Stand til at bevise at der er uendelig mange af dem, men man kan vise at de - indenfor Primtalfølgen - ihvertfald maa blive ret sjældne.

Der findes uendeligt mange Primtal af Formen $p = 4h - 1$, saa Rækken 3 - 7 - 11 - 19 - ... fortsætter uendeligt.

Bevis: Ideen er den samme som ved Beviset for Euklids Sætning, idet vi konstruerer en Følge af indbyrdes parvis primiske Tal, saa hvert af dem maa have sine egne Primdivisorer; desuden indretter vi det saa hvert Tal er af Formen $4h - 1$, og det maa derfor have en Primdivisor af samme Form (idet de ikke alle kan være af Formen $p = 4h + 1$), og dermed vil Beviset være ført.

Vi sætter

$$\begin{aligned} a_1 &= 3 \\ a_2 &= 4a_1 - 1 \\ a_3 &= 4a_1a_2 - 1 \\ &\cdots\cdots\cdots\cdots \\ a_n &= 4a_1a_2\ldots a_{n-1} - 1 \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

At de er parvis primiske sas ganske som i det forrige Bevis (og ogsaa her kunde Beviset benyttes til at give en grov kvantitativ Vurdering). □

Der findes ogsaa uendeligt mange Primtal af Formen $p = 4h + 1$, men det er ejendommeligt nok noget sværere at bevise, og vi maa udskyde det lidt.

Derimod ser man, at man paa tilsvarende Maade kunde vise at der findes uendeligt mange Primtal $p = 6h - 1$ (idet hvis et Primtal større end 3 ikke er af denne Art, saa vil det være af Typen $p = 6h + 1$), men det gaar ikke med nogen Tal større end 6.

De nævnte Resultater er Specialtilfælde af Dirichlet's Sætning: Enhver primisk Restklasse, d.v.s. enhver Differensrække $m, m+d, m+2d, \ldots$ hvor $(m,d) = 1$, indeholder uendeligt mange Primtal, som vi senere skal komme tilbage til.

Man har ofte prøvet at angive Funktioner $f: \mathbb{N} \to \mathbb{N}$, saaledes at $f(n)$ bliver Primtal, enten for alle n, eller i hvert Fald for uendeligt mange n.

Eksempel: $f(n) = n^2 - n + 17$, $n \in \mathbb{N}$,

n :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
f(n):	17	19	23	29	37	47	59	73	89	107	127	149	173	199	227	257	289

Samtlige Værdier i Tabellen er Primtal undtagen $289 = f(17)$, som naturligvis er delelig med 17.

Intet Polynomium $f(n) = a_0 + a_1 n + a_2 n^2 + \ldots + a_h n^h$ $(h \geq 0)$ kan fremstille lutter Primtal for $n \in \mathbb{N}_0$ (at vi lader $n \in \mathbb{N}_0$ i.St.f. $n \in \mathbb{N}$ er jo uvæsentligt).

Bevis: Indirekte. Værdierne $f(0), f(1), \ldots, f(h) \in \mathbb{Z}$, og udfra dem bestemmes Koefficienterne $a_0, a_1, \ldots, a_h$ ved de sædvanlige Determinantformler (altsaa Polynomiumsinterpolation), hvoraf ses at $a_0, a_1, \ldots, a_h \in \mathbb{Q}$; deres Fællesnævner kaldes M. Endvidere er ifølge Forudsætning $a_0 = f(0)$ et Primtal.

Saa er, for $j \in \mathbb{N}$,

$$f(ja_0M) = a_0 + a_1(ja_0M) + \ldots + a_h(ja_0M)^h$$

aabenbart heltallig og delelig med a_0 (da ethvert af Leddene har disse Egenskaber), og Værdien $f(ja_0M)$ er altsaa ikke noget Primtal (undtagen for de højst endelig mange j for hvilke den er a_0).

NB: At f er et Polynomium som afbilder $\mathbb{Z} \to \mathbb{Z}$ medfører ikke at $f \in \mathbb{Z}[x]$. Modeksempel: $\binom{n}{2} = (n^2-n)/2$ afbilder $\mathbb{Z} \to \mathbb{N}_0$. □

Man formoder at ethvert Polynomium $f \in \mathbb{Z}[x]$ fremstiller uendelig mange Primtal for $n \in \mathbb{N}$, medmindre det er "aabenlyst umuligt", hvor det sidste betyder, at Polynomiet ikke maa være reducibelt over $\mathbb{Z}$ (man maa altsaa hverken kunne trække en fælles Talfaktor (større end 1) ud af Koefficienterne, eller kunne skrive f som Produkt af to Polynomier af lavere Grad), og endvidere skal Højestegradsleddet være positivt. Det indgaar i den generelle Schinzel's Hypotese, som ogsaa vil medføre, at der findes uendelig mange Primtaltvillinger, men man er overhovedet ikke i Stand til at bevise den undtagen for ét Førstegradspolynomium, hvor den som nævnt i det moniske Tilfælde (x+m) er vist af Euklid, og i det ikke-moniske (dx+m) af Dirichlet (1857).

Det er klart, at det at definere en Funktion f ved "f(n) = det n'te Primtal" ikke oplyser noget, men lige saa intetsigende Definitioner har nu og da haft Held til at vække en ufortjent Interesse. For Eks: Der findes et reelt Tal A saa $\lfloor A^{3^n} \rfloor$ altid er et Primtal. For at afsløre Tomheden i noget saadant kan vi tage et lidt ændret Eksempel: Vi sætter, idet det n'te Primtal kaldes p_n

$$A = \sum_n p_n / 10^{2^n} = 0{,}020300050000000700000000000001100\ldots$$

(Decimalerne fra de forskellige Primtal vil aldrig gribe ind over hinanden, thi som foran vist er $p_n < 2^{2^n}$). Saa er

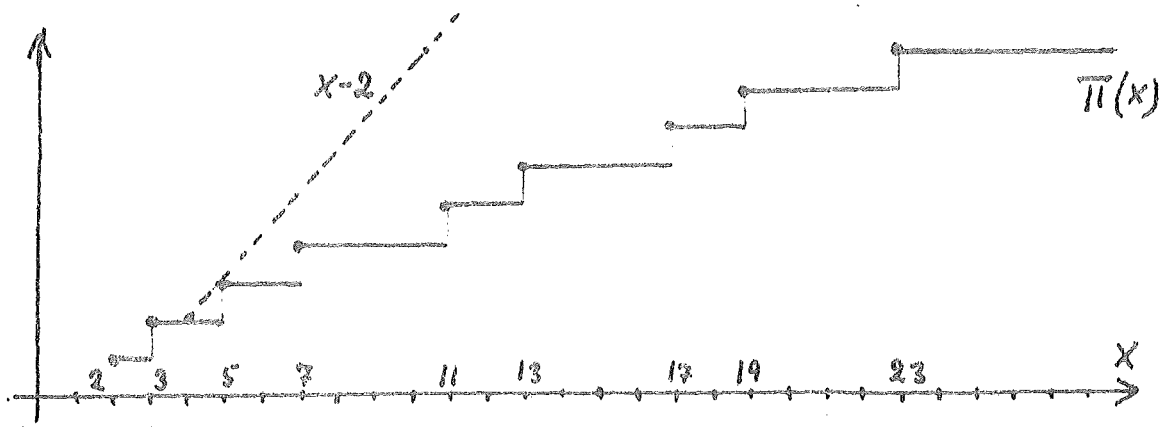
$$p_n = \left\lfloor 10^{2^{n-1}} \cdot \left(10^{2^{n-1}} \cdot A - \left\lfloor 10^{2^{n-1}} \cdot A \right\rfloor\right) \right\rfloor .$$

Det er klart at der ikke er opnaaet noget, da A kun kendes hvis man kender alle Primtallene. Mængden af Delfølger af naturlige Tal har Kontinuets Mægtighed, saa en vilkaarlig Bijektion mellem disse Mængder vil lade Primtalfølgen svare til et reelt Tal, og saa kan man jo godt sige at det "rummer alle Primtalfølgens Hemmeligheder".

Til Angivelse af Primtallene kan man benytte deres Antalfunktion Primtalfunktionen $\pi(x)$, der defineres ved

$$\pi(x) = \sum_{p \leqq x} 1 = (\text{Antallet Primtal} \leqq x), \qquad x \in \mathbb{R}^+$$

(Bogstavet p skal her som overalt i det følgende betegne Primtal).



Det er aabenbart en monoton Trappefunktion med Spring +1 i Primtallene. Et Par Funktionsværdier er

$$\pi(10) = 4, \quad \pi(100) = 25, \quad \pi(1000) = 168.$$

Euklids Sætning udsiger at $\pi(x) \to \infty$ for $x \to \infty$, og den ved Beviset angivne Størrelsesvurdering gav endda at $\pi(2^{2^n}) \geqq n$, d.v.s. noget i Retning af at $\pi(x) > \log\log x$.

En triviel Vurdering den anden Vej er at $\pi(x) < x$, og om lidt vil vi benytte at for $x \geqq 4$ er $\pi(x) \leqq x - 2$, hvilket ogsaa umiddelbart ses at være rigtigt (se Fig.).

Vi vil vurdere Størrelsen $n^{\pi(n)}$ opad og nedad, $n \in \mathbb{N}$.

Opad: Vi vil vise at Størrelsen er mindre end 2^{4n}; det skal ske ved Induktion, og man ser umiddelbart at det er gyldigt for $n < 4$.

n	$n^{\pi(n)}$	2^{4n}
1	1	2^4
2	2	2^8
3	9	2^{12}

Lad os nu antage $n \geqq 4$, og at Paastanden $m^{\pi(m)} < 2^{4m}$ er gyldig for alle $m < n$.

Vi tager $m = \begin{cases} \frac{n}{2} & \text{for } n \text{ lige} \\ \frac{n+1}{2} & \text{for } n \text{ ulige} \end{cases}$, saa vil Binomialkoefficienten

$$\binom{n}{m} = \frac{n(n-1).....(m+1)}{1\cdot 2\cdot .....(n-m)}$$

i Tælleren indeholde alle Primtal p i Intervallet $]m,n]$, og de kan ikke bortforkortes med Nævneren, da $n-m < m+1$. Derfor er

$$\binom{n}{m} \geqq \prod_{p \in]m,n]} p \geqq {}_m\pi(n)-\pi(m).$$

Samtidig er

$$\binom{n}{m} \leqq \sum_{j \in [0,n]} \binom{n}{j} = (1+1)^n = 2^n,$$

og da nu

$${}_n\pi(n) = (n/m)\,{}_m\pi(n)\cdot {}_m\pi(n)-\pi(m)\cdot {}_m\pi(m)$$

faar vi ved at benytte at $n/m \leqq 2$ og Induktionsforudsætningen ${}_m\pi(m) < 2^{4m} \leqq 2^{2n+2}$ samt at $\pi(n) \leqq n-2$ at

$${}_n\pi(n) < 2^{n-2}\cdot 2^n \cdot 2^{2n+2} = 2^{4n}. \qquad \square$$

<u>Nedad:</u> Vi vil vise, at ${}_n\pi(n)$ er større end eller lig 2^{n-1}. Da $2^{n-1} = (1+1)^{n-1}$ er lig Summen af de n Stk. Binomialkoefficienter $\binom{n-1}{j}$, saa er $2^{n-1} \leqq n\cdot\binom{n-1}{k}$, hvor $\binom{n-1}{k}$ er en maximal blandt Binomialkoefficienterne. Men ifølge Eksemplet S.23 vil $n\cdot\binom{n-1}{k}$ gaa op i $\{n,n-1,\ldots,n-k\}$. I Primopløsningen for denne sidste Størrelse vil der aabenbart kun kunne forekomme Primtalspotenser som er mindre end eller lig n, og Antallet af dem er højst lig $\pi(n)$, da der ikke kan forekomme nogen Primtal større end n i dem; altsaa er Størrelsen majoriseret af ${}_n\pi(n)$. Kombineres disse Kendsgerninger ses at ${}_n\pi(n) \geqq 2^{n-1}$. $\square$

For $n \geqq 2$ er $n-1 \geqq n/2$, saa at

$$2^{n/2} \leqq n^{\pi(n)} < 2^{4n}, \qquad n \geqq 2,$$

og tager vi her Logaritmer og dividerer med log n faar vi

$$\tfrac{1}{2}\log 2 \cdot \frac{n}{\log n} \leqq \pi(n) < 4 \log 2 \cdot \frac{n}{\log n} .$$

Med naturlige Logaritmer er log 2 = 0,6931.., og vi faar

$$\boxed{\frac{1}{3} \cdot \frac{n}{\log n} < \pi(n) < 3 \cdot \frac{n}{\log n}, \qquad n \geqq 2}$$

Uligheder af denne Type er vist af Tchebychef (1821-94), som ogsaa kunde gøre det med et mindre Interval mellem Talkonstanterne, fx

fransk	Tchebychef
nyere engelsk	Chebyshev
Mathem.Review	Čebyšev
tysk	Tschebyscheff
russisk	Чебышев
Autograf	Tschebyscheff

$$0{,}8 < \frac{\pi(n)}{\frac{n}{\log n}} < 1{,}2 \qquad \text{for n tilstr. stor.}$$

(det er evident at vi i Regningerne ovenfor nogle Steder kunde have vurderet lidt skarpere, men Formaalet var kun med de simplest mulige Midler at faa en kvalitativ Vurdering, gyldig for alle n. Med nogle trivielle Regninger kan man iøvrigt let se at $\boxed{}$ er gyldig ogsaa hvis n erstattes med en reel Variabel x, $x \geqq 2$; for $x < 2$ gaar det naturligvis ikke, idet saa $\pi(x) = 0$, medens $x/\log x$ endog gaar mod uendelig for $x \to 1$).

Vi skal senere komme tilbage til den berømte "Primtalsætning" som udsiger at

$$\frac{\pi(x)}{\frac{x}{\log x}} \to 1 \qquad \text{for} \quad x \to \infty,$$

men det er ejendommeligt nok et væsentligt dybere liggende Resultat, som kun med Brug af langt stærkere Hjælpemidler (analytiske Funktioner af komplex Variabel) blev vist i 1896 af Hadamard (1865-1963) og de la Vallée-Poussin (1866-1962) (uafhængigt af hinanden). Væsentlige Simplifikationer af Beviserne kom i 1930'erne (Brug af Fouriertransformation), men i 1949 skete det sensationelle at Atle Selberg (1917- , norsk) gav et "elementært" Bevis, d.v.s. et Bevis som nok var teknisk indviklet, men ikke benytter dybere Hjælpemidler end at det principielt kunde benyttes som Specialelæsning i Gymnasiet.

Tchebychefs Resultat var forbavsende, idet det med smaa Midler kunde opklare noget som man tidligere havde regnet for inaccessibelt. At der tilsyneladende gjaldt noget i Retning af Primtalsætningen havde man allerede ca. 1800 (Gauss, Legendre (L.1752-1833)) faaet Formodning om ved Optælling i Tabeller.

Af Vurderingen ses specielt, at i Middel vil Primtallene komme til at ligge mere og mere spredt jo længere man gaar frem i Talrækken, saa der er intet forbavsende ved de lange primtalfri Stykker. Idet

$$\frac{d}{dt}\left\{\frac{t}{\log t}\right\} = \frac{1}{\log t} - \frac{1}{(\log t)^2} \approx \frac{1}{\log t}$$

ses at "Gennemsnitsafstanden" mellem to paa hinanden følgende Primtal af Størrelse som t vil være af Størrelsesordenen $\log t$ (da dette er Abscissetilvæksten svarende til funktionstilvækst 1).

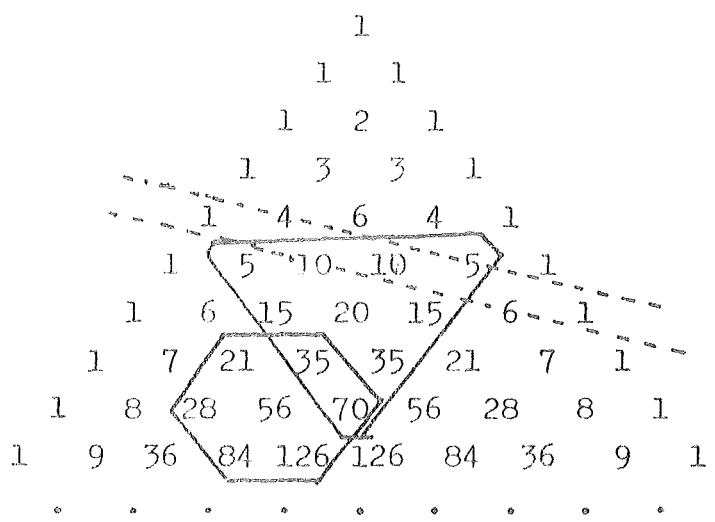
Lad os vise, at <u>ethvert Primtal er mindre end 10 gange det foregaaende</u> (hvoraf følger, at der for ethvert n findes et Primtal som i Decimalsystemet skrives med n Cifre). Vi skal blot vise at $\Pi(10n) > \Pi(n)$. Vi kan antage $n > 10$, idet Paastanden umiddelbart ses at gælde for $n \leqq 10$; endvidere vil vi for Simpelheds Skyld benytte de lidt skarpere Vurderinger fra Beviserne paa S.33. Den

ene Vurdering giver $\pi(n) < 4 \log 2 \cdot n/\log n$; den anden Vurdering giver $\pi(10n) > \log 2 \cdot (10n-1)/\log(10n)$, og idet $n > 10$ ses at dette sidste er større end $\frac{9}{2} \cdot \log 2 \cdot n/\log n$ som er større end første Vurdering. □

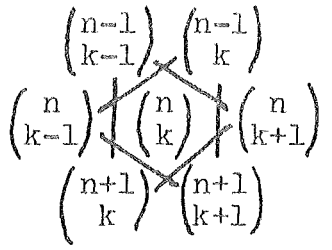
Paa tilsvarende Maade kunde Tchebychef med sine skarpere Vurderinger og lidt mere Regning godtgøre det paa hans Tid opstillede Bertrands Postulat: Mellem n og 2n findes altid et Primtal (som havde en vis Interesse for Sætninger om endelige Grupper). (Vi kan bemærke, at selv den tilsyneladende stærke Primtalsætning ikke forhindrer at der for ethvert positivt ε kunde findes vilkaarligt store Par af paa hinanden følgende Primtal hvis Differens opfylder $p_{m+1} - p_m > p_m^{1-\varepsilon}$, men udfra forbedrede Resultater ved man at dette ikke kan ske for helt smaa ε).

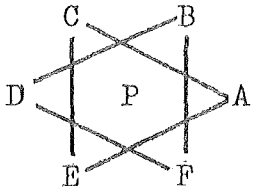
Vi har ovenfor set at der er en vis Forbindelse mellem Primtalteori og Binomialkoefficienter og Størrelsen $\{n, n-1, \ldots, n-k\}$. Faktisk vil det senere vise sig, at $\{n, n-1, \ldots, 2, 1\}$ betragtet som Funktion af n (og optrædende under en anden Betegnelse) er aldeles afgørende for Studiet af Primtallenes Fordeling. Vi benyttede at $n \cdot \binom{n-1}{k} \mid \{n, \ldots, n-k\}$ (bevist S.23), medens vi af praktiske Grunde ikke brugte den tilsvarende Vurdering den anden Vej $\{n, \ldots, n-k+1\} \mid \binom{n}{k} \cdot \{k, k-1, \ldots, 1\}$ (lidt sværere at indse og at haandtere). Vi kan i den Forbindelse ogsaa bemærke at $\{k, k-1, \ldots, 1\} \mid \{n, n-1, \ldots, n-k+1\}$, hvilket er klart, da ethvert Tal $\leq k$ vil gaa op i et blandt k paa hinanden følgende hele Tal.

Binomialkoefficienternes iøjnefaldende Delelighedsegenskaber fremgaar dels (som foran benyttet) af Udtrykket for dem og dels af deres Forekomst i "Pascal's Trekant", hvori enhver $\binom{n}{k}$ er Summen af de to ovenover staaende. Fx er (idet p er et Primtal) alle $\binom{p}{j} = \frac{p!}{j!(p-j)!}$, $j \in \,]0,p[$, delelige med p, hvilket bevirker at der i Pascal's Trekant fremkommer en hel Trekant af Tal delelige med p. Se Fig., paa hvilken den indrammede Trekant har Tal delelige med 5; under Rækken $\binom{10}{j}$ opstaar to tilsvarende Trekanter o.s.v.



Davidsstjernen (Gould, 1972): Lad os betragte en Binomialkoefficient $\binom{n}{k}$ og dens seks nærmeste Naboer, fx $\binom{8}{3} = 56$ omgivet af ⬡ paa Fig. ovenfor. Situationen er tegnet ud, og vi vil benytte de afkortede Betegnelser angivet t.h. Der gælder at (A,C,E) = (B,D,F). Bevis: Da hvert Element er Summen af de to nærmeste ovenover har vi A = F - P, C = P - B og E = D + P, hvoraf man ser at A,C og E og trivielt ogsaa P tilhører Idealet (B,D,F,P); af Symmetrigrunde kan man lade de to Trekanter bytte Roller, og vi har derfor (A,C,E,P) = (B,D,F,P). Af Udtrykkene for Binomialkoefficienterne faar man (k+1)A = (n-k)P, nC = kP og (n-k+1)E = (n+1)P, og trækkes de to første fra den sidste faas P som Linearkombination af A,C og E; altsaa er P ∈ (A,C,E) og analogt P ∈ (B,D,F), ⇒ (A,C,E) = (B,D,F).





□

Taleksemplet: Omkring $\binom{8}{3}$ faas $(70,21,84) = 7 = (35,28,126)$.

En ejendommelig Iagttagelse er gjort af Mann og Sharks, 1972: Et Tal $p > 1$ er et Primtal hvis og kun hvis det for alle n gælder at n gaar op i $\binom{n}{3n-p}$. Man ser, at Binomialkoefficienten kun er ulig 0 for $n \in [p/3, p/2]$, saa det er kun disse n som har Interesse. For fast p vil de paagældende Binomialkoefficienter ligge paa en Skraalinie (Hældningen uafhængig af p) i Pascals Trekant; paa Fig. foran er tegnet Skraalinierne svarende til p = 11 og p = 13, og man ser at de Binomialkoefficienter som de møder er delelige med det tilsvarende Rækkenummer, i Overensstemmelse med at 11 og 13 er Primtal; Linien for p = 12 ligger midt imellem og møder 1-10-1, hvor 1-Tallerne ikke har Egenskaben i Overensstemmelse med at 12 er sammensat.

Bevis: Vi har $n \in [p/3, p/2]$.

1) For p = 2 er der kun n = 1; Egenskaben opfyldt, da $1 \mid \binom{1}{1} = 1$.

2) For $p > 2$ og lige betragter vi $n = p/2$; Binomialkoefficienten bliver lig $\binom{n}{n} = 1$, som ikke er delelig med n.

3) For p = 3 er der kun n = 1; Egenskaben opfyldt, da $1 \mid \binom{1}{0} = 1$.

4) For $p > 3$ og delelig med 3 betragter vi $n = p/3$; Binomialkoefficienten bliver lig $\binom{n}{0} = 1$, som ikke er delelig med n.

5) For p lig et Primtal > 3 har vi $(n, 3n-p) = (n,p) = 1$; af Udtrykket for Binomialkoefficienterne ses at $(3n-p) \cdot \binom{n}{3n-p} = n \cdot \binom{n-1}{3n-p-1}$ hvori begge Sider er positive, da $3n-p > 0$; da nu n er primisk med 3n-p ses at det gaar op som ønsket i Binomialkoefficienten.

6) Hvis ingen af de forrige Tilfælde indtræffer vil p være sammensat og ulige og have en Primdivisor $q \in]3, p[$; vi betragter $n = (p-q)/2$ som aabenbart er delelig med q, saaledes at

vi har $q^{\alpha} \| n$ og $q^{\beta} \| n-q$, hvor baade α og β er positive (iøvrigt er i hvert Fald en af dem lig 1). Den Binomialkoefficient vi skal betragte er saa $\binom{n}{3n-p} = \binom{n}{p-2n} = \binom{n}{q}$. Vi bruger nu Eksemplet fra S.23 ifølge hvilket $n!/(n-q-1)!q!$ som er lig $(n-q)\cdot\binom{n}{q}$ gaar op i $\{n, n-1, \ldots, n-q\}$; i dette sidste fælles Multiplum vil q kun gaa op i Yderleddene og med Eksponent hhv. α og β, saa Størrelsen indeholder q med Eksponenten $\alpha \vee \beta$, og da $q^{\beta} \| n-q$ ses at i $\binom{n}{q}$ kan q højst gaa op med en Eksponent $(\alpha \vee \beta) - \beta = (\alpha-\beta) \vee (\beta-\beta) = (\alpha-\beta) \vee 0$ som er mindre end α, saa n gaar ikke op i $\binom{n}{q}$. □

Til Slut kan nævnes en vist endnu ubevist Hypotese (Newman, 1971): For ethvert $a \in \mathbb{N}$, $b \in \mathbb{N}_0$ findes en Bijektion $f:]0,a] \to]b,b+a]$ for hvilken $(n,f(n)) = 1$ for alle $n \in]0,a]$. Med andre Ord: Idet

$$\binom{a+b}{a} = \frac{(b+1)(b+2)\cdot\ldots\cdot(b+a)}{1 \cdot 2 \cdot\ldots\cdot a}$$

skal det være muligt at bytte om paa Tællerfaktorerne saaledes at Binomialkoefficienten bliver skrevet som et Produkt af uforkortelige Brøker. Eksempler:

$$\frac{1\cdot2\cdot3\cdot4}{1\cdot2\cdot3\cdot4} = \frac{2}{1}\cdot\frac{3}{2}\cdot\frac{4}{3}\cdot\frac{1}{4}, \qquad \frac{21\cdot22\cdot23\cdot24}{1\cdot2\cdot3\cdot4} = \frac{24}{1}\cdot\frac{23}{2}\cdot\frac{22}{3}\cdot\frac{21}{4}.$$

KAPITEL III : Legemet $(\mathbb{Z}_p, +, \cdot)$.

Naar p er et Primtal, saa er som bekendt (p) et Maximalideal i $(\mathbb{Z},+,\cdot)$, og Kvotientringen $(\mathbb{Z},+,\cdot)/(p) = (\mathbb{Z}_p,+,\cdot)$ er altsaa et Legeme. Det har p Elementer.

Men ethvert Legeme med p Elementer maa være af denne Type, thi det har Karakteristik p og er sit eget Primlegeme, og dette er netop af denne Type. Og det gælder endda at enhver Ring med p Elementer er af denne Type eller af den trivielle Art, hvori alle Produkter er 0. Thi Ringens additive Gruppe har p Elementer og er altsaa isomorf med $(\mathbb{Z}_p,+)$, d.v.s. Ringen har Elementer $\{A, 2A, \ldots, (p-1)A, pA=0\}$, og hvis $A \cdot A \neq 0$ ses at alle øvrige Produkter $(hA)\cdot(kA) \neq 0$ for $p \nmid hk$, saaledes at Nulreglen gælder, og det medfører som bekendt for en endelig Ring at den er et Legeme. Undersøgelsen af $(\mathbb{Z}_p,+,\cdot)$ bliver altsaa samtidig en Undersøgelse af alle Ringe med p Elementer. Hvis Elementtallet i en Ring ikke er et Primtal er der langt flere Muligheder (alene af Ringe med 4 Elementer findes der 11 forskellige ikke-isomorfe (!)).

Elementerne i $\mathbb{Z}_p$ er Restklasser modulo p, og vi betegner dem A eller $\textcircled{a}$, hvor det sidste skal betyde den Restklasse som indeholder Repræsentanten $a \in \mathbb{Z}$. Specielt bliver Etelementet E lig $\textcircled{1}$ og Nulelementet 0 lig $\textcircled{0}$.

For en Endomorfi (homomorf Afbildning ind i sig selv) af den additive Gruppe $(\mathbb{Z}_p,+)$ gælder, at den er bestemt ved Billedet A af E, idet jo saa 2E vil afbildes i 2A o.s.v., og heraf ser man umiddelbart at den additive Gruppes Endomorfiring bliver isomorf med Ringen $(\mathbb{Z}_p,+,\cdot)$. Den eneste Automorfi af $(\mathbb{Z}_p,+,\cdot)$ er Iden-

titeten, idet den hidrører fra en Endomorfi af den additive Gruppe ved hvilken E gaar over i E.

Mængden af invertible Elementer er $\mathbb{Z}_p \setminus \{0\}$, og den betegnes (som sædvanlig) $\mathbb{Z}_p^*$.

Den multiplikative Gruppe $(\mathbb{Z}_p^*, \cdot)$ er abelsk og af Orden p-1.

Ifølge Lagrange's Sætning (L. 1736-1813) gælder saa for ethvert A i Gruppen at $A^{p-1} = E$, og vi har dermed

Fermat's Sætning: I $(\mathbb{Z}_p, +, \cdot)$ gælder for ethvert $A \neq 0$ at $A^{p-1} = E$, eller udtrykt i $\mathbb{Z}$: For $p \nmid a$ vil $p \mid a^{p-1}-1$.

Eksempel: $7 \mid 3^6 - 1 = 728$.

Multipliceres med A faas $A^p = A$, som ogsaa er opfyldt af $A = 0$, og vi har altsaa som anden Form af Sætningen:

For alle $A \in \mathbb{Z}_p$ gælder $A^p = A$, eller udtrykt i $\mathbb{Z}$: For alle a vil $p \mid a^p - a$.

Fermat angav Sætningen 1640 i et Brev til Frénicle, og han har utvivlsomt haft et Bevis, men det kendes ikke. Det første publicerede Bevis skyldes Euler (1707-83).

Da Sætningen er saa fundamental skal vi give endnu et Par Beviser for den, ogsaa fordi forskellige Beviser giver Muligheder for forskellige Generaliseringer.

2' Bevis: I den endelige Gruppe $(\mathbb{Z}_p^*, \cdot)$ vil Multiplikation med A afbilde Elementmængden bijektivt paa sig selv. Derfor

$$\prod_{X \in \mathbb{Z}_p^*} X = \prod_{X \in \mathbb{Z}_p^*} (AX)$$

og idet Gruppen er abelsk faas $\prod X = A^{p-1} \cdot \prod X$, hvoraf ved Division med $\prod X$ faas $A^{p-1} = E$. Det var altsaa egentlig et Bevis for Lagrange's Sætning i abelske Grupper. □

3' Bevis: Idet Legemet $(\mathbb{Z}_p, +, \cdot)$ har Karakteristik p gælder $(A + B)^p = A^p + B^p$, thi i Binomialudviklingen er alle de

øvrige Led $\binom{p}{j}A^jB^{p-j}$ lig 0, da (som tidligere omtalt) $p\mid\binom{p}{j}$ for $j\in\,]0,p[$. Endvidere er $(AB)^p = A^p\cdot B^p$, og Afbildningen $X\mapsto X^p$ er altsaa en Endomorfi af Legemet $(\mathbb{Z}_p,+,\cdot)$, og idet den fører E over i E er det endda en Automorfi, altsaa Identiteten, saa $A^p = A$. □

4' Bevis: Medens de forrige Beviser var algebraiske skal vi nu give et kombinatorisk Bevis; det er en Bevistype som (paa lignende Problemer) har haft en af sine første Anvendere i Julius Petersen (1839-1910). Vi vil vise, at for $a\in\mathbb{N}$ vil $p\mid a^p-a$. Vi betragter Afbildninger $f:\mathbb{Z}\to M$, hvor M er en Mængde med a Elementer; endvidere skal Afbildningerne være periodiske med Perioden p, altsaa $f(n) = f(n+p)$. Antallet saadanne Afbildninger er lig a^p, idet man indenfor en Periodelængde, fx for $n\in\,]0,p]$, har a Muligheder for hvert $f(n)$. Den korteste Periode for et f maa gaa op i p, og den er altsaa lig p eller 1. Den korteste Periode lig 1 indtræffer for a Stk. f, nemlig dem for hvilke f er konstant, og for de øvrige a^p-a Stk. f er den korteste Periode altsaa p. Disse f samler vi nu i Klasser, idet Funktioner som kan gaa over i hinanden ved en Translation i Argumentet puttes i samme Klasse; derved vil hver Klasse komme til at indeholde p Stk. f; altsaa gælder $p\mid a^p-a$. □

Legemet $(\mathbb{Z}_p,+,\cdot)$ er kommutativt, og vi kan nu benytte den kendte Teori for Polynomier over dette Legeme.

For et vilkaarligt kommutativt Legeme med q Elementer kan vi anvende Lagrange's Sætning paa Legemets multiplikative Gruppe, og vi faar: For alle $X\neq 0$ er $X^{q-1} - E = 0$; dette Polynomium har

altsaa alle $\Lambda \neq 0$ som Rødder, og vi har derfor

$$X^{q-1} - E = \prod_{\Lambda \neq 0} (X - \Lambda) .$$

Polynomiets Koefficienter er de symmetriske Grundfunktioner af Rødderne, og disse er altsaa alle lig 0 undtagen Røddernes Produkt som er lig $-E$ (egl. $-E\cdot(-1)^{q-1}$, men enten er q ulige, og saa er det $-E$, eller ogsaa er q lige og saa er Legemets Karakteristik lig 2 og derfor $+E = -E$). Nu gælder som bekendt Sætningen "Ethvert symmetrisk homogent Polynomium i Rødderne kan skrives som et Polynomium i de elementarsymmetriske Funktioner"; man har derfor umiddelbart, at ethvert saadant Polynomium er lig 0 undtagen hvis dets Grad er delelig med q-1 i hvilket Tilfælde det kan antage en egentlig Værdi (nemlig hvis dets Fremstilling ved de elementarsymmetriske Funktioner indeholder et Led som er en Konstant gange en Potens af Rødddernes Produkt).

I vort $(\mathbb{Z}_p,+,\cdot)$ er $q = p$. Udtrykt i $\mathbb{Z}$ siger det ovenstaaende at <u>ethvert homogent symmetrisk Polynomium i Tallene $1,2,\ldots,p-1$ har en Værdi som er delelig med p undtagen (eventuelt) hvis $p-1$ gaar op i Polynomiets Grad</u>.

<u>Eksempel</u>: $s_2 = 1\cdot2+1\cdot3+\ldots+(p-2)\cdot(p-1)$ er delelig med p undtagen for $p = 3$ i hvilket Tilfælde $s_2 = 2$.

<u>Eksempel</u>: Ifølge Fermats Sætning er $1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1} \equiv p-1 \equiv -1$ (modulo p), men dets Grad er jo ogsaa netop $p-1$.

Resultatet om at Rødddernes Produkt er lig $-E$ kan med Betegnelserne fra $\mathbb{Z}$ udtrykkes ved

<u>Wilson's Sætning</u> (W. 1741-93): <u>For alle Primtal p gælder at p gaar op i $(p-1)! + 1$.</u>

Wilson synes kun at have haft den som en empirisk Sætning. Det første publicerede Bevis skyldes Lagrange.

Eksempler:

$$2 \mid 1! + 1 = 2$$
$$3 \mid 2! + 1 = 3$$
$$5 \mid 4! + 1 = 25$$
$$7 \mid 6! + 1 = 721$$
$$11 \mid 10! + 1 = 3628801 = 11 \cdot 329891$$

Lad os ogsaa her give endnu et Bevis for at i et endeligt kommutativt Legeme er Produktet af de fra 0 forskellige Elementer lig $-E$. Hvis A er forskellig fra A^{-1} tager vi et sandant Par reciprokke Elementer sammen i Produktet, det giver ialt en Faktor E. Tilbage er der de A for hvilke $A = A^{-1}$, d.v.s. $A^2 = E$, men dette er opfyldt af E og $-E$ (ikke af flere da Polynomiet X^2-E højst har 2 Rødder) og Produktet bliver derfor $-E$; hvis Legemet har karakteristik 2 har X^2-E kun én Rod som er $\pm E$ og altsaa ogsaa bidrager med en Faktor $-E$. □

Iøvrigt er Wilsons Betingelse $p \mid (p-1)! + 1$ baade nødvendig og tilstrækkelig for at et naturligt Tal $p \geq 1$ er et Primtal, thi hvis p er sammensat vil det have en Divisor $d \in]1,p[$ og saa vil d gaa op i $(p-1)!$, saa Wilsons Betingelse kan ikke være tilfredsstillet. Sætningen giver altsaa et Primtalkriterium, men det er naturligvis uanvendeligt til praktisk Regning, da $(p-1)!$ vokser voldsomt med p.

Det er nærliggende at spørge om Fermats Sætning kan vendes om og altsaa bruges som Primtalkriterium. Det gaar i hvert Fald ikke umiddelbart, fx vil $15 \mid 4^{14} - 1 = (4^2 - 1) \cdot (4^{12} + \ldots)$ skønt 15 ikke er et Primtal. Vi kommer senere tilbage til dette Spørgsmaal.

Gauss har vist: Den multiplikative Gruppe $(\mathbb{Z}_p^*, \cdot)$ er cyklisk (af Orden p-1).

Vi vil mere generelt vise:

I den multiplikative Gruppe for et kommutativt Legeme er enhver endelig Undergruppe cyklisk.

Eksempel: $(\mathbb{R}, +, \cdot)$ har den multiplikative Gruppe $(\mathbb{R}^*, \cdot)$ som ikke er cyklisk. Undergruppen $(\{\pm 1\}, \cdot)$ er endelig og cyklisk, medens Undergruppen $(\mathbb{R}^+, \cdot)$ er uendelig og ikke cyklisk.

Vi skal senere omtale Wedderburns Sætning, som udsiger at ethvert endeligt Legeme er kommutativt. Kombineres dette med det ovenstaaende ser man, at i ethvert endeligt Legeme vil den multiplikative Gruppe være cyklisk.

Bevis: Først lidt generelt om abelske Grupper.

1) Hvis k er Orden for et Gruppeelement A, og $h \mid k$, saa er h ogsaa Elementorden i Gruppen, nemlig for Elementet $A^{k/h}$; klart. 2) Hvis r og s er Ordenerne for Elementer, hhv. A og B, i en abelsk Gruppe, og $(r,s) = 1$, saa er r·s ogsaa Elementorden, nemlig for AB; thi dels er $(AB)^{rs} = A^{rs}B^{sr} = E \cdot E = E$, saa at ord(AB) gaar op i rs, og dels vil $(AB)^m = E$ medføre at $B^{mr} = A^{-mr}$ som er lig E, hvorfor s vil gaa op i mr og altsaa i m, og analogt ses at r gaar op i m, og tilsammen ses at rs gaar op i ord(AB).

Ved at kombinere det nævnte faas at hvis m er mindste fælles Multiplum af de i en abelsk Gruppe forekommende Elementordener, saa er m selv Elementorden (og Mængden af Elementordener udgøres netop af Divisorerne i m). Thi m er Produktet af de højeste Potenser af de forskellige Primtal som forekommer i Elementordenernes Primopløsninger; ifølge 1) er disse Primtalpotenser selv Elementordener, og ifølge 2) er deres Produkt en Elementorden.

Det er væsentligt for det understregede Resultat at Gruppen er

abelsk; Permutationsgruppen S_3 har 6 Elementer, og de forekommende Elementordener er 1,2 og 3. Vi noterer ogsaa, at Betingelsens Opfyldelse er ikke tilstrækkelig til at sikre at Gruppen er abelsk (der findes som bekendt en ikke-abelsk Gruppe af Orden 8, og de forekommende Elementordener er 1,2 og 4).

Lad os nu betragte en Undergruppe af Orden q i et kommutativt Legemes multiplikative Gruppe. Ifølge Lagranges Sætning vil den største Elementorden m gaa op i q, altsaa $m \leqq q$. Men da enhver Elementorden gaar op i m er $X^m - E = 0$ for alle Gruppens q Elementer, altsaa $q \leqq m$ (Antallet Rødder i en Ligning er mindre end eller lig dens Grad). Følgelig er $q = m$ = en Elementorden, saa Undergruppen er cyklisk. □

Dermed har vi altsaa en Isomorfi $(\mathbb{Z}_p^*, \cdot) \approx (\mathbb{Z}_{p-1}, +)$. Multiplikationen overføres herved i Addition, og det betyder at vi kan lave "Logaritmeregning", i dette Tilfælde ofte betegnet med det gamle (maaske lidt uheldige) Navn Indexregning:

Hvis A er Frembringerelement i $(\mathbb{Z}_{p-1}, +)$, saa vil det svare til et G som er Frembringerelement i $(\mathbb{Z}_p^*, \cdot)$, og Potenserne af G giver alle Elementer i $\mathbb{Z}_p^*$, og Multiplikation af Elementer betyder Addition af Exponenterne. Hvis $G = (g)$, saa betegner man ogsaa g som Primitivrod modulo p, og hvis $(m) = M = G^h$, saa betegnes h som "Index" for m, $h = \text{ind}_g\, m = \text{ind}\, m$; dette Index er kun bestemt paanær et Multiplum af p-1.

Som Frembringerelement i den additive Gruppe $(\mathbb{Z}_{p-1}, +)$ kan man benytte Restklassen (1), men der er (for $p > 2$) flere Frembringerelementer. Et Element (a) er Frembringer hvis og kun hvis Multipla af a giver alle Restklasser modulo p-1, d.v.s. naar - indenfor $\mathbb{Z}$ - Idealet (a) adderet til Mængden af Multipla af p-1 giver alle Tal, altsaa - skrevet med Idealer - naar

(a) + (p-1) = (a,p-1) er lig (1). Betingelsen er altsaa at a er primisk med p-1. Antallet af forskellige Frembringerelementer A ses at være lig Antallet af primiske Restklasser modulo p-1; dette Antal betegnes iøvrigt $\varphi(p-1)$, hvor φ er en Funktion som vi senere skal omtale.

(Det ovenstaaende viser - stort set - at Automorfigruppen for $(\mathbb{Z}_{p-1},+)$ er isomorf med $(\mathbb{Z}_{p-1}^{*},\cdot)$, hvor $\mathbb{Z}_{p-1}^{*}$ er Mængden af de $\varphi(p-1)$ Stk. primiske Restklasser modulo p-1).

Eksempel: p = 17.

Vi skal først finde en Primitivrod g (og Beviset foran for Gauss' Sætning hjælper os jo ikke, da det var et rent Eksistensbevis). Vi skal i $(\mathbb{Z}_{p}^{*},\cdot)$ have ord(g) = p-1 = 16. Ord(1) = 1, saa g=1 vil aldrig kunne bruges (undt. for p = 2). Prøves med g = 2 faar vi $g^4 = 16 \equiv -1 \pmod{17}$, og derfor $g^8 \equiv 1$, saa det gaar heller ikke. Det viser sig at gaa med g = 3:

Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$(\mathbb{Z}_{16},+)$ mod.16
m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	mod.17 $(\mathbb{Z}_{17}^{*},\cdot)$

Tabellen giver den mindste positive Repræsentant for $m \equiv 3^{index}$. Eksempler paa dens Anvendelse som "Logaritmetabel" kommer senere. De indices a som svarer til brugbare Primitivrødder er dem hvor (a,16) = 1, altsaa de ulige a, og som Primitivrødder kan vi altsaa bruge 3,10,5,11,14,7,12 og 6, ialt 8 = $\varphi(16)$ Stk.

Det kan være besværligt at finde en Primitivrod (en Del Tabeller er publiceret i Tidens Løb); desuden ses, at Tabellen er springende, man kan ikke interpolere i den, saa for større Tal bør man ogsaa have en Tabel ordnet efter m hvis man skal have Glæde af det (medens sædvanlige "Antilogaritmetabeller"er ganske overflødige, kun til Glæde for Bogtrykkere).

Ved en algebraisk Kongruens modulo p forstaas en Ligning

$$A(X) = A_h X^h + \ldots + A_1 X + A_0 = 0,$$

hvor A(X) er et Polynomium $\in \mathbb{Z}_p[X]$, d.v.s. at alle Koefficienterne $A_j \in \mathbb{Z}_p$, og hvori man søger Løsninger X indenfor $\mathbb{Z}_p$. Dersom $A_j = \overline{(a_j)}$ med $a_j \in \mathbb{Z}$ og $X = \overline{(x)}$ med $x \in \mathbb{Z}$, ser man, at Opgaven ogsaa kan skrives

$$a_h x^h + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$$

thi hvis man har et x som opfylder denne Ligning vil hele Restklassen $\overline{(x)} = X$ aabenbart ogsaa gøre det, og dermed være Løsning til Ligningen foroven, og har man omvendt Restklasser X som opfylder Ligningen foroven vil de bestaa af Tal x som opfylder Kongruensen i $\mathbb{Z}$. Ifølge den almene Teori for Polynomier over et kommutativt Legeme har vi saa: En Ligning som ovenfor, $A(X) = 0$ med $A_h \not\equiv 0$, har højst h Løsninger $X_1, \ldots X_r$, og A(X) kan skrives som $(X-X_1)^{\alpha_1} \ldots (X-X_r)^{\alpha_r} \cdot B(X)$, hvori B(X) er et polynomium uden Rødder. Formuleret i $\mathbb{Z}$ faas

En algebraisk Kongruens modulo et Primtal p

$a(x) = a_h x^h + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$, $p \nmid a_h$, har som Løsningsmængde et Antal Restklasser modulo p, højst h Stk., og hvis vi som Repræsentanter for Løsningsklasserne tager $x_1, \ldots, x_r$, saa har vi - med koefficientvis Kongruens - at

$a(x) \equiv (x-x_1)^{\alpha_1} \cdot \ldots \cdot (x-x_r)^{\alpha_r} \cdot b(x)$, hvor $b(x) \not\equiv 0$ er uden Løsninger.

Vi bemærker, at da vi i $\mathbb{Z}_p$ altid har $X^p = X$, kan vi altid reducere en Opgave til at være af Grad lavere end p.

Eksempel: Løs

$$x^{13}+x^4+30x^3+16x^2-8x-40 \equiv 0 \pmod{11}.$$

Her kan x^{13} erstattes med x^3, og endvidere reducerer vi Koefficienterne til deres numerisk mindste Værdier modulo 11:

$$x^4-2x^3+5x^2+3x+4 \equiv 0 \pmod{11}.$$

Idet $x = 1$ opdages at være Rod kan man dividere med $(x-1)$ og faar

$$(x-1)(x^3-x^2+4x+7) + 11 \equiv 0$$

eller

$$(x-1)(x^3-x^2+4x-4) \equiv 0$$

og her er $x = 1$ igen Rod i den store Parentes, saa det kan skrives

$$(x-1)^2(x^2+4) \equiv 0.$$

Da x^2 kun antager Værdierne $0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 = 16 \equiv 7, (\pm 5)^2 = 25 \equiv 3$ ses at x^2+4 aldrig kan være kongruent 0. Opgavens Løsningsmængde er altsaa $\underline{x \equiv 1 \pmod{11}}$.

Det kan være praktisk at udvide Kongruensbegrebet modulo p til ogsaa at gælde en større Mængde rationale Tal:
Lad $\mathbb{Q}^{(p)}$ være Mængden af uforkortelige Brøker a/b, hvor $p \nmid b$. Man ser umiddelbart, at $\mathbb{Q}^{(p)}$ er en Ring, ægte Delring af de rationale Tals Ring. Idet φ betegner Homomorfien $(\mathbb{Z},+,\cdot) \to (\mathbb{Z}_p,+,\cdot)$, udvider vi nu φ til en Afbildning af $\mathbb{Q}^{(p)}$ ind paa $\mathbb{Z}_p$, idet vi sætter Billedet af a/b til $\varphi(a)/\varphi(b)$. Afbildningen er veldefineret, idet hvis $a/b = c/d$, altsaa $ad = bc$, ses let at $\varphi(a)/\varphi(b) = \varphi(c)/\varphi(d)$. Det er en Udvidelse af φ, thi $\varphi(a) = \varphi(a)/\varphi(1) = \varphi(a/1)$. Det er en Homomorfi, da Produkt gaar over i Produkt: $\varphi(a/b)\cdot\varphi(c/d) = (\varphi(a)/\varphi(b))\cdot(\varphi(c)/\varphi(d)) = \varphi(a)\varphi(c)/\varphi(b)\varphi(d) = \varphi(ac)/\varphi(bd) = \varphi(ac/bd)$ og paa lignende Maade ses at Sum gaar over i Sum. Værdimængden er stadig $\mathbb{Z}_p$, og vi kan altsaa for ethvert $a/b \in \mathbb{Q}^{(p)}$ finde et $k \in \mathbb{Z}$ saa $a/b \equiv k$ (modulo p).
Ringen $\mathbb{Q}^{(p)}$ er paa sin Vis simplere end $(\mathbb{Z},+,\cdot)$, idet det er en saakaldt lokal Ring, idet samtlige ikke-invertible Elementer, altsaa alle Brøker a/b hvor $p \mid a$, udgør ét Ideal som altsaa trivielt maa være Maximalideal (og det eneste saadanne), og er Kerne for φ.

Iøvrigt kan man bemærke, at det foregaaende egentlig er en generel algebraisk Konstruktion: Der er givet en kommutativ Ring $(M,+,\cdot)$ med Etelement og hvori Nulreglen gælder, og en homomorf Afbildning φ af denne over paa et Legeme K; Homomorfiens Kerne er et Maximalideal I. Ringen har et Brøklegeme, og i dette tager vi nu den Delmængde $M^{(I)}$ som bestaar alle Kvotienter a/b mellem Ringelementerne for hvilke $b \notin I$. Vi definerer $\varphi(a/b)$ som $\varphi(a)/\varphi(b) \in K$, og det ses let at være en veldefineret homomorf Afbildning $M^{(I)} \longrightarrow K$, hvis Restriktion til M er det oprindelige φ. Afbildningens Kerne i $M^{(I)}$ er Brøkerne a/b, hvor $a \in I$, $b \notin I$, hvilket netop er Mængden af ikke-invertible Elementer, og denne Mængde er altsaa trivielt et Maximalideal (og det eneste), og vi har faaet Ringen M udvidet til en"lokal Ring" $M^{(I)}$.

Eksempel:

Løs $x^2 + x + 2 \equiv 0 \pmod{11}$.

Vi faar $(x + \frac{1}{2})^2 \equiv -\frac{7}{4}$ og da $-7 \equiv 4$ er højre Side $\equiv 1$. Altsaa $x + \frac{1}{2} \equiv \pm 1$, og vi faar Løsningerne

$$x \equiv \begin{cases} \frac{1}{2} \equiv 6 \\ -\frac{3}{2} \equiv 4 \end{cases} \pmod{11}$$

Kontrol: $(x - 6)(x - 4) = x^2 - 10x + 24 \equiv x^2 + x + 2$.

Førstegradskongruenser kræver ikke mange Ord, da vi er i et Legeme. Vi har: En Førstegraaskongruens $ax \equiv b \pmod{p}$, hvor $p \nmid a$, har som Løsningsmængde netop én Restklasse modulo p.

Eksempel:

$$22x \equiv 12 \pmod{17}$$

1' Metode: Man kan prøve med $x \equiv 1,2,3,\ldots,16$; et besværligt men endeligt Arbejde.

2' Metode: Vi har $x \equiv 12/22$ og i Brøken kan vi nu forlænge og forkorte og erstatte Tæller eller Nævner med dermed kongruente: $x \equiv 12/22 \equiv 6/11 \equiv 6/(-6) \equiv -1 \pmod{17}$

3' Metode: Vi kan bortskaffe Nævneren v.Hj.a. Fermats Sætning: $x \equiv 12/22 \equiv 12 \cdot 22^{15} \equiv 12 \cdot 5^{15} \equiv 12 \cdot 125^5 \equiv 12 \cdot 6^5 \equiv 12 \cdot 6 \cdot 36^2 \equiv 4 \cdot 2^2 \equiv 16 \pmod{17}$.

4' Metode: Vi kan bruge Indextabellen S.47:

ind x = ind 12 - ind 22 = ind 12 - ind 5 = 13 - 5 = 8,

og ved at gaa tilbage i Tabellen findes $x \equiv 16 \pmod{17}$.

Binome Kongruensopgaver: Opgaven $x^a \equiv b$ (modulo p), hvor $p \nmid b$, kan umiddelbart oversættes til Indices og bliver til

$a \cdot \text{ind } x \equiv \text{ind } b$ (modulo p-1).

Eksempler:

1) $x^4 \equiv 15 \pmod{17}$ bliver til $4 \text{ ind } x \equiv 6 \pmod{16}$, altsaa $16 \mid 6 - 4 \text{ ind } x$, som aabenbart er uløselig.

2) $x^6 \equiv 15 \pmod{17}$ bliver til $6 \text{ ind } x \equiv 6 \pmod{16}$, altsaa $16 \mid 6 - 6 \text{ ind } x = 6(1 - \text{ind } x)$; her kan forkortes med 2, og det er ensbetydende med $8 \mid 3(1 - \text{ind } x)$, som igen er ensbetydende med at $8 \mid 1 - \text{ind } x$, altsaa

$$\text{ind } x \equiv \begin{cases} 1 \\ 9 \end{cases} \pmod{16}, \text{ eller } x \equiv \begin{cases} 3 \\ 14 \end{cases} \pmod{17}$$

3) For hvilke b har $x^4 \equiv b$ (modulo 17) Løsninger ? omskrives til $4 \mid \text{ind } b \pmod{16}$, eller ind b = 4,8,12,16, hvoraf faas $b \equiv \pm 1$ eller $b \equiv \pm 4 \pmod{17}$.

Alt i alt faar man nedenstaaende Sætning; Beviset skal ikke detailleres, men fremgaar af Eksemplerne ovenfor (man bemærker ogsaa at Problemet føres over i Kongruenser modulo p-1, som normalt er et sammensat Tal, og saadanne Kongruenser skal vi senere betragte nærmere); dersom $x^a \equiv b \pmod{p}$, hvor $p \nmid b$, siges at b er en a'te Potensrest modulo p.

Nødvendigt og tilstrækkeligt for at $x^a \equiv b \pmod{p}$, hvor $p \nmid b$, har Løsninger, altsaa at b er en a'te Potensrest modulo p, er det at $(a,p-1) \mid$ ind b, hvilket er ensbetydende med at b opløftet til Potensen $(p-1)/(a,p-1)$ er kongruent med 1 (mod.p). Hvis Betingelsen er opfyldt er Antallet af Løsningsrestklasser $\textcircled{x} \in \mathbb{Z}_p$ lig $(a,p-1)$.

Udtrykt med Grupper har vi: Mængden af a'te Potensrester udgør en Undergruppe i $(\mathbb{Z}_p^*, \cdot)$, og er altsaa cyklisk og er af Orden $(p-1)/(a,p-1)$.

Endvidere kan vi bemærke, at Summen af de a'te Potensrester modulo p vil være delelig med p, undtagen hvis p-1 gaar op i a. Thi hvis p-1 gaar op i a vil alle a'te Potenser være $\equiv 1$ (Fermats Sætning) saa der er kun denne ene a'te Potensrest; og hvis p-1 ikke gaar op i a er $1^a + 2^a + \ldots + (p-1)^a \equiv 0 \pmod{p}$ (se S.43), og her staar jo netop Summen af de a'te Potensrester multipliceret med $(a,p-1)$ (for hver af dem kommer med for $(a,p-1)$ Stk. inkongruente x ifølge Sætningen ovenfor).

Eksempel: $a = 3$, d.v.s der er Tale om "kubiske Rester".

For $p = 7$ er $(a,p-1) = (3,6) = 3$; Antallet af kubiske Rester er $(p-1)/(a,p-1) = 6/3 = 2$, og de opfylder Ligningen $b^2 \equiv 1 \pmod{7}$. De kubiske Rester er derfor $b \equiv \pm 1 \pmod{7}$, og de udgør med Multiplikation en Undergruppe af Orden 2; endvidere er Summen af dem $\equiv 0 \pmod{7}$. Alt dette ses at være rigtigt, idet

$$\left.\begin{matrix} 1^3 \\ 2^3 \\ 4^3 \end{matrix}\right\} \equiv 1, \qquad \left.\begin{matrix} 3^3 \\ 5^3 \\ 6^3 \end{matrix}\right\} \equiv -1 \pmod{7}.$$

For $p = 17$ er $(a,p-1) = (3,16) = 1$. Antallet kubiske Restklasser er 16, d.v.s. ethvert b er kubisk Rest, og enhver Kongruens $x^3 \equiv b$ har netop én Løsningsrestklasse $\textcircled{x}$.

Fx $x^3 \equiv 14 \Leftrightarrow x \equiv 10$ (Benyt Indextabellen S.47).

Vi vil nu betragte Tilfældet a = 2 mere indgaaende, men lad os først gøre Rede for at enhver kvadratisk Kongruens kan reduceres til en binom kvadratisk Kongruens: Vi ser paa $ax^2 + bx + c \equiv 0$ (modulo p), hvor $p \nmid a$. Tilfældet p = 2 kan vi lade ude af Betragtning, thi her er jo $x^2 \equiv x$, saa vi de facto har en lineær Opgave $(a + b)x + c \equiv 0$ (mod.2), som er umiddelbar at diskutere (for $2 \nmid a+b$ er der netop én Løsningsrestklasse, for $2 \mid a+b$ er der to eller ingen). For $p > 2$ benytter vi den sædvanlige Omskrivning af Polynomiet til $a(x + b/2a)^2 + (c - b^2/4a)$, saa at Problemet er reduceret til $(x + b/2a)^2 \equiv -(c - b^2/4a)/a$; hvis p gaar op i Højresiden finder vi Løsningen $x \equiv - b/2a$, og hvis p ikke gaar op i Højresiden har vi en binom Kongruens af den foran betragtede Type.

Vi skal altsaa nu benytte de foran angivne Sætninger paa Opgaven $x^2 \equiv b$ (modulo p), hvor p er et ulige Primtal.

Dersom $x^2 \equiv b$ (mod.p), $p \nmid b$, har Løsninger siger vi at b er kvadratisk Rest modulo p, og ellers siger vi at b er kvadratisk Ikke-Rest modulo p.

Men da Tilfældet er saa vigtigt vil vi give direkte Beviser for Resultaterne, hvilket er muligt uden at benytte den cykliske Struktur af $(\mathbb{Z}_p^*, \cdot)$, og ogsaa historisk er rimeligt, idet de kvadratiske Rester var kendt allerede af Euler (og væsentlig ogsaa af Fermat), altsaa før Gauss' Tid.

Udtrykt i $(\mathbb{Z}_p, +, \cdot)$ er Opgaven $X^2 = B$, $B \neq 0$. Man ser, at dersom der er en Løsning X_0, saa er der netop to Løsninger, nemlig $\pm X_0$ (ikke flere, da Graden er 2).

Antallet af forskellige kvadratiske Restklasser B bliver derfor $\frac{p-1}{2}$ (nemlig Halvdelen af Antallet mulige X), og Antallet af kvadra-

tiske Ikke-Rester bliver lige saa stort.

De kvadratiske Rester B udgør en Undergruppe i $(\mathbb{Z}_p^*, \cdot)$, thi det er en Delmængde som er stabil ved Division da $X_1^2 = B_1$ og $X_2^2 = B_2$ giver $(X_1 X_2^{-1})^2 = B_1 B_2^{-1}$. Da alt er abelsk er det en normal Undergruppe i $(\mathbb{Z}_p^*, \cdot)$, og Kvotientgruppen er altsaa af Orden 2 og kan fx repræsenteres ved $(\{\pm 1\}, \cdot)$.

Eulers Kriterium: For de kvadratiske Restklasser B gælder $B^{\frac{p-1}{2}} = E$, og for de kvadratiske Ikke-Rester gælder $B^{\frac{p-1}{2}} = -E$.

Bevis: Ifølge Fermat er for $B \neq 0$

$$B^{p-1} - E = \left(B^{\frac{p-1}{2}} - E\right) \cdot \left(B^{\frac{p-1}{2}} + E\right) = 0,$$

og for de kvadratiske Rester B er $B^{\frac{p-1}{2}} = X^{p-1} = E$, saa for dem er den første Parentes lig 0, og den er ikke 0 for flere B (Graden er $\frac{p-1}{2}$), saa for de øvrige B, altsaa Ikke-Resterne, er den anden Parentes lig 0. □

Man ser ogsaa at for en vilkaarlig Undergruppe med $\frac{p-1}{2}$ Elementer i $(\mathbb{Z}_p^*, \cdot)$ gælder for et Element B at $B^{\frac{p-1}{2}} = E$ (Lagrange's Sætning), saa $\{$kvadratiske Rester$\}$ er den eneste Undergruppe med $\frac{p-1}{2}$ Elementer (hvilket jo ogsaa stemmer med den cykliske Struktur af $(\mathbb{Z}_p^*, \cdot)$).

Legendre-Symbolet er

$$\left(\frac{b}{p}\right) = \begin{cases} 1 & \text{hvis b er kvadr. Rest mod.p} \\ -1 & \text{hvis b er kvadr. Ikke-Rest} \end{cases}$$

Man ser, at Afbildningen $(b) \mapsto \left(\frac{b}{p}\right)$ netop er den ovenfor omtalte Homomorfi af $(\mathbb{Z}_p^*, \cdot)$ ind paa en Gruppe $(\{\pm 1\}, \cdot)$; Afbildningens Kerne udgøres af de kvadratiske Rester. Heraf følger at Legendre-Symbolet er multiplikativt, altsaa at $\underline{\left(\frac{b \cdot c}{p}\right) = \left(\frac{b}{p}\right) \cdot \left(\frac{c}{p}\right)}$.

Endvidere ses at Eulers Kriterium kan udtrykkes: modulo p er $\underline{b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right)}$.

Man ser Overensstemmelsen mellem det her udviklede om kvadratiske Rester og de generelle Sætninger fra S.52, som i denne Situation bliver simplere, idet a = 2 og p ulige giver (a,p-1) = 2 altid. Og de kvadratiske Rester udgør den Undergruppe som dannes af alle de lige Potenser af en Primitivrod.

Eksempel: De kvadratiske Rester modulo 17 ses af Tabellen S.47 at være 1,9,13,15,16,8,4 og 2. I dette specielle Tilfælde gælder, at enhver kvadratisk Ikke-Rest er Primitivrod, men det skyldes at p-1 = 16 ikke har andre Primdivisorer end 2, i Almindelighed er Primitivrødderne kun nogle faa blandt de kvadratiske Ikke-Rester.

Eksempel (som senere vil indgaa som en Bestanddel af "Reciprocitetssætningen"): Vi har

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{for } p = 4h + 1 \\ -1 & \text{for } p = 4h - 1 \end{cases}$$

hvilket umiddelbart faas af Eulers Kriterium, idet $(-1)^{\frac{p-1}{2}}$ netop har denne Værdi i de to Tilfælde.

Anvendelse: I Eksemplet S.49 fandt vi at $x^2 \equiv -4 \pmod{11}$ ikke havde Løsninger; nu kan det let begrundes, idet

$$\left(\frac{-4}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{-1}{11}\right) = \left(\frac{-1}{11}\right) = -1.$$

Der findes uendeligt mange Primtal af Formen $p = 4h + 1$. (det var det Tilfælde, som vi ikke tidligere kunde klare). Vi konstruerer Følgen

$$\begin{aligned} a_1 &= 5 \\ a_2 &= (2a_1)^2 + 1 \\ &\cdots\cdots \\ a_n &= (2a_1a_2\ldots a_{n-1})^2 + 1 \\ &\cdots\cdots \end{aligned}$$

Tallene har hver sine egne ulige Primdivisorer, og hvis p er en saadan ser man at der er et Kvadrat kongruent -1 modulo p, saa p maa være af Formen 4h + 1 ifølge Eksemplet ovenfor.

Eksempler paa Teknik. Vi vil vise, hvorledes dette Kapitels Sætninger kan anvendes paa mange forskellige Maader.

1) Følgen $a-1, 2a-1, 4a-1, 8a-1, \ldots$ kan ikke bestaa af lutter Primtal (Følgen vokser saa hurtigt, at der tæthedsmæssigt ikke var noget i Vejen for det).

Bevis: Antag at $a-1$ er et Primtal $p \geq 2$. Saa er ifølge Fermat $2^{p-1}a - 1 = (2^{p-1}-1)a + (a-1)$ delelig med p, og da det er større end p maa det være sammensat. Man bemærker at for $a = 3$ bliver $a-1 = 2$ saa Beviset ikke kan anvendes, men saa kan man blot begynde med $2a - 1 = 5$, og Følgen $2, 5, 11, 23, 47, \ldots$ kan altsaa heller ikke bestaa af lutter Primtal.

2) For ethvert naturligt Tal $n > 1$ gælder $n \nmid 2^n - 1$.

Bevis: Hvis n er et Primtal er der ikke noget Problem, thi saa har man jo $n \mid 2^n - 2$, men vi skal vise det for et vilkaarligt naturligt Tal. Lad nu p være en Primdivisor i n. I $(\mathbb{Z}_p^*, \cdot)$ sættes ord(2) = h, altsaa h lig den mindste Exponent saa $p \mid 2^h - 1$. Vi har [1] $h > 1$, [2] ifølge Fermat gælder $h \mid p-1$ [3] saafremt $n \mid 2^n-1$ vil $p \mid 2^n-1$ saa $h \mid n$. Altsaa er [1] $h > 1$, [2] $h < p$ og [3] h er Divisor i n; men hvis p var valgt som den mindste Primdivisor i n ses der at være Modstrid.

Et Eksempel som $20 \mid 3^{20} - 1 = (3^4 - 1)(3^{16} + \ldots)$ hvori $3^4-1 = 80$ viser at Resultatet kun gælder med Potenser af 2.

3) Hvis a er et lige Tal større end 2, saa er $a-1$ og $a+1$ Primtaltvillinger hvis og kun hvis $a^2-1 \mid 4 \cdot (a-2)! + a + 3$.

Bevis: Hvis et eller begge af Tallene $a-1$ og $a+1$ er sammensatte, saa findes der en Divisor d i a^2-1 med $1 < d \leq \frac{a+1}{3}$ (begge Tallene er jo ulige), og da $a \geq 4$ er d mindre end $a-2$ og gaar altsaa op i $(a-2)!$; og idet d gaar op i $a-1$ el-

ler a+1 kan d ikke gaa op i a+3 da d ikke gaar op i 2 eller 4 (d er jo ulige). Relationen kan altsaa kun haabes opfyldt af Primtaltvillinger.

Antag nu at a-1 og a+1 begge er Primtal; vi skal saa blot vise at de hver for sig gaar op i Relationens Højreside. Ifølge Wilson gaar a-1 op i $4((a-2)!+1) + a-1$, saa det er i Orden. Og betragter vi Højresiden modulo a+1 er den kongruent med

$4\cdot(a-2)! + 2 \equiv 2\cdot(-1)\cdot(-2)\cdot(a-2)! + 2 \equiv 2\cdot a\cdot(a-1)\cdot(a-2)! + 2 \equiv 2\cdot(a! + 1)$ som ifølge Wilson er kongruent med 0.

4) <u>For ethvert naturligt Tal n er nedenstaaende Tal lige</u>

$$\left[\frac{(n-1)!}{n\cdot(n+1)}\right] .$$

Bevis: For $n \leqq 5$ er $(n-1)! < n(n+1)$, saa Talværdien er 0; for n = 6 faas $\left[120/42\right] = 2$ og for n = 7 faas $\left[720/56\right] = 12$, saa vi behøver kun at betragte $n \geqq 8$.

Hvis baade n og n+1 er sammensatte vil de hver for sig gaa op i (n-1)! og da de er indbyrdes primiske vil deres Produkt ogsaa gaa op, og man overbeviser sig let om at der vil være et Overskud af lige Faktorer i Tælleren, saa hele Brøken bliver et lige helt Tal.

Hvis n er et Primtal p, saa er n+1 sammensat og vil gaa op i (n-1)!, og ligesom ovenfor vil Kvotienten blive lige. Lad os imidlertid addere $\frac{1}{p}$ til den opskrevne Brøk, hvorved den faar Formen $\frac{(p-1)! + p + 1}{p(p+1)}$; forkorter vi nu med p+1 faar den Formen $\frac{\text{ulige Tæller}}{p}$, men her gaar p op i Tælleren, thi ifølge Wilson gik p op i Tælleren ovenover, og det er ikke ødelagt ved Forkortningen med p+1 (som jo er primisk med p). Altsaa er den oprindelige store Brøk + $\frac{1}{p}$ lig et ulige helt Tal, saa

den opskrivne Hel-Dels-Værdi er lige.

Dersom n+1 er et Primtal p gaar det analogt, idet igen Brøken $+\frac{1}{p}$ bliver et ulige helt Tal.

5) Hvis p er et Primtal af Form $p = 4h + 1$, saa vil Kongruensen $x^4 \equiv h \pmod{p}$ have 4 Løsninger, som er $x \equiv \pm a, \pm(a+1) \pmod{p}$, hvor a er et helt Tal.

Eksempler: $p = 17$, $x^4 \equiv 4$, af Tabellen S.47 faas $x \equiv \pm 6, \pm 7$.
$p = 13$, $x^4 \equiv 3$, Løsninger $x \equiv \pm 2, \pm 3$.
$p = 5$, $x^4 \equiv 1$, Løsninger $x \equiv \pm 1, \pm 2$.

Bevis: $x^4 - h \equiv x^4 + \frac{1}{4} = (x^2 + \frac{1}{2})^2 - x^2$

$= (x^2 + x + \frac{1}{2}) \cdot (x^2 - x + \frac{1}{2})$.

Dette kongruent med 0 giver for hhv. første og anden Faktor

$$(x + \tfrac{1}{2})^2 \equiv -\tfrac{1}{4} \quad \text{og} \quad (x - \tfrac{1}{2})^2 \equiv -\tfrac{1}{4}.$$

Kongruensen $y^2 \equiv -\frac{1}{4}$ eller $(2y)^2 \equiv -1$ har en Løsning b fordi $\left(\frac{-1}{p}\right) = 1$, og som Løsninger til de opskrevne Kongruenser finder vi derfor ialt $x \equiv \pm b \pm \frac{1}{2}$, hvilket ses at være netop det ovenfor paastaaede.

6) Lad k være et naturligt Tal. Den største fælles Divisor $N_k = (2^{k+1}-2, 3^{k+1}-3, 4^{k+1}-4, \ldots\ldots)$ er da bestemt ved Formlen

$$N_k = \prod_{p-1 \mid k} p$$

(hvor som sædvanlig p betegner Primtal).

Eksempel: $k = 6$; p kan antage Værdierne 2,3 og 7, og vi har

$$N_6 = (2^7-2, 3^7-3, \ldots) = (126, 2184, \ldots) = 2 \cdot 3 \cdot 7 = 42.$$

Vi kunde ogsaa defimere N_k som største fælles Divisor for alle Tallene $z^{k+1}-z$, $z \in \mathbb{Z}$. Thi $1^{k+1}-1 = 0^{k+1}-0 = 0$, og iøvrigt er for k lige $(-z)^{k+1}-(-z) = -(z^{k+1}-z)$; for k ulige giver Formlen at $N_k = 2$, men dette er ogsaa lig den største fælles Divisor for $2^{k+1}-2$ og $(-2)^{k+1}-(-2) = 2^{k+1}+2$.

Bevis: 1) For et Primtal p ses at $p \nmid p^{k+1}-p$, hvoraf følger at N_k i hvert Fald er kvadratfri. 2) Dersom $p-1 \mid k$ vil $p \mid a^{k+1}-a = a(a^k-1)$ ifølge Fermat, baade hvis $p \mid a$ og hvis $p \nmid a$; det opskrevne Produkt vil altsaa i hvert Fald gaa op i N_k. 3) Dersom $p-1 \nmid k$ betragter vi $g^{k+1}-g$, hvor g er en Primitivrod modulo p; da vil p ikke gaa op i g^k-1, og da p er primisk med g gaar det heller ikke op i g. Dermed er Formlen bevist.

Anvendelse: Ligningen $x^{k+1} + y^{k+1} = z^{k+1}$ har ifølge en berømt - til Dato ubevist - Paastand af Fermat ingen Løsninger med $x,y,z \in \mathbb{N}$, $k > 1$ (for $k = 1$ findes Løsninger, fx $3^2 + 4^2 = 5^2$). For evt. Løsninger er $y < z < x+y$ (det sidste fordi $(x+y)^{k+1} = x^{k+1} + \ldots + y^{k+1}$), og endvidere $0 = x^{k+1} + y^{k+1} - z^{k+1} \equiv x + y - z \pmod{N_k}$ og da dette sidste er positivt er det altsaa $\geq N_k$. Tilsammen faas at $x > N_k$, og analogt med y. For evt. Løsninger til $x^7 + y^7 = z^7$ er altsaa i hvert Fald x,y (og ogsaa z) > 42.

7) "Wolstenholme's Sætning": For et Primtal p større end 3 vil p^2 gaa op i Tælleren a i Brøken

$$\frac{a}{b} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} .$$

Eksempler: $p = 3$, $\frac{1}{1} + \frac{1}{2} = \frac{3}{2}$, $3^2 = 9$ gaar ikke op

$p = 5$, $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}$, 5^2 gaar op

$p = 7$, $\frac{1}{1} + \ldots\ldots + \frac{1}{6} = \frac{49}{20}$, 7^2 gaar op

$p = 11$, Summen lig $\frac{7381}{2520} = \frac{121 \cdot 61}{2520}$ (uforkortelig).

Bevis: Vi sætter $(x-1)(x-2)\ldots(x-p+1) = x^{p-1} - s_1 x^{p-2} + \ldots + s_{p-1}$, hvor $s_1, s_2, \ldots, s_{p-2}, s_{p-1}$ er de symmetriske Grundfunktioner af Tallene $1,2,\ldots,p-1$. Her er $s_{p-1} = (p-1)!$ medens alle de øvrige er delelige med p (se S.43). Den betragtede Brøk $\frac{a}{b}$ er

lig $\frac{s_{p-2}}{(p-1)!}$ og vi skal blot vise, at $p^2 | s_{p-2}$, thi selv om den er forkortelig (som fx for $p = 7$ ovenfor) kan det ikke fjerne nogen Faktor p, da $p \nmid (p-1)!$.

Indsættes $x = p$ faas

$$(p-1)! = p^{p-1} - s_1 p^{p-2} + \ldots + s_{p-3}p^2 - s_{p-2}p + (p-1)!$$

hvor $(p-1)!$ gaar ud, og da de øvrige Led paa Højresiden til og med $s_{p-3}p^2$ er delelige med p^3 (NB kun for $p > 3$) maa p^2 gaa op i s_{p-2}, hvormed det ønskede er vist.

Potenssummer og Bernoulli's Tal.

For $k,n \in \mathbb{N}$ sættes

$$1^k + 2^k + 3^k + \ldots + (n-1)^k = S_k(n).$$

(det kan opfattes som en Skønhedsfejl at Summationen paa venstre Side ophører ved n-1 i.St.f. ved n, men det har baade saglige og historiske Aarsager). Som bekendt er $S_1(n) = \frac{1}{2}n^2 - \frac{1}{2}n$.
Vi skal vise, at der for ethvert k eksisterer et Polynomium $S_k(x)$ for hvilket $S_k(0) = 0$ og $S_k(x+1) - S_k(x) = x^k$, $x \in \mathbb{R}$. Dette Polynomium vil aabenbart netop angive Værdierne $S_k(n)$. Vi bemærker, at der i hvert Fald højst kan findes ét Polynomium som har de rigtige Værdier for alle $n \in \mathbb{N}$.

Bevis: Det angivne $S_1(x)$ har den ønskede Egenskab, og vi fører saa Beviset ved Induktion efter k. Vi antager altsaa at der findes et Polynomium $S_{k-1}(x)$ for hvilket $S_{k-1}(x+1) - S_{k-1}(x) = x^{k-1}$, og vi sætter saa

$$T(x) = \int_0^x k \cdot S_{k-1}(v)dv.$$

Ved Differentiation faas

$$T'(x+1) - T'(x) = k \cdot x^{k-1},$$

som ved Integration giver $T(x+1) - T(x) = x^k - B_k$, hvor B_k er en Konstant. Vi sætter saa $S_k(x) = T(x) + B_k x$, og har dermed faaet et Polynomium for hvilket $S_k(x+1) - S_k(x) = x^k$ og $S_k(0) = 0$. Ethvert S_k faas altsaa af det foregaaende S_{k-1} ved Multiplikation med k og Integration og Addition af et lineært Led. □

De første er

$$S_1(x) = \frac{1}{2}x^2 - \frac{1}{2}x$$
$$S_2(x) = \frac{1}{3}x^3 - \frac{1}{2}x^2 + \frac{1}{6}x$$
$$S_3(x) = \frac{1}{4}x^4 - \frac{1}{2}x^3 + \frac{1}{4}x^2$$
$$S_4(x) = \frac{1}{5}x^5 - \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x\ .$$

Vi sætter $B_0 = 1$, $B_1 = -\frac{1}{2}$, og saa faar vi som almindelig Formel

$$S_k(x) = k! \sum \frac{B_j}{j!} \cdot \frac{x^{k+1-j}}{(k+1-j)!}$$

hvor der summeres for $j \in [0,k]$ (den første Faktor k! skyldes Multiplikationerne, og man ser, at $j = k$ netop giver det lineære Led $B_k x$). Iøvrigt bemærkes, at Faktoren $k!/j!(k+1-j)!$ ogsaa kan skrives som $\frac{1}{k+1}\cdot\binom{k+1}{j}$ eller som $\frac{1}{k+1-j}\cdot\binom{k}{j}$.

Tallene $B_0, B_1, B_2, \ldots$ er de saakaldte Bernoulli-Tal (indført af Jacob Bernoulli, 1654-1705). De kan bestemmes sukcessivt ved Integrationerne ovenfor, men faas simplere ved at bemærke, at $S_k(1) = 0$ thi sætter man $x = 1$ i Formlen ovenfor og benytter det første alternative Udtryk for Koefficienten ses at man for alle $k \in \mathbb{N}$ har $\sum_j \binom{k+1}{j} B_j = 0$ (NB Værdien $j = k+1$ er udeladt i Summationen), altsaa et Formelsystem som hosstaaende, til sukcessiv Bestemmelse af Bernoulli-Tallene.

$$\begin{aligned} B_0 + 2B_1 &= 0 \\ B_0 + 3B_1 + 3B_2 &= 0 \\ B_0 + 4B_1 + 6B_2 + 4B_3 &= 0 \\ &\cdots\cdots \end{aligned}$$

For Formelsystemet benytter man iøvrigt ofte den symbolske Skrivemaade $(B+1)^{(m)} - B^{(m)} = 0$, hvor Meningen er at man efter Binomialudvikling skal erstatte symbolsk Exponent med Index.

For j ulige og større end 1 er $B_j = 0$. Det ses saaledes: Idet

$$S_k(-n)+(-n)^k+(-n+1)^k+\ldots+(-1)^k = S_k(0)$$

haves for k lige $S_k(-n) + n^k + S_k(n) = 0$, og sættes $S_k(x)+\frac{1}{2}x^k$ lig $S_k^*(x)$ er altsaa $S_k^*(-n) + S_k^*(n) = 0$ for alle $n \in \mathbb{N}$, saa at $S_k^*(x)$ er en ulige Funktion, og derfor kun indeholder x-Potenser af ulige Grad, hvilket viser Paastanden.

De første fra 0 forskellige Bernoulli-Tal er

B_0	B_1	B_2	B_4	B_6	B_8	B_{10}	B_{12}	B_{14}	B_{16}
1/1	-1/2	1/6	-1/30	1/42	-1/30	5/66	-691/2730	7/6	-3617/510

Af Formlerne er det klart, at alle $B_k \in \mathbb{Q}$, men iøvrigt ses de at være meget uregelmæssigt dannede.

Ad anden Vej, nemlig ved Fourierrækkeudvikling af en Funktion  og dens sukcessive periodiske Integraler, kan man vise at for de lige positive k vil B_k være af alternerende Fortegn, og dens numeriske Værdi er $2 \cdot k!/(2\pi)^k$ gange $\sum_n \frac{1}{n^k}$; specielt ses at man for denne sidste Sum kan angive et kort sluttet Udtryk for de lige k (for de ulige kender man ikke noget saadant Udtryk), og endvidere ses at for disse k vil $|B_k|$ gaa mod uendelig for $k \to \infty$ p.G.a. Faktoren k!.

Vi skal imidlertid ved Kongruensbetragtning vise en ejendommelig Sætning om Værdien af B_k.

Clausen-v.Staudt's Sætning (Cl. ,v.St.1798-1867): Lad k være lige og positiv; idet p gennemløber de Primtal for hvilke $p-1 \mid k$, saa er $B_k + \sum \frac{1}{p}$ et helt Tal.

Eksempler: $k = 2: \quad \frac{1}{6} + \left(\frac{1}{2} + \frac{1}{3}\right) = 1.$

$k = 4: \quad -\frac{1}{30} + \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5}\right) = 1.$

$k = 12: \quad -\frac{691}{2730} + \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13}\right) = 1.$

$k = 14: \quad \frac{7}{6} + \left(\frac{1}{2} + \frac{1}{3}\right) = 2.$

Beviset skal føres ved Induktion efter k, og da vi lige (i Eksemplet) har vist Paastanden for k = 2 skal vi kun betragte $k \geq 4$.

Vi skal for et vilkaarligt Primtal p benytte Kongruens modulo p, og minder om at det fungerer indenfor Ringen $\mathbb{Q}^{(p)}$ bestaaende af de Brøker $\frac{a}{b}$, hvor $p \nmid b$. Vi konstaterer at pB_0, pB_1 og $pB_2 \in \mathbb{Q}^{(p)}$; den første fordi $pB_0 = p \in \mathbb{Z}$, den anden fordi $pB_1 = -\frac{p}{2}$ baade for $p = 2$ og for $p > 2$ ses at tilhøre $\mathbb{Q}^{(p)}$, og den tredie fordi $pB_2 = \frac{p}{6}$ baade for $p = 2$ og for $p = 3$ og for $p > 3$ ses at tilhøre $\mathbb{Q}^{(p)}$.

For fastholdt p vil vi nu ved Induktion efter k, (som skal være lige og ≥ 4), vise at $pB_k \equiv S_k(p)$ (modulo p), og da $S_k(p) \in \mathbb{Z}$ ligger der heri specielt at $pB_k \in \mathbb{Q}^{(p)}$.

Værdien $S_k(p)$ faas af Formlen S.61, hvori vi dog benytter det andet alternative Udtryk for Koefficienten. Vi har

$$S_k(p) = \sum_{j \in [0,k[} \frac{1}{k+1-j} \cdot \binom{k}{j} \cdot B_j \cdot p^{k+1-j} + p \cdot B_k ,$$

og da $B_{k-1} = 0$ vil j de facto kun løbe til k-2. Ethvert af Leddene under $\sum$-Tegnet er $\equiv 0$, hvilket fremgaar af følgende: ifølge Induktionsforudsætningen vil $pB_j \in \mathbb{Q}^{(p)}$, og $\binom{k}{j} \in \mathbb{Z}$; der resterer $p^{k-j}/1+(k-j)$ som er $\equiv 0$, fordi p kun kan gaa op i Nævneren med en Eksponent som er mindre end k-j, idet $p^{k-j} \geq 2^{k-j} = 1+(k-j)+\ldots$ som er større end $1+k-j$ (vi havde $k-j \geq 2$); ialt bliver Leddet $\equiv 0$.

Dermed har vi vist at $pB_k \equiv S_k(p)$.

Ifølge det tidligere (S.43, ogsaa S.52 midtpaa) er $S_k(p) \equiv 0$ for $p-1 \nmid k$ og $S_k(p) \equiv -1$ for $p-1 \mid k$. Sættes $B_k + \sum \frac{1}{p} = C_k$ (Summation over de p hvor $p-1 \mid k$), faas $pC_k \equiv 0$ (mod. p) for ethvert p, hvilket kun er muligt naar $C_k \in \mathbb{Z}$ (skrevet som uforkortelig Brøk kan C_k ikke have en Nævner som indeholder noget p). Af Resultatet ses at B_k maa have en Nævner som er $\prod_{p-1 \mid k} p$, d.v.s. netop N_k fra Eks.6), S.58. □

KAPITEL IV : Talteoretiske Funktioner.

Vi skal betragte Afbildninger $f: \mathbb{N} \to$ kommutativt Legeme (dette vil som oftest være $\mathbb{R}$). Det er afgørende at vi for de naturlige Tal har en entydig Primopløsning $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ eller skrevet kort $n = \prod p^{\alpha}$ (overalt staar p for Primtal). Og et Hovedobjekt for vores Undersøgelse skal være Samspillet mellem denne Halvgruppestruktur og saa den ordnede Talrække.

Vi siger at f er multiplikativ dersom $(m,n) = 1 \Rightarrow f(mn) = f(m)f(n)$ og f ikke er Nulfunktionen.

For en multiplikativ Funktion f er $f(1) = 1$, thi der findes et $f(n) \neq 0$, og saa har vi $f(n) = f(n \cdot 1) = f(n) \cdot f(1)$, (fordi $(n,1)=1$) hvoraf ved Division med f(n) faas det ønskede.

Idet $n = \prod p^{\alpha}$ ser man umiddelbart at for en multiplikativ Funktion er $f(n) = \prod f(p^{\alpha})$, hvor Produktet tages over Primtalpotenserne p^{α} med $p^{\alpha} \| n$. Omvendt ser man, at man kan vælge Værdierne $f(p^{\alpha})$ vilkaarligt, og saa vil det angivne Udtryk for f(n) give en multiplikativ Funktion.

Et Specialtilfælde af de multiplikative Funktioner er de Funktioner for hvilke $f(mn) = f(m)f(n)$ for alle Talpar (m,n); vi vil kalde dem stærkt multiplikative (i Litteraturen sommetider betegnet "fuldstændigt multiplikative"). For vort Formaal er de mindre væsentlige, og man ser ogsaa, at det er ikke andet end de Funktioner som afbilder Strukturen $(\mathbb{N}, \cdot)$ homomorft. Som Eksempler paa stærkt multiplikative Funktioner kan man tage $f(n) = n^k$ (k = Konstant), og - lidt mindre trivielt - $f(n) = 2^h$, hvor $2^h \| n$. Man ser ogsaa, at en stærkt multiplikativ Funktion er bestemt ved sine Værdier paa Prim-

tallene $f(p)$, idet saa $f(n) = \prod f(p)^{\alpha}$, omvendt vil ethvert Valg af Værdierne $f(p)$ give en stærkt multiplikativ Funktion. Som Eksempel paa en Funktion der er multiplikativ, men ikke stærkt multiplikativ, kan vi tage den "kvadratfri Kerne", altsaa Funktionen $f(n) = p_1 \cdot \ldots \cdot p_r$, idet $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, (alle Exponenter α_j forudsat positive).

Betydningen af Betingelsen $(m,n) = 1$ ligger i at hvis vi sætter

$$E = \{\text{Divisorer e i mn}\}$$
$$C = \{\text{Divisorer c i m}\}$$
$$D = \{\text{Divisorer d i n}\}$$

saa har vi en bijektiv Forbindelse $E \leftrightarrow C \times D$ realiseret ved $e = c \cdot d$, idet Kravet $(m,n) = 1$ jo medfører at enhver Divisor e i mn paa netop én Maade kan skrives som Produkt af en Divisor c i m og en Divisor d i n; den anden Vej er det klart, at hvis c og d er et saadant Par Divisorer, saa vil deres Produkt være Divisor i mn.

Den første talteoretiske Funktion vi skal betragte er

$$\tau(n) = \text{Antallet af Divisorer i n} = \sum_{d|n} 1 .$$

Den er multiplikativ idet

$$\tau(mn) = \sum_{e|mn} 1 = \sum_{c|m} \sum_{d|n} 1 = \left(\sum_{c|m} 1\right)\left(\sum_{d|n} 1\right) = \tau(m) \cdot \tau(n)$$

og vi skal derfor blot bestemme dens Værdi for en Primtalpotens p^{α}. Idet $d | p^{\alpha}$ hvis og kun hvis $d = p^{\delta}$ hvor $0 \leq \delta \leq \alpha$, ses at der er $\alpha + 1$ mulige Værdier δ, saa at $\tau(p^{\alpha}) = \alpha + 1$.

Vi har altsaa

$$\tau(n) = \prod_j (\alpha_j + 1).$$

De første Funktionsværdier er anført paa Tabelbladet S. 78

Vi har $\tau(1) = 1$, og for $n > 1$ er $2 \leq \tau(n) < 2\sqrt{n}$, hvor Lighedstegnet gælder hvis og kun hvis n er et Primtal, medens Ulighedstegnet

t.h. følger af at Divisorerne i n kan samles i Par af komplementære, $n = a \cdot b$, af hvilke den ene vil være mindre end eller lig $\sqrt{n}$ (og hvis den er lig $\sqrt{n}$ er den anden ogsaa $\sqrt{n}$, saa Parret tæller kun for en Divisor). Af den sidste parentetiske Bemærkning ses ogsaa, at $\tau(n)$ er ulige hvis og kun hvis n er et Kvadrattal.

For fast $\varepsilon > 0$ vil $\tau(n)/n^{\varepsilon} \to 0$ for n gaaende mod uendelig, saa $\tau(n)$ vokser svagere end enhver Potens af n.

Bevis: For fast p vil $\tau(p^{\alpha})/(p^{\alpha})^{\varepsilon} = (\alpha+1)/(p^{\varepsilon})^{\alpha} \to 0$ for $\alpha \to \infty$, hvoraf følger at der findes en Konstant $K_{\varepsilon,p}$ saa $\tau(p^{\alpha})/(p^{\alpha})^{\varepsilon} < K_{\varepsilon,p}$ uafhængigt af α. Endvidere ses at $\tau(p^{\alpha})/(p^{\alpha})^{\varepsilon} = (\alpha+1)/(p^{\varepsilon})^{\alpha} \leqq 2^{\alpha}/(p^{\varepsilon})^{\alpha} = (2/p^{\varepsilon})^{\alpha} < 1$ for $p > L_{\varepsilon}$, igen uafhængigt af α.

Altsaa er

$$\frac{\tau(n)}{n^{\varepsilon}} = \prod_{p} \frac{\tau(p^{\alpha})}{(p^{\alpha})^{\varepsilon}} < \prod_{p \leqq L_{\varepsilon}} K_{\varepsilon,p} = M_{\varepsilon},$$

hvor M_{ε} er en Konstant. Altsaa $\tau(n) < M_{\varepsilon} \cdot n^{\varepsilon}$, og hvis vi i denne Ulighed erstatter ε med $\frac{\varepsilon}{2}$ har vi den ønskede Sætning.

Som det fremgaar af Tabellen er $\tau(n)$ en meget uregelmæssig Funktion, men vi kan supplere det ovenstaaende med Sætningen

$\tau(n)$ vokser "gennemsnitligt" som $\log n$ i den Forstand at

$$\sum_{n \leqq K} \tau(n) \sim \sum_{n \leqq K} \log n \qquad \text{for } K \to \infty,$$

hvor $\sim$ betyder at Forholdet mellem Størrelserne paa de to Sider af Tegnet konvergerer mod 1 ved Grænseovergangen. (Størrelserne selv gaar mod uendelig).

Bevis:

$$\sum_{n \leqq K} \tau(n) = \sum_{n \leqq K} \sum_{d \mid n} 1 = \sum_{d} \sum_{d \mid n,\, n \leqq K} 1 = \sum_{\substack{d \\ (d \leqq K)}} \left[\frac{K}{d}\right],$$

og da $\left|\frac{K}{d} - \left[\frac{K}{d}\right]\right| < 1$ faas $\left|\sum_{n \leqq K} \tau(n) - \sum_{d \leqq K} \frac{K}{d}\right| \leqq \sum_{d \leqq K} 1 = K.$

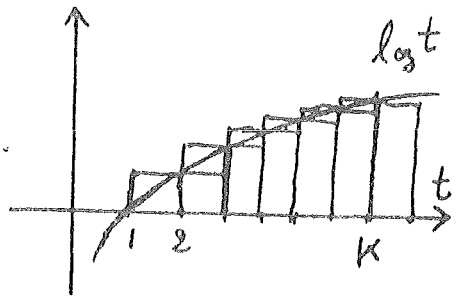
Idet nu $\sum_{d \leqq K} \frac{1}{d}$ = log K + begrænset Restled er

$\sum_{d \leqq K} \frac{K}{d} \sim K \cdot \log K$, og derfor $\sum_{n \leqq K} \tau(n) \sim K \cdot \log K$.

En Integralsammenligning viser - med en simpel Fejlvurdering - at

$$\sum_{n \leqq K} \log n \sim \int_1^K \log t \, dt = K \log K - K + 1$$

som ogsaa er $\sim K \cdot \log K$, hvormed det ønskede er vist. □



Den næste talteoretiske Funktion vi skal betragte er

$$\sigma(n) = \text{Summen af Divisorerne i } n = \sum_{d \mid n} d \, .$$

Den er multiplikativ idet (stadig forudsat (m,n) = 1)

$$\sigma(mn) = \sum_{e \mid mn} e = \sum_{c \mid m} \sum_{d \mid n} cd = \left(\sum_{c \mid m} c\right) \cdot \left(\sum_{d \mid n} d\right) = \sigma(m) \cdot \sigma(n)$$

og vi skal derfor blot bestemme dens Værdi for en Primtalpotens p^α.

Vi finder $1 + p + p^2 + \ldots + p^{\alpha-1} + p^\alpha = (p^{\alpha+1} - 1)/(p - 1)$.

Altsaa

$$\sigma(n) = \prod_j \frac{p_j^{\alpha_j+1} - 1}{p_j - 1} \, .$$

De første Funktionsværdier er anført paa Tabelbladet S. 78.

Vi har $\sigma(1) = 1$, og for $n > 1$ er $n+1 \leqq \sigma(n) < \tau(n) \cdot n$, hvor Lighedstegnet gælder hvis og kun hvis n er et Primtal, medens Uligheds-tegnet t.h. er evident. Af Resultatet for τ faar vi altsaa at for ethvert positivt ε gælder $n \leqq \sigma(n) < n^{1+\varepsilon}$, hvor den højre Ulighed er opfyldt saasnart n er tilstrækkelig stor.

Her gælder: $\sigma(n)$ vokser "gennemsnitligt" som $\frac{\pi^2}{6} \cdot n$

Bevis: Vi har

$$\sum_{n \leqq K} \frac{\pi^2}{6} \cdot n = \frac{\pi^2}{6} \cdot \frac{K^2+K}{2} \sim \frac{\pi^2}{12} \cdot K^2 \, ,$$

og vi skal altsaa vise at dette $\sim \sum_{n \leqq K} \sigma(n)$.

Vi har $\sum_{n \leqq K} \sigma(n) = \sum_{n \leqq K} \sum_{d \mid N} d$; i St.f. n indfører vi nu $h = \frac{n}{d}$ som Summationsvariabel og faar $\sum_{h} \sum_{d} d$, hvor den indre Sum tages over $d \leqq \frac{K}{h}$, og altaa er lig $\frac{1}{2} \cdot \left(\left[\frac{K}{h} \right]^2 + \left[\frac{K}{h} \right] \right)$, som vi de facto kun skal betragte for $h \leqq K$.

Da vi har $x - 1 < [x] \leqq x$ faas for $1 \leqq x$ at

$$x^2 - x < [x]^2 + [x] \leqq x^2 + x,$$

saa vi har $\left| [x]^2 + [x] - x^2 \right| \leqq x$, og vi har dermed

$\sum_{n \leqq K} \sigma(n)$ lig $\sum_{h \leqq K} \frac{1}{2} \cdot \left(\frac{K}{h} \right)^2$ med en Fejl som numerisk er mindre end $\sum_{h \leqq K} \frac{1}{2} \cdot \frac{K}{h}$. Men dermed har vi at den betragtede Sum er lig

$$\frac{K^2}{2} \cdot \sum_{h \leqq K} \frac{1}{h^2} = \frac{K^2}{2} \cdot \left(\frac{\pi^2}{6} - \varepsilon_K \right)$$

med en Fejl der højst er som $K \cdot \log K$, og man ser at det ønskede er vist. □

Et <u>fuldkomment Tal</u> var hos de gamle Grækere Betegnelsen for et Tal som var lig Summen af sine ægte Divisorer (d.v.s. Divisorerne, Tallet selv exclusive). Eksempel: Tallet 6 har de ægte Divisorer 1,2 og 3, hvis Sum netop er 6.

Med vore Betegnelser kan Betingelsen udtrykkes: <u>N er fuldkomment hvis og kun hvis $\sigma(N) = 2N$</u>.

Euklid viste: <u>Hvis $2^m - 1$ er et Primtal, saa er $2^{m-1} \cdot (2^m - 1)$ et fuldkomment Tal</u>.

Det er Højdepunktet og Slutstykket (IX,36) i hans tre talteoretiske Bøger (VII,VIII og IX).

Bevis: Vi har $N = 2^{m-1} \cdot p$, hvor $p = 2^m - 1$ er et Primtal. Saa er $\sigma(N) = \sigma(2^{m-1}) \cdot \sigma(p)$ (de to Faktorer i N er jo indbyrdes primiske); $\sigma(2^{m-1}) = 2^m - 1$, og $\sigma(p) = p + 1 = 2^m$, og $\sigma(N)$ bliver altsaa $(2^m - 1) \cdot 2^m = 2N$. □

Eksempler paa fuldkomne Tal:

$n = 2,\ 2^2-1 = 3$ = Primtal, $N = 2\cdot 3 = 6$

$n = 3,\ 2^3-1 = 7$ = do. , $N = 4\cdot 7 = 56$

$n = 5,\ 2^5-1 = 31$ = do. , $N = 16\cdot 31 = 496$

$n = 7,\ 2^7-1 = 127$ = do. , $N = 64\cdot 127 = 8128$

$n = 9,\ 2^9-1 = 511 = 7\cdot 73$, ikke Primtal.

Man ser, at lige n-Værdier aldrig vil kunne bruges, da $2^{2h}-1$ altid vil være delelig med 3. (indtil $n = 2$)

Langt senere viste Euler: Ethvert lige fuldkomment Tal maa være af den af Euklid angivne Form.

Bevis: Sæt $N = 2^m \cdot v$, hvor $m > 0$ og v er ulige.

Indsættes i $\sigma(N) = 2N$ faas $\sigma(2^m)\cdot\sigma(v) = (2^{m+1}-1)\cdot\sigma(v) = 2^{m+1}\cdot v$, eller

$$\sigma(v) = \frac{2^{m+1}}{2^{m+1}-1}\cdot v = v + \frac{v}{2^{m+1}-1}.$$

Da $\sigma(v)$ og v er hele maa den sidste Brøk ogsaa være et helt Tal, og da Nævneren er større end 1 (fordi $m > 0$) maa det være en ægte Divisor i v. Naar v + denne Divisor i v tilsammen giver $\sigma(v)$ maa Divisoren være lig 1,

saa at $v = 2^{m+1}-1$, og der kan ikke være andre Divisorer, saa v maa være et Primtal. □

Man ved til Dato ikke om der findes noget ulige fuldkomment Tal, men hvis der findes nogen maa de i hvert Fald være meget store ($> 10^{150}$) og komplicerede af Opbygning (d.v.s. med adskillige forskellige Primdivisorer).

Af fuldkomne Tal kendes altsaa ialt ligesaa mange som man kender Primtal af Formen $p = 2^m - 1$, og det er i Øjeblikket 24 Stk. Blandt disse findes det største kendte Primtal, som i Decimalsystemet skrives med ca. 6000 Cifre. Vi skal senere komme tilbage til Spørgsmaalet om hvorledes det er muligt at godtgøre at et saadant Tal er Primtal.

Foldningsringen.

Vi betragter stadig Funktioner (ikke nødvendigvis multiplikative) som afbilder $\mathbb{N}$ over i et kommutativt Legeme.

Vi definerer Foldningen $h = f * g$ ved

$$h(n) = f*g(n) = \sum_{d|n} f(d)\cdot g(\tfrac{n}{d}).$$

Kompositionen $*$ er aabenbart kommutativ, idet $h(n)$ ses at være lig $\sum f(d)g(c)$, hvor der summeres over alle Par (d,c), hvor $d\cdot c = n$.

Den er associativ, thi man ser let at uanset hvorledes man sætter Parenteser i $f*g*k$, saa bliver Værdien af $f*g*k(n)$ lig $\sum f(d)g(c)k(e)$, hvor der summeres over alle Tripler (d,c,e) hvor $d\cdot c\cdot e = n$.

Den er distributiv med Hensyn til Addition, idet man helt evident faar $f*(g_1+g_2) = f*g_1 + f*g_2$ (ligesom ved sædvanlig Multiplikation er + og − "Hovedtegn", saa Parenteser er overflødige paa Højresiden); her er g_1+g_2 naturligvis Funktionen defineret ved $g(n) = g_1(n)+g_2(n)$.

Altsaa er $(\{f\},+,*)$ en kommutativ Ring.

Dens Nulelement er Funktionen defineret ved $o(n) = 0$ for alle n.

Den har et Etelement e defineret ved

$$e(n) = \begin{cases} 1 & \text{for } n = 1 \\ 0 & \text{ellers} \end{cases}$$

idet denne Funktion umiddelbart ses at være neutral Faktor ved $*$.

Endvidere gælder Nulreglen: Antag $f \neq o$, saa findes et mindste n for hvilket $f(n) \neq 0$, og antag $g \neq o$, saa findes et mindste m for hvilket $g(m) \neq 0$; saa faar man umiddelbart at $f*g(nm) = f(n)\cdot g(m) \neq 0$, altsaa at $f*g \neq o$. □

Altsaa er $(f,+,*)$ et Integritetsomraade.

Nødvendigt og tilstrækkeligt for at f er invertibel er $f(1) \neq 0$.

Bevis: Betingelsen er nødvendig, thi hvis $f(1) = 0$ faar man $f*g(1) = f(1)\cdot g(1) = 0$ for ethvert g.

Betingelsen er tilstrækkelig; thi antag $f(1) \neq 0$, vi kan da bestemme g saaledes at $f*g = e$: som $g(1)$ tager vi $1/f(1)$, og de følgende Værdier $g(n)$ bestemmer vi induktivt ved

$$f(1)\cdot g(n) = - \sum_{d|n,\, d>1} f(d)g(\tfrac{n}{d}) \ .$$

□

Idet vi har $f*g(1) = f(1)\cdot g(1)$ ses at Afbildningen $f \mapsto f(1)$ vil være en homomorf Afbildning af $(\{f\},+,*)$ over paa Funktionsværdiernes Legeme; Kernen ved denne Afbildning er netop Mængden af de ikke-invertible f, og denne Mængde er altsaa et Maximalideal i Ringen. Følgelig er Foldningsringen en lokal Ring. Men den er af en noget anden Type end den tidligere betragtede lokale Ring $\mathbb{Q}^{(p)}$, thi medens i denne Maximalidealet var et Hovedideal - nemlig (p) - saa kan man med lidt Regning overbevise sig om at i $(\{f\},+,*)$ er Maximalidealet ikke noget Hovedideal.

Hvis vi kun tænker paa $*$-Kompositionen, saa gælder som bekendt at $(\{\text{invertible } f\},*)$ er en Gruppe (og den størst mulige). Der gælder nu den vigtige Sætning:

I Foldningsringen er $(\{\text{multiplikative } f\},*)$ en Gruppe.

Bevis: Vi bemærker først, at f multiplikativ medfører $f(1) = 1$, altsaa at f er invertibel. Endvidere konstateres at Etelementet e, som jo var defineret ved $e(n) = \begin{cases} 1 & \text{for } n = 1 \\ 0 & \text{ellers} \end{cases}$, aabenbart er multiplikativt.

Vi skal vise, at hvis f og g er multiplikative, saa er $h = f*g$ ogsaa multiplikativ. Vi antager $(m,n) = 1$, og skal udregne $h(mn)$; hvis k gaar op i mn, saa er $k = cd$ (bijektivt), hvor $c|m$ og $d|n$, altsaa $(c,d) = 1$. Saa forløber Regningen

$$h(mn) = \sum_{k \mid mn} f(k)g(\tfrac{mn}{k}) = \sum_{c \mid m, d \mid n} f(cd)g(\tfrac{m}{c}\cdot\tfrac{n}{d}) =$$

$$\sum_{c \mid m, d \mid n} f(c)f(d)g(\tfrac{m}{c})g(\tfrac{n}{d}) = (\sum_{c \mid m} f(c)g(\tfrac{m}{c}))\cdot(\sum_{d \mid n} f(d)g(\tfrac{n}{d})) = h(m)\cdot h(n) .$$

Endelig skal vi godtgøre, at hvis g er multiplikativ og $h = f * g$ er multiplikativ, saa maa f ogsaa have været multiplikativ (for deraf følger jo - ved at sætte $h = e$ - at g^{-1} er multiplikativ); men hvis f ikke havde været multiplikativ vilde der findes et mindste mn for hvilket $f(mn) \neq f(m)f(n)$, og naar vi saa udregner $h(mn)$ som ovenfor vil der optræde netop én Ændring, nemlig i Leddet med $k = mn$, altsaa $c = m$ og $d = n$ saaledes at $f(cd) \neq f(c)f(d)$, og da dette multipliceres med $g(1) = 1$ vil det sidste Lighedstegn i første Linie briste (medens alle øvrige Lighedstegn i Regningen bevares), altsaa: (f ikke mult. $\wedge$ g mult.) $\Rightarrow$ (h ikke mult.). □

Det simpleste Eksempel (forskelligt fra e) paa en multiplikativ Funktion er ξ defineret ved $\xi(n) = 1$ for alle n.
Vi finder $\xi * \xi(n) = \sum_{d \mid n} 1\cdot 1 = \tau(n)$, og der er altsaa ikke noget overraskende i at τ er multiplikativ.
En anden multiplikativ Funktion er ν defineret ved $\nu(n) = n$ for alle n; vi finder $\nu * \xi(n) = \sum_{d \mid n} d\cdot 1 = \sigma(n)$, og der er altsaa ikke noget overraskende i at σ er multiplikativ.
Baade ξ og ν er stærkt multiplikative, medens hverken τ eller σ er det, og heraf fremgaar det at $\{$stærkt multiplikative $f\}$ ikke er nogen Undergruppe i $(\{f\}, *)$, hvorfor denne Mængde ikke har saa megen Interesse i denne Forbindelse.
Iøvrigt kan man bemærke, at hvis h er stærkt multiplikativ, saa er $(h\cdot f) * (h\cdot g) = h\cdot(f * g)$, altsaa en "betinget distributiv Regel"; det følger let, idet $(h\cdot f) * (h\cdot g)(n) = \sum h(d)f(d)h(\tfrac{n}{d})g(\tfrac{n}{d}) =$
$h(n)\cdot \sum f(d)g(\tfrac{n}{d}) = h(n)\cdot((f * g)(n))$.

(Vi har altsaa nu to Ringe af Funktioner f - eller mere generelt udtrykt: Algebraer over Billedelementernes Legeme - og der er et vist Samspil mellem dem, som vi dog ikke skal udforske videre. Det er [1] Funktionsringen $(\{f\},+,\cdot)$ med sædvanlig Addition og Multiplikation af Funktioner og [2] Foldningsringen. Man ser let, at i [1] er baade $\{$multiplikative f$\}$ og $\{$stærkt multiplikstive f$\}$ Undergrupper ved Multiplikationen $\cdot$. Og vi har altsaa vist, at i [2] er $\{$multiplikative f$\}$ en Undergruppe medens $\{$stærkt multiplikative f$\}$ ikke er det, begge i Relation til Foldningen $*$.)

Flere Eksempler paa multiplikative Funktioner kan nu let opbygges, f.Eks. $f = \xi * \xi * \xi = \xi * \tau$. Vi har $f(n) = \sum_{d|n} \tau(d)$. Den er multiplikativ, og for en Primtalpotens p^α finder vi

$$f(p^\alpha) = 1 + 2 + \ldots + (\alpha+1) = \frac{(\alpha+1)(\alpha+2)}{2} = S_1(\alpha+2).$$

Endvidere $\gamma * \gamma$ hvis Værdier bliver $\sum_{d|n} d \cdot \frac{n}{d} = n \cdot \tau(n)$ (smlgn. Bemærkningen foran om en Foldnings Multiplikation med en stærkt multiplikativ Faktor).

Eksempel: Liouville (1809-1882) har opdaget Formlen

$$\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d)\right)^2.$$

Taleksempel: n = 12,

d =	1	2	3	4	6	12	
$\tau(d)$ =	1	2	2	3	4	6	Sum = 18
$\tau(d)^3$ =	1	8	8	27	64	216	Sum = 324 = 18^2

Bevis: Formlen kan aabenbart udtrykkes $\tau^3 * \xi = (\tau * \xi)^2$, idet Eksponenterne refererer til sædvanlig Multiplikation. Da de indgaaende Funktioner og deres Potenser og Foldninger alle er multiplikative vil det være tilstrækkeligt at bevise Formlen for en Primtalpotens, $n = p^\alpha$. For denne bliver Højresiden ifølge det ovenstaaende lig $S_1(\alpha+2)^2$, medens Venstresiden bliver $1^3+2^3+\ldots+(\alpha+1)^3 = S_3(\alpha+2)$. Men af Udtrykkene for Potenssummerne (se S.61) ses at $S_3(x) = S_1(x)^2$. □

Vigtig for Anvendelserne: Möbius' Funktion μ (M.1790-1868), defineret ved $\mu * \xi = e$, altsaa at μ er den (Foldnings-)inverse til ξ.

Ifølge Definitionen er $\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{for } n = 1 \\ 0 & \text{ellers} \end{cases}$, og desuden ved vi at μ er multiplikativ.

For en Primtalpotens p^{α} finder vi

$$\mu(p^{\alpha}) = \sum_{d|p^{\alpha}} \mu(d) - \sum_{d|p^{\alpha-1}} \mu(d) = e(p^{\alpha}) - e(p^{\alpha-1}) = \begin{cases} -1 \text{ for } \alpha = 1 \\ 0 \text{ ellers} \end{cases}.$$

Möbiusfunktionens Værdier er derfor

$$\mu(n) = \begin{cases} (-1)^r & \text{for n kvadratfri, Produkt af r forsk.Primt.} \\ 0 & \text{naar n ikke er kvadratfri} \end{cases}$$

De første Funktionsværdier er anført paa Tabelbladet S.78.

Idet

$$f = g * \xi \iff g = f * \xi$$

faas Möbius' Omvendingsformel:

For talteoretiske Funktioner f og g er følgende to Formelsæt ensbetydende:

$$\forall_n: \quad f(n) = \sum_{d|n} g(d) \quad \text{og} \quad \forall_n: \quad g(n) = \sum_{d|n} \mu(d) \cdot f\left(\frac{n}{d}\right).$$

Eksempler: $n = 12$, $d|12$ for

d	1	2	3	4	6	12
$\mu(d)$	1	-1	-1	0	1	0
$\frac{12}{d}$	12	6	4	3	2	1

$g = \xi$, $f = \tau$, $\sum \mu(d)\tau\left(\frac{12}{d}\right) = \tau(12) - \tau(6) - \tau(4) + \tau(2) = 6 - 4 - 3 + 2$

$= 1 = \xi(12)$.

$g = \nu$, $f = \sigma$, $\sum \mu(d)\sigma\left(\frac{12}{d}\right) = \sigma(12) - \sigma(6) - \sigma(4) + \sigma(2) = 28 - 12 - 7 + 3$

$= 12 = \nu(12)$

Vi kan nu let bestemme Eulers φ-Funktion

$$\varphi(n) = \text{Antallet primiske Restklasser mod.}n = \sum_{\substack{(h,n)=1 \\ h \in]0,n]}} 1 .$$

For ethvert h vil $d = (h,n)$ være en Divisor i n, og $d = (h,n)$ ses at være ensbetydende med at $(\frac{h}{d}, \frac{n}{d}) = 1$; Antallet af $h \in]0,n]$ for hvilke dette indtræffer er derfor $\varphi(\frac{n}{d})$. Naar vi lader d gennemløbe Divisorerne i n faar vi alle h med. Altsaa

$$n = \sum_{d|n} \varphi(\tfrac{n}{d}) = \sum_{d_1|n} \varphi(d_1).$$

Men her staar jo netop at Funktionerne ν og φ er et Möbiuspar af Funktioner, $\nu = \varphi * \xi$, eller $\varphi = \nu * \mu$, og Omvendingsformlen giver $\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$. Da φ ogsaa er multiplikativ behøver vi kun at bestemme $\varphi(p^\alpha)$. For $d | p^\alpha$ vil $\mu(d)$ kun være ulig 0 for $d = 1$ og $d = p$, og vi faar $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Det almindelige Udtryk for φ bliver altsaa

$$\varphi(n) = \prod_j (p_j^{\alpha_j} - p_j^{\alpha_j - 1}) = n \cdot \prod_{p_j|n} (1 - \frac{1}{p_j}) .$$

De første Funktionsværdier er anført paa Tabelbladet S. 78.

Vi har $\varphi(1) = 1$, og for $n > 1$ er $\varphi(n) \leqq n-1$, hvor Lighedstegnet gælder naar n er et Primtal. Til videre Vurdering viser vi at

$$\frac{1}{2} < \frac{\varphi(n) \cdot \delta(n)}{n^2} \leqq 1 .$$

Brøken er en multiplikativ Funktion, og for $n = p^\alpha$ er den

$$\frac{(p^\alpha - p^{\alpha-1}) \cdot \frac{p^{\alpha+1}-1}{p-1}}{p^{2\alpha}} = 1 - p^{-\alpha-1}.$$

For vilkaarligt n er Brøken altsaa $\prod_{p|n}(1-p^{-\alpha-1})$, hvoraf den højre Ulighed ovenfor er indlysende, medens den venstre faas ved at vurdere dette Produkt nedad ved $\prod_{p|n}(1-p^{-2}) > \prod_{m \in [2,\infty[} (1-m^{-2})$ som

Tabelblad

n-Værdierne er pr.definition angivet ved $\nu(n)$.

ν	τ	σ	μ	φ	Λ
1	1	1	1	1	0
2	2	3	-1	1	log 2
3	2	4	-1	2	log 3
4	3	7	0	2	log 2
5	2	6	-1	4	log 5
6	4	12	1	2	0
7	2	8	-1	6	log 7
8	4	15	0	4	log 2
9	3	13	0	6	log 3
10	4	18	1	4	0
11	2	12	-1	10	log 11
12	6	28	0	4	0
13	2	14	-1	12	log 13
14	4	24	1	6	0
15	4	24	1	8	0
16	5	31	0	8	log 2
17	2	18	-1	16	log 17
18	6	39	0	6	0
19	2	20	-1	18	log 19
20	6	42	0	8	0
21	4	32	1	12	0
22	4	36	1	10	0
23	2	24	-1	22	log 23
24	8	60	0	8	0
Begræns.nedad	n	2	n	-1	$n^{1-\varepsilon}$	0
Begræns.opad	n	n^{ε}	$n^{1+\varepsilon}$	1	n	log n
Gennemsnitlig	n	log n	$\frac{\pi^2}{6}\cdot n$	0 *)	$\frac{6}{\pi^2}\cdot n$	1 *)

Begrænsningerne nedad og opad er kun gyldige for tilstrækkelig store n-Værdier.

*) De anførte Gennemsnitsværdier er ikke bevist for μ og Λ, og deres Gyldighed er "ækvivalent" med Primtalsætningens Gyldighed.

naar det opskrives som $\prod \frac{(m-1)(m+1)}{m \cdot m}$ teleskoperer til $\frac{1}{2}$:

$$\frac{1\cdot 3}{2\cdot 2}\,\frac{2\cdot 4}{3\cdot 3}\,\frac{3\cdot 5}{4\cdot 4}\cdots\cdots = \frac{1}{2}\,.$$

For n tilstrækkelig stor gjaldt $n < \delta(n) < n^{1+\varepsilon}$, og Vurderingen af $\varphi(n)\cdot\delta(n)$ viser saa at $n^{1-\varepsilon} < \varphi(n) < n$ for n tilstrækkelig stor.

Der gælder: $\varphi(n)$ vokser gennemsnitlig som $\frac{6}{\pi^2}\cdot n$.

Bevis: Vi har $$\sum_{n\leqq K} \frac{6}{\pi^2}\cdot n = \frac{6}{\pi^2}\cdot\frac{K^2+K}{2} \sim \frac{3}{\pi^2}\cdot K^2\,,$$

og vi skal altsaa blot vise at dette $\sim \sum_{n\leqq K}\varphi(n)$. Det sker paa lignende Maade som Vurderingen af $\sum \delta(n)$ (S.68 øverst):

Vi har

$$\sum_{n\leqq K}\varphi(n) = \sum \mu(d) \sum_{d\mid n,\, n\leqq K} \frac{n}{d} = \sum_{d\leqq K}\mu(d)\cdot\frac{1}{2}\left(\left[\frac{K}{d}\right]^2 + \left[\frac{K}{d}\right]\right)$$

og dette

$$\sum_{d\leqq K}\mu(d)\cdot\frac{K^2}{2d^2} \sim \frac{K^2}{2}\cdot\sum_{d}\frac{\mu(d)}{d^2}\,.$$

Men $\sum_d \frac{\mu(d)}{d^2}$ og $\frac{\pi^2}{6} = \sum_c \frac{1}{c^2}$ er reciprokke, thi opskriver man deres Produkt og erstatter cd med n faar man

$$\sum_d \frac{\mu(d)}{d^2}\cdot\sum_c\frac{1}{c^2} = \sum_n \frac{1}{n^2}\sum_{d\mid n}\mu(d) = 1\,,$$

idet der jo den sidste Sum kun kommer ét eneste Bidrag, for $n = 1$: □

(Det sidste Bevis beror egentlig paa at de talteoretiske Funktioner n^{-2} og $\mu(n)\cdot n^{-2}$ er foldningsinverse; Exponenten -2 kan her erstattes med et vilkaarligt lige negativt Tal, og man kan paa denne Maade indse, at for et lige positivt k er $\sum_n \mu(n)\cdot n^{-k}$ lig $2\cdot k!\cdot(2\pi)^{-k}\cdot|B_k|^{-1}$, hvor B_k er Bernoullitallet).

Som en lille Illustration til φ-Funktionen kan vi tage følgende: Fra Algebraen vides, at en regulær n-Kant er konstruerbar med

Passer og Lineal naar og kun naar n er et Tal af Formen $n = 2^h \cdot p_1 \cdot \ldots \cdot p_r$, hvor $p_1, \ldots, p_r$ er forskellige Primtal af Formen 2^k+1. Vi vil vise, at dette ogsaa kan udtrykkes: En regulær n-Kant er konstruerbar med Passer og Lineal naar og kun naar $\varphi(n)$ er en Potens af 2. (Rent sagligt er dette ogsaa den "korrekte" Form af Sætningen, hvilket hænger sammen med at Konstruktion med Passer og Lineal tillader Legemsudvidelser af Grad 2, saaledes at de "konstruerbare Tal" vil tilhøre et Legeme hvis Grad over $\mathbb{Q}$ er en Potens af 2).

Bevis: Hvis n har den angivne Form, saa er $\varphi(n)$ lig $\varphi(2^h) \cdot \varphi(p_1) \ldots$ og her er enhver af Faktorerne en Potens af 2, saa Produktet er det ogsaa. Omvendt: Hvis $n = \prod p^{\alpha}$, saa er $\varphi(n) = \prod \varphi(p^{\alpha})$; naar $\varphi(n)$ er en Potens af 2, saa er ethvert $\varphi(p^{\alpha})$ en Potens af 2, og da $\varphi(p^{\alpha}) = (p-1) \cdot p^{\alpha-1}$ ses at det gælder naar enten $p = 2$ og α vilkaarlig eller naar $p = 2^k+1$ og $\alpha = 1$. □

De hidtil betragtede Funktioner har alle været multiplikative, og kan iøvrigt alle indgaa som Eksempler i Möbiuspar $f = g * \xi \Leftrightarrow g = f * \mu$; lad os iøvrigt understrege, at ifølge tidligere Resultater gælder: Hvis den ene Funktion i et Möbiuspar er multiplikativ, saa er den anden det ogsaa. Vi skal nu betragte et Par af ikke-multiplikative Funktioner, nemlig $f = \log$ og det tilsvarende g som betegnes Λ.

Möbiuspar:

$f = g * \xi$	e	ξ	τ	σ	ν	$\log$	$-\Lambda$
$g = f * \mu$	μ	e	ξ	ν	φ	Λ	$M \cdot \log$
	multiplikative					ikke-mult.	

Λ betegnes ogsaa som v.Mangoldt-Funktionen.

Dens Værdier er

$$\Lambda(n) = \begin{cases} \log p & \text{for } n = p^{\alpha} \\ 0 & \text{ellers.} \end{cases}$$

Man ser umiddelbart, at $\log = \Lambda * \xi$ idet

$$\log n = \sum_{p^\alpha \| n} \alpha \log p = \sum_{p|n} \sum_{p^\alpha | n} \log p = \sum_{d|n} \Lambda(d) .$$

Prøver man at anvende Omvendingsformler, altsaa sætte $\Lambda = \mu * \log$ faas

$$\Lambda(n) = \sum_{d|n} \mu(d) \cdot \log \frac{n}{d} = \log n \cdot \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \cdot \log d ;$$

i sidste Udtryk er første Bidrag 0 (baade for $n = 1$ og for $n > 1$) saa at kun andet Bidrag resterer, og det ses at være lig $-((\mu \cdot \log) * \xi)(n)$. Vi har derfor ogsaa – som anført i Tabellen foran – at $f = -\Lambda$ og $g = \mu \cdot \log$ er et Möbiuspar.

Funktionen Λ og Problemet om dens "Gennemsnitsværdi" er vigtigt for Primtalteorien.

Tchebychef indførte

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{p} \left[\frac{\log x}{\log p}\right] \cdot \log p$$

(Rigtigheden af det sidste Udtryk ses, idet der kommer lige saa mange Bidrag af Størrelse $\log p$ som der er Potenser af p mindre end eller lig x, og det er $\left[\frac{\log x}{\log p}\right]$).

Man ser, at $\exp \psi(x)$ netop er det i Kapitel II betragtede mindste fælles Multiplum $\{1,2,\ldots,[x]\}$, idet dette jo er Produktet af de højeste forekommende Potenser af de forskellige Primtal inden-for Talsættet $\{1,2,\ldots,[x]\}$.

Vi skal senere vise Relationen $\psi(x) \sim x$, altsaa at $\psi(x)/x \to 1$ for $x \to \infty$. Med andre Ord: Vi skal vise, at $\Lambda(n)$ "gennemsnitligt" er lig 1.

Vi skal her vise, at Primtalsætningen vil være en Konsekvens af Relationen $\psi(x)/x \to 1$ for $x \to \infty$.

Bevis: Vi har $\psi(x) = \sum_p \left[\frac{\log x}{\log p}\right] \cdot \log p$; vi kan nøjes med at summere for $p \leqq x$ da de efterfølgende led er 0, og Heldelen vurderer vi opad, $[t] \leqq t$. Saa faas

$$\psi(x) \leqq \sum_{p \leqq x} \frac{\log x}{\log p} \cdot \log p = \log x \cdot \pi(x).$$

Vurderingen den anden Vej mellem $\psi(x)$ og $\pi(x)$ er lidt vanskeligere. Vi har $\psi(x) + \psi(y) = \sum_p \left(\left[\frac{\log x}{\log p}\right] + \left[\frac{\log y}{\log p}\right]\right) \cdot \log p$, og vurderer nedad, idet vi kun summerer for $p \leqq x$, saa er $\left[\frac{\log x}{\log p}\right]$ mindst lig 1, og saa benytter vi at $1 + [t] \geqq t$ og faar

$$\psi(x) + \psi(y) \geqq \sum_{p \leqq x} \frac{\log y}{\log p} \cdot \log p = \log y \cdot \pi(x).$$

Vi kombinerer Uligheder ne idet vi dividerer saa det giver Vurderinger nedad og opad for $\pi(x)/(x/\log x)$, som er den Størrelse om hvilken Primtalsætningen udsiger at den konvergerer mod 1:

$$\frac{\psi(x)}{x} \leqq \frac{\pi(x)}{\frac{x}{\log x}} \leqq \frac{\log x}{\log y} \cdot \left\{ \frac{\psi(x)}{x} + \frac{y}{x} \cdot \frac{\psi(y)}{y} \right\}.$$

Vi antager nu at $\psi(x)/x \to 1$ for $x \to \infty$, og tager $y = y(x)$ saa ogsaa $y \to \infty$, men $y/x \to 0$ samtidig med at $\log x/\log y \to 1$ (dette er muligt, fx med $y = x/\log x$). Ovenstaaende konvergerer saa mod nedenstaaende

$$\downarrow \qquad\qquad \downarrow \cdot \left\{ \downarrow + \downarrow \cdot \downarrow \right\}$$
$$1 \qquad\qquad 1 \cdot \{ 1 + 0 \cdot 1 \}$$

hvori begge Sider er 1, saaledes at Midterbrøken med $\pi(x)$ bliver tvunget til at konvergere paa den Maade som Primtalsætningen siger at den skal. □

(Uden Bevis skal anføres, at man ved en lignende Regning kan se at Primtalsætningens Gyldighed vil medføre at $\psi(x) \backsim x$, saaledes at dette "ækvivalent" med Primtalsætningen; man kan ogsaa relativt let se at denne er "ækvivalent" med: $\mu(n)$ "gennemsnitligt" er lig 0 i den Forstand at $\sum_{n \leqq x} \mu(n) / x \to 0$ for $x \to \infty$).

Cirkeldelingspolynomierne.

Vi skal betragte en vigtig Afbildning $\mathbb{N} \to \mathbb{Z}[x]$; for at naa frem til Resultatet benytter vi dog undervejs Polynomiumsringen $\mathbb{C}[x]$.

Den binome Ligning $x^n = 1$ har som bekendt n forskellige Rødder indenfor $\mathbb{C}$, og det er aabenbart netop de Tal ξ for hvilke det gælder - naar man betragter dem som Elementer i Gruppen $(\mathbb{C}^*, \cdot)$ - at ord ξ gaar op i n. Vi definerer nu det saa: Cirkeldelingspolynomium:

$$\Phi_d(x) = \prod_{\text{ord}\,\xi = d} (x - \xi);$$

dermed har vi

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

Vi faar umiddelbart at $\Phi_1(x) = x - 1$, og ved Induktion kan vi bestemme alle de følgende, idet $\Phi_n(x) = (x^n - 1) / \prod \Phi_d(x)$, hvor Nævnerproduktet er taget over alle $d < n$, $d \mid n$. Vi ved, at Polynomiumsdivisionen gaar op, og da alle forekommende Polynomier er moniske (d: Højestegradskoefficienten = 1) ser man ved Induktion at alle $\Phi_n(x)$ faar heltallige Koefficienter, saa at alle $\Phi_n(x) \in \mathbb{Z}[x]$. Iøvrigt er det let at opstille et konkret Udtryk for $\Phi_n(x)$: Möbius' Omvendingsformel (S.74) lød

$$\forall_n: \quad f(n) = \sum_{d \mid n} g(d) \quad \Longleftrightarrow \quad \forall_n: \quad g(n) = \sum_{d \mid n} \mu(d) \cdot f\left(\frac{n}{d}\right),$$

og den er aabenbart gyldig naar blot f og g er Afbildninger af Typen $\mathbb{N} \to (H, +)$, hvor $(H, +)$ er en kommutativ Gruppe; men dersom Gruppen skrives multiplikativt med $\cdot$ faar vi en multiplikativ Form for Omvendingsformlen

$$\forall_n: \quad F(n) = \prod_{d \mid n} G(d) \quad \Longleftrightarrow \quad \forall_n: \quad G(n) = \prod_{d \mid n} F\left(\frac{n}{d}\right)^{\mu(d)},$$

gyldig for Afbildninger af $\mathbb{N}$ over i en multiplikativ kommutativ

Gruppe (her er det naturligvis væsentligt, at Möbiusfunktionens Værdimængde kun er $\{0,1,-1\}$). For Cirkeldelingspolynomiet faar vi dermed Formlen

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$$

De første Polynomier er

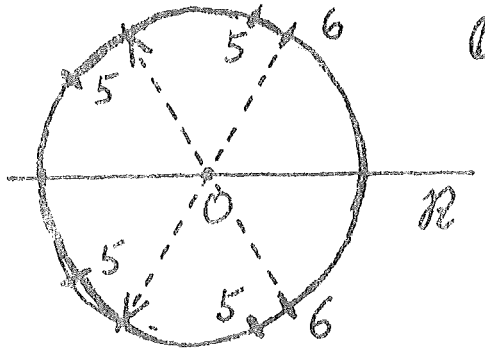
$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1
\end{aligned}$$

alment for p = Primtal: $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1,$

$$\begin{aligned}
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\
\Phi_{12}(x) &= x^4 - x^2 + 1 \quad .
\end{aligned}$$

Det er ovenfor nævnt, at ethvert $\Phi_n(x)$ er monisk. Polynomiet $\Phi_1(x)$ har Konstantleddet -1, men for $n > 1$ vil ethvert $\Phi_n(x)$ have Konstantleddet $+1$, thi sættes $x = 0$ i Produktfremstillingen ovenfor af $\Phi_n(x)$ faas $\Phi_n(0)$ lig (-1) opløftet til Potensen $\sum_{d|n} \mu(d)$ og for $n > 1$ er denne Eksponent lig 0.

I $\mathbb{C}$-Planen vil Enhedsrødderne ligge paa Cirklen $|z| = 1$, og af Definitionen paa $\Phi_n(x)$ ses at dette Polynomiums Rødder netop er Tallene $e^{2\pi i q}$, hvor q er rational og har Nævneren n naar det er skrevet som uforkortelig Brøk. Dette retfærdiggør Navnet Cirkeldelingspolynomium. Figuren viser de Delepunkter paa Cirklen som svarer til at q har Nævneren 5 hhv. 6; deres Antal er 4 ($=\varphi(5)$) hhv. 2 ($=\varphi(6)$).



For ethvert n vil Delepunkterne ligge symmetrisk om den reelle Akse, altsaa være komplekst konjugerede, og ethvert saadant Par er reciprokke Tal (da deres numeriske Værdi er 1); heraf følger at $\phi_n(x)$ og $\phi_n(\frac{1}{x})$ har de samme Rødder, og altsaa er ens paanær en Potens af x, saa at Sættet af Koefficienter i $\phi_n(x)$ vil for $n>1$ være ens hvadenten det læses fra venstre eller fra højre (idet Sættet udfyldes med 0 paa de tomme Pladser).

Vi har: Graden af $\phi_n(x)$ er lig $\varphi(n)$. Det er allerede antydet ovenfor ved Cirkeldelingsfiguren, men kan ogsaa ses af Produktfremstillingen af $\phi_n(x)$ som giver at $\deg \phi_n = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = \varphi(n)$.

Af andre Egenskaber ved Udseendet af ϕ_n kan nævnes at Koefficientsummen, $(n>1)$ altsaa Værdien $\phi_n(1)$, er lig $e^{\Lambda(n)}$. Bevis: v.Mangoldt-Funktionen Λ var bestemt ved at $\sum_{d|n} \Lambda(d) = \log n$; tager vi nu $\prod \phi_d(x)$ over alle d hvor $d|n$, $d>1$, vil det være lig $(x^n-1)/(x-1) = x^{n-1}+x^{n-2}+ \ldots +x+1$, og for $x = 1$ vil dette være lig n, saa at $\sum \log \phi_d(1) = \log n$, hvoraf følger at $\log \phi_d(1)$ maa være det samme som $\Lambda(d)$ (vi kan se bort fra $d = 1$, da $\Lambda(1) = 0$). □

Koefficienten til $x^{\varphi(n)-1}$ er lig $-\mu(n)$; da $\phi_n(x)$ har Højestegradsleddet $x^{\varphi(n)}$ ses at Resultatet ogsaa kan udtrykkes: Summen af Rødderne i $\phi_n(x)$ (de "primitive n'te Enhedsrødder" i den komplexe Plan $\mathbb{C}$) er lig $\mu(n)$. Bevis: Multipliceres to moniske Polynomier $(x^h - cx^{h-1} + \ldots)(x^k - bx^{k-1} + \ldots)$ faas $x^{h+k} - (c+b)x^{h+k-1} \ldots$ saa at de næsthøjeste Koefficienter er blevet adderet. Da $\phi_d(x)$ er af Formen $x^h - c_d x^{h-1} + \ldots$ ses at Formlen $\prod_{d|n} \phi_d(x) = x^n-1$ giver $\sum_{d|n} c_d = \left\{ \begin{matrix} 1 & \text{for } n = 1 \\ 0 & \text{ellers} \end{matrix} \right\} = e(n)$ hvilket jo netop vår den ligning som bestemte Möbiusfunktionen. Altsaa $c_d = \mu(d)$. □

(Af dette Resultat sammen med Udseendet af de opskrevne Eksempler paa $\phi_n(x)$ kunde man forledes til at tro, at Koefficienterne i $\phi_n(x)$ kun kan antage Værdierne $0,1,-1$, men dette er forkert; det

simpleste Modeksempel er $\Phi_{105}(x) = x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}\ldots$).

(Vi kan nævne et Par indre Sammenhænge mellem Cirkeldelingspolynomiernes Udseender, begge illustreret ved Eksemplerne (S.82):

Hvis $n = k \cdot m$, hvor k er den kvadratfri Kerne af n, saa er $\Phi_n(x) = \Phi_k(x^m)$, hvilket let følger, da vi kun faar Bidrag for $d \mid k$ i følgende

$$\Phi_n(x) = \prod_{d \mid n} (x^{\frac{n}{d}}-1)^{\mu(d)} = \prod_{d \mid k} ((x^m)^{\frac{k}{d}}-1)^{\mu(d)} = \Phi_k(x^m)$$

Og: Hvis n er ulige, saa er $\Phi_{2n}(x) = \Phi_n(-x)$, dog $\Phi_2(x) = -\Phi_1(x)$ som kan ses paa lignende Maade, eller ved at observere at de $2n$'te primitive Enhedsrødder netop er minus de n'te primitive Enhedsrødder (paa Cirkelfiguren foran er ζ og ζ^5 de primitive 3'te Enhedsrødder)).

Vigtig for Talteorien er Sætningen:

Hvis et Primtal p gaar op i $\Phi_n(m)$, hvor $x \in \mathbb{N}$, saa gælder $p \mid n \vee n \mid p-1$.

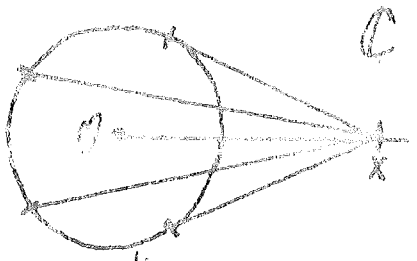
Bevis: Naar p gaar op i $\Phi_n(x)$, saa vil p ogsaa gaa op i x^n-1. Lad d være den mindste positive Exponent for hvilken $p \mid x^d-1$, altsaa $d = \text{ord}(x)$ indenfor Gruppen $(\mathbb{Z}_p^*, \cdot)$. Da vil $d \mid n$, og endvidere ifølge Fermat gælder $d \mid p-1$. Saafremt $d = n$ staar her at $n \mid p-1$, altsaa den sidste af de to Muligheder i Sætningen. Saafremt $d < n$ vil $\Phi_n(x)$ forefindes som Faktor i $(x^n-1)/(x^d-1)$ som jo er lig $\prod \Phi_{d'}(x)$, hvor Produktet tages over alle d' med $d' \mid n \wedge d' \nmid d$; den opskrevne Brøk er lig $1 + x^d + x^{2d} + x^{3d} + \ldots$ med ialt $\frac{n}{d}$ Led, og denne er altsaa delelig med p; men samtidig er $x^d \equiv 1 \pmod{p}$, saa Brøken er $\equiv \frac{n}{d} \pmod{p}$, hvoraf følger at $p \mid n$, altsaa den første Mulighed i Sætningen. □

Som en Konsekvens af Sætningen faar vi:

For ethvert $m \in \mathbb{N}$ vil Følgen $m+1, 2m+1, 3m+1, \ldots$ indeholde uendelig mange Primtal. (Specialtilfælde af Dirichlet's Sætning).

Bevis: Bevisideen er den flere Gange tidligere anvendte: Vi konstruerer en voksende Følge af indbyrdes parvis primiske Tal - som altsaa hver maa have sine egne Primdivisorer - og sørger for at Tallenes Primdivisorer er af den onskede Type.

At Følgen bliver voksende (den maa jo i hvert Fald ikke ende stationært som 1) sikrer vi os ved at bemærke at ethvert $\phi_m(x)$ er voksende med x for $x > 1$ (Værdien er Produktet af Afstandene fra x til de primitive m'te Enhedsrødder, se Fig.). Iøvrigt bemærker vi, at for $m > 1$ er $\phi_m(1) = 1$, og derfor $\phi_m(x) \geqq x$ (da ϕ_m strengt voksende og afbilder $\mathbb{Z} \to \mathbb{Z}$); dette til en senere Brug.



Følgen er ($m > 1$ antages):

$$a_1 = \phi_m(m)$$
$$a_2 = \phi_m(m \cdot a_1)$$
$$\cdots\cdots$$
$$a_n = \phi_m(m \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1})$$
$$\cdots\cdots$$

Da $\phi_m(x)$ har Konstantleddet 1 er $(\phi_m(x), x) = 1$ hvilket medfører at Følgen bestaar af parvis primiske Tal, og desuden at deres Primdivisorer er primiske med m. Men ifølge Sætningen foran gælder saa for enhver Primdivisor p at $m \mid p-1$. □

Anvendelse: For k lige og positiv er Nævneren N_k i det k'te Bernoullital lig $\prod_{p-1 \mid k} p$ (se S.63 nederst). Vi har $N_2 = 2 \cdot 3 = 6$, og for alle k vil $6 \mid N_k$. Men: Der findes uendelig mange k for hvilke $N_k = 6$, og almindeligt gælder at enhver Værdi for N_k vil forekomme for vilkaarligt store k. Bevis for $N_k = 6$: der findes uendelig mange Primtal q saa $6 \mid q-1$; da er $N_{2q} = 6$, thi Divisorerne d i 2q er 1, 2, q, og 2q, og d+1 er Primtal kun for d = 1 og 2, idet $2 \mid q+1$ og $3 \mid 2q+1$. Det almene Bevis forløber analogt: hvis k har

Divisormængden $\{d'\}$, saa findes uendelig mange Primtal q saa $\prod(d'+1) \mid q-1$. Nu har kq som Divisorer dels $\{d'\}$ og dels $\{d'q\}$, men de sidste kan aldrig give Anledning til nogle Primtal p idet $d'_0 \cdot q+1$ er delelig med d'_0+1. Da Divisorerne $\{d'\}$ netop giver N_k vil denne altsaa gentages uendelig ofte. □

For sammensatte n-Værdier kan Formlen $x^n-1 = \prod_{d \mid n} \phi_d(x)$ give Anledning til ret kraftige Faktoriseringer, fx

$$\phi_1 \cdot \phi_2 \cdot \phi_3 \cdot \phi_4 \quad \phi_6 \cdot \phi_{12}$$
$$x^{12} - 1 = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)$$

giver

$$2^{12} - 1 = 1 \cdot 3 \cdot 7 \cdot 5 \cdot 3 \cdot 13$$
$$3^{12} - 1 = 2 \cdot 4 \cdot 13 \cdot 10 \cdot 7 \cdot 73$$
$$4^{12} - 1 = 3 \cdot 5 \cdot 21 \cdot 17 \cdot 13 \cdot 241$$
$$5^{12} - 1 = 4 \cdot 6 \cdot 31 \cdot 26 \cdot 21 \cdot 601$$
$$6^{12} - 1 = 5 \cdot 7 \cdot 43 \cdot 37 \cdot 31 \cdot 1261$$

Man ser Overensstemmelsen med Sætningen om Primdivisorerne i $\phi_n(x)$. Det kan bemærkes, at 1261 ikke er et Primtal, men er $13 \cdot 97$, og begge disse Faktorer er af Formen $p = 12h + 1$.

Enhver Faktoropløsning i $\mathbb{Z}[x]$ kan umiddelbart opfattes som en Faktoropløsning i $K[X]$, hvor K er et vilkaarligt kommutativt Legeme (da jo $(\mathbb{Z},+,\cdot)$ kan afbildes homomorft ind i K ved $1 \mapsto E$ o.s.v.).

Altsaa i $K[X]$: $X^n - E = \prod_{d \mid n} \phi_d(x)$.

Hvis ord $X = n$ i den multiplikative Gruppe $(K,\cdot)$, saa er X Rod i $\phi_n(X)$.

Bevis: ord $X = n$ medfører $X^n - E = 0$, altsaa $\prod_{d \mid n} \phi_d(X) = 0$, saa at en af Faktorerne her maa være 0, og hvis X Rod i et $\phi_d(X)$ med $d < n$ vilde vi faa $X^d - E = 0$, umuligt. (NB man kan ikke slutte den anden Vej; fx i $\mathbb{Z}_3[X]$ er E Rod i baade $\phi_1(X)=X-E$ og i $\phi_3(X)=X^2+X+E$, skønt vi her har ord $E = 1$). □

Lad os specielt afbilde over i Legemet $(\mathbb{Z}_p,+,\cdot)$. Ifølge Fermat er alle Elementerne i den multiplikative Gruppe $(\mathbb{Z}_p^*,\cdot)$ Rødder i $X^{p-1} - E = \prod_{d \mid p-1} \Phi_d(X)$. Da Polynomiets Grad netop er lig Antallet p-1 af Elementer, vil ethvert $\Phi_d(X)$ som Rødder have netop de $\varphi(d)$ Stk. X for hvilke ord X = d.

Taleksempel: Vi vil betragte $(\mathbb{Z}_{13},+,\cdot)$, og opskriver en Indextabel svarende til Primitivroden 2 . Nedenfor Index anføres den paagældende Restklasses Orden i Gruppen $(\mathbb{Z}_{13}^*,\cdot)$ som jo er det samme som Ordenen af Indexet indenfor $(\mathbb{Z}_{12},+)$, og derfor - idet vi generelt skriver p i St.f. 13 - er bestemt ved ord x = (p-1)/(p-1,ind x), iøvrigt uafhængigt af Primitivroden.

x (mod.13)	1	2	3	4	5	6	7	8	9	10	11	12
Index (mod.12)	0	1	4	2	9	5	11	3	8	10	7	6
ord ⓧ	1	12	3	6	4	12	12	4	3	6	12	2

Faktoriseringen er

$$X^{12} - E = \underset{\Phi_1}{(X-E)}\underset{\Phi_2}{(X+E)}\underset{\Phi_3}{(X^2+X+E)}\underset{\Phi_4}{(X^2+E)}\underset{\Phi_6}{(X^2-X+E)}\underset{\Phi_{12}}{(X^4-X^2+E)}$$

Ethvert $\Phi_d(X)$ har som Rødder netop de Restklasser, hvis Orden er lig d, fx har $\Phi_4(X) = X^2+E$ som Rødder Restklasserne 5 og 8, Prøve: $5^2+1 = 26$, $8^2+1 = 65$, begge $\equiv 0 \pmod{13}$; ligeledes vil de 4 Primitivrødder 2, 6, 7, 11 være Rødder i $\Phi_{12}(X)$, Prøve (paa en anden Maade): $(X-2)(X-6)(X-7)(X-11) =$
$X^4 - 26X^3 + 233X^2 - 832X + 924 \equiv X^4 - X^2 + E$.

Foran blev vist, at Summen af Rødderne i $\Phi_d(X)$ (altsaa næsthøjeste Koefficient med modsat Fortegn) er lig $\mu(d)$, og man ser hvorledes dette ogsaa stemmer her, idet $\sum_{\text{ord } x = d} x \equiv \mu(d) \pmod{p}$; fx er 4 og 10 de Restklasser hvis Orden er 6, og vi har $4 + 10 = 14 \equiv 1 = \mu(6) \pmod{13}$; specielt ses, at indenfor $(\mathbb{Z}_p^*,\cdot)$

vil Summen af Primitivrødderne altid være lig $\mu(p-1)$; i Eksemplet her er Primitivrødderne 2,6,7 og 11, hvis Sum 26 er $\equiv 0 = \mu(12) \pmod{13}$. Af Eksemplet fremgaar hvorledes de tilsyneladende helt uoverskuelige Isomorfier mellem $(\mathbb{Z}_p^*, \cdot)$ og $(\mathbb{Z}_{p-1}, +)$ har en Masse indre Baand.

Eksempler paa Teknik. Vi vil vise, hvorledes dette Kapitels Resultater kan benyttes til Løsning af mange Opgaver, og vi begynder bagfra med Cirkeldelingspolynomierne.

Polynomier $x^n - y^n$. Faktoriseringen af $x^n - 1$ giver Anledning til en tilsvarende Faktorisering af $x^n - y^n$, idet

$$x^n - y^n = y^n \cdot ((\tfrac{x}{y})^n - 1) = \prod_{d/n} (\phi_d(\tfrac{x}{y}) \cdot y^{\varphi(d)}) ,$$

hvor Produktets Faktorer er Polynomier i x og y. Fx faar vi

$$\Downarrow \quad \begin{aligned} x^4 - 1 &= (x-1)(x+1)(x^2+1) \\ x^4 - y^4 &= (x-y)(x+y)(x^2+y^2). \end{aligned}$$

Dersom nu $(x,y) = 1$ maa enhver Primdivisor p i $x^n - y^n$ ogsaa være primisk med baade x og y; altsaa vil $\frac{x}{y} \in \mathbb{Q}^{(p)}$, saa vi uden Skrupler kan regne med Kongruenser modulo p, og vi har $\frac{x}{y} \equiv z$ hvor z heltallig. Dersom p gaar op i en Faktor $\phi_d(\frac{x}{y}) \cdot y^{\varphi(d)}$ maa p altsaa gaa op i $\phi_d(z)$, og vi har $p/n \vee n/p-1$ (se S.84). Fx svarer x^2+y^2 til ϕ_4, og for $(x,y) = 1$ kan dette Polynomium kun være deleligt med Primtal af Formen $p = 4h+1$ eller evt. $p=2$. Og svarende til ϕ_{12} kan $x^4-x^2y^2+y^4$ kun være deleligt med Primtal af Formen $p = 12h+1$ og evt. $p = 2$ eller 3 (og saa altsaa eventuelle fælles Faktorer for x og y).

Om Fermats Problem: Lad os benytte Faktoriseringen ovenfor af x^4-y^4 til (i første Omgang) at vise at Ligningen $x^4 = y^4 + 4z^4$ ikke har nogen Løsninger $x,y,z \in \mathbb{N}$.

Hvis der fandtes en Løsning, saa maatte der ogsaa være en Løs-

ning hvor x,y,z er parvis primiske, thi hvis et p gik op i to af Bogstaverne, saa maatte p^4 gaa op i Ligningens tredie Led, saa at det tredie Bogstav ogsaa var deleligt med p, og dette p kunde saa bortforkortes, da Ligningen er homogen. I det følgende antages derfor at x,y,z er parvis primiske. Dette ses umuddelbart at medføre at x og y er ulige.

Vi skriver Ligningen som

$$z^4 = (\frac{x-y}{2}) \cdot (\frac{x+y}{2}) \cdot (\frac{x^2+y^2}{2}) \cdot 2$$

hvori alle Brøkerne er heltallige. Den sidste af dem er ulige (da ulige Kvadrat $\equiv 1 \pmod 4$), og de to første har Differensen y , saa en af dem er ulige. De tre Brøker er parvis primiske, thi hvis et ulige p gik op i de to første vilde det gaa op i deres Sum og Differens, altsaa i x og y, og hvis det gaar op i den sidste og i en af de første, saa er $x \equiv \pm y$ og dermed den sidste $\equiv x^2$ saa at $p \mid x$, og da samtidig $p \mid z$ faas Modstrid.

Paa Grund af den entydige Primopløsning maa saa de ulige Brøker være 4'Potenser, og ligesaa den lige sammen med 2-faktoren. Altsaa $\frac{x^2+y^2}{2} = a^4$ og af Brøkerne $\frac{x-y}{2}$ og $\frac{x+y}{2}$ er den ene et Kvadrat b^2 og den anden er et dobbelt Kvadrat $2c^2$ (vi behøver ikke fuldtud at benytte at $\sim$ 4'Potenser).

Da nu

$$(\frac{x-y}{2})^2 + (\frac{x+y}{2})^2 = (\frac{x^2+y^2}{2})$$

faar vi $b^4 + 4c^4 = a^4$, hvormed vi er kommet tilbage til Udgangsligningen, men i mindre Tal, idet $2a^4 = x^2 + y^2 < 2x^2 \leqq 2x^4$. Fermats Ide med Descente infinie viser saa Paastanden. □

Ligningen $x^4 = y^4 + z^4$ har heller ingen Løsninger $\in \mathbb{N}$. Dertil behøver vi blot at bemærke at vi ogsaa her kan antage x,y,z parvis primiske, og endvidere at det lige Tal maa staa paa højre Side (igen: Kvadrat modulo 4), saa vi kan antage z lige. Derefter

kan Ligningen skrives

$$z^4 = (\tfrac{x-y}{2}) \cdot (\tfrac{x+y}{2}) \cdot (\tfrac{x^2+y^2}{2}) \cdot 2^3$$

hvorefter Betragtningerne markeret $\lceil^x_x$ ordret kan gentages, saa at vi naar til en Ligning $b^4 + 4c^4 = a^4$, som ikke har nogen Løsninger. □

Som tidligere nævnt (S.59) har Fermat angivet, at han havde et bemærkelsesværdigt Bevis for at en Ligning $x^n + y^n = z^n$ ikke har nogen Løsninger $x,y,z \in \mathbb{N}$ for $n > 2$, "men at Margenen er for smal til at skrive Beviset" (det er et Randnotat i hans Eksemplar af en Udgave af Oldtidsmatematikeren Diofant, som behandlede Tilfældet $n = 2$). Som nedenfor omtales er Tilfældet $n = 4$ ret specielt, og for det har han et andet Sted givet et Bevis (et af de faa af hans overleverede Beviser), som er noget i Retning af ovenstaaende, idet det ogsaa beror paa en "Descente infinie"; men medens vi ovenfor saa at sige fra et Sidespor kom ind paa den nedstigende Kæde, saa kan man sige at Fermat drejede det saaledes at han straks var inde paa Kæden, men at det han beviste var en stærkere Sætning (nemlig at $x^4 + y^4 = z^2$ ikke har Løsninger $\in \mathbb{N}$); det er bemærkelsesværdigt, at man ved en Descente Infinie (som jo blot er et indirekte Induktionsbevis) kan være nødt til at gøre en Paastand stærkere for at være i Stand til at bevise den.

Dersom Fermats Paastand er bevist med en Eksponent n, saa er den ogsaa bevist for alle Eksponenter som er Multipla af n, da jo $x^{hn} + y^{hn} = z^{hn}$ kan skrives $(x^h)^n + (y^h)^n = (z^h)^n$. Heraf følger at vi nu har vist Sætningen for alle Eksponenter som er delelige med 4. Dette medfører at det for at bevise den generelle Sætning vil være tilstrækkeligt at bevise den for alle ulige Eksponenter n, thi ethvert Tal større end 2 vil jo være deleligt enten med 4 eller med et ulige Tal. Samme Ræsonnement viser endda, at det

vil være tilstrækkeligt at bevise den for Eksponenter som er ulige Primtal.

Det er nu nærliggende at skrive Ligningen som $x^n = z^n - y^n$ og saa benytte Faktoriseringen af Højresiden (ved Hjælp af Cirkeldelingspolynomier), men desværre fører det ikke ret langt, idet naar n er et Primtal kan $z^n - y^n$ kun faktoriseres til $(z-y)(z^{n-1}+z^{n-2}y+\ldots+y^{n-1})$, hvor man kan vise, at den sidste Faktor er et irreducibelt Polynomium (over $\mathbb{Q}$), saa man kan ikke som ved $n = 4$ faa tre Faktorer. Saa har man prøvet at gaa ud i algebraiske Udvidelseslegemer indenfor hvilke man kan faktorisere videre, og det har for adskillige specielle n-Værdier ført til det ønskede Bevis, men trods overordentlig store Anstrengelser i denne Retning er man ikke naaet frem til et generelt Bevis, saa det er næppe ad denne Vej man skal bevise Sætningen (Vanskeligheden er at man kommer ud i Legemer indenfor hvilke der ikke gælder entydig Faktorisering, hvori altsaa de "hele" Tal ikke udgør en fri Halvgruppe; Forsøgene paa at raade Bod paa dette var iøvrigt den historisk første Oprindelse til Idealbegrebet). At man kun behøver at betragte ulige n-Værdier giver dog en lille Fordel, idet man saa kan betragte Problemet som en Opgave indenfor $\mathbb{Z} \setminus \{0\}$, og flytte alle Leddene over paa samme Side, $x^n + y^n + z^n = 0$, saa man faar Symmetri. Ejendommeligt er det, at det eneste ulige Primtal for hvilket der eksisterer et simpelt Bevis (dog med nogen Regning) er $n = 7$ (!).

Eksempler til talteoretiske Funktioner.

Ændring af Summationsvariable: Dette er en vigtig Metode ved talteoretiske Opgaver, som vi illustrerer med et lille første Eks: For $x \geq 1$ gælder

$$\sum_n \mu(n) \cdot \left[\frac{x}{n}\right] = 1.$$

Bevis: $\sum_n \mu(n)\left[\frac{x}{n}\right] = \sum_n \mu(n) \sum_{t \leqq \frac{x}{n}} 1 = \sum_n \sum_t \mu(n)$, hvor der summeres over alle Par (n,t) med $nt \leqq x$. Vi indfører nu $h = nt$ som ny Variabel, og da der er bijektiv Forbindelse mellem Par (n,t) og Par (h,n)hvor $n|h$, kan vi skrive Summen som

$$\sum_{h \leqq x} \sum_{n|h} \mu(n) = \sum_{h \leqq x} \left\{ \begin{matrix} 1 \text{ for } h = 1 \\ 0 \text{ ellers} \end{matrix} \right\} = 1. \qquad \square$$

Regning med multiplikative Funktioner: Man staar sig hyppigt ved at huske paa at Mængden af multiplikative Funktioner er en Gruppe baade ved $*$-Foldning og ved Multiplikation. Lad os som Eksempel betragte Funktionen $\lambda = \mu * (\mu^2)$, hvor Eksponenten 2 refererer til sædvanlig Multiplikation (μ^2 er altsaa den Funktion som er 1 paa de kvadratfri Tal og 0 ellers). Da μ er multiplikativ ses, at λ ogsaa er multiplikativ, og vi behøver derfor kun at udregne den for en Primtalpotens p^α. For $d|p^\alpha$ er $\mu^2(d)$ lig 1 for $d = 1$ og p og lig 0 ellers. Følgelig er

$$\lambda(p^\alpha) = \sum_{d|p^\alpha} \mu^2(d)\mu\left(\frac{p^\alpha}{d}\right) = \mu(p^\alpha) + \mu(p^{\alpha-1}) = \left\{ \begin{matrix} 0 \text{ for } \alpha = 1 \\ -1 \text{ for } \alpha = 2 \\ 0 \text{ for } \alpha > 2 \end{matrix} \right. ,$$

hvoraf man ser, at $\lambda(n)$ er lig 0 hvis n ikke er et Kvadrattal, og at $\lambda(a^2)$ er lig $\mu(a)$.

Eksempel: Idet vi som sædvanlig antager at $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ er Primopløsning med alle $\alpha_j > 0$ sættes $f(n) = (-1)^{\alpha_1 + \ldots + \alpha_r}$ og $g(n) = 2^r$. Foldningen $f * g$ ønskes bestemt. Man observerer at baade f og g er multiplikative, og det er derfor nok at bestemme Foldningen paa en Primtalpotens p^α. For $d|p^\alpha$ har vi $g(d) = 2$ undtagen for $d = 1$ hvor $g(1) = 1$, medens $f(\frac{p^\alpha}{d})$ alternerende er $+1$ og -1. Vi finder dermed

$$\sum_{d|p^\alpha} f\left(\frac{p^\alpha}{d}\right) g(d) = 1 \cdot 2 - 1 \cdot 2 + \ldots \pm 1 \cdot 2 \mp 1 \cdot 1 = 1 \text{ altid},$$

og følgelig har Foldningsfunktionen $f * g$ Værdien 1 for al-

le n, saa at vi har Relationen $f * g = \xi$.

Man kan regne videre med disse Funktioner f og g, og som Eksempel kan vi uden Bevis (men son en Opgave) nævne Formlen

$$(f \circ \varphi) * \delta = g * h ,$$

hvor φ og δ er de tidligere definerede Funktioner, medens $h(n)$ betyder den Funktion som er $\mathfrak{N}$ i Kvadrattallene og 0 ellers (den er multiplikativ !).

Endnu et Eksempel: Idet φ og τ har de sædvanlige Betydninger betragter man ligningen

$$\varphi * f = \tau \cdot f ;$$

Løsningsfunktionerne f søges.

Da begge Sider af Ligningen er lineære i f er det klart, at Mængden af Løsningsfunktioner maa være et Vektorrum (over $\mathfrak{R}$).

Men til en given Værdi af $f(1)$ svarer kun én Løsningsfunktion f, som kan bestemmes induktivt: For $n = 1$ siger Ligningen blot at $1 \cdot f(1) = 1 \cdot f(1)$ som er indholdsløs, men for $n > 1$ kan man flytte Bidraget med $f(n)$ fra Venstresiden over til Højresiden, hvorved man faar

$$\sum_{d \mid n, d > 1} \varphi(d) \cdot f\left(\frac{n}{d}\right) = (\tau(n) - 1) \cdot f(n)$$

og idet $\tau(n) > 1$ vil denne Ligning bestemme $f(n)$ entydigt udfra de foregaaende f-Værdier.

Da f indgaar paa begge Sider af Lighedstegnet kan man ikke umiddelbart slutte at f er multiplikativ, og det kan jo i hvert Fald ogsaa kun gælde for den Løsning for hvilken $f(1) = 1$; men denne er virkelig multiplikativ, hvilket kan ses saaledes: Vi tager f_0 som den multiplikative Funktion der paa Primtalpotenserne stemmer overens med f, saa vil for $n = p^{\alpha}$ Værdien af $\varphi * f_0$ være lig Værdien af $\varphi * f$, og ligesaa er for disse n Værdien af $\tau \cdot f_0$ lig

Værdien af $\tau \cdot f$; da nu $\varphi * f_0$ og $\tau \cdot f_0$ begge er multiplikative maa de stemme overens for alle n, saa f_0 maa netop være lig den entydigt bestemte Løsning f til Ligningen.

Til Bestemmelse af en Løsning f er det derfor tilstrækkeligt at bestemme dens Værdi for $n = p^{\alpha}$. Man finder ved en Regning at (idet $f(1) = 1$)

$$f(p^{\alpha}) = \frac{p-1}{1} \cdot \frac{2p-1}{2} \cdot \ldots \cdot \frac{\alpha p-1}{\alpha} .$$

Vi har altsaa: <u>En Løsning til Ligningen $\varphi * f = \tau \cdot f$ er af Formen en Konstant gange den multiplikative Funktion f som er bestemt ved det angivne Udtryk for $f(p^{\alpha})$.</u>

<u>Gandhi's Primtalformel:</u> <u>Lad k være et naturligt Tal større end 1.</u>

<u>Det hele Tal</u>

$$p = -\left[\frac{\log \left(\sum_{d \mid k} \frac{\mu(d)}{2^d - 1} - \frac{1}{2} \right)}{\log 2}\right]$$

<u>er defineret (Størrelsen under Logaritmetegnet er positiv) og er netop det mindste Primtal p som ikke gaar op i k.</u>

Bevis: Lad $a_1 + a_2 + \ldots$ være en absolut konvergent Række. Vi sætter $s_d = a_d + a_{2d} + a_{3d} + \ldots$ Saa er

$$\sum_{d \mid k} \mu(d) \cdot s_d = \sum_{d \mid k} \sum_{d \mid j} \mu(d) a_j = \sum_j a_j \sum_{d \mid k, d \mid j} \mu(d) ,$$

(da d kun kan antage endelig mange Værdier er det tilladt at ombytte Summationsrækkefølgen), og da $d \mid k \wedge d \mid j \Leftrightarrow d \mid (k,j)$ og endvidere $\sum_{d \mid n} \mu(d) = 0$ undtagen for $n = 1$ hvor Summen er 1 ses at hele Udtrykket simpelthen bliver lig $\sum a_j$ summeret over de j for hvilke $(j,k) = 1$. Det første j af denne Art er Tallet 1, og det næste ses at være netop det mindste Primtal p som ikke gaar op i k. Dersom man vælger $a_j = 2^{-j}$ bliver $s_d = 1/(2^d - 1)$ og $\sum_{d \mid k} \mu(d)/(2^d - 1)$ altsaa $2^{-1} + 2^{-p} + \underbrace{\ldots}$, hvor Resten $\underbrace{\ldots}$ er mindre end 2^{-p}; heraf følger Paastanden umiddelbart. □

Monotone multiplikative Funktioner.

De ikke-trivielle multiplikative Funktioner som er behandlet i det foregaaende har alle været stærkt springende. Det er ikke tilfældigt, idet vi vil vise at de eneste Funktioner $f:\mathbb{N}\to\mathbb{R}$ som er multiplikative og monotone er de trivielle $f(n) = n^{\alpha}$ (tidligere omtalt som det simpleste og uinteressante Eksempel paa stærkt multiplikative Funktioner) samt de f hvor $f(1) = 1$, $f(2) \in [0,1]$ og $f(n) = 0$ for $n > 2$ (Erdös). Dette er en af Grundene til at det i Talteorien er svært at naa til Resultater med kraftige Størrelsesvurderinger.

Bevis: Vi har altid $f(1) = 1$. Dersom der fandtes et $f(n) < 0$ vilde det samme gælde for alle de følgende n, men det strider mod at $f((n+1)(n+2)) = f(n+1)\cdot f(n+2) > 0$. Værdimængden tilhører altsaa $[0,\infty[$.

Dersom 0 antages som Funktionsværdi, da lad m være det mindste Tal for hvilket $f(m) = 0$; $m = 2$ eller 3 giver de i Sætningen omtalte specielle multiplikative monotone Funktioner. Og $m \geqq 4$ kan ikke forekomme, thi saa er $(m-1)(m-2) > m$, saa at $f(m) = 0$ strider mod at $f((m-1)(m-2)) = f(m-1)\cdot f(m-2) > 0$.

Vi skal derfor blot vise, at de f for hvilke Værdimængden tilhører $\mathbb{R}^+$ er af Formen $f(n) = n^{\alpha}$. Og vi behøver kun at gøre det for voksende f, thi hvis f er aftagende kan vi blot gaa over til $1/f$.

For at klargøre Metoden kan vi i første Omgang nøjes med at betragte stærkt multiplikative f. Dersom $m^a < n^b$ (hvor $m,n,a,b \in \mathbb{N}$) har vi $f(m^a) = f(m)^a \leqq f(n^b) = f(n)^b$, eller altsaa

$$\frac{\log m}{\log n} < \frac{b}{a} \Rightarrow \frac{\log f(m)}{\log f(n)} \leqq \frac{b}{a} .$$

Holder vi m og n fast og lader b/a variere $\in \mathbb{Q}^+$ følger saa at

$$\frac{\log f(m)}{\log f(n)} \leqq \frac{\log m}{\log n},$$

og da vi heri kan ombytte m og n maa der gælde $=$, altsaa

$$\frac{\log f(n)}{\log n} = \frac{\log f(m)}{\log m} = \alpha,$$

hvor Højresiden er konstant for fastholdt m, altsaa $f(n) = n^{\alpha}$. Hvis f kun er multiplikativ (ikke stærkt) bliver det lidt vanskeligere. Først vises ved Induktion at for $n > 1$ gælder

$$f(n^{a-1}+1) \leqq f(n)^a \leqq f(n^{a+1}-1);$$

for $a = 1$ staar der $f(2) \leqq f(n) \leqq f(n^2-1)$ som gælder, og hvis Uligheden er opfyldt som den er skrevet med a, saa faar vi $f(n^a+1) \leqq f(n^a+n) = f(n^{a-1}+1)f(n) \leqq f(n)^{a+1} \leqq f(n^{a+1}-1)f(n) = f(n^{a+2}-n) \leqq f(n^{a+2}-1)$, altsaa Gyldigheden med a+1. Af Formlen faas direkte $f(n^{a-1}) \leqq f(n)^a \leqq f(n^{a+1})$, hvoraf som foran faas at $m^a < n^b \Rightarrow f(m)^{a-1} \leqq f(n)^{b+1}$, eller $\frac{\log m}{\log n} < \frac{b}{a} \Rightarrow \frac{\log f(m)}{\log f(n)} \leqq \frac{b+1}{a-1}$. Lader vi heri $\frac{b}{a}$ variere $\in \mathbb{Q}^+$ følger som før $\frac{\log f(m)}{\log f(n)} \leqq \frac{\log m}{\log n}$ og som før finder vi $f(n) = n^{\alpha}$. □

Medens de betragtede talteoretiske Funktioner er relativt gammelkendte, saaledes som det fremgaar af de historiske Angivelser, saa er det benyttede algebraiske Synspunkt - som især kom til Udtryk i Foldningsringen - først kommet frem ca.1960 selvom nogle af Ideerne i det (Benyttelse af analytiske Funktioner for hvilke det i Virkeligheden er ligegyldigt om de fremstillende Rækker konvergerer) i en vis Grad var anet tidligere. Senere er man dog blevet klar over at Prioriteten maa gives til E.T.Bell ca.1920 (B.1883-1960, foruden talrige algebraiske Arbejder har han skrevet mere populære matematiske Bøger, af hvilke nogle (fx"Development of Mathematics") er gode (omend ikke korrekte i alle Detailler), og under Pseudonymet "John Taine" var han ogsaa en produktiv Science Fiction Skribent).

KAPITEL V : Primtalsætningen.

Som tidligere nævnt udsiger Sætningen at

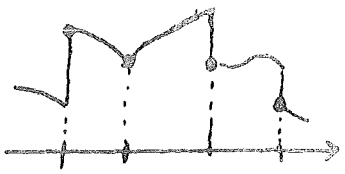
$$\Pi(x) \sim \frac{x}{\log x}$$

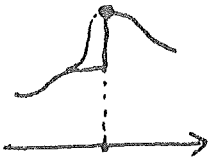
i den Forstand at Forholdet mellem Relationens to Sider konvergerer mod 1 for $x \to \infty$. Det er (ejendommeligt nok) betydeligt sværere at vise end Tchebycheff's Resultat om at Forholdet ligger mellem to positive Konstanter. Vi skal gøre det "elementært", og det betyder dybere set, at vi skal gøre det uden nogen af de Konvergensproblemer som knytter sig til de mere funktionsteoretiske Metoder. De Funktioner vi skal betragte vil være sammenbyggede af simple Elementer (Trappefunktioner og "Spline"-Funktioner) og Konvergensspørgsmaal vil kun optræde paa lavt Niveau, men kan naturligvis ikke helt undgaas, da selve Sætningen udtaler sig om en Konvergens.

Vi har foran (S.80) vist, at Sætningen vil være en Konsekvens af at $\Psi(x)/x \to 1$, hvor $\Psi(x) = \sum_{n \leq x} \Lambda(n)$ idet $\Lambda(n)$ (v.Mangoldtfunktionen) er defineret ved at $\sum_{d|n} \Lambda(n) = \log n$, og vi fandt at $\Lambda(n) \geq 0$, men alt om den behøver vi ikke at huske. Endvidere skal vi benytte Möbiusfunktionen μ defineret ved at $\sum_{d|n} \mu(n)$ er lig 0 undtagen for $n = 1$ hvor $\mu(1) = 1$, og om den fandt vi at $|\mu(n)| \leq 1$ (Værdimængden var jo $\{0, \pm 1\}$), men andet om den behøver vi ikke at huske.

Vi skal operere med endelige Summer, og det vil være praktisk at benytte Stieltjesintegral-Skrivemaaden (S.1856-1894), fx $\Psi(x) = \int_0^x d\Psi(t)$, hvor saa Differentialet $d\Psi(t)$ er 0 undtagen i Springene i de heltallige t, for hvilke det er $\Lambda(t)$.

Vi skal kun anvende det paa "pæne" Funktioner. Dermed mener vi Funktioner som har en Mængde af "Sammensætningspunkter" som ikke fortætter sig i det endelige; mellem to Sammensætningspunkter skal Funktionen være givet ved et simpelt analytisk Udtryk (brugbart ogsaa i Endepunkterne af Intervallet); i Sammensætningspunkterne kan der være Diskontinuiteter, og som Funktionsværdi tager vi saa Grænseværdien fra højre. Denne Funktionsmængde er aabenbart en Ring, og de sædvanlige Regler fra Integralregningen gælder for den (dog kan der for et Integral af Typen $\int_A^B f(t)dg(t)$ hvor $f(t)$ og $g(t)$ har Diskontinuiteter i samme Punkt komme en Vanskelighed naar man anvender partiel Integration, men derom senere); Rigtigheden heraf kan let ses, f.Eks. ved at man i Omegnen af en Diskontinuitet erstatter med en approksimerende kontinuert Funktion, men saaledes at Ændringen kun er foretaget til venstre for Diskontinuiteten. Vi bemærker, at de omtalte Regninger har intet at gøre med den vanskeligere dybere Teori for Stieltjesintegraler.





Vi sætter $h(x) = \sum_{n \leq x} \frac{\Lambda(n)}{n}$. I Stedet for at vise at $\Psi(x)/x \to 1$ vil vi vise at $h(x) - \log x \to$ en Grænseværdi, $-c$, idet det sidste vil medføre det første.

Bevis for denne Implikation: Vi har $dh(t) = \frac{\Lambda(n)}{n}$ for $t = n$ og $dh(t) = 0$ ellers. Vi forudsætter nu $h(t) = \log t - c + \varepsilon_t$, hvor $\varepsilon_t \to 0$, og faar saa med en delvis Integration

$$\Psi(x) = \sum_{n \leq x} \Lambda(n) = \int_0^x + dh(t) = \left[t \cdot h(t)\right]_0^x - \int_0^x h(t)\, dt =$$

$$x \cdot h(x) - \int_0^x (\log t - c + \varepsilon_t)\, dt = x \cdot \log x - x \cdot c + x \cdot \varepsilon_x - \int_0^x \log t\, dt$$

$$+ c \cdot x - \int_0^x \varepsilon_t\, dt.$$

Da nu $\int_0^x \log t\, dt = \left[t \cdot \log t - t\right]_0^x = x \cdot \log x - x$ (i 0 er Grænseværdien lig 0), og endvidere $\int_0^x \varepsilon_t\, dt = \varepsilon'_x \cdot x$ (trivielt ε-Bevis) ses at $\Psi(x) = x + \varepsilon''_x \cdot x$. □

Da vi skal vise noget med log x er det rimeligt at substituere $x \to e^x$, og idet vi sætter

$$w(x) = \sum_{n \leqq e^x} \frac{\Lambda(n)}{n}$$

er Opgaven altsaa at vise, at for $x \to \infty$ vil $w(x) - x$ gaa mod en Grænseværdi, -c.

Vi skal fra nu af udelukkende operere i Klassen K bestaaende af Funktioner F som afbilder $\mathbb{R} \to \mathbb{R}$ men er identisk 0 paa den negative Halvakse (altsaa $\mathbb{R}^- \to 0$) og endvidere er "pæne" (i den foran angivne Betydning).

Da vi imidlertid ofte skal bruge analytiske Udtryk f(x) paa den positive Halvakse indfører vi Skrivemaaden f(x) for Funktionen

$$f(x) = \begin{cases} f(x) & \text{for } x \geqq 0 \\ 0 & \text{for } x < 0 \end{cases} \quad {}^{+})$$

hvorved vi opnaar at $f(x) \in K$.

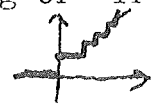
Det er klart at K med sædvanlig Addition og Multiplikation er en Ring, hvis Etelement er Funktionen 1 (altsaa Funktionen som er 1 for $x \geqq 0$ og er 0 for $x < 0$).

Indenfor K har vi Integraloperationen: Vi definerer $\int F$ som den Funktion, der i x har Værdien $\int_0^x F(t)\, dt$. Den vil aabenbart tilhøre K (og er iøvrigt kontinuert).

Endvidere skal vi stærkt benytte Operationen T defineret ved at Funktionen TF i Punktet x har Værdien

+) I Resten af Kapitlet anvendes betonende Understregning kun under Tekst, for at undgaa Fejltolkninger.

$$TF(x) = \sum_n \frac{F(x-\log n)}{n} = F(x) + \frac{1}{2} F(x-\log 2) + \frac{1}{3} F(x-\log 3)\ldots$$

Man bemærker, at for ethvert x vil Leddene blive 0 fra et vist Trin, saa der er intet Konvergensproblem. Og $TF(x)$ tilhører K. (Indskud: Almindeligt kunde man indenfor K definere en "Foldning" $F*G$ ved $F*G(x) = \int F(x-t)\, dG(t)$, hvor der integreres over $t \in \mathbb{R}$, men jo kun effektivt over $t \in [0,x]$, saa der er intet Konvergensproblem. Selvom det egentlig er saadanne Foldninger vi skal benytte, vil det dog for os næppe betale sig, og ogsaa tilsløre det "elementære", at lave en generel Teori for dem. Men man kan have dem i Tankerne. Man kan vise, at $*$ er en kommutativ Komposition indenfor K, det sker via delvis Integration, som i dette Tilfælde viser sig ogsaa at være formelt gyldig for Stieltjesintegraler(uanset eventuelt Sammenfald af Diskontinuiteter), og Kompositionsresultatet bliver kontinuert fra højre saa det tilhører K. Foldningen ses ogsaa at være associativ og dens Neutralelement E er Funktionen $\underline{1}$ (altsaa  , det samme som Multiplikationens Neutralelement) idet vi har $dE(t) = \begin{cases} 1 \text{ for } t=0 \\ 0 \text{ ellers} \end{cases}$. Udtrykt som Foldning er $TF(x) = F*g(x) = \int F(x-t)dg(t)$, hvor $g(x) = \sum_{n \in e^x} \frac{1}{n}$,  . Analogt ses at $\int F$ ogsaa kan skrives som $F*\underline{x}$ (idet $\underline{x} =$  med $d\underline{x} = \begin{cases} dx & \text{for } x>0 \\ 0 & \text{for } x<0 \end{cases}$). Og den nu umiddelbart følgende Bemærkning er en Konsekvens af at $*$ er kommutativ og associativ. Indskud slut.)

Operationerne $\int$ og T kommuterer, altsaa $\int TF(x) = T\int F(x)$.

Bevis: $\int^x TF(t)\, dt = \int^x \sum_n F(t-\log n)\cdot\frac{1}{n}\, dt = \sum_n \frac{1}{n}\int^x F(t-\log n)dt$.

For hvert enkelt x var der kun endelig mange Addender, saa der var intet Problem ved Ombytningen af $\sum$ og $\int$. □

Det skal betones, at $\int$ og T er lineære Operationer.

T har en invers Afbildning defineret ved

$$T^{-1}F(x) = \sum_n \frac{\mu(n)}{n} \cdot F(x-\log n),$$

thi sammensættes denne med T faas

$$\sum_n \frac{\mu(n)}{n} \cdot TF(x-\log n) = \sum_n \sum_m \frac{\mu(n)}{n \cdot m} F(x - \log n - \log m),$$

og sættes $n \cdot m = h$ faas

$$\sum_h \frac{1}{h} F(x-\log h) \cdot \sum_{n|h} \mu(n) = \sum_h \frac{1}{h} F(x-\log h) \cdot \begin{cases} 1 \text{ for } h=1 \\ 0 \text{ ellers} \end{cases} = F(x).$$

Det var Sammensætning fra den ene Side, sammensættes fra den anden Side faas et fuldstændigt lignende Regnestykke. □

Vi har altsaa en Bijektion T: K → K.

Og en Trivialitet er

Iseki-Tatuzawa's Sætning: $|T^{-1}F(x)| \leqq T|F|(x)$.

Bevis:
$$|T^{-1}F(x)| = \left|\sum_n \frac{\mu(n)}{n} \cdot F(x-\log n)\right| \leqq \sum_n \frac{1}{n} \cdot |F(x-\log n)|,$$

idet vi benytter, at $|\mu(n)| \leqq 1$. □

Vi skal betragte Grænseovergang $x \to \infty$, og indfører "smaa Restled" R: R skal betegne en Funktion R(x) for hvilken der eksisterer et $\alpha > 0$ og en positiv Konstant M saa $|R(x)| < M \cdot e^{-\alpha x}$. Vi skriver R for enhver saadan Funktion, uden at det behøver at være den samme, og vi kan derfor skrive R + R = R og x·R = R o.s.v.

Vi har $\int R = c + R$, hvor c er en Konstant.

Bevis: $\int_{-\infty}^{x} R(t)\,dt = \int_{-\infty}^{\infty} R(t)\,dt - \int_x^{\infty} R(t)\,dt$, hvori det første Led bliver Konstanten c og det sidste kan vurderes numerisk opad ved $M \cdot \int_x^{\infty} e^{-\alpha t} dt = \frac{M}{\alpha} \cdot e^{-\alpha x}$ og altsaa er R. □

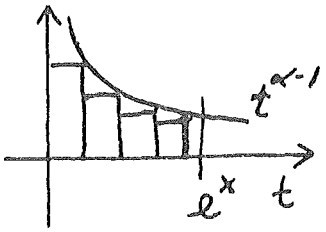
For de smaa Restled R gælder at baade TR og $T^{-1}R$ er begrænsede.

Bevis: Det sidste følger umiddelbart af det første, idet $|R| = R$, saa at Iseki-Tatuzawa direkte giver det ønskede.
Det første følger ved en lille Regning, til hvilken vi antager at $|R(x)| < M \cdot e^{-\alpha x}$ med $\alpha \in]0,1[$ (man kan jo altid tage et mindre α). Saa er

$$|TR(x)| = \Big| \sum_{n \leqq e^x} \frac{1}{n} R(x - \log n) \Big| <$$

$$\sum_{n \leqq e^x} \frac{1}{n} \cdot M \cdot e^{-\alpha(x-\log n)} = e^{-\alpha x} \cdot M \cdot \sum_{n \leqq e^x} n^{\alpha-1},$$

og idet $\alpha < 1$ kan vi let vurdere Rækkesummen ved Integralsammenligning ($t^{\alpha-1}$ er aftagende), saa



$$|TR(x)| < M \cdot e^{-\alpha x} \int_0^{e^x} t^{\alpha-1} dt = M \cdot e^{-\alpha x} \cdot \frac{1}{\alpha} \cdot e^{\alpha x} = \frac{M}{\alpha}. \qquad \square$$

Nu kan vi begynde at regne:

$$T\,\underline{e^{-x}} = \sum_{n \leqq e^x} \frac{1}{n} e^{-(x-\log n)} = \sum_{n \leqq e^x} \frac{n}{n} \cdot e^{-x} = \frac{[e^x]}{e^x},$$

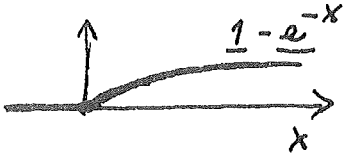
altsaa

$$(\Theta) \qquad T\,\underline{e^{-x}} = \underline{1} + R.$$

Integration giver

$$T\,(\underline{1 - e^{-x}}) = \underline{x} + \underline{c}' + R$$

som adderet til den forrige giver



$$(\Phi) \qquad T\,\underline{1} = \underline{x} + \underline{c} + R \qquad \text{(hvor } c \text{ er en Konstant)}$$

(foreløbig er der intet overraskende, thi egl. staar her blot den bekendte Vurdering af Afsnittet i den harmoniske Række (!)).
Ny Integration giver

$$(\Omega) \qquad T\,\underline{x} = \frac{1}{2}\underline{x^2} + \underline{cx} + \underline{d} + R.$$

Vi havde at $T^{-1}R$ begrænset, og sammen med Formel (Θ) giver det at $T^{-1}\,\underline{1} = \underline{e^{-x}} +$ begrænset = begrænset, og kombineres dette

med Formel (ϕ) giver det at $T^{-1}\underline{x} = \underline{1} - \underline{c}\cdot$begrænset + begrænset = begrænset. Ialt har vi dermed faaet at naar a,b er Konstanter, saa er $T^{-1}(\underline{ax} + \underline{b} + R)$ begrænset.

Forbindelsen mellem Primtalproblemet og Operationen T kommer frem ved Formlen

$$\boxed{T(\underline{x}\cdot F(x) + \int_{t=-\infty}^{\infty} F(x-t)\,dw(t)) = \underline{x}\cdot(TF(x))}$$

Integralleddet er - skrevet ud - lig $\sum_m F(x-\log m)\cdot\frac{\Lambda(m)}{m}$; man ser, at Formlen udtrykker, at T af dette Led er lig Differensen $\underline{x}\cdot(TF(x)) - T(\underline{x}\cdot F(x))$ (og dermed udtrykker, at Operationerne T og "Multiplikation med $\underline{x}$" ikke kommuterer).

Bevis: Vi udregner den sidstnævnte Differens (kun $n \leqq e^x$ forekommer):

$$\underline{x}\cdot\sum_n \frac{1}{n} F(x-\log n) - \sum_n \frac{1}{n}\cdot(x-\log n)\,F(x-\log n) = \sum_n \frac{\log n}{n} F(x-\log n).$$

Dette skal ifølge Formlen være lig $T(\sum_m F(x-\log m)\cdot\frac{\Lambda(m)}{m})$ som udregnes (idet T-Variablen kaldes h) til

$$\sum_h \frac{1}{h} \sum_m \frac{\Lambda(m)}{m} F(x-\log h-\log m) = \left[\text{(hm sættes = n)}\right.$$

$$\sum_n \frac{1}{n} F(x-\log n) \sum_{m\mid n} \Lambda(m) = \sum_n \frac{1}{n} F(x-\log n)\cdot\log n.$$

stemmer! □

I Formlen kan vi nu indsætte forskellige F(x), og dermed faa Oplysninger om w. Simplest er det at sætte $F(x) = \underline{1}$, saa er $\underline{x}\cdot F(x) = \underline{x}$ og $\int F(x-t)\,dw(t) = \int_0^x dw(t) = w(x)$ (smlgn. det tidligere antydede om at $\underline{1}$ er neutral Foldningsfaktor).

Altsaa er

$$T(\underline{x} + w(x)) = \underline{x}\cdot T\,\underline{1} = \underline{x}\cdot(\underline{x} + \underline{c} + R) = \underline{x^2} + \underline{cx} + R\ ,$$

hvoraf med Formlerne (ϕ) og ($\varnothing$) faas

$$\# \qquad T(w(x) - \underline{x} + \underline{c}) = \underline{c^2} - \underline{2d} + R\ .$$

Højresiden er af Formen $\underline{b} + R$ hvor b er en Konstant, og dersom der gjaldt en Sætning om at $T^{-1}(\underline{b} + R)$ er en Funktion som gaar mod 0, saa var vi færdige, men saa godt er det desværre ikke, idet man kan give Eksempler paa smaa Restled R for hvilke $T^{-1}R \not\to 0$ (at Konstanten b er uvæsentlig i denne Forbindelse fremgaar af Formel(-Θ-)).

Men vi skal dog vise, at i vort specielle Tilfælde, $w(x)-\underline{x}+\underline{c} = T^{-1}(\underline{b} + R)$, kan vi slutte at Venstresiden $\longrightarrow 0$, idet vi benytter Egenskaber ved w(x) (og Grænseværdien for $w(x) - \underline{x}$ vil altsaa netop blive -c, hvor c er det ved Formel (ϕ) bestemte Tal (det blev ved denne Formel bemærket, at den udtrykte en Vurdering af Afsnittene i den harmoniske Række, og c bliver den saakaldte Eulers Konstant 0,5772...)).

<u>En Relation</u> $F(x) = T^{-1}(\underline{b} + R)$ <u>vil dog medføre et Par Egenskaber ved</u> F(x) som vi vil notere; de er Konsekvenser af den paa forrige Side noterede: "$T^{-1}(\underline{ax} + \underline{b} + R)$ er begrænset"! Vi har

1) F(x) <u>er begrænset</u>.

   Det var en umiddelbar Konsekvens.

2) $\int F(x)$ <u>er begrænset</u>.

   Det følger idet $T\int F(x) = \int TF(x) = \underline{bx} + \underline{c}'' + R$.

3) <u>Dersom</u> $F(x) \geqq -1$ <u>gælder</u> $\limsup_{x\to\infty} F(x) \leqq 1$.

   Bevis: I Formel $\square$ bliver Højresiden $\underline{x}\cdot(\underline{b}+R) = \underline{bx}+R$, og T^{-1} af dette er begrænset, saa at (da $dw(t)\geq 0$ og $F\geq -1$)

   $x\cdot F(x) = -\int_{t=-\infty}^{\infty} F(x-t)dw(t) + \text{begr.} \leqq w(x) + \text{begr.}$.

   Anvender vi nu 1) paa # faar vi $w(x) = \underline{x} + \text{begr.}$, og indsætter vi dette og dividerer med $\underline{x}$ faar vi at $F(x) \leqq 1 + \frac{\text{begr.}}{x}$, hvoraf det ønskede (vi skal kun bruge 3) som den er formuleret, men ved ret trivielle Modifikationer af Beviset og Betragtning af baade F(x) og -F(x)

faas at $\limsup_{x \to \infty} F(x) = -\liminf_{x \to \infty} F(x)$, og man bemærker, at dette harmonerer meget godt med Egenskab 2)).

Vi sætter $w(x) = x + c$ lig $q(x)$, og Formel # udsiger saa at $Tq(x) = b + R$ (hvor b er en Konstant), og vort Maal er herudfra at vise at $q(x) \to 0$.

Vi har ifølge 1) at $q(x)$ begrænset, altsaa at $w(x) = x + \text{begr.}$ (ogsaa brugt i Beviset for 3)), d.v.s. at

$$\sum_{n \leqq y} \frac{\Lambda(n)}{n} = \log y + \text{begr.},$$

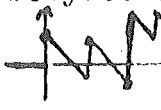
hvilket er et Resultat af Mertens fra sidste Halvdel af forrige Aarhundrede (d.v.s. Tiden efter Tchebychef og før Hadamard - de la Vallée-Poussin's Bevis for Primtalsætningen), som ret let kan vises at være "ækvivalent" med Tchebychefs Resultat. I St.f. at have indsat $F(x) = 1$ i Formel □, kunde vi have indsat andre analytiske Udtryk for $F(x)$, og derved opnaa andre Resultater, men de vilde stadig tilhøre den samme "Ækvivalenskreds" og kun give "begrænset" hvor vi ønsker "konvergent"; fx vil $F(x) = e^{-x}$ direkte give at $\psi(y)/y$ er begrænset; det fører altsaa ikke videre.

Da det er $q(x)$ som er væsentlig for os indfører vi den i St.f. $w(x)$ i □, $w(x) = q(x) + x - c$, saa vi faar

$$T(x \cdot F(x)) + \int_t F(x-t)\,dq(t) + \int_t F(x-t)\,d(t-c)) = x \cdot TF(x);$$

nu er (se S.100) $\int_t F(x-t)\,dt = \int F(x)$ og $\int_t F(x-t)\,dl = F(x)$, saa vi som ny Form for □ faar (idet vi tager T^{-1})

$$\boxed{x \cdot F(x) + \int_{t=-\infty}^{\infty} F(x-t)\,dq(t) = T^{-1}(x \cdot TF(x)) - \int F(x) + c \cdot F(x)}$$

Desuden havde vi $Tq(x) = b + R$, og vi vil nu kun operere videre med q og glemme alt om w. Blot skal vi bruge at $w(x)$ var voksende (i svag Forstand), fordi $\Lambda(n) \geqq 0$, hvilket betyder at for $h > 0$ er $q(x) - q(x-h) \geqq -h$ (Grafen for q er  ,

saa at Hældningskoefficienten for enhver Sekant er $\geqq -1$; ogsaa for $x = 0$ er Diskontinuitetsspringet positivt, nemlig lig c, der som foran bemærket er 0,5772.., og at $c > 0$ fremgaar iøvrigt ogsaa let ved en simpel Analyse af Beviset for Formel (ϕ)); vi har altsaa at for $h > 0$ er

$$\frac{q(x) - q(x-h)}{h} \geqq -1 .$$

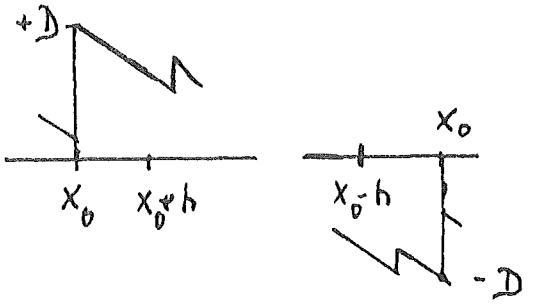
Paa denne Brøk kan vi anvende 3) foran, idet $T(\frac{1}{h}(q(x)-q(x-t))$ $= \frac{1}{h}(\underline{b}+R - \underline{b}-R) = R$ (idet $(TF)(x-h) = T(F(x-h))$ hvilket er klart), og Resultatet kan aabenbart skrives under ét som

$$\limsup_{x \to \infty} \left| \frac{q(x) - q(x-h)}{h} \right| \leqq 1.$$

Vi sætter $\limsup_{x \to \infty} |q(x)| = D$, og skal vise at $D = 0$. For at komme igennem trods Diskontinuiteterne i $q(x)$ foretager vi en Udjævning, idet vi danner Middelværdien (som bliver kontinuert)

$$q^{\div}(x) = \frac{1}{h} \int_{x-h}^{x} q(t)\, dt ;$$

man ser, at $q^{\div}(x) \in K$ og at $\frac{d}{dx} q^{\div}(x)$ netop er den ovenfor betragtede Brøk, saa at $\limsup_{x \to \infty} \left| \frac{d}{dx} q^{\div}(x) \right| \leqq 1$. Det er klart at $\limsup_{x \to \infty} |q^{\div}(x)| \leqq D$, men der gælder ogsaa at $\limsup_{x \to \infty} |q^{\div}(x)| \geqq D-h$ (for hvis $q(x_0)$ er nær $+D$, saa er $q(x)$ paa det efterfølgende h-Interval større end $D-h$ næsten, og hvis $q(x_0)$ er nær $-D$ gælder tilsvarende paa det foregaaende h-Interval, se Fig.).



Iøvrigt er $q^{\div}(x)$ mindst lige saa "jævn" som $q(x)$, og hvis vi endnu engang tager Middelværdi (med det samme h) faar vi en Funktion $q^{\div\div}(x)$ for hvilken $\limsup |q^{\div\div}(x)| \geqq D - 2h$.

Da $T(\frac{d}{dx} q^{\div}(x)) = R$ bliver $Tq^{\div}(x) = \underline{konst.} + R$, hvoraf paa samme Maade findes at $Tq^{\div\div}(x) = \underline{konst.} + R$ (man ser iøvrigt let at Konstanten bliver det samme b som indgik i $Tq(x) = \underline{b} + R$).

Vi anvender nu Formel [ ] paa $q^{\div\div}(x)$ og faar

$$\underline{x}\cdot q^{\div\div}(x) + \int_t q^{\div\div}(x-t)dq(t) = T^{-1}(\underline{x}\cdot\text{konst.}+R) - \int q^{\div\div}(x) + c\cdot q^{\div\div}(x) \ ;$$

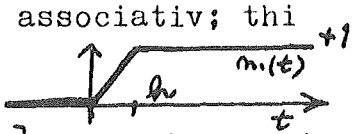
hele Højresiden er begrænset (de to sidste Led p.G.a. 1) og 2) foran), og isoleres Venstresidens $q^{\div\div}(x)$ faas

$$q^{\div\div}(x) = -\frac{1}{x}\int_t q^{\div\div}(x-t)\ dq(t) + \frac{\text{begr.}}{x} \ .$$

Endelig bemærker vi, at i Integralleddet her kan vi flytte den ene Middelværdidannelse over fra $q^{\div\div}(x-t)$ til $q(t)$, altsaa

$$\int_t q^{\div\div}(x-t)\ dq(t) = \int_s q^{\div}(x-s)\ dq^{\div}(s);$$

det er triviel Integralregning, men med de indgaaende Variabelskifter er det ubehageligt at skrive op, og det skal derfor ikke gøres her, men lad os bemærke, at selvom de variable t og s formelt løber over $\mathbb{R}$, saa er Integrationerne jo kun effektive paa endelige Intervaller, saa der er intet Konvergensproblem. (Gyldigheden af Overflytningen bliver umiddelbart forstaalig udfra det tidligere Indskud, S.100, om Integralfoldningen $F*G(x) = \int_t F(x-t)\ dG(t)$ som er kommutativ og associativ; thi $F^{\div}(x) = F*m(x) = \int_t F(x-t)\ dm(t)$, hvor $m(t)$ vokser lineært fra 0 til 1 paa Intervallet $[0,h]$ og er konstant udenfor dette Interval; saa udtrykker Formlen ovenfor blot at $(q*m*m)*q = (q*m)*(q*m)$).



Altsaa, idet vi nu betoner at Integrationen kun er effektiv for $t \in [0,x]$

$$q^{\div\div}(x) = -\frac{1}{x}\int_{s=0}^{x} q^{\div}(x-s)\ dq^{\div}(s) + \frac{\text{begr.}}{x} \ .$$

Vi lader nu $x \to \infty$ og betragter limsup af Udtrykkets numeriske Værdi. Paa venstre Side faar vi ifølge det ovenstaaende mindst D - 2h. Paa højre Side benytter vi at $\underset{K\to\infty}{\text{limsup}}\left|q^{\div}(x)\right| \leqq D$

og at limsup $\left|\frac{d}{dx}\, q^{\div}(x)\right| \leqq 1$, hvorefter den nedenfor følgende Uligheds-sætning om reelle Funktioner giver at Højresidens limsup er mindre end eller lig $\sqrt{\frac{2}{\pi}}\cdot D$, da jo Leddet $\frac{\text{begr.}}{x}$ gaar mod 0. Men da $\sqrt{\frac{2}{\pi}}$ er mindre end 1, og h var vilkaarlig positiv ses, at man maa have $D = 0$ for at $D - 2h \leqq \sqrt{\frac{2}{\pi}} D$.

Primtalsætningen vil dermed være bevist !

Vi vil vise:

Dersom $h(x) \in K$ og er kontinuert (altsaa differentiabel undt. i eventuelle Knækpunkter) og $\limsup_{x \to \infty} |h(x)| \leqq D$ og $\limsup_{x} |h'(x)| \leqq 1$, saa er

$$\limsup_{x \to \infty} \left|\frac{1}{x}\int_0^x h(x-t)\, dh(t)\right| \leqq \sqrt{\frac{2}{\pi}} \cdot D .$$

Det er en Konsekvens af følgende almindelige Ulighed for reelle Funktioner:

Dersom $f(t), g(t) \in K$ og

$$\begin{matrix} |f(t)| \leqq A \\ |g(t)| \leqq A \end{matrix} \quad \text{og} \quad \begin{matrix} |f'(t)| \leqq B \\ |g'(t)| \leqq B \end{matrix}$$

saa er

$$\left|\int_0^y f(t)\, dg(t)\right| \leqq \sqrt{\frac{2}{\pi}} \cdot (y + C) \cdot AB$$

hvor C er en Konstant (for hvilken man kan bruge $A \cdot \sqrt{8}$).

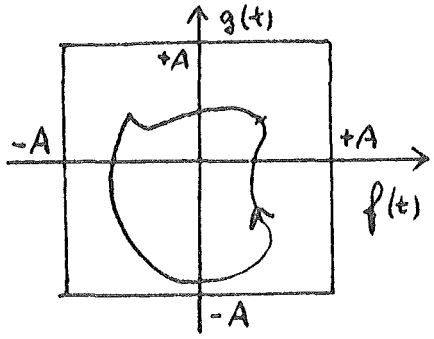
Overgangen fra limsup i det foregaaende til den absolutte Begrænsning i den sidste Sætning er triviel ε-Regning: Ved Ændring af $h(x)$ paa et endeligt Interval bliver Ændringen i Integralet begrænset, og man opnaar et h for hvilket $|h(x)| < D+\varepsilon$ og $|h'(x)| < 1+\varepsilon$, saa disse Tal kan bruges som A og B i den sidste Sætning. Naar man saa dividerer igennem med y i denne faar man den foregaaende Sætning.

Beviset for Primtalssætningen lykkedes fordi $\sqrt{\frac{2}{\pi}}$ er mindre end 1, men et hvilketsomhelst fast Tal mindre end 1 kunde have udrettet det samme. Nu ser man, at den sidste Sætning bliver triviel dersom man erstatter $\sqrt{\frac{2}{\pi}}$ med 1, idet saa en umiddelbar Integralvurdering giver Begrænsningen $y \cdot AB$, og derved er endda kun brugt at $|f(t)| \leqq A$ og $|g'(t)| \leqq B$; ved en partiel Integration kan man komme til at bruge de andre to Betingelser, men man har stadig Faktoren 1. Problemet er at udnytte alle fire Betingelser paa en Gang og derved faa en bedre Konstant.

Beviset for Uligheden:

Naar t gennemløber Intervallet $[0,y]$ vil Punktet $(f(t),g(t))$ i en euklidisk Plan gennemløbe en Kurve, som p.G.a. Begrænsningerne for $|f'|$ og $|g'|$ har en veldefineret Buelængde, som bliver mindre end eller lig $y\sqrt{2}\cdot B$.

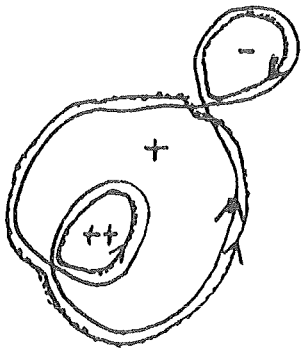
Lad os først antage at Kurven er en Jordankurve, altsaa en lukket Kurve uden Selvoverskæring. Det Areal som den omslutter er netop $\left|\int_0^y f(t)\,dg(t)\right|$, og da det er indeholdt i det paa Fig. viste Kvadrat er det $\leqq 4A^2$. Da Omkredsens Længde er $\leqq y\sqrt{2}B$ er Arealet ogsaa $\leqq \frac{1}{4\pi}(y\sqrt{2}B)^2$ (ifølge den isoperimetriske Ulighed vil en Kurve af given Længde omslutte størst Areal naar den er en Cirkel, og den svarer til Lighedstegnet).



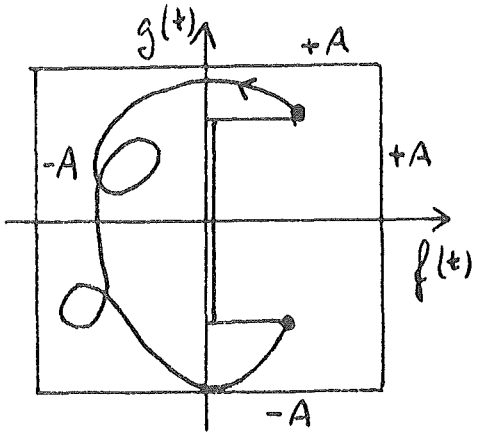
Arealet er da ogsaa mindre end eller lig Mellemproportionalen mellem Vurderingerne, altsaa $\left|\int_0^y f(t)dg(t)\right| \leqq \sqrt{4A^2 \cdot \frac{2y^2}{4\pi}B^2} = \sqrt{\frac{2}{\pi}} \cdot yAB$.

Lad os dernæst blot antage at Kurven er en lukket Kurve (altsaa gerne med Selvoverskæringer, men disse kan kun forekomme i endeligt Antal, thi ifølge Definitionen af K bestaar Kurven af endeligt mange analytiske Buer, og to saadanne kan kun have endeligt

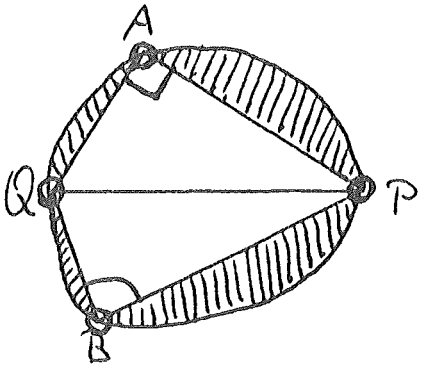
mange Fællespunkter). Integralet angiver da det omsluttede Areal regnet med Multiplicitet (= det Antal Gange Arealelementet er omkredset i positiv Omløbsretning). Kurven kan opfattes som en Sum af Jordankurver (se Fig.), saaledes at Arealet med Multiplicitet bliver Summen af de enkelte Arealer med + eller −, og Kurvelængden bliver Summen af de enkelte Kurvelængder (Summen $\leqq \sqrt{2}\ y\mathfrak{B}$), og vi faar derfor igen at Integralet er majoriseret af $\sqrt{\frac{1}{\pi}}\sqrt{2}yA\mathfrak{B}$.



Hvis endelig Kurven ikke er lukket, saa kan vi lukke den ved at tilføje Liniestykker som vist paa Fig. Paa de vandrette Stykker er $dg(t) = 0$ og paa det lodrette er $f(t) = 0$, saa Integralets Værdi er uændret, og Kurvelængden er højst blevet forøget med 4A. Altsaa faar vi at Integralet er majoriseret af $\sqrt{\frac{1}{\pi}} \cdot (y\sqrt{2} + 4A) \cdot AB$. □



Den isoperimetriske Ulighed er velkendt, fx fra Variationsregningen, men lad os skitsere et elementærgeometrisk Bevis: At der for given Omkreds eksisterer en Kurve der omslutter maximalt Areal er klart af Kompakthedsgrunde, og den maa være konvex (Arealet øges hvis eventuelle "Buler" rettes udad). I Kurven indlægges $\sphericalangle PAQ = \frac{\pi}{2}$ og paa den modsatte Kurvedel vælges B. Vi tænker os nu Led i Punkterne A,P,B,Q, medens de skraverede Arealer tænkes stive. Dersom $\sphericalangle PBQ \neq \frac{\pi}{2}$ kunde vi "vrikke" paa Firkanten saa $\sphericalangle$ B nærmedes mod $\frac{\pi}{2}$; derved ændres Arealet af $\triangle$ APQ med Diffkvot. = 0, og Arealet af $\triangle$ BPQ med Diffkvot. > 0, saa større Areal kan opnaas. Altsaa ligger B paa Halvcirklen over PQ som Diameter. Ræsonnementet gentages med A og B ombyttet. □



KAPITEL VI : Endelige Grupper i talteoretisk Belysning.

I dette Kapitel betegnes Gruppeelementer med store Bogstaver, A, B, .. medens Mængder af Elementer betegnes $\tilde{A}$, $\tilde{B}$, .. og smaa Bogstaver betegner som sædvanlig hele Tal n, m, .., og specielt betegner p Primtal.

Vi betragter en endelig Gruppe $(\tilde{G}, \cdot)$, og dens Orden betegnes $n = |\tilde{G}|$. Bekendt er Lagranges Sætning: Enhver Undergruppes Orden er Divisor i n. Ordenen af et Element, ord A, er Ordenen af den cykliske Undergruppe frembragt af Elementet, og er altsaa Divisor i n. Den cykliske Gruppe af Orden n betegnes $\tilde{C}_n$ (Kompositionsangivelsen udelades), og vi har $\tilde{C}_n \approx (\mathbb{Z}_n, +)$. Hvis ord A = m gælder $A^h = E \Leftrightarrow m \mid h$, og endvidere $\text{ord}(A^h) = \frac{m}{(m,h)}$. For cykliske Grupper er alle Undergrupper og alle Homomorfibilleder igen cykliske.

Lad os minde om nogle simple ikke-abelske Grupper (i Standardbetegnelserne udelades Kompositionsangivelsen):

1) Permutationsgrupperne $\tilde{S}_n$ og de alternerende Grupper $\tilde{A}_n$; deres Ordener er hhv. n! og $\frac{1}{2}$ n! (de er ikke-abelske for hhv. $n > 2$ og $n > 3$).

2) Kvaterniongruppen som har 8 Elementer $\{\pm E, \pm i, \pm j, \pm k\}$ med Multiplikatiinsreglerne $i^2 = j^2 = k^2 = -E$, og $i \cdot j = -j \cdot i = k$ og de tilsvarende med i, j, k kredsforskudt (de fire Elementer $1 = E$, i, j og k er Basiselementer for det ikke-kommutative Legeme af Kvaternioner).

3) Diedergrupperne $\tilde{D}_n$, hvor $\tilde{D}_n$ er Gruppen af Flytninger af en regulær n-Kant over i sig selv (Vending af Planen tilladt); dens Orden er 2n.

Orden	1	2	3	4	5	6	7	8	9	10	11	12
Antal abelske	1	1	1	2	1	1	1	3	2	1	1	2
Antal ikke-ab.	.	.	.	.	.	1	.	2	.	1	.	3

Tabellen angiver hvormange abelske og ikke-abelske Grupper der findes af Ordener $\leqq 12$. De ikke-abelske er for 6'Orden $\tilde{S}_3 \approx \tilde{D}_3$, for 8'Orden Kvaterniongruppen og D_4, for 10'Orden $\tilde{D}_5$ og for 12'Orden $\tilde{A}_4$ og $\tilde{D}_6$ og endnu en Gruppe.

Ved det <u>direkte Produkt</u> $(\tilde{A},\circ) \times (\tilde{B},\circ)$ af to Grupper forstaas som bekendt en Gruppe bestaaende af Elementpar (A,B), og hvor Gruppekompositionen er komponentvis Komposition (eller enhver med den saaledes dannede Gruppe isomorf). Der gælder

1) Ordenen af Produktgruppen er Produktet af Faktorernes Ordener.
2) Produktet er abelsk hvis og kun hvis Faktorerne er abelske.
3) Produktet har normale Undergrupper isomorfe med Faktorerne.
4) Direkte-Produktdannelse er kommutativ og associativ.
5) Ordenen af (A,B) = m.fls.Mult.{ord A, ord B}.

For (r,s) = 1 vil de to cykliske Gruppers direkte Produkt $\tilde{C}_r \times \tilde{C}_s$ blive en cyklisk Gruppe af Orden rs (thi ifølge 5) vil den have Elementer af Orden rs). I Almindelighed kan man blot sige at det direkte Produkt af cykliske Grupper bliver en abelsk Gruppe, men fra Algebraen kendes den vigtige <u>Basissætning</u> som udsiger at enhver endelig abelsk Gruppe kan skrives som direkte Produkt af (en, to eller flere) cykliske Grupper; ved en Opspaltning som af $\tilde{C}_{rs}$ ovenfor kan man opnaa at disse Gruppers Ordener bliver Primtalpotenser, og til en given abelsk Gruppe svarer netop ét Sæt Primtalpotenser (deres Rækkefølge ligegyldig), Gruppens "Invarianter". Anderledes udtrykt siger Basissætningen at enhver endelig abelsk Gruppe er isomorf med Gruppen af Forskydninger af et Heltalsgitter $\mathbb{Z}^k$ modulo et k-dimensionalt Interval.

Vi betragter nu en Gruppe $(\tilde{G},\cdot)$ - gerne ikke-abelsk:

Lad $(r,s) = 1$. Hvis $X^{rs} = E$, saa findes netop ét Elementpar (P,Q), saa $PQ = QP = X$ og $P^r = Q^s = E$. Hvis omvendt $P^r = Q^s = E$ og $PQ = QP$, saa er $(PQ)^{rs} = E$.

Foruden denne Sætning som handler om Potenser lig E findes en ganske analog omhandlende Elementordener:

Lad $(r,s) = 1$. Hvis ord $X = rs$, saa findes netop ét Elementpar (P,Q), saa $PQ = QP = X$ og ord $P = r$ og ord $Q = s$. Hvis omvendt ord $P = r$ og ord $Q = s$ og $PQ = QP$, saa er ord$(PQ) = rs$.

Bevis: $(r,s) = 1$ betyder idealteoretisk at $(1) = (r) + (s)$, og der findes altsaa $h,k \in \mathbb{Z}$ saa $1 = h\cdot r + k\cdot s$.

Første Sætning: Det søgte P skal opfylde $P = P^{hr+ks} = P^{ks} = P^{ks}Q^{ks} = (PQ)^{ks} = X^{ks}$, og analogt skal vi have $Q = X^{hr}$; det var altsaa den eneste Mulighed. Men det opfylder virkelig det ønskede da X-Potenser jo kommuterer og vi har $PQ = X^{hr+ks} = X$ og $P^r = X^{rks} = E$ og ligesaa $Q^s = E$ (man bemærker, at h og k ikke er entydigt bestemt, men det afficerer ikke Bevisets Gyldighed). Sætningens sidste Del er evident, thi naar P og Q kommuterer er $(PQ)^{rs} = P^{rs}Q^{rs} = E$.

Anden Sætning: Da ord $X = rs \Rightarrow X^{rs} = E$ maa vi igen have $P = X^{ks}$ og $Q = X^{hr}$ hvoraf faas $PQ = QP = X$. Vi faar ord $P = \frac{\text{ord}X}{(\text{ord}X, ks)} = \frac{rs}{(rs,ks)} = \frac{r}{(r,k)} = r$ og analogt ord $Q = s$. Sætningens sidste Del ses idet $(PQ)^m = E \Rightarrow P^m = Q^{-m}$ og den fælles Orden af disse sidste er Divisor i baade r og s og er altsaa 1, hvoraf følger at baade r og s gaar op i m, hvilket igen medfører at ord(PQ) $= rs$. □

Eksempel: Lad os betragte en ikke-cyklisk Gruppe af Orden pq, hvor p og q er forskellige Primtal. De fra E forskellige Elementer har Orden p eller q. Hvis ord $P = p$ og ord $Q = q$ ses at P og Q ikke kommuterer, thi ellers vilde der findes et Element

af Orden pq, saa at Gruppen var cyklisk. En saadan Gruppe er altsaa ret stærkt ikke-abelsk. Fx har $\tilde{S}_3$ 3 Elementer P af Orden 2 (Transpositioner) og 2 Elementer Q af Orden 3 (Kredsforskydninger), og her kan et P og et Q aldrig kommutere.

For en Gruppe $(\tilde{G}, \cdot)$ definerer vi nu en talteoretisk Funktion

$$f(r) = (\text{Antallet } X, \text{ hvor } X^r = E).$$

Vi kan kalde den Gruppens Frobeniusfunktion (F.1849-1917). Man ser, at den kun afhænger af Gruppens Struktur, idet isomorfe Grupper faar samme f.

Da $X^r = E \Rightarrow \text{ord } X \mid r$ faar vi, naar vi sætter

$$g(r) = (\text{Antallet } X, \text{ hvor ord } X = r),$$

at

$$f(r) = \sum_{d \mid r} g(d) \quad \text{og dermed} \quad g(r) = \sum_{d \mid r} \mu(d) f(\tfrac{r}{d}),$$

idet f og g udgør et Möbiuspar.

Ifølge Lagranges Sætning er $f(n) = n$, og trivielt er det at $f(1) = 1$. Endvidere gælder at $f(r) = f((r,n))$, hvilket viser, at for given Gruppeorden n er f bestemt ved sine Værdier paa Divisorerne d i n, idet (r,n) er et d; Rigtigheden ses ved at vi til Betingelsen $X^r = E$ tilføjer den ifølge Lagrange betydningsløse Betingelse $X^n = E$, hvorefter de to Betingelser tilsammen giver $X^{(r,n)} = E$. Iøvrigt er jo $f(r) \leqq n$ altid.

For den cykliske Gruppe $\tilde{C}_n$ er $f(r) = r$ og $g(r) = \varphi(r)$ for alle r som gaar op i n, og det indtræffer ikke for andre Grupper.

Bevis: Elementerne er $\{A, A^2, \ldots, A^n = E\}$. Vi har $(A^h)^r = E$ netop naar $n \mid hr \Leftrightarrow \frac{n}{r} \mid h$, altsaa for $h = \frac{n}{r}, 2 \cdot \frac{n}{r}, \ldots, r \cdot \frac{n}{r}$, ialt r Stk., saa at $f(r) = r$. Idet $d \mid r \Rightarrow d \mid n$ og dermed $f(d) = d$ faar vi af

Möbiusformlen at $g(r) = \sum_{d|r} \mu(\frac{r}{d}) \cdot d = \varphi(r)$. Sætningens sidste Paastand er triviel, idet allerede $g(n) > 0$ medfører at Gruppen er cyklisk; da der er entydig Forbindelse mellem f og g ses at fx allerede Betingelsen $f(r) = r$ medfører at Gruppen er cyklisk. □

For g gælder trivielt at $\underline{r|t \wedge g(r) = 0 \text{ medfører at } g(t) = 0}$, og endvidere

$\underline{\text{Vi har altid } \varphi(r)|g(r)}$. Det er trivielt for $r \nmid n$, da saa $g(r)=0$.

Bevis: Paa Mængden af Elementer af Orden r sætter vi $X \sim Y$ dersom der findes et h saa $X = Y^h$. Her er $\sim$ evident reflexiv og transitiv, og den er ogsaa symmetrisk, thi da $(h,r) = 1$ findes et k saa $hk \equiv 1 \pmod r$, hvoraf faas $Y = X^k$. Vi har altsaa Ækvivalensklasser, og Klassen med X indeholder netop $\varphi(r)$ Stk., nemlig Elementerne X^h hvor $(h,r) = 1$. □

$\underline{\text{Frobeniusfunktionen for et direkte Produkt er Produktet af Faktorernes Frobeniusfunktioner}}$.

Bevis: Vi betragter Produktet $(\tilde{A},\cdot) \times (\tilde{B},\cdot)$. Dets Etelement er (E_A,E_B). Hvis $(A,B)^r$ er lig Etelementet har vi $A^r = E_A \wedge B^r = E_B$, og Antallet af saadanne Par (A,B) ses at være netop $f_A(r) \cdot f_B(r)$. □

Lidt interessantere er Sætningen

$\underline{\text{Hvis } (r,s) = 1 \text{ er } f(rs) \leq f(r) \cdot f(s) \text{ og } g(rs) \leq g(r) \cdot g(s), \text{ saa at f og g er "submultiplikative". For abelske Grupper gælder Lighedstegnene, saa at for disse er f og g multiplikative.}}$

Bevis: Ifølge Sætningen øverst S.113 er f(rs) lig Antallet af Par (P,Q) for hvilke $P^r = E$ og $Q^s = E$ og hvor P og Q kommuterer. Stryger vi den sidstnævnte Betingelse ses at vi som Vurdering opad for f(rs) faar $f(r) \cdot f(s)$, hvilket ønskedes. For abelske Grup-

per er det ligegyldigt om Betingelsen stryges, og derfor faar vi Lighedstegn. Og den anden Sætning paa S.113 giver paa samme Maade Paastanden om g. □

For abelske Grupper vil vi nu udlede en Række yderligere Resultater om Frobeniusfunktionen.

Medens vi for ikke-abelske Grupper kun kan paastaa at $r|t \Rightarrow f(r) \nmid f(t)$ (trivielt idet $X^r = E$ medfører $X^t = E$) gælder der:

For abelske Grupper vil $r|t$ medføre at $f(r)|f(t)$, og vi har altid at $f(r)|n$.

Bevis: I en abelsk Gruppe er en Mængde $\{X: X^r = E\}$ en Undergruppe (thi den er stabil ved Multiplikation da $(XY)^r = X^rY^r$); idet nu $\{X: X^r = E\} \subseteq \{X: X^t = E\}$ vil den første af disse være en Undergruppe i den anden, og endvidere er de begge Undergrupper i hele Gruppen. Dette viser Paastanden. □

I en abelsk Gruppe gælder for $r,s,t \in \mathbb{N}$ at $f(rst)f(t)|f(rt)f(st)$.

Bevis: Vi vil vise, at

$$\frac{f(rst)}{f(rt)} \mid \frac{f(st)}{f(t)} \quad ;$$

ifølge forrige Sætning er begge Brøkerne hele Tal, og vi skal angive en Fortolkning af dem. Mængden af Elementer af Formen $X = Y^t$ er en Undergruppe, da den er stabil ved Multiplikation, og man ser umiddelbart at ethvert X antages for $f(t)$ Stk. forskellige Y. Vi tager nu Fællesmængden for denne Undergruppe og Undergruppen bestaaende af de X for hvilke $X^s = E$; vi skal have $Y^{st} = E$, hvilket er opfyldt af $f(st)$ Stk. Y, og Antallet af forskellige X bliver saa ifølge det foregaaende lig $\frac{f(st)}{f(t)}$ og dette er altsaa Elementtallet i Fællesmængden. Vi erstatter nu t med rt og betragter altsaa Elementer af Form $X = Z^{rt}$ hvilket er et stærkere Krav end at $X = Y^t$. Paa denne Maade faar vi en Fællesmængde med $\frac{f(rst)}{f(rt)}$ Elementer. Da begge Fællesmængder er Under-

grupper, og den sidste er indeholdt i den første, har vi den ønskede Gaa-op-Relation. □

Lad os med et Par Smaaeksempler vise, at Betingelsen"abelsk" er væsentlig for de sidste Sætninger. Vi opskriver Tabeller for f og g, og her er det jo kun deres Værdier for n's Divisorer r som har Interesse.

1) $\tilde{S}_3$. $n = 6$.

r	1	2	3	6
g(r)	1	3	2	0
f(r)	1	4	3	6

Man ser, at $f(2) \nmid f(n)$.

f og g er submultiplikative, men ikke multiplikative.

2) Kvaterniongruppen. $n = 8$.

r	1	2	4	8
g(r)	1	1	6	0
f(r)	1	2	8	8

Man ser, at $f(4)\cdot f(1) = 8$ ikke gaar op i $f(2)\cdot f(2) = 4$. Frobeniusfunktionen, og altsaa ogsaa g, er multiplikativ da dens Værdi kun afhænger af de i r indgaaende 2-Potenser:

$$f(r) = \begin{cases} 1 & \text{for } 2 \nmid r \\ 2 & \text{for } 2 \parallel r \\ 8 & \text{for } 4 \mid r \end{cases}$$

og man kan altsaa ikke heraf slutte at Gruppen er abelsk.

At den næstfølgende Sætning heller ikke gælder hvis Gruppen ikke er abelsk vil til Overflod fremgaa af et senere Eksempel.

<u>I en abelsk Gruppe kan f(m) ikke have andre Primdivisorer end m har, og specielt er altsaa $f(p^\beta)$ lig en Potens af p.</u>

Bevis: Da f er multiplikativ ser man at Sætningens almene første udsagn følger af dens sidste specielle Udsagn.

Endvidere vil det være tilstrækkeligt at bevise at f(p) er en Potens af p, thi af den forrige Sætning med $t = 1$, $r = p^\beta$ og $s = p$ ses at $f(p^{\beta+1}) \mid f(p^\beta)\cdot f(p)$, som ved Induktion giver $f(p^\beta) \mid f(p)^\beta$.

Nu er f(p) lig Antallet Elementer i Undergruppen $\{X: X^p = E\}$; i denne udtager vi et størst muligt Sæt, t Stk., af Elementer X,Y,... for hvilke Ligningen $X^j\cdot Y^k\cdot\ldots = E$ kun er opfyldt naar $X^j = Y^k = \ldots = E$; paa sædvanlig Maade ses nu, at naar vi lader (j,k,...) variere frit, saa vil Sæt (j,k,...) som er forskellige

modulo p give Anledning til forskellige Elementer $X^j \cdot Y^k \cdot \ldots$ og at samtlige Elementer frembringes paa denne Maade. Følgelig er $f(p) = p^t$. □

For en endelig abelsk Gruppe er altsaa

^{0}) f multiplikativ, og logaritmisk

og for et fast Primtal p er

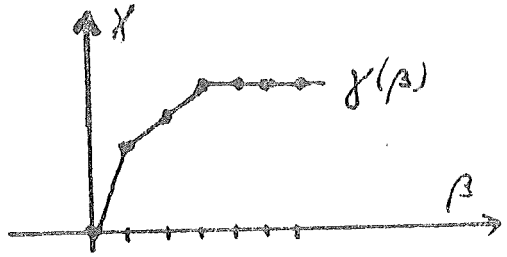
^{1}) $f(p^\beta) = p^\gamma$, hvor $\gamma = \gamma(\beta)$ afbilder $\mathbb{N}_0 \to \mathbb{N}_0$,

^{2}) $\gamma(0) = 0$,

^{3}) $\gamma(\beta)$ er ikke-aftagende

^{4}) fra et vist Trin er $\gamma(\beta)$ konstant,

^{5}) $\gamma(\beta)$ er konkav, d.v.s. $\gamma(\beta+1) - \gamma(\beta) \leqq \gamma(\beta) - \gamma(\beta-1)$.



Heraf er ^{0}) og ^{1}) direkte omtalt; ^{2}) udtrykker at $f(1) = 1$; ^{3}) gælder da $f(p^\beta) \leqq f(p^{\beta+1})$; ^{4}) er evident da Gruppen er endelig, og ^{5}) er en Konsekvens af at $f(ppt) \cdot f(t)$ gaar op i $f(pt) \cdot f(pt)$ ifølge tidligere Sætning.

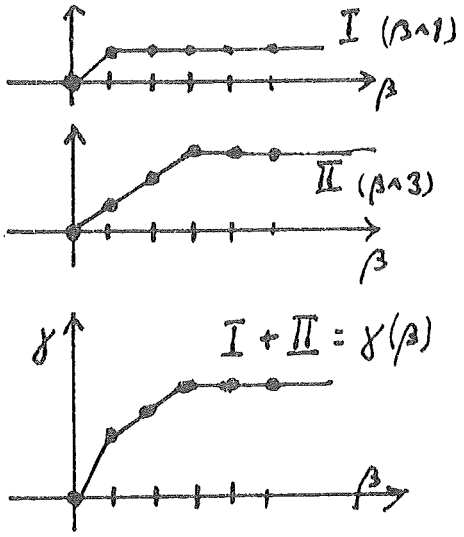
Egenskaberne ^{0})-^{5}) udtrykker alt hvad der kan siges om Frobeniusfunktionen for en endelig abelsk Gruppe, idet vi ved Hjælp af Basissætningen kan godtgøre at ethvert f som opfylder dem er Frobeniusfunktion for en - og paanær Isomorfi kun en - endelig abelsk Gruppe.

For det første ses at det vil være tilstrækkeligt at betragte Grupper hvis Orden er Potens af et fast Primtal p. Thi ifølge Basissætningen kan den abelske Gruppe skrives som direkte Produkt af saadanne Grupper (med forskellige p) og da f for det direkte Produkt er Produktet af de forskellige Faktorers f, og disse ifølge Sætningen forrige Side er Potenser af det samme p, og vi ifølge ^{0}) har at f er multiplikativ indses den ønskede Reduktion af Proble-

met. Ved denne Opspaltning fremkommer for et fast p et f, hvor man for $p^\beta \| r$ har $f(r) = f(p^\beta) = p^\gamma$, hvor $\gamma = \gamma(\beta)$ opfylder [1)-5)].

Vi skal nu vise, at et saadant f er Frobeniusfunktion for et direkte Produkt af cykliske Grupper hvis Ordener er Potenser af p, og at dette Produkt er entydigt bestemt. Og vi behøver kun at se paa Funktionsværdierne $f(p^\beta)$.

For en cyklisk Gruppe af Orden p^h er $f(p^\beta) = (p^\beta, p^h) = p^{\beta \wedge h}$, og for det direkte Produkt af saadanne Grupper skal deres f multipliceres, d. v.s. at Eksponenterne skal adderes. Grafen for $\gamma(\beta)$ bestaar af Liniestykker med heltallig Hældning, og hvis den har et Knæk i Punktet $\beta = h$ tager vi et Bidrag $\beta \wedge h$ (og hvis Hældningen falder med mere end 1 i Punktet tager vi flere Bidrag med dette h). Paa denne Maade kan det givne $\gamma(\beta)$ skrives som Sum af Bidrag $\beta \wedge h_j$, og man ser ogsaa umiddelbart at det kun er muligt paa denne ene Maade. □



Vi skal nu betragte ikke-abelske Grupper, og der er Forholdene desværre betydelig vanskeligere. Og medens vi lige har set at en abelsk Gruppes Struktur er bestemt ved dens Frobeniusfunktion, saa gælder noget tilsvarende ikke for de ikke-abelske, idet det kan ske at to ikke-isomorfe Grupper har samme f; den laveste Orden for hvilken Fænomenet indtræffer er 16.

Inden vi gaar videre skal vi minde om nogle gruppeteoretiske Begreber: Vi definerer en Relation $\sim$ ved at $P \sim Q$ saafremt der eksisterer et A saa $APA^{-1} = Q$. Relationen $\sim$ er reflexiv (da $EPE^{-1} = P$), den er symmetrisk (da $APA^{-1} = Q$ medfører $A^{-1}Q(A^{-1})^{-1} = P$) og den er transitiv (da $APA^{-1} = Q \wedge BQB^{-1} = R$ medfører $(BA)P(BA)^{-1} = R$). Det er altsaa en Ækvivalensrelation ved hvilken Gruppen opdeles i Ækvivalensklasser, ofte kaldt Frobeniusklasser. Man ser, at de abelske Grupper netop er dem for hvilke enhver Klasse kun bestaar af ét Element.

Ækvivalente Elementer P og Q har strukturelt de samme Egenskaber, thi for et fast A vil Afbildningen $X \mapsto AXA^{-1}$ være en Automorfi af Gruppen, hvilket let ses, en saakaldt"indre Automorfi" (Betegnelsen antyder at der ogsaa findes andre Automorfier ("ydre"), og at dette er Tilfældet fremgaar allerede af at abelske Grupper kan have andre Automorfier end Identiteten, det simpleste Tilfælde er $\tilde{C}_3$). Af det nævnte er det klart at E maa udgøre en Klasse for sig.

Man definerer Normalisatoren af P som $\tilde{N}_P = \{X: XP = PX\}$. Man ser let at $\tilde{N}_P$ er en Undergruppe. Nu er $APA^{-1} = BPB^{-1}$ ensbetydende med at $(A^{-1}B)P = P(A^{-1}B)$, d.v.s. at A og B giver det samme Q hvis og kun hvis A og B ligger i samme Sideklasse til $\tilde{N}_P$. Heraf følger at Antallet af Elementer som ligger i samme Klasse som P er lig $\frac{n}{|\tilde{N}_P|}$, nemlig Antallet af Sideklasser til $\tilde{N}_P$ (dens "Index"). Det er p.G.af Automorfien klart at ækvivalente Elementer har isomorfe Normalisatorer.

Da P kommuterer med $|\tilde{N}_P|$ Elementer og det samme gælder for ethvert Q i Klasse med P vil det,naar Q gennemløber en Klasse,gælde,at $|\tilde{N}_P| \cdot n/|\tilde{F}_P| = n$ af Produkterne QX er lig deres kommuterede XQ.

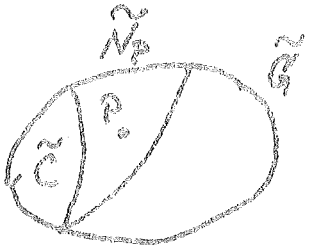
Altsaa: n•Antallet af Frobeniusklasser angiver hvormange af de

n^2 Stk. ordnede Par (A,B) som giver et kommutativt Produkt AB = BA.

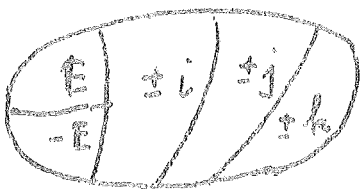
En Gruppes Centrum $\tilde{C}$ defineres som Mængden af Elementer der kommuterer med samtlige Gruppeelementer, altsaa $\tilde{C} = \{X;\ \tilde{N}_X = \tilde{G}\} = \bigcap_P \tilde{N}_P$. Det er aabenbart en Undergruppe, og abelsk, og man ser at det bestaar netop af de Elementer som hver for sig udgør en hel Frobeniusklasse.

Eksempel: Hvis man paa tilfældig Maade udtager et ordnet Elementpar (A,B) i en ikke-abelsk Gruppe, saa er Sandsynligheden for at AB = BA højst lig 5/8, og denne Vurdering er bedst mulig.

Bevis: Ifølge foregaaende Sætning gaar Paastanden ud paa at Antallet af Klasser højst er lig 5n/8.



Centrum giver $|\tilde{C}|$ Klasser, og de øvrige Elementer er fordelt i Klasser paa hver mindst to Elementer, altsaa højst $\frac{1}{2}(n - |\tilde{C}|)$ Klasser, og ialt højst $\frac{1}{2}(n + |\tilde{C}|)$ Klasser.



Tager man et $P \notin \tilde{C}$, saa er dels $\tilde{N}_p$ en ægte Undergruppe af $\tilde{G}$, og dels er $\tilde{C}$ en ægte Undergruppe af $\tilde{N}_P$ (thi da P kommuterer med sig selv haves $P \in \tilde{N}_P \setminus \tilde{C}$), hvoraf følger at $|\tilde{C}| \leqq \frac{n}{4}$. Indsættes dette i Vurderingen ovenfor faar man de ønskede 5n/8.

At Vurderingen ikke kan forbedres ses af Kvaternionegruppen. For den er $\tilde{C} = \{\pm E\}$ og $\tilde{N}_i = \{\pm 1, \pm i\}$ og analogt for $\tilde{N}_j$ og $\tilde{N}_k$, og dens 8 Elementer fordeles i de 5 Klasser vist paa nederste Figur. □

Eksempel: Vi vil betragte $\tilde{S}_5$. Her er n = 120. Et Gruppeelement er en Permutation af 5 Elementer, og den kan som bekendt fremstilles ved Cykler saaledes at fx (a b c)(d e) betyder

der Permutationen $\downarrow \begin{bmatrix} a & b & c & d & e \\ b & c & a & e & d \end{bmatrix}$. Rækkefølgen af Cyklerne er ligegyldig, og vi vil kun interessere os for de forskellige mulige Opdelinger af 5 Elementer i Cykler.

Tabellen nedenfor angiver de forskellige Muligheder, og for hver af dem de paagældende Permutationers Orden og Antallet af de paagældende Permutationer (altsaa Antallet af Maader man kan placere Bogstaver a,b,c,d,e i Cyklerne saaledes at der fremkommer forskellige Permutationer; det er en triviel kombinatorisk Opgave, men kontroller Angivelserne !).

	Orden	g	Antal	
(.)(.)(.)(.)(.)	1	1	1	(Identiteten=E)
(. .)(.)(.)(.)	2	25	10	(Transpositioner)
(. .)(. .)(.)	2		15	
(. . .)(.)(.)	3	20	20	
(. . .)(. .)	6	20	20	
(. . . .)(.)	4	30	30	
(. . . . .)	5	24	24	
		Ialt	120	

Det er let at se (og iøvrigt bekendt fra tidligere Kurser) at hver af disse 7 Parentesinddelinger giver en Frobeniusklasse, og der er altsaa $7 \cdot 120 = 840$ kommutative blandt de ialt 14400 Produkter AB.

Lad os tabellægge $g(r)$ og $f(r)$ for Divisorerne r i 120.

r	1	2	3	4	5	6	8	10	12	15	20	24	30	40	60	120
g(r)	1	25	20	30	24	20	.	.	.	.	.	.	.	.	.	.
f(r)	1	26	21	56	25	66	56	50	96	45	80	96	90	80	120	120

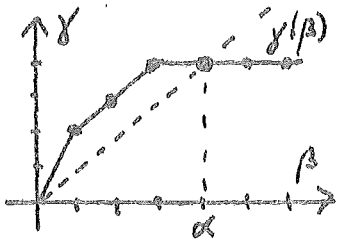
Af dette Eksempel ser man hvor uregelmæssig Funktionen f kan være for en dog meget simpel og nærliggende Gruppe, men man

faar samtidig en Illustration til Gyldigheden af den følgende vigtige Sætning.

Frobenius' Sætning: For en Gruppe af Orden n gælder for enhver Divisor r i n at r gaar op i f(r).

Da det tidligere er nævnt at man for ethvert r har f(r) = f((r,n)), saa kan Sætningen aabenbart ogsaa udtrykkes: For alle r gælder $(r,n) \mid f(r)$, hvor n er Ordenen og f er Frobenius-funktionen for Gruppen.

For r = n gælder Sætningen da f(n) = n ifølge Lagrange. For r = 1 gælder Sætningen trivielt. For en abelsk Gruppe af Orden p^α gælder Sætningen idet man (med Benævnelserne fra S.119) har at $\beta \leqq \alpha$ medfører $\beta \leqq \gamma(\beta)$ (se Fig.) og Sætningens almene Gyldighed for abelske Grupper følger saa direkte af at f er multiplikativ.



Bevis for Sætningen: For n = 1 gælder Sætningen, og Beviset skal nu ske ved Induktion efter n. For r = n gælder Sætningen og for en fast Gruppe af Orden n vil vi benytte nedadgaaende Induktion efter r (gennemløbende Divisorerne i n). Vi betragter $r < n$, og til dette findes et Primtal p saa $pr \mid n$ og vore Induktionsforudsætninger er at $pr \mid f(pr)$ og at Sætningen gælder for Grupper af Orden mindre end n.

Vi sætter $r = p^\alpha \cdot s$, hvor $p \nmid s$, og saa skal vi vise [1]) at $p^\alpha \mid f(r)$ og [2]) at $s \mid f(r)$, og som Forudsætning har vi at $p^{\alpha+1}s$ gaar op i $f(p^{\alpha+1}s)$.

[1]) kan hurtigt klares: Da $f(r) = \sum g(d)$, hvor d gennemløber Divisorerne i r, faar vi at $f(pr) - f(r) = f(p^{\alpha+1}s) - f(p^\alpha s)$ bliver $\sum g(k)$, hvor k er Produkt af $p^{\alpha+1}$ og en Divisor d i s. Men da $g(p^{\alpha+1}d)$ er delelig med $\varphi(p^{\alpha+1}d) = \varphi(p^{\alpha+1}) \cdot \varphi(d)$

og $\varphi(p^{\alpha+1}) = p^{\alpha}\cdot(p-1)$ vil p^{α} gaa op i $f(pr) - f(r)$, og ifølge Induktionsforudsætningen gaar det altsaa ogsaa op i $f(r)$.

[2]) er sværere, og først skal vi benytte Sætningen øverst S.113. Ifølge den er $f(p^{\alpha}s)$ lig Antallet Par (P,Q) som kommuterer og hvor $P^{p^{\alpha}} = E$ og $Q^s = E$. For et fast P skal altsaa $Q \in \tilde{N}_P$ og $Q^s = E$, hvilket er opfyldt af $f_{\tilde{N}_P}(s)$ Stk. Q.

Enten er $\tilde{N}_P = \tilde{G}$, d.v.s. at P tilhører Centrum $\tilde{C}$. Da ogsaa krævedes $P^{p^{\alpha}} = E$ bliver Antallet saadanne P lig $f_{\tilde{C}}(p^{\alpha})$, og for hvert af dem har vi $f(s)$ Stk. Q, saa det samlede Antal af disse Par (P,Q) bliver lig $f_{\tilde{C}}(p^{\alpha})\cdot f(s)$, og da $\tilde{C}$ er abelsk har det Formen $p^{\gamma}\cdot f(s)$, (at evt. $\gamma = 0$ vil ikke genere).

Eller $\tilde{N}_P$ er en ægte Undergruppe af $\tilde{G}$; saa kan vi ifølge Induktionsforudsætningen anvende Frobenius' Sætning paa $\tilde{N}_P$, og vi vil vise at s gaar op i Antallet af disse Par (P,Q). Nu tager vi en hel Klasse af disse P sammen, den indeholder $n/|\tilde{N}_P|$ Elementer, og giver et samlet Bidrag paa $(n/|\tilde{N}_P|)\cdot f_{\tilde{N}_P}(s)$ Stk. Par (P,Q). Frobenius' Sætning (anden Formulering) anvendt paa $\tilde{N}_P$ giver saa at dette Antal er deleligt med $(n/|\tilde{N}_P|)\cdot(|\tilde{N}_P|,s) = (n,(n/|\tilde{N}_P|)\cdot s)$ som er delelig med s (da begge Komponenter er det). Tilsammen faas at $f(p^{\alpha}s) = p^{\gamma}\cdot f(s)$ + Mult.af s; for $f(p^{\alpha+1}s)$ gælder et Udtryk af samme Art, og da dette ifølge Induktionsforudsætning er deleligt med s vil $f(s)$ ogsaa være det, og dermed ogsaa $f(p^{\alpha}s)$. □

Paa dette Sted kan vi passende give et Bevis for den berømte Wedderburns Sætning (W.1882-1948): Ethvert endeligt Legeme er kommutativt.

Det er tidligere (S.45) bemærket, at dette medfører at ethvert endeligt Legemes multiplikative Gruppe er cyklisk.

(Uden Bevis skal det nævnes, at af endelige Legemer findes der

(paanær Isomorfi) for enhver Primtalpotens p^{α} netop ét Legeme med p^{α} Elementer, og der findes derudover ikke andre, idet Elementtallet som bekendt skal være en Potens af Karakteristikken, der er et Primtal).

Bevis: Dersom $(\tilde{L},+,\cdot)$ er et Legeme med $\tilde{M}$ som Dellegeme, saa kan $\tilde{L}$ opfattes som et Vektorrum over $\tilde{M}$, idet ethvert $L \in \tilde{L}$ paa netop én Maade kan skrives paa Formen

$$L = M_1 \cdot L' + M_2 \cdot L'' + \ldots + M_h \cdot L^{(h)} ,$$

hvor $L', \ldots, L^{(h)}$ er en Basis for $\tilde{L}$ over $\tilde{M}$, og hvor $M_1, \ldots, M_h$ kan variere frit indenfor $\tilde{M}$, og h er Vektorrummets Dimension; ved dette (velkendte) Bevis skal man blot konsekvent placere M-Faktorerne t.v. i Produkter. Følgelig er $|\tilde{L}| = |\tilde{M}|^h$.

Lad nu $(\tilde{L},+,\cdot)$ være et endeligt, (gerne ikke-kommutativt) Legeme; det har den multiplikative Gruppe $(\tilde{L}^*,\cdot)$, og vi skal vise at denne er kommutativ.

For et $P \in \tilde{L}^*$ tager vi dets Normalisator i $(\tilde{L}^*,\cdot)$ og betegner den $\tilde{N}_P^*$, og suppleret med 0-Elementet betegner vi den $\tilde{N}_P$. Da er $\tilde{N}_P$ et Dellegeme af $(\tilde{L},+,\cdot)$: M.H.t. Multiplikationen er det i Orden da $\tilde{N}_P^*$ er en Undergruppe af $(\tilde{L}^*,\cdot)$, og m.H.t. Additionen ses det let, idet $\tilde{N}_P$ er stabil overfor Subtraktion da $[XP = PX \wedge YP = PY] \Rightarrow (X-Y)P = XP-YP = PX-PY = P(X-Y)$ (Beviset ogsaa gyldigt selvom X eller Y skulde være 0).

Saa er ogsaa $\tilde{C} = \bigcap_P \tilde{N}_P$ et Dellegeme baade i $\tilde{L}$ og i alle $\tilde{N}_P$. Og her er $\tilde{C} = \tilde{C}^* \cup \{0\}$, hvor $\tilde{C}^*$ er Centrum i den multiplikative Gruppe $(\tilde{L}^*,\cdot)$. Dersom $|\tilde{C}| = c$, saa er altsaa $|\tilde{L}| = c^h$ og ethvert $|\tilde{N}_P|$ er af Form $|\tilde{N}_P| = c^n$, og de tilsvarende multiplikative Grupper er af Ordener $|\tilde{C}^*| = c-1$, $|\tilde{L}^*| = c^h-1$ og $|\tilde{N}_P^*| = c^n-1$.

Vi betragter nu Opdelingen af den multiplikative Gruppe $\tilde{L}^*$ i Frobeniusklasser. I hver Klasse er Elementtallet af Formen

$$\frac{|\tilde{L}^*|}{|\tilde{N}_p^*|} = \frac{c^h - 1}{c^n - 1} \quad ,$$

hvor ethvert n er Divisor i h (da $\tilde{N}_p$ var Dellegeme af $\tilde{L}$). Her kan n = h forekomme, nemlig for de Klasser der kun bestaar af ét Element, altsaa Centrumelementerne, og dem er der c-1 Stk. af. I de øvrige Brøker vil n være en ægte Divisor i h, men vi skal godtgøre at der ikke findes nogen Brøker af den Slags, altsaa at Centrum udfylder hele Gruppen, som saa er abelsk, og desuden har vi at n = 1.

Vi har $|\tilde{L}^*| = c^h - 1$. Men $c^h - 1 = \prod \phi_d(c)$, hvor d gennemløber Divisorerne i h (se om Cirkeldelingspolynomier, S.81), og dette Tal er (indenfor $\mathbb{Z}$) deleligt med $\phi_h(c)$. Og ligeledes vil $\phi_h(c)$ gaa op i enhver Brøk $(c^h-1)/(c^n-1)$ hvor n er ægte Divisor i h, idet Brøkens Værdi er $\prod \phi_d(c)$ hvor d gennemløber de Divisorer i h som ikke gaar op i n. Men for h > 1 vil $\phi_h(c) \neq c-1$, da $\phi_h(c) \geq c$ (se S.85). Dermed har vi for h > 1 en Modstrid med Ligningen

$$c^h - 1 = (c - 1) + \sum \frac{c^h - 1}{c^n - 1}$$

som udtrykker at Antallet af Elementer i $\tilde{L}^*$ er lig Antallet af Elementer i Centrum plus Summen af Antallene i de Klasser som har mere end ét Element.

Beviset skyldes Wedderburn, som dog i St.f. Cirkeldelingspolynomier benyttede at dermed stærkt beslægtet Udsagn af Blichfeldt (B.18 -19 , dansk-amk.) om Divisorer i Udtryk c^k-1. □

Lad os betragte endnu et Par gruppeteoretiske Sætninger som har nær Forbindelse med talteoretiske Begreber.

Sylows Sætning: (S.1832-1918,norsk) Dersom en Gruppes Orden er delelig med p^α, saa findes der Undergrupper af Orden p^α, og deres Antal er $\equiv 1 \pmod{p}$.

For $\alpha = 1$ er Paastanden en simpel Konsekvens af Frobenius' Sætning. Thi Undergrupper af Orden p er cykliske, og to forskellige af dem har kun E fælles, og iøvrigt indeholder hver p-1 fra E forskellige Elementer. Hvis Antallet af disse Undergrupper er h har vi altsaa $g(p) = h\cdot(p-1)$, og dermed $f(p) = 1 + h\cdot(p-1)$, og da dette Antal ifølge Frobenius skal være deleligt med p finder vi $h \equiv 1 \pmod{p}$, hvilket paastodes.

Bevis: Vi har Gruppen $(\tilde{G},\cdot)$ med $|\tilde{G}| = n$, og i denne betragter vi Delmængder $\tilde{M}$ som indeholder Etelementet E.

Vi sætter $\tilde{M} \sim \tilde{M}_1$ dersom der findes et X saa $X\tilde{M} = \tilde{M}_1$. Relationen $\sim$ er reflexiv (da $\tilde{M} = E\tilde{M}$), symmetrisk (da $X\tilde{M} = \tilde{M}_1 \Rightarrow X^{-1}\tilde{M}_1 = \tilde{M}$) og transitiv (da $[X\tilde{M} = \tilde{M}_1 \wedge Y\tilde{M}_1 = \tilde{M}_2] \Rightarrow (YX)\tilde{M} = \tilde{M}_2$) og vi faar derfor Ækvivalensklasser (her af Delmængder $\tilde{M}$!).

Paa sædvanlig Maade udregner vi Antallet af Mængder $\tilde{M}$ indenfor en Ækvivalensklasse: vi har $X\tilde{M} = X_o\tilde{M} \Leftrightarrow (X_o^{-1}X)\tilde{M} = \tilde{M}$, og hver Mængde i Klassen frembringes altsaa for r Stk. X, hvor r er Antallet Y for hvilke $Y\tilde{M} = \tilde{M}$; det samlede Antal X for hvilke $X\tilde{M}$ er en af de Mængder vi betragter er $|\tilde{M}|$ (da vi jo maa have $X^{-1} \in \tilde{M}$ for at E kan tilhøre $X\tilde{M}$, saaledes som det forlangtes). Antallet Elementer i Klassen bliver derfor $|\tilde{M}|/r$, og er altsaa en Divisor i $|\tilde{M}|$.

Nu er $\tilde{M}$ en Undergruppe hvis og kun hvis $r = |\tilde{M}|$, thi dette betyder jo at (smlgn. ovenfor) ethvert $Y = X^{-1} \in M$ giver $Y\tilde{M} = \tilde{M}$, og altsaa at $\tilde{M}$ er stabil ved Division fra venstre (hvilket medfører at $\tilde{M}$ ogsaa er stabil ved Division fra højre, thi naar $A,B \in \tilde{M}$ medfører $A^{-1}B \in \tilde{M}$ faas med $B = A$ at $E \in \tilde{M}$, og dernæst med $B = E$ at $A^{-1} \in \tilde{M}$ saa man kan gaa over til reciprokke, og dermed at $AB^{-1} \in \tilde{M}$).

At $\tilde{M}$ er en Undergruppe er følgelig ensbetydende med at $\tilde{M}$ er al-

ne i sin Ækvivalensklasse. Og for de øvrige Klasser er Antallet af Mængder en Divisor i $|\tilde{M}|$.

Vi betragter nu alle Mængder $\tilde{M}$ forhvilke $|\tilde{M}| = p^{\alpha}$. Da det krævedes at $E \in \tilde{M}$ bliver det Antallet af Maader vi kan udtage $p^{\alpha}-1$ Elementer blandt $n-1$. Og endvidere er en Divisor i p^{α} enten lig 1 eller et Multiplum af p. Følgelig

$$\binom{n-1}{p^{\alpha}-1} = \text{Ant.Undergr. af Orden } p^{\alpha} \quad + \quad \text{Mult. af p} \quad .$$

Direkte at udregne Binomialkoefficienten modulo p er ubehageligt (Udtrykket for den vil indeholde Potenser af p i baade Tæller og Nævner), men det kan omgaas ved at betænke at Formler gælder for enhver Gruppe med n Elementer, og hvis vi tager den cykliske ved vi, at Antallet af Undergrupper med p^{α} Elementer er lig 1 for $p^{\alpha} | n$ og lig 0 for $p^{\alpha} \nmid n$. □

Vi skal sluttelig se lidt paa Spørgsmaalet om Antallet K(n) af (ikke-isomorfe) Grupper af Orden n. Foran (S.112) er givet en Tabel med Værdier for $n \leqq 12$. Vi ved at for Primtal p er $K(p) = 1$ (den cykliske Gruppe).

Lad os godtgøre at $K(p^2) = 2$ (nemlig $\tilde{C}_{p^2}$ og $\tilde{C}_p \times \tilde{C}_p$, abelske). Ifølge Basissætningen er der af abelske kun de to nævnte, og vi vil vise at der ikke findes nogen ikke-abelske. Antallet Elementer i en Frobeniusklasse er en Divisor i n, altsaa lig 1, p eller p^2, men det sidste er udelukket, da vi ved at E er ene i sin Klasse. Ialt findes p^2 Elementer, og der er derfor mindst p Klasser paa 1 Element, altsaa $|\tilde{C}| \geqq p$. Men $|\tilde{C}| = p$ er udelukket, thi som paa S.121 (øverste Fig.) ses at i en ikke-abelsk Gruppe er $\tilde{C}$ ægte Undergruppe i en Normalisator som igen er ægte Undergruppe i hele Gruppen. □

Med lignende Argumenter (og evt. en spæd Brug af Sylows og Frobenius' Sætninger) kan man se at $K(2p) = 2$. Grupperne er den cykliske $\mathfrak{C}_{2p} = \mathfrak{C}_2 \times \mathfrak{C}_p$, og Diedergruppen $\mathfrak{D}_p$ (ikke-abelsk for $p > 2$).

For $(r,s) = 1$ er $K(rs) \geq K(r) \cdot K(s)$, saa at K er "supermultiplikativ". Bevis: Hvis $(\mathfrak{A}, \circ)$ og $(\mathfrak{B}, \circ)$ er Grupper af Orden hhv. r og s, saa er det direkte Produkt $(\mathfrak{A}, \circ) \times (\mathfrak{B}, \circ)$ af Orden rs, og det har netop én Undergruppe af Orden r og denne er isomorf med $(\mathfrak{A}, \circ)$, fordi et Par (A,B) kun kan have en Orden som gaar op i r saafremt $B = E_B$; ligeledes har det netop én Undergruppe af Orden s og den er isomorf med $(\mathfrak{B}, \circ)$. Naar vi lader $(\mathfrak{A}, \circ)$ og $(\mathfrak{B}, \circ)$ gennemløbe de hhv. K(r) og K(s) forskellige Undergrupper af Orden hhv. r og s faar vi $K(r) \cdot K(s)$ Stk. Produktgrupper af Orden rs, og disse er alle forskellige da de har forskellige Par Undergrupper af Ordener r og s. □

Som en Vurdering den anden Vej kan vi nævne at $K(n) \leq n^{n^2}$. Det ses let, idet en sædvanlig Gruppemultiplikationstavle har n^2 Felter som hver er udfyldt med et af de n Gruppeelementer. Saadanne mere overfladiske Vurderinger af K(n) kan let forbedres, men en præcis Bestemmelse af K-Funktionen er næppe opnaaelig. De abelske Gruppers Antal kan ret let bestemmes af Basissætningen, men de langt mere talrige ikke-abelske volder Problemer. Som Eksempel kan nævnes, at medens det let ses at der findes 11 abelske Grupper af Orden 64, saa har K(64) i den tidligere Litteratur været angivet til 294, men en fornyet Undersøgelse som er publiceret 1964 angiver det (formodentlig) rigtige Tal 267. Et Resultat som kræver et lidt større Bevis er følgende Sætning:

Széles Sætning: Nødvendigt og tilstrækkeligt for at K(n) = 1 (S.19 -) er det at $(n, \varphi(n)) = 1$.

Bevis: Indledningsvis bemærker vi, at dersom $p^{\alpha} \| n$ med et α større end 1, saa er baade n og $\varphi(n)$ delelige med $p^{\alpha-1}$, saa $(n,\varphi(n)) > 1$. Men samtidig er $K(n) > 1$, thi p.G.a. Supermultiplikativiteten er $K(n) \geq K(p^{\alpha})$, og dette er større end 1 fordi $\tilde{C}_{p^{\alpha}}$ og $\tilde{C}_p \times \tilde{C}_p \times \ldots \times \tilde{C}_p$ er forskellige abelske Grupper af Orden p^{α}.

Vi behøver derfor kun at betragte kvadratfri n.

Lad os antage $(n,\varphi(n)) = 1$. Vi vil vise, at for $r|n$ gælder $f(r) = r$, hvilket medfører at Gruppen er cyklisk (S.114-115), og der er altsaa kun denne ene Gruppe. Vi har $f(n) = n$ og vi vil benytte nedadgaaende Induktion, altsaa antage at $f(rp) = rp$ og vise at $f(r) = r$ idet $rp|n$; da $p-1$ gaar op i $\varphi(n)$ vil Udgangsforudsætningen medføre at $(p-1,r) = 1$.

Vi benytter Forbindelsen mellem f og g paa lignende Maade som i Beviset for Frobenius' Sætn. ([1]), S.123): $f(rp) - f(r) = rp - f(r) = \sum g(dp)$, hvor d gennemløber Divisorerne i r (her benyttedes at $(r,p) = 1$, opfyldt da n kvadratfri). Hvert Led $g(dp)$ er deleligt med $\varphi(dp)$ og altsaa med $\varphi(p) = p-1$, og Summen er positiv da $g(p) > 0$, fx p.G.a. Sylow. Ifølge Frobenius har $f(r)$ Formen $h \cdot r$, og derfor $rp - f(r) = r \cdot (p-h)$, og da det samtidig skal være positiv og deleligt med $p-1$, som er primisk med r, maa vi have $h = 1$ og dermed $f(r) = r$, hvormed denne Del af Beviset er ført.

Lad os antage $(n,\varphi(n)) > 1$. Det medfører at n er delelig med et Produkt pq af to Primtal, hvor $q|p-1$. Vi vil vise at der eksisterer en ikke-abelsk Gruppe af Orden pq, saa at $K(pq) > 1$, hvilket p.G.a. Supermultiplikativiteten medfører at $K(n) > 1$.

Da $(\mathbb{Z}_p^*, \cdot)$ er cyklisk af Orden $p-1$ findes i denne Gruppe et $T \neq E$ for hvilket $T^q = E$. Vi konstruerer nu en Gruppe, hvis Elementer skal være Par (A,B) med $A \in \mathbb{Z}_p$ og $B \in \mathbb{Z}_q$ og med følgende Produktdannelse (betegnet med $\circ$):

$$(A,B) \circ (C,D) = (A + C \cdot T^B,\ B + D).$$

Man ser at Produktet er veldefineret, Eksponenten B er ganske vist ikke et Tal, men en Restklasse modulo q, men da $T^q = E$ er det ligesaagodt, og første Komponent tilhører igen $\mathbb{Z}_p$ og anden Komponent tilhører $\mathbb{Z}_q$. Der findes et Neutralelement, nemlig $(0,0)$ (baade fra højre og venstre), og (A,B) har et inverst (baade fra højre og venstre), nemlig $(-A \cdot T^{-B}, -B)$. Kompositionen er associativ idet $(A,B) \circ (C,D) \circ (E,F)$ bliver lig $(A+C \cdot T^B + E \cdot T^{B+D}, B+D+F)$ hvorledes det end udregnes. Gruppens Orden er $p \cdot q$. Den er ikke abelsk, $(E,0) \circ (0,E) = (E,E)$ og $(0,E) \circ (E,0) = (T,E)$. □

Konstruktionen minder om det direkte Produkt $(\mathbb{Z}_p,+) \times (\mathbb{Z}_q,+)$, og man ser at dersom vi i St.f. T havde indsat E saa var Kompositionsreglen blevet til $(A,B) \circ (C,D) = (A+C, B+D)$ og vi havde det direkte Produkt.

Man bemærker at $q = 2$ kan bruges sammen med et vilkaarligt ulige p, og man kan let overbevise sig om at den Gruppe som derved fremkommer bliver isomorf med Diedergruppen $\tilde{D}_p$.

Som Taleksempel ses, at der af Orden 15 kun findes den cykliske Gruppe, medens der af Orden 21 findes en ikke-abelsk Gruppe.

Eksempel til Sylows Sætning: Gruppen $\tilde{A}_4$. $n = 12$

Orden af Undergrupper	1	2	3	4	6	12
Antal Undergrupper	1	3	4	1	0	1

KAPITEL VII : Mere om algebraiske Kongruenser.

Lad os betragte algebraiske Ligninger i en Restklassering $(\mathbb{Z}_n,+,\cdot)$, altsaa Ligninger af Typen

$$A(X) = A_h X^h + A_{h-1} X^{h-1} + \ldots + A_1 X + A_o = 0,$$

hvor alle Bogstaverne betegner Elementer i $(\mathbb{Z}_n,+,\cdot)$. Udtrykt i $\mathbb{Z}$ bliver Opgaven

$$a(x) = a_h x^h + a_{h-1} x^{h-1} + \ldots + a_1 x + a_o \equiv 0 \pmod{n},$$

som jo netop føres over i den foregaaende ved Homomorfien $(\mathbb{Z},+,\cdot) \rightarrow (\mathbb{Z},+,\cdot)/(n) = (\mathbb{Z}_n,+,\cdot)$.

Der er her Tale om Polynomier over en Ring som ikke nødvendigvis er et Legeme. Stadig gælder

Dersom P er Rod i A(X), saa er (X - P) Faktor i A(X).

Bevis: $A(X) = A_h X^h + \ldots\ldots\ldots + A_1 X + A_o$

$0 = A_h P^h + \ldots\ldots\ldots + A_1 P + A_o$

Subtrakt: $A(X) = A_h(X^h - P^h) + \ldots\ldots\ldots + A_1(X-P)$,

hvori (X-P) er Faktor. □

Men den entydige Faktorisering af Polynomier er ikke sikret, og et Polynomium kan have flere Rødder end dets Grad.

Eksempel: I $(\mathbb{Z}_8,+,\cdot)$ er $X^2 - \textcircled{1} = (X - \textcircled{1})(X + \textcircled{1}) = (X - \textcircled{3})(X + \textcircled{3})$ og dette Polynomium har de 4 Rødder $\pm\textcircled{1}$ og $\pm\textcircled{3}$.

Ringen $(\mathbb{Z}_n,+,\cdot)$ har Nulelement $0 = \textcircled{0}$ og Etelement $E = \textcircled{1}$. De invertible Elementer i Ringen udgør med Multiplikation en Gruppe $(\mathbb{Z}_n^*,\cdot)$, den største Gruppe som kan udtages i den multiplikative Struktur $(\mathbb{Z}_n,\cdot)$.

Det er en almen Ringsætning, som let indses: 1) E er invertibel, 2) A invertibel $\Rightarrow$ A^{-1} invertibel og 3) A,B invertible medfører at $(AB)^{-1}$ eksisterer, nemlig lig $B^{-1}A^{-1}$. □

De invertible Elementer i Ringen er de "primiske Restklasser", d.v.s. de Restklasser $A = \overline{a}$, hvor $(a,n) = 1$.

Thi en Ligning $ax \equiv 1 \pmod{n}$ har en Løsning x hvis og kun hvis der findes x og y saa $ax - 1 = ny$, altsaa $1 = ax - ny$, ensbetydende med at 1 tilhører Idealet (a,n). □

Ordenen af Gruppen $(\mathbb{Z}_n^*, \cdot)$, altsaa Antallet af primiske Restklasser modulo n, er Funktionsværdien $\varphi(n)$ (se S.75).

Man ser Overensstemmelsen med det tidligere, idet for et Primtal p er $\varphi(p) = p-1$, og $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$; men for et sammensat n kan vi have Elementer som hverken er 0 eller invertible (sommetider kaldt"Nuldivisorer"), og $AB = 0$ er ensbetydende med at A er 0 eller at B er 0 eller at A og B begge er Nuldivisorer.

Eulers Generalisation af Fermats Sætning:

I $(\mathbb{Z}_n, \cdot)$ gælder for enhver primisk Restklasse A at $A^{\varphi(n)} = E$.

Udtrykt i $\mathbb{Z}$ lyder Sætningen: $(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$.

Bevis: Lagranges Sætning anvendt paa Gruppen $(\mathbb{Z}_n^*, \cdot)$. □

Eksempel: $n = 12$, $\varphi(n) = 4$, $a = 7$ primisk med 12.

$$7^4 = 2401 \equiv 1 \pmod{12}.$$

Hvis vi generaliserer det sidste af de tidligere givne Beviser for Fermats Sætning (S.42) føres vi til en anden Generalisation af Sætningen; først formulerer vi den almindeligt:

Lad M være en Mængde af Funktioner, som afbilder $\mathbb{Z}$, og som er stabil overfor Translation, altsaa $\psi(z) \in M \Rightarrow \psi(z+h) \in M$ for alle heltallige h. Dersom f(n) er Antallet ψ som er periodiske med Perioden n, saa gælder at $n \mid \sum_{d \mid n} \mu(d) \cdot f(\frac{n}{d})$.

Bevis: Lad g(d) være Antallet ψ som er periodiske med kortest Periode lig d, da er $f(n) = \sum_{d \mid n} g(d)$. Ifølge Möbius' Omvendingsformel er saa

$$g(n) = \sum_{d \mid n} \mu(d) \cdot f(\tfrac{n}{d}).$$

Men $g(n)$ er delelig med n, thi de ψ som har korteste Periode n kan samles i Klasser bestaaende af Funktioner som er ens paa-nær Translation, og hver Klasse vil indeholde n Funktioner, nemlig et Sæt $\psi(z), \psi(z+1), \ldots, \psi(z+n-1)$. □

Hvis vi lader M være Mængden af Funktioner $\psi : \mathbb{Z} \to \{1,2,\ldots,a\}$ faar vi $f(n) = a^n$, og dermed har vi

Generalisation af Fermats Sætning:

$$\forall_{a,n \in \mathbb{N}} : \; n \mid \sum_{d \mid n} \mu(d) \cdot a^{\frac{n}{d}} .$$

Da ethvert negativt a er kongruent modulo n med et positivt a er det klart, at Paastanden gælder for alle $a \in \mathbb{Z}$.

Eksempel: $n = 12$, $f(n) = a^n$, $g(12) = a^{12}-a^6-a^4+a^2$.

$a = 7$ giver $12 \mid 7^{12}-7^6-7^4+7^2 \equiv 0$ (da $7^4 \equiv 1$, se S.133)

$a = 8$ giver $12 \mid 8^{12}-8^6-8^4+8^2 \equiv 0$, stemmer, thi det er klart at 4 gaar op, og modulo 3 er det kongruent med $(-1)^{12}-(-1)^6-(-1)^4+(-1)^2 = 0$.

Fibonaccis og Lucas's Følger. Et ikke-trivielt Eksempel til den almene Sætning:

Lad M være Mængden af $\psi : \mathbb{Z} \to \{0,1\}$, men ψ maa ikke i to konsekutive Tal antage Værdien 1 (hvilket kan udtrykkes ved at $\psi(z) \cdot \psi(z+1) = 0$). M er aabenbart invariant overfor Translation. Lad os først bestemme $h(n)$ = Antallet af Afbildninger af $(1,2,\ldots,n)$ over i $\{0,1\}$ som opfylder den stillede Betingelse. Aabenbart er $h(1) = 2$ (da to mulige Værdier) og $h(2) = 3$ (Billedsættene kan være $(0,0)$, $(0,1)$ og $(1,0)$. For større n gælder $h(n) = h(n-1) + h(n-2)$, thi for $\psi(n) = 0$ er der $h(n-1)$ mulige Afbildninger af $1,2,\ldots,n-1$, og for $\psi(n) = 1$ maa vi have $\psi(n-1) = 0$ medens der er $h(n-2)$ mulige Afbildninger af $1,..,n-2$.

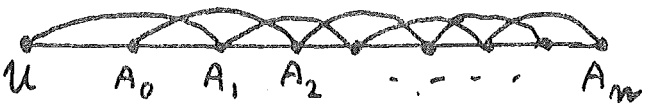
Hvis vi tilføjer en Funktionsværdi h(0) = 1 faar vi for $n \in \mathbb{N}_0$ en Følge af Funktionsværdier

1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610,...

bestemt udfra Udgangselementerne ved at ethvert senere Element er Summen af de to umiddelbart foregaaende.

Denne Følge er Fibonaccis Følge (Fibonacci = Leonardo fra Pisa, ca.1175-1250). F. kom til den som Model for Størrelsen af en Population af Kaniner udfra en simpel Antagelse om disse Dyrs Formeringsevne.

Men ogsaa ved mange andre Opgaver kan man møde denne Følge. Fx hvis man søger Antallet af Permutationer δ af Tallene $\{0,1,\ldots,n\}$ med Bibetingelsen $|\delta(j)-j| \leqq 1$ (altsaa Permutationer hvor ethvert Tal j er "lænket til sin egen Plads med en Kæde af Længde 1"); saa er aabenbart h(0) = 1, h(1) = 2 og h(n) lig h(n-1) + h(n-2), første Bidrag for $\delta(n) = n$ og andet Bidrag for $\delta(n) = n-1$ (hvoraf følger $\delta(n-1) = n$). Eller Antallet af Veje fra venstre til højre langs Linierne i hosstaaende Graf,



hvor man ogsaa umiddelbart ser at Antallet h(n) opfylder de samme Betingelser.

Vi vender nu tilbage til den oprindelige Opgave, idet vi ønsker at en Afbildning $\Psi: \{1,2,\ldots,n\} \to \{0,1\}$ med Bibetingelsen $\Psi(z) \cdot \Psi(z+1) = 0$ skal kunne gentages periodisk saaledes at Bibetingelsen ogsaa er opfyldt i Sammensætningspunkterne. Den eneste Maade det kan gaa galt paa er aabembart ved at $\Psi(1) = 1$ og $\Psi(n) = 1$ hvilket medfører at $\Psi(2) = \Psi(n-1) = 0$, medens Ψ er vilkaarlig paa de n-4 midterste Pladser. Altsaa er $f(n) = h(n) - h(n-4)$. Heraf ses, at for $n > 4$ vil f opfylde den samme Rekurrensligning $f(n) = f(n-1) + f(n-2)$ som h opfylder. Idet

de første Funktionsværdier let bestemmes direkte og ogsaa ses at opfylde Ligningen faar man for $n \in \mathbb{N}$ en Følge af Funktionsværdier f(n)

n	1	2	3	4	5	6	7	8	9	10	11	12	13 ..
f(n)	1	3	4	7	11	18	29	47	76	123	199	322	521 ..

som er den saakaldte Lucas' Følge (L.1842-1891).

For denne Følge gælder den almene Sætning

$$n \mid \sum_{d \mid n} \mu(d) \cdot f(\tfrac{n}{d}) \ .$$

Vi kan fx betragte n = 12: saa er $\mu(d) \neq 0$ for d = 1,2,3,6 og Højresiden bliver 322-18-7+3 = 300 som er delelig med 12. (Erstattes f med h vil n ikke gaa op: $12 \nmid 377-21-8+3 = 351$, og n vil heller ikke gaa op hvis man translaterer $f(n) \mapsto f(n+1)$, hvilket er bemærkelsesværdigt idet det jo gælder i den generaliserede Fermats Sætning (S.134) naar man erstatter $f(n) = a^n$ med $f(n+1) = a^{n+1}$, hvorved alle Led blot multipliceres med a).

Saadanne rekurrente Følger er et interessant (men i tidligere Tider lidt foragtet) Studieomraade. Vi skal ikke her gaa nærmere ind paa det. Vi kan dog bemærke, at Funktioner g der som f og h ovenfor opfylder Ligningen $g(n) = g(n-1) + g(n-2)$ aabenbart kan skrives paa Formen $g(n) = \alpha \cdot \xi^n + \beta \cdot \eta^n$, hvor ξ og η er Rødderne i Ligningen $x^2 = x + 1$ (Følgerne udgør et 2-dimensionalt Vektorrum, da 2 Udgangsværdier kan vælges frit og dette ogsaa stemmer med at der er 2 Koefficienter α og β). Generelt vil en Rekurrensligning $g(n) = a_1 g(n-1) + \ldots + a_k g(n-k)$ paa samme Maade svare til en Ligning $x^k = a_1 x^{k-1} + \ldots + a_k$. Umiddelbar talteoretisk Interesse har det, at en rekurrent Følge (med heltallige Koefficienter) aabenbart for ethvert r bliver periodisk modulo r, thi p.G.af Skuffeprincippet vil der være et Sæt Rester mod.r som gentages, og p.G.af Rekurrensligningen vil det forplante sig som en Periodicitet i hele Følgen. Eksemplet slut.

Gauss' Generalisation af Wilsons Sætning: I $(\mathbb{Z}_n,+,\cdot)$ er Produktet af de primiske Restklasser lig +E eller -E (nemlig - for $n > 2$ - lig $(-E)^{\frac{1}{2}f}$, hvor f = Frobeniusfunktionsværdien f(2) i Gruppen $(\mathbb{Z}_n^*,\cdot)$).

For $n = 2$ findes kun den primiske Restklasse $E = -E$, saa begge Udtryk gælder.

For $n > 2$ og A invertibel gælder $A \neq -A$, idet $2A \neq 0$.

Dersom nu A er forskellig fra A^{-1} tager vi et saadant Par reciprokke Elementer sammen i Produktet, det giver ialt en Faktor E. Tilbage er de A for hvilke $A = A^{-1}$, d.v.s. $A^2 = E$, men hvis det gælder for A saa gælder det ogsaa for -A, og vi tager saa dem sammen, det giver en Faktor -E, hvoraf man ser Rigtigheden af Sætningen (med dens Eftersætning). □

Eksempel: n = 12. Repræsentanter for de primiske Restklasser er 1,5,7,11, og for dem alle gælder at Kvadratet $\equiv 1 \pmod{12}$, saa f = 4. Vi har $1\cdot5\cdot7\cdot11 = 385 \equiv 1 = (-1)^{\frac{1}{2}\cdot4} \pmod{12}$.

Lineære Kongruenser.

Hvis A er invertibel har Ligningen $AX = B$ netop én Løsning, nemlig $X = A^{-1}B$.

Udtrykt i $\mathbb{Z}$: For $(a,n) = 1$ har Kongruensen $ax \equiv b \pmod{n}$ netop én Løsningsrestklasse modulo n.

Eksempel: $7x \equiv 9 \pmod{12}$. Nu er $⑦^{-1} = ⑦$ (som nævnt syv Linier ovenfor), altsaa $x \equiv 7\cdot9 = 63 \equiv 3 \pmod{12}$.

Som Eksempler paa Sætninger om lineære Kongruenser (og samtidig som Eksempler paa mangelfuld Sætningsformulering) kan nævnes:

Det er tilladt at multiplicere en Kongruens med et Tal [idet Løsningsmængden i hvert Fald ikke formindskes derved].

og

Hvis man i en Kongruens $ax \equiv b \pmod{n}$ dividerer med et Tal h paa begge Sider af Kongruenstegnet, skal man samtidig dividere Modulen n med $d = (h,n)$ [for at Løsningsmængden skal være uændret].

Læst for sig er de understregede Sætninger meningsløse, men formulerede som man hyppigt vil gøre det; de $[\cdot\,\cdot]$-indrammede Eftersætninger maa med for at give Mening, som altsaa i den første er en Implikation $\Rightarrow$, i den anden en Biimplikation $\Leftrightarrow$.

Den første Sætning: $ax \equiv b \pmod{n} \Rightarrow hax \equiv hb \pmod{n}$ er triviel, og man ser let at man kan ikke slutte $\Leftarrow$.

Taleksempel: $6x \equiv 6 \pmod{12} \Rightarrow 12x \equiv 12 \pmod{12}$,
(x ulige) (x vilkaarlig)

Den anden Sætning ses let, idet $(h,n) = d$ medfører at $\frac{h}{d}$ og $\frac{n}{d}$ er primiske, og naar man saa sætter $a = ha_1$ og $b = hb_1$ ses at

Udgangspaastand: $n \mid ha_1x - hb_1$

$\Updownarrow$

$n \mid h(a_1x - b_1)$

$\Updownarrow$

$\frac{n}{d} \mid \frac{h}{d}(a_1x - b_1)$

$\Updownarrow$

Slutpaastand: $\frac{n}{d} \mid a_1x - b_1$

Taleksempel: $10x \equiv 10 \pmod{12} \Leftrightarrow x \equiv 1 \pmod{6}$ □

Moral: Man skal ikke formulere Sætninger om altfor simple Ting, men i Stedet blot tænke over hvad man foretager sig.

En lineær Kongruens kan altid løses ved Prøve, da der kun er endelig mange Restklasser at forsøge med, men der findes ogsaa

teoretiske Opstillinger med Kædebrøker eller andre Hjælpemidler. Lad os her give et praktisk Eksempel baseret paa Princippet: For en fælles Modul n er givet to Kongruenser

$$\text{I)}\quad ax \equiv b \qquad \text{og} \qquad \text{II)}\quad cx \equiv d \qquad \text{med} \quad a > c > 0,$$

vi danner $$\text{III)}\quad \left(a - \left[\frac{a}{c}\right]c\right)\cdot x \equiv b - \left[\frac{a}{c}\right]d \qquad (\text{mod}.n)$$

og man ser umiddelbart at $\text{I)} \wedge \text{II)} \Leftrightarrow \text{II)} \wedge \text{III)}$.

Paa denne Maade kan man formindske Koefficienten til x (idet man altsaa anvender "Euklids Algoritme" paa a og c).

Eksempel:

Løs $\text{II)}\quad 384\,x \equiv 856 \quad (\text{mod}.1000)$

Vi tilføjer $\text{I)}\quad 1000\,x \equiv 0 \quad (\text{mod}.1000)$ (indholdsløst Krav) og gaar frem som nævnt (Højresiden reduceres mod.1000):

I) - 2·II):	III)	$232\,x \equiv 288$
II) - III):	IV)	$152\,x \equiv 568$
III) - IV):	V)	$80\,x \equiv 720$
IV) - V):	VI)	$72\,x \equiv 848$
V) - VI):	VII)	$8\,x \equiv 872$
VI) - 9·VII):	VIII)	$0\cdot x \equiv 0$

Vi er endt med Koefficienten 0 paa Venstresiden (Euklids Algoritme slut); hvis vi ikke havde faaet 0 paa Højresiden havde der ikke været nogen Løsninger; nu har vi imidlertid faaet 0, saa VIII) er betydningsløs, og ialt har vi derfor

$$\text{II)} \Leftrightarrow \text{I)} \wedge \text{II)} \Leftrightarrow \text{VII)} \wedge \text{VIII)} \Leftrightarrow \text{VII)}$$

saa Opgavens Løsninger faas af $\text{VII)}\quad 8\,x \equiv 872 \quad (\text{mod}.1000)$; p.G.a. Euklids Algoritme maa Koefficienten til x, altsaa 8, være Divisor i n = 1000, og Kongruensen kan med en tidligere Sætning divideres med 8, og vi finder

$$x \equiv 109 \quad (\text{mod}.125).$$

Modulo 1000 er Løsningerne $x \equiv 109, 234, 359, 484, 609, 734, 859, 984$.

Simultane Kongruenser.

Antag $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r$, hvor alle n_j er parvis primiske. En Restklasse modulo n betegnes A og en Restklasse modulo n_j betegnes A_j. Nu er

$$x \equiv a \ (\mathrm{mod}.n) \Leftrightarrow n \mid x-a \Leftrightarrow \bigwedge_j : n_j \mid x-a \Leftrightarrow \bigwedge_j : x \equiv a \ (\mathrm{mod}.n_j).$$

Heraf ses at ethvert A er af Formen $\bigcap_j A_j$.
Lad os paa Mængden af Sæt $(A_1,\ldots,A_r)$ se paa Afbildningen $(A_1,\ldots,A_r) \mapsto \bigcap_j A_j$ (Billedet er en Delmængde af $\mathbb{Z}$). Ethvert af de n Stk. A kommer med som Billede, og da der ogsaa er $n_1 \cdot \ldots \cdot n_r = n$ Stk. Sæt $(A_1,\ldots,A_r)$ maa Afbildningen være en Bijektion over paa Mængden af Restklasser A.
Vi har dermed Den kinesiske Restklassesætning:
Hvis $n_1,\ldots,n_r$ er parvis primiske og $n = n_1 \cdot \ldots \cdot n_r$, saa vil Løsningerne til et System $x \equiv a_j \ (\mathrm{mod}.n_j)$, $j = 1,\ldots,r$, netop udgøre én Restklasse $x \equiv a \ (\mathrm{mod}.n)$. Omvendt: Enhver Restklasse $x \equiv a \ (\mathrm{mod}.n)$ er Løsningsmængde til et System af Kongruenser $x \equiv a_j \ (\mathrm{mod}.n_j)$, $j = 1,\ldots,r$.

Resultatet har været kendt fra Oldtiden (fx Opgaver af Typen: Hvis en Hær stilles op i Rækker med 7 Mand i hver bliver 2 Mand til overs, hvis den stilles op med 8 i hver Række bliver 5 Mand til overs, ... , Problem: hvor mange Mand er der ?), men da Princippet var navnløst, og man saa i nyere Tid har opdaget at det ogsaa har været kendt i det gamle Kina (der nævnes Sun Tse ca 250 e.Kr.) har man (omkring Midten af dette Aarhundrede) hæftet Navnet "den kinesiske Sætning" paa det (og dets Generalisationer i Algebraen), og det er jo praktisk som Betegnelse for noget ellers navnløst, som har vist sig betydningsfuldt.

I den sidste Del af Sætningen kunde vi specielt sætte alle a_j lig a (smlgn. Begyndelsen af Beviset for Sætningen), saa at den benyttede Afbildning bliver

$$(\textcircled{a}_{n_1}, \ldots, \textcircled{a}_{n_r}) \quad \longleftrightarrow \quad \textcircled{a}_n$$

og ligesaa

$$(\textcircled{b}_{n_1}, \ldots, \textcircled{b}_{n_r}) \quad \longleftrightarrow \quad \textcircled{b}_n \ .$$

Vi har Summen

$$(\textcircled{a+b}_{n_1}, \ldots, \textcircled{a+b}_{n_r}) \quad \longleftrightarrow \quad \textcircled{a+b}_n$$

og Produktet

$$(\textcircled{ab}_{n_1}, \ldots, \textcircled{ab}_{n_r}) \quad \longleftrightarrow \quad \textcircled{ab}_n \ ,$$

hvoraf vi ser at

$$\boxed{(\mathbb{Z}_{n_1},+,\cdot) \times \ldots \times (\mathbb{Z}_{n_r},+,\cdot) \ = \ (\mathbb{Z}_n,+,\cdot) \ .}$$

Venstresiden er det "direkte Produkt" (i Algebraen sommetider kaldt "Sum") af de anførte Ringe, d.v.s. den kartesiske Produktmængde $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ forsynet med Regnepperationer + og $\cdot$, som defineres som komponentvis Addition og Multiplikation, og hvor Lighedstegnet (som sædvanligt i denne Forbindelse) blot betyder Isomorfi.

Ved Hjælp af Sætningen kan Kongruensopgaver reduceres til Kongruenser modulo Primtalpotenser.

Eksempel: Løs $15x \equiv 51 \ (\mathrm{mod}.72) \ \wedge \ x \equiv 5 \ (\mathrm{mod}.28)$

$15x \equiv 51 \ (\mathrm{m}.9) \wedge 15x \equiv 51 \ (\mathrm{m}.8) \wedge x \equiv 5 \ (\mathrm{m}.4) \wedge x \equiv 5 \ (\mathrm{m}.7)$

$6x \equiv 6 \ (\mathrm{m}.9) \wedge 7x \equiv 3 \ (\mathrm{m}.8) \wedge x \equiv 5 \ (\mathrm{m}.4) \wedge x \equiv 5 \ (\mathrm{m}.7)$

$x \equiv 1 \ (\mathrm{m}.3) \wedge x \equiv 5 \ (\mathrm{m}.8) \wedge x \equiv 5 \ (\mathrm{m}.4) \wedge x \equiv 5 \ (\mathrm{m}.7)$

$x \equiv 1 \ (\mathrm{m}.3) \wedge x \equiv 5 \ (\mathrm{m}.8) \wedge x \equiv 5 \ (\mathrm{m}.7)$

$x \equiv 1 \ (\mathrm{m}.3) \wedge x \equiv 5 \ (\mathrm{m}.56)$

$x \equiv 61 \ (\mathrm{mod}.168)$

Qvod erat demonstrandum.

Andet Eksempel: Løs

$$x^4 + 29x^3 + 10x^2 - 28x - 45 \equiv 0 \pmod{33}$$

Den reduceres til

$$x^4 - 4x^3 + 10x^2 + 5x - 12 \equiv 0$$

Aabenbart er $x = 1$ Rod. Derfor

$$(x-1)(x^3 - 3x^2 + 7x + 12) \equiv 0 \pmod{33}$$

Vi spalter

$$(x-1)(x^3+x) \equiv 0 \ (\text{m}.3) \wedge (x-1)(x^3-3x^2-4x+1) \equiv 0 \ (\text{m}.11)$$

$(x-1)\cdot x\cdot(x^2+1) \equiv 0 \ (\text{m}.3)$ — ing. Løsn.

Altsaa

$$x \equiv 0,1 \pmod{3}$$

$(x-1)(x^3-3x^2-4x+12) \equiv 0 \ (\text{m}.11)$ — $x=3$ gaar op

$(x-1)(x-3)(x^2-4) \equiv 0 \ (\text{m}.11)$

$(x-1)(x-3)(x-2)(x+2) \equiv 0 \ (\text{m}.11)$

Altsaa

$$x \equiv 1,3,2,-2 \pmod{11}$$

Ifølge den kinesiske Sætning kan vi igen samle, og skal finde $2\cdot 4 = 8$ Restklasser modulo 33 som Løsning.

mod.3 \ mod.11	1	3	2	-2
0	12	3	24	9
1	1	25	13	31

Løsning:

$$x \equiv \begin{cases} 12 & 3 & 24 & 9 \\ 1 & 25 & 13 & 31 \end{cases} \pmod{33}.$$

□

Betingelsen for den kinesiske Sætning er $n = n_1 \cdot \ldots \cdot n_r$, hvor de forskellige n_j er parvis primiske. Man ser (smlgn. Slutningen af det sidste Eksempel), at

betragter man en algebraisk Kongruens $P(x) \equiv 0 \pmod{n}$ for forskellige n, men med fastholdt $P(x)$, saa er Antallet af Løsningsrestklasser modulo n til Kongruensen en multiplikativ Funktion af n.

Af Formlen □ med direkte Produkt af Ringe kan vi aflede Resultater for de indgaaende Grupper.

For de additive Grupper faar vi direkte

$$(\mathbb{Z}_{n_1},+) \times \ldots \times (\mathbb{Z}_{n_r},+) = (\mathbb{Z}_n,+),$$

men det overrasker ikke, thi Grupperne er alle cykliske, saa her staar blot $\tilde{C}_{n_1} \times \ldots \times \tilde{C}_{n_r} = \tilde{C}_n$, hvilket vi vidste i Forvejen.

For at faa Grupper ved Multiplikationen maa vi indskrænke os til de primiske Restklasser, men det sker samtidig paa begge Sider idet $(a,n_1) = 1 \wedge \ldots \wedge (a,n_r) = 1 \iff (a,n) = 1$ og Bijektionen var jo $(\textcircled{a}_{n_1}, \ldots, \textcircled{a}_{n_r}) \leftrightarrow \textcircled{a}_n$. Vi har saa

$$(\mathbb{Z}^*_{n_1}, \cdot) \times \ldots \times (\mathbb{Z}^*_{n_r}, \cdot) = (\mathbb{Z}^*_n, \cdot) .$$

For Gruppens Orden faar vi $\varphi(n_1) \cdot \ldots \cdot \varphi(n_r) = \varphi(n)$, i Overensstemmelse med at φ er multiplikativ.

Lad n have Primopløsningen $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. Vi kan da tage $n_1, \ldots, n_r$ som de indgaaende Primtalpotenser, og for at finde Strukturen af $(\mathbb{Z}^*_n, \cdot)$ maa vi derfor først kende Strukturen af en Gruppe $(\mathbb{Z}^*_{p^\alpha}, \cdot)$; for $\alpha = 1$ ved vi at Gruppen er cyklisk (multiplikativ Gruppe i Legemet $(\mathbb{Z}_p, +, \cdot)$).

<u>Den multiplikative Gruppe $(\mathbb{Z}^*_{p^\alpha}, \cdot)$ er cyklisk, undtagen naar p^α er en Potens af 2 som er større end 4; i dette Tilfælde er den det direkte Produkt af en cyklisk Gruppe af Orden $2^{\alpha-2}$ og en af Orden 2.</u>

Bevis: Ordenen af Gruppen er $\varphi(p^\alpha) = (p-1) \cdot p^{\alpha-1}$.

Nu har Gruppen i hvert Fald et Element $\textcircled{g}$ hvis Orden er delelig med $p-1$ (og dermed ogsaa et Element af Orden $p-1$), nemlig med g lig en Primitivrod modulo p (som vi ved eksisterer da $(\mathbb{Z}^*_p, \cdot)$ er cyklisk), thi $g^r \equiv 1 \pmod{p^\alpha} \Rightarrow g^r \equiv 1 \pmod{p} \Rightarrow p-1 \mid r$.

Dernæst vil vi vise, at Gruppen i det almindelige Tilfælde har et Element af Orden $p^{\alpha-1}$, og da $(p-1, p^{\alpha-1}) = 1$ følger heraf (S.45) at den har et Element af Orden $(p-1) \cdot p^{\alpha-1}$ og altsaa er cyklisk.

Som Element af Orden $p^{\alpha-1}$ kan vi benytte Restklassen $\overline{p+1}$.
For at vise dette godtgør vi først at (med en enkelt Undtagelse) vil, idet $h \in \mathbb{N}$ og p er et Primtal, Relationen $p^h \| m-1$ medføre $p^{h+1} \| m^p - 1$. Forudsætningen siger at $m = 1 + p^h \cdot A$, hvor $p \nmid A$, og heraf følger ved Binomialudvikling at

$$m^p = (1+A\cdot p^h)^p = 1 + p\cdot A\cdot p^h + \underbrace{\binom{p}{2}\cdot A^2\cdot p^{2h} + \binom{p}{3}\cdot A^3\cdot p^{3h} + \ldots}_{\text{Mult. af } p^{2h+1}}$$

hvori de sidste Led er delelige med $p^{2h+1} > p^{h+1}$ (fordi Binomialkoeffisienterne $\binom{p}{j}$ er delelige med p); dette beviser det nævnte. Undtagelsen fremkommer for $p = 2$, $h = 1$, hvor $\binom{p}{2} = 1$, og hvor vi har $(1+A\cdot 2)^2 = 1 + 4A + 4A^2$ hvor Summen af de to sidste Led altid er delelig med 8.

Lad os nu betragte Restklassen $\overline{p+1}$. Vi har

$$p \| (p+1)-1 \Rightarrow p^2 \| (p+1)^p - 1 \Rightarrow \ldots \Rightarrow p^{\alpha-1} \| (p+1)^{p^{\alpha-2}} - 1 \Rightarrow p^{\alpha} \| (p+1)^{p^{\alpha-1}} - 1$$

som viser at i $(\mathbb{Z}_{p^\alpha}^*, \cdot)$ vil ord $\overline{p+1} \nmid p^{\alpha-2}$ men at ord $\overline{p+1}$ gaar op i $p^{\alpha-1}$. Altsaa er ord $\overline{p+1}$ lig $p^{\alpha-1}$.

Undtagelsen for $p = 2$ bevirker at i $(\mathbb{Z}_8, \cdot)$ forekommer kun Ordenerne 2 og 1, og fx ord $\overline{5} = 2$. Derefter ruller Beviset ovenfor, og i $(\mathbb{Z}_{2^\alpha}^*, \cdot)$ er ord $\overline{5} = 2^{\alpha-2}$. Men Potenserne af $\overline{5}$ kan jo kun give Restklasser $\overline{a}$, hvor $a \equiv 1 \pmod 4$, og de øvrige primiske Restklasser kan saa faas ved at man som andet Frembringerelement tager $\overline{-1}$. Dermed har vi $(\mathbb{Z}_{2^\alpha}^*, \cdot)$ fremstillet som $(\{\overline{5}^s\}, \cdot) \times (\{\overline{-1}^t\}, \cdot)$, d.v.s. paa Formen $\tilde{C}_{2^{\alpha-2}} \times \tilde{C}_2$. □

For et vilkaarligt $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ er vi dermed helt klar over Strukturen af den multiplikative Gruppe, idet vi kan skrive den som direkte Produkt af cykliske.

Indenfor $(\mathbb{Z}_n^*,\cdot)$ kan vi nu let bestemme den maximale Elementorden $\rho(n)$ (ρ er kun en ad-hoc- Betegnelse), nemlig som det mindste fælles Multiplum af Ordenerne af de cykliske Grupper af hvilke den er opbygget. For $n = 1,2$ er $\rho(n)$ lig 1, men for alle større n er $\rho(n)$ lige fordi $\varphi(p^\alpha)$ er lige.

Eksempel: $n = 1400 = 8\cdot 7\cdot 25 = 2^3\cdot 7\cdot 5^2$.

$$(\mathbb{Z}_{1400}^*,\cdot) = (\mathbb{Z}_8^*,\cdot)\times(\mathbb{Z}_7^*,\cdot)\times(\mathbb{Z}_{25}^*,\cdot) = \tilde{C}_2 \times \tilde{C}_2 \times \tilde{C}_6 \times \tilde{C}_{20} .$$

Gruppens Orden er $\varphi(1400) = 480$. $\rho(n) = 60$.

For alle A i Gruppen er $A^{60} = E$ (Fermat-Euler giver kun $A^{480}=E$).

Eksempel: Find det største n for hvilket

$$(a,n) = 1 \Rightarrow a^{12} \equiv 1 \pmod{n}.$$

Det er aabenbart det samme som at spørge om det største n for hvilket $\rho(n) = 12$ (eller en Divisor i 12).

Facit: $n = 16\cdot 9\cdot 5\cdot 7\cdot 13 = 65520$

$$(\mathbb{Z}_{65520}^*,\cdot) = \tilde{C}_2 \times \tilde{C}_4 \times \tilde{C}_6 \times \tilde{C}_4 \times \tilde{C}_6 \times \tilde{C}_{12} .$$

$\varphi(65520) = 13824$; $\rho(65520) = 12$.

Forsøg paa Omvendinger af Fermats Sætning.

Vi har tidligere bemærket at Sætningen (i det simple Tilfælde hvor den kun handler om Primtal) ikke umiddelbart kunde vendes om (S.44). Men lad os gøre et Par Forsøg som skærer dybere. Svarende til de to Former af den gamle Sætning sætter vi

$$F_1 = \{n: (a,n) = 1 \Rightarrow n \mid a^{n-1}-1\} \text{ og } F_2 = \{n: \forall_a: n \mid a^n - a\} .$$

Ifølge Fermat vil $F_1 \supseteq P$ og $F_2 \supseteq P$, hvor P betyder Mængden af Primtal suppleret med Tallet 1 (det er klart at 1 tilhører begge Mængder, og i denne Forbindelse er det altsaa praktisk at regne 1 som et Primtal).

Vi har $F_2 \subseteq F_1$, thi for $(a,n) = 1$ vil $n \mid a^n - a$ medføre at $n \mid a^{n-1} - 1$. Endvidere gælder $4 \notin F_1$, idet $4 \nmid 3^{4-1} - 1 = 26$. Altsaa

$$P \subseteq F_2 \subseteq F_1 \subset \mathbb{N},$$

men spørgsmaalet er om vi kan sige mere, og lad os først betragte F_1.

Nu ser man af Definitionen, at F_1 netop bliver Mængden af de n for hvilke $\rho(n)$ gaar op i $n-1$. For $n = 1,2$ er $\rho(n) = 1$, saa her gælder det; for alle større n er $\rho(n)$ lige, saa for dem maa n være ulige, saa 2 er altsaa det eneste lige Tal i F_1. Vi kan derfor nøjes med at betragte de n som er Produkt af ulige Primtalpotenser p^{α}.

Da saa $(\mathbb{Z}_{p^{\alpha}}^{*}, \cdot)$ er cyklisk af Orden $(p-1)p^{\alpha-1}$ bliver Betingelsen at for alle de i n indgaaende Primtalpotenser skal $(p-1)p^{\alpha-1}$ gaa op i $n - 1$. Da samtidig p gaar op i n ses at α maa være lig 1. Udover det foran fundne Tal 2 kan F_1 altsaa kun bestaa af ulige kvadratfri Tal.

Lad os prøve at finde et sammensat Tal som tilhører F_1, d.v.s. et saakaldt Carmichael-Tal (C.1879-1967).

Vi kan først forsøge med et Produkt af to Primtal, $n = pq$ hvor $p < q$. Da vi specielt skal have $q-1 \mid n-1 = pq-1 \equiv p-1$ er vi stødt paa noget uopfyldeligt. Et Carmichaeltal maa altsaa være Produkt af mindst tre Primtal.

Saa forsøger vi med $n = pqr$, hvor $p < q < r$ er ulige Primtal, og lad os tage $p = 3$. Betingelserne bliver saa

$$2 \mid 3qr - 1, \quad q-1 \mid 3qr - 1 \quad \text{og} \quad r-1 \mid 3qr - 1.$$

Den første er altid opfyldt, og de to sidste reduceres umuiddelbart til

$$q-1 \mid 3r-1 \quad \text{og} \quad r-1 \mid 3q-1,$$

Da $q < r$ faas af den sidste at $3q - 1$ er lig $r-1$ eller $2r-2$, af hvilke det første maa forkastes da r er et Primtal. Altsaa $3q-1$ lig $2r-2$ eller $9q-9 = 6r-12$ og dette Tal er derfor deleligt med $q-1$. Ifølge den første (forr.Side) er $6r-2$ ogsaa delelig med $q-1$, og tilsammen fa$_a$s $q-1 \mid 10$, som for q giver Mulighederne $2,3,6,11$, af hvilke kun 11 er brugbar naar q er et Primtal større end 3. Indsættes dette faas $r = 17$, og dermed Carmichaeltallet $3 \cdot 11 \cdot 17 = 561$. Det opfylder virkelig Betingelserne, idet man finder $\varphi(561) = \text{m.f.Mult.}\{2,10,16\} = 80$ som gaar op i $561-1 = 560$. Formodentlig findes der uendelig mange Carmichaeltal (senere skal nævnes, at det i hvert Fald vil gælde hvis "Schinzels Hypotese" er rigtig); man kender mange, og man kan let bevise at 561 er det mindste af dem.

Vi havde $F_2 \subseteq F_1$ og faktisk gælder Lighedstegnet. hvilket skyldes at F_1 kun indeholder kvadratfri Tal. Antag $n = \prod p_j \in F_1$, og vi skal vise at for alle a vil $n \mid a^n - a$, altsaa at ethvert p_j gaar op i a^n-a. Men enten gælder $p_j \mid a$, og saa er det godt, eller ogsaa gælder $(p_j,a) = 1 \Rightarrow p_j \mid a^{p_j-1}-1$ og da $p_j-1 \mid n-1$ (fordi $n \subseteq F_1$) følger heraf $p_j \mid a^{n-1}-1 \Rightarrow p_j \mid a^n-a$.

Ialt har vi altsaa nu fundet at

$$P \subset F_2 = F_1 \subset \mathbb{N} \ .$$

□

Lad os omtale et Forsøg paa at forbedre den foregaaende Idé. Vi vil"summere"Betingelsen fra F_1, og spørger om der findes sammensatte Tal n for hvilke

$$n \mid \sum_{a \in]0,n[} (a^{n-1} - 1) \ , \quad \text{d.v.s.} \quad n \mid 1 + \sum_{a \in]0,n[} a^{n-1} \ .$$

Saadanne Tal kan kaldes Giuga-Tal (betragtet af G. 1950).

Hvis vi kun havde summeret over de a hvor $(a,n) = 1$ maatte et-

hvert Tal fra F_1 i hvert Fald tilfredsstille, men ved at summere over alle $a \in]0,n[$ faar vi noget, som i hvert Fald er opfyldt af P, og som kan anvendes uden Kendskab til Primopløsningen af n. Men da det kun er én Betingelse som kræves opfyldt, og ikke de mange Enkeltbetingelser, maa man nærmest formode at Løsningsmængden er ret stor.

Nu er

$$1^{n-1}+2^{n-1}+\ldots+(p-1)^{n-1} \equiv \begin{cases} -1 \pmod{p} & \text{for } p-1 \mid n-1 \\ 0 \pmod{p} & \text{for } p-1 \nmid n-1 \end{cases}.$$

Det øverste er klart af Fermats Sætning, og det nederste er omtalt tidligere (S.43 og 52).

Lad nu p være en Primdivisor i n. De Tal i $]0,n[$ som ikke er delelige med p udgør Intervallerne $]0,p[,]p,2p[, \ldots,]n-p,n[$, ialt n/p Stk., og dermed finder vi at modulo p er

$$1 + \sum_{a \in]0,n[} a^{n-1} \equiv 1 + \frac{n}{p} \cdot \sum_{a \in]0,p[} a^{n-1} \equiv \begin{cases} 1 - \frac{n}{p} & \text{for } p-1 \mid n-1 \\ 1 & \text{for } p-1 \nmid n-1 \end{cases}.$$

Da det skal være $\equiv 0$ maa vi have $p-1 \mid n-1$ og yderligere $p \mid 1 - \frac{n}{p}$. Det sidste viser at $p^2 \mid n-p$, hvoraf følger at n er kvadratfri. Det første viser at hvis n er lige, saa kan n ikke have nogen ulige Primdivisor, og det eneste lige Tal som opfylder Betingelsen er derfor $n = 2$. Tilbage er ulige kvadratfri Tal $n = \prod p$, hvor vi for ethvert p har at $p-1 \mid n-1$, men det er jo netop den foran fundne Talmængde F_1. Tallene n som opfylder Betingelsen er altsaa en Delmængde af F_1 (saa Enkeltkravet var i Virkeligheden meget stærkt !), og yderligere skal for enhver af n's Primdivisorer p gælde at $p \mid \frac{n}{p} - 1$.

Den sidste Betingelse kan man give en stor Slagkraft: Hvis p_o er en af Primdivisorerne, saa udsiger den at $p_o \mid \frac{n}{p_o} - 1$, men samtidig har vi for de øvrige p at $p_o \mid \frac{n}{p}$. Ved Addition faar

vi at $p_o \mid \sum \frac{n}{p} - 1$, hvor Summen er taget over samtlige Primdivisorer i n, og naar vi dernæst lader p_o gennemløbe alle Primdivisorerne i n (som var kvadratfri) faar vi at $n \mid \sum \frac{n}{p} - 1$.
Men det betyder jo igen at for det ulige kvadratfri Tal $n = \prod p$ gælder

$$\sum \frac{1}{p} - \frac{1}{n} \quad \text{er et helt Tal.}$$

Hvis n selv er et Primtal faar man 0. For et Giugatal (sammensat) faar man 1 eller et større naturligt Tal.
Det er let at angive et lige kvadratfrit $n = \prod p$ for hvilket den nævnte Størrelse er et naturligt Tal, nemlig $n = 2 \cdot 3 \cdot 5 = 30$, idet

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} - \frac{1}{30} = 1.$$

Men et ulige n som opfylder Betingelsen kendes næppe. Summen af de reciprokke af de 8 første ulige Primtal, altsaa $\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{23}$, er mindre end 1, og et saadant n maa derfor have mindst 9 Primfaktorer (hvoraf allerede følger at det er større end 10^9).
Og hvis Tallet skal være et Giugatal giver Betingelsen $p-1 \mid n-1$ mange yderligere Krav, idet fx $3 \mid n$ udelukker Primtallene $p = 7, 13, 19, \ldots$ som Faktorer i n o.s.v. Der eksisterer næppe nogen Giugatal, men det synes svært at bevise det; Giuga viste at der findes i hvert Fald ingen mindre end 10^{1000}.

Tilstrækkeligt for at p er et Primtal er det, at der eksisterer et a saaledes at $p \mid a^{p-1} - 1$ medens det for ethvert d som gaar op i p-1 gælder at $p \nmid a^d - 1$. Thi dette viser jo at $(a) \in (\mathbb{Z}_p^*, \cdot)$ og at i denne Gruppe er ord $(a) = p-1$, hvilket kun er muligt naar p er et Primtal med a som Primitivrod.

Til praktisk Anvendelse kan Kriteriet modificeres paa mange Maader, fx er det jo umiddelbart klart at man ikke behøver at prøve med alle d, men kun med dem som er af Form $(p-1)/q$, hvor q er et Primtal; dets Anvendelse kræver dog et vist Kendskab til Faktoropløsningen af p-1.

Ved Hjælp af det kan man bestemme talrige store Primtal. Sandsynligheden for at et ulige Tal af Størrelse t er et Primtal er $\sim \frac{2}{\log t}$ (se S.35), altsaa ikke negligerbar; Sandsynligheden for at et tilfældigt Tal a er primisk med t er $\frac{6}{\pi^2} \sim 0{,}6$ (da Gennemsnitsværdien af $\varphi(t)$ er $6t/\pi^2$ (S.76)), og Sandsynligheden for at $(a) \in (\mathbb{Z}_p^*, \cdot)$ er Frembringerelement (Primitivrod) i denne Gruppe er igen $\sim 0{,}6$ (nemlig $\varphi(p-1)/(p-1)$).
(det her benyttede Sandsynlighedsbegreb skal selvfølgelig kun opfattes som noget svarende til Middelværdidannelse).

Altialt ser man at det er overkommeligt at bestemme mange store Primtal (med moderne Datamatteknik af Størrelsesordenen 10^{30} fx). Men hvis Kriteriet svigter, saa faar man kun at vide at man har at gøre med et sammensat Tal, og at bestemme Faktoropløsningen af dette viser sig at være et langt større Problem, som i Praksis er uoverkommeligt (i næste Kapitel omtales nogle konkrete Eksempler paa - ganske vist langt større - Tal, dels Primtal og dels sammensatte Tal med ubekendt Faktorisering).

En Maade at oversende hemmelige Meddelelser.

En Meddelelse kan altid omsættes til et Tal (fx a = 01, b = 02, ... Mellemrum = 99, ...; saa bliver "en Abe" omsat til 051499010205). Et saadant Tal m kan saa omdannes ved en Funktion f til et uforstaaeligt Tal f(m), dette Tal forsendes saa, og Modtageren kan dechiffrere Meddelelsen v.Hj.af den omvendte Funktion f^{-1}.

Et altfor langt Tal m kan opdeles i mindre Ciffergrupper, som hver behandles paa denne Maade. En simpel Metode er fx at erstatte hvert Bogstav med det følgende saa at a = 01 ↦ 02,.. 99 ↦ 00, og "en Abe" oversendes i Formen 061500020306; hvis en Fjende blot har opfanget nogle faa Meddelelser af denne Art, saa er Koden let at bryde.

Inden vi beskriver en langt mere raffineret Metode skal det bemærkes at selv med store Tal er Operationen $a(\mathrm{mod}n) \mapsto a^r(\mathrm{mod}.n)$ relativ let at udføre med Datamat, idet r skrives i Dualsystemet og Potensopløftningen derved reduceres til et lille Antal Kvadreringer og Multiplikationer modulo n.

Man kan nu tage et stort Primtal p og et Talpar r,s hvor rs - 1 er delelig med p-1. Ifølge Fermat er saa $a^{rs} \equiv a\ (\mathrm{mod}.p)$, og idet m opdeles i Ciffergrupper som hver er mindre end p kan hver af disse omsættes ved Koden $a \mapsto a^r(\mathrm{mod}.p)$ og Modtageren kan saa dechiffrere Meddelelsen ved at benytte den omvendte Funktion $b \mapsto b^s(\mathrm{mod}.p)$. Det hemmelige i Koden er altsaa Talparret (p,r), og da et eventuelt Mønster i a fuldstændigt forsvinder i $a^r(\mathrm{mod}.p)$ er Koden forsaavidt god. Men den har den Ulempe, at hvis en Fjende blot hos én Person opsnapper (p,r) saa er det let at bestemme s og dermed bryde Koden.

Derfor har man fornylig foreslaaet følgende: i St.f. et Primtal p tager man et Produkt af to store Primtal n = pq og r,s bestemmes saa $rs \equiv 1(\mathrm{mod}.\varphi(n))$. Idet p-1 og q-1 begge gaar op i $\varphi(n)$ faar man igen at $a^{rs} \equiv a$ baade (mod.p) og (mod.q), altsaa (mod.n) (NB uanset om a er primisk med n eller ej). Koden bestaar igen i Talparret (n,r), som ikke engang behøver at være hemmeligt, men kan offentliggøres saa enhver kan afsende Meddelelser; kun Modtagercentralen kender Exponenten s, og da den ikke kan findes uden Kendskab til de to Primfaktorer i n, vil det - som beskrevet foran - med passende store Tal være uoverkommeligt for en Fjende at bestemme s. Matematisk har man altsaa her en simpel og let beregnelig Funktion $f: \mathbb{Z}_n \to \mathbb{Z}_n$, for hvilken Bestemmelsen af f^{-1} er umulig for den uindviede. Ogsaa: en Agent ved Navn A kan faa meddelt en Underskrift $f^{-1}(A)$, kontrollerbar for ham selv, og ingen anden kunde finde paa den.

KAPITEL VIII : Kvadratiske Kongruensopgaver.

Kongruensen $$a\,x^2 + b\,x + c \equiv 0 \pmod{n}$$

kan ved den sædvanlige Omskrivning (NB: nu er vi i en Ring, ikke i et Legeme) overføres i en rent kvadratisk, nemlig

$$4\,a^2\,x^2 + 4\,ab\,x + 4\,ac \equiv 0 \pmod{4an}$$

eller

$$(2a\,x + b)^2 \equiv b^2 - 4\,ac \pmod{4an}\ ;$$

hvis man heraf kan bestemme $2ax + b$, saa kan man dernæst finde x ved Løsning af en lineær Kongruens.

Vi vil derfor blot se paa en Opgave af Typen

$$y^2 \equiv a \pmod{n}\ ,$$

og ved den kinesiske Sætning kan den opløses i Opgaver

$$y^2 \equiv a \pmod{p^\alpha}\ .$$

Dersom $p|a$ tager vi γ saa $p^\gamma \| a$. Hvis $\gamma \geq \alpha$ staar der blot at $p^\alpha | y^2 \Leftrightarrow p^{\left[\frac{\alpha+1}{2}\right]} | y$. Hvis $\gamma < \alpha$ vil $p^\gamma \| y^2$; dersom γ er ulige er der ingen Løsning, og dersom γ er lige, $\gamma = 2\delta$, vil $p^\delta | y$ og vi faar

$$(y/p^\delta)^2 \equiv (a/p^\gamma) \pmod{p^{\alpha-\gamma}}.$$

Den Opgave som vi skal undersøge nærmere er derfor

$$z^2 \equiv d \pmod{p^\alpha}\ , \quad \text{hvor } p \nmid d\ ;$$

dersom den har Løsninger siger vi at d er kvadratisk Rest og ellers at d er kvadratisk Ikke-Rest (begge Dele modulo p^α).

For et ulige p er d kvadratisk Rest modulo p^α hvis og kun hvis d er kvadratisk Rest modulo p.

Bevis: Gruppen $(\mathbb{Z}_{p^\alpha}^*, \cdot)$ er cyklisk af den lige Orden $(p-1)p^{\alpha-1}$,

og hvis g er et Frembringerelement, saa vil de kvadratiske Rester være g^h, hvor h er lige. De udgør netop Halvdelen af Gruppens Elementer. Naar d er kvadratisk Rest modulo p^α er d trivielt ogsaa kvadratisk Rest modulo p, men disse sidste udgør Halvdelen af de primiske Restklasser modulo p, og da $p \mid p^\alpha$ vil Tallene i dem ogsaa udgøre Halvdelen af de primiske Restklasser modulo p^α, og altsaa netop den Halvdel som er de kvadratiske Rester modulo p^α. □

Et d er kvadratisk Rest modulo 2^α ($\alpha \geq 3$) hvis og kun hvis $d \equiv 1 \pmod 8$ (d.v.s. hvis og kun hvis d er kvadr. Rest mod.8).

Bevis: Elementerne i $(\mathbb{Z}_{2^\alpha}^*, \cdot)$ kan skrives paa Formen $(-1)^h \cdot 5^k$, og de kvadratiske Rester karakteriseres ved at h og k er lige, og de udgør altsaa en Fjerdedel af de primiske Restklasser. Men et ulige Kvadrat er $\equiv 1 \pmod 8$, hvilket ogsaa udgør en Fjerdedel af de primiske Restklasser modulo 2^α, og det er altsaa de samme. □

Hvis d er kvadratisk Rest modulo p, saa er der to Løsningsrestklasser, og de er af Formen $\{\pm x_0\}$.

Thi det er klart at hvis x_0 er Løsning, saa er $-x_0$ det ogsaa, og der kan ikke være mere end to Løsninger for hvert d, da de kvadratiske Restklasser udgjorde Halvdelen. □

Hvis d er kvadratisk Rest modulo 2^α ($\alpha \geq 3$), saa er der fire Løsningsrestklasser, og de er af Formen $\{\pm x_0, \pm (x_0 + 2^{\alpha-1})\}$.

Thi for $\alpha \geq 3$ er disse fire Restklasser alle forskellige, og udregner man deres Kvadrat ser man at det i alle Tilfælde bliver x_0^2; og der kan ikke være mere end fire Løsninger for hvert d, da de kvadratiske Restklasser udgjorde Fjerdedelen. □

I Praksis kan en Opgave $x^2 \equiv d \pmod{p^\alpha}$ ogsaa føres tilbage til en Opgave $x^2 \equiv d \pmod p$.

Eksempel: Løs $x^2 \equiv 11 \pmod{49}$.

Løsningen er af Formen $x \equiv \pm x_0 \pmod{49}$, og da $x^2 \equiv 4 \pmod{7}$ kan vi tage $x_0 \equiv 2 \pmod{7}$, altsaa $x_0 = 2 + 7h$.

Saa faas $x_0^2 = 4 + 28h + 49h^2 \equiv 4 + 28h \pmod{49}$, og idet

$4 + 28h \equiv 11 \pmod{49} \Leftrightarrow 28h \equiv 7 \pmod{49} \Leftrightarrow 4h \equiv 1 \pmod{7}$

som giver $h \equiv 2 \pmod{7}$, saa faar vi $x_0 \equiv 2 + 2 \cdot 7 = 16 \pmod{49}$.

Facit: $x \equiv \pm 16 \pmod{49}$. Prøve: $16^2 = 256$, stemmer med $49 \mid 245$.

Reciprocitetssætningen.

Vi har tidligere betragtet Isomorfien $(\mathbb{Z}_p^*, \cdot) \simeq (\mathbb{Z}_{p-1}, +)$. Den var meget uoverskuelig, men vi skal nu give et ejendommeligt konkret Resultat om den. I alt det følgende er p et ulige Primtal.

Vi havde (se S.53-54)

(d) kvadr.Restklasse mod.p $\Leftrightarrow \left(\frac{d}{p}\right) = 1 \Leftrightarrow (d)^{\frac{p-1}{2}} = (1) \Leftrightarrow$

$(d) = (g)^h$ med et lige h (idet g er en Primitivrod mod.p),

og i modsat Fald

(d) kvadr.Ikke-Rest mod.p $\Leftrightarrow \left(\frac{d}{p}\right) = -1 \Leftrightarrow (d)^{\frac{p-1}{2}} = (-1)$

$\Leftrightarrow (d) = (g)^h$ med et ulige h. Problemet er at afgøre hvornaar hvilket af Tilfældene indtræffer.

Først skal udledes endnu et Udtryk for $\left(\frac{d}{p}\right)$.

Gauss' Lemma: $\left(\frac{d}{p}\right)$ er $(-1)^k$, hvor k angiver Antallet af negative blandt de numerisk mindste Rester af $d, 2d, \ldots, \frac{p-1}{2}d$ modulo p.

Bevis: De numeriske Værdier af de numerisk mindste Rester af $d, 2d, \ldots, \frac{p-1}{2}d$ udgør netop Tallene $1, 2, \ldots, \frac{p-1}{2}$ (hvert med én Gang), idet intet af dem kan komme med to Gange fordi $s, t \in]0, \frac{p}{2}[$ medfører at $p \nmid sd \pm td = (s \pm t)d$.

Altsaa er $d^{\frac{p-1}{2}} \equiv d \cdot 2d \cdot \ldots \cdot \frac{p-1}{2} d \,/\, 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$ med Tælleren $\equiv (-1)^k \cdot (\frac{p-1}{2})!$ hvoraf Rigtigheden ses. □

Nu ses, at sd giver negativ numerisk mindste Rest naar der findes et $h \in \mathbb{Z}$ saa $(h - \frac{1}{2})p < sd < hp$, d.v.s. naar $\left[\frac{2sd}{p}\right]$ er af Formen $2h - 1$, altsaa ulige, medens vi faar positiv numerisk mindste Rest naar $\left[\frac{2sd}{p}\right]$ er lige.

Følgelig vil k have samme Paritet som $m = \sum \left[\frac{2sd}{p}\right]$ hvor der summeres over $s \in \left]0, \frac{p}{2}\right[$.

Altsaa

$$\left(\frac{d}{p}\right) = (-1)^m \quad \text{med} \quad m = \sum_{s \in \left]0, \frac{p}{2}\right[} \left[\frac{2sd}{p}\right] .$$

Prøver vi med $d = -1$ faas $\left[\frac{-2s}{p}\right]$, som er -1 for alle de $\frac{p-1}{2}$ Stk. s, og vi har dermed følgende Resultat (tidligere nævnt S.55):

"Første Supplement til Reciprocitetssætningen":

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{for } p \text{ af Form } 4h+1 \\ -1 & \text{for } p \text{ af Form } 4h-1 \end{cases} .$$

Prøver vi med $d = 2$ faas $\left[\frac{4s}{p}\right]$, som er lig 0 for de første Værdier af s og er lig 1 for $\frac{p}{4} < s < \frac{p}{2}$, d.v.s. for $\left[\frac{p}{2}\right] - \left[\frac{p}{4}\right]$ Stk. s.

Man faar

$$\left[\frac{p}{2}\right] - \left[\frac{p}{4}\right] = \begin{cases} 4h - 2h = 2h & \text{for } p = 8h+1 \\ (4h+1) - 2h = 2h+1 & \text{for } p = 8h+3 \\ (4h+2) - (2h+1) = 2h+1 & \text{for } p = 8h+5 \\ (4h+3) - (2h+1) = 2h+2 & \text{for } p = 8h+7 \end{cases}$$

altsaa ulige for de to midterste og lige for de to yderste. Dermed har vi følgende Resultat:

"Andet Supplement til Reciprocitetssætningen":

$$\left(\frac{2}{p}\right) = \left\{ \begin{array}{ll} 1 & \text{for } p \text{ af Form } 8h \pm 1 \\ -1 & \text{for } p \text{ af Form } 8h \pm 3 \end{array} \right\} = (-1)^{\frac{p^2-1}{8}} .$$

(det sidste Udtryk er blot en fiks Maade at skrive 1 eller -1 paa).

For ulige d kan Udtrykket for $(\frac{d}{p})$ simplificeres lidt. Thi vi har

$$\left[\frac{(p-t)d}{p}\right] = \left[d - \frac{td}{p}\right] = d - 1 - \left[\frac{td}{p}\right]$$

(ingen af Brøkerne er heltallige, $t \in]0,p[$). Heldelsstørrelserne i Formlen har derfor samme Paritet. I Udtrykket for m kan vi derfor erstatte Summanden $\left[\frac{2sd}{p}\right]$ med $\left[\frac{(p-2s)d}{p}\right]$ uden at Værdien $(-1)^m$ ændres; det gør vi nu for $2s \in]\frac{p}{2},p[$, hvorved $p-2s$ ses at give netop de ulige Tal $\in]0,\frac{p}{2}[$, og da de øvrige Værdier for 2s giver de lige Tal i dette Interval, faar vi ialt

$$\left(\frac{d}{p}\right) = (-1)^{m_1} \text{ med } m_1 = \sum_{t \in]0,\frac{p}{2}[} \left[\frac{td}{p}\right] .$$

Vi kan nu let bevise den ejendommelige Reciprocitetssætning. Den var fuldstændigt kendt, men uden Bevis, af Euler; den vistes første Gang af Gauss i "Disquisitiones Arithmeticæ" 1801, og man regner at ialt har Gauss givet 8 Beviser for den; senere er der angivet talrige andre Beviser for den, de er dog blot Varianter af nogle ganske enkelte Hovedtyper.

Reciprocitetssætningen:

Hvis p og q er forskellige ulige Primtal, saa er

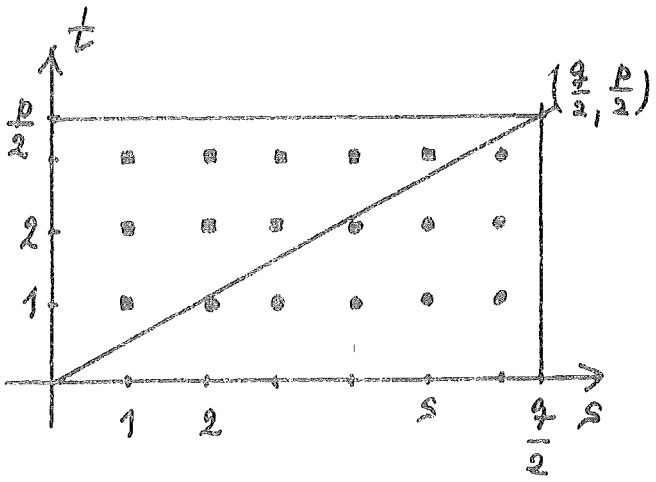
$$\left(\frac{p}{q}\right),\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1 \text{ for } & p = 4h+1 \vee q = 4h+1 \\ -1 \text{ for } & p = 4h-1 \wedge q = 4h-1 \end{cases}$$

Bevis: Venstresiden er $(-1)^{m_1+m_1'}$, hvor $m_1 + m_1'$ er lig

$$\sum_{s \in]0,\frac{q}{2}[} \left[\frac{sp}{q}\right] + \sum_{t \in]0,\frac{p}{2}[} \left[\frac{tq}{p}\right] .$$

Vi betragter nu følgende Figur:

Skraalinien har Hældningen p/q, og man ser, at den første af Summerne netop angiver Antallet af Gitterpunkter under Skraalinien, og (idet man ombytter s med t og p med q) at den anden netop angiver Antallet af Gitterpunkter over Skraalinien, og tilsammen er de to Summer altsaa lig det samlede Antal Gitterpunkter, som netop er $\frac{p-1}{2} \cdot \frac{q-1}{2}$.



□

Ved Hjælp af Sætningen med dens to Supplementer samt Brug af Reglerne $(\frac{cd}{p}) = (\frac{c}{p}) \cdot (\frac{d}{p})$ og $(\frac{d}{p}) = (\frac{d \pm p}{p})$ kan Bestemmelsen af et Legendresymbol reduceres til et lille Antal Operationer. Selve Reciprocitetssætningen anvendes i Praksis let ved at benytte at hvis p eller q er af Form 4h+1 saa er $(\frac{p}{q})$ lig $(\frac{q}{p})$, og at hvis p er af Form 4h-1, saa er $(\frac{p}{q}) = (\frac{-1}{q}) \cdot (\frac{q}{p}) = (\frac{-q}{p})$.

Eksempel 1):

$$(\frac{-2}{p}) = (\frac{-1}{p}) \cdot (\frac{2}{p}) = \begin{cases} 1 \text{ for } p = 4h+1 \wedge p = 8h' \pm 1 \\ 1 \text{ for } p = 4h-1 \wedge p = 8h' \pm 3 \\ -1 \text{ for } p = 4h+1 \wedge p = 8h' \pm 3 \\ -1 \text{ for } p = 4h-1 \wedge p = 8h' \pm 1 \end{cases}$$

$$\text{altsaa} \quad (\frac{2}{p}) = \begin{cases} 1 & \text{for } p = 8h+1 \text{ eller } p = 8h+3 \\ -1 & \text{for } p = 8h-1 \text{ eller } p = 8h-3 \end{cases}$$

Eksempel 2):

$$(\frac{3}{p}) = (\frac{-1}{p}) \cdot (\frac{p}{3}) = \begin{cases} 1 \text{ for } p = 4h+1 \wedge p = 3h'+1 \\ 1 \text{ for } p = 4h-1 \wedge p = 3h'-1 \\ -1 \text{ for } p = 4h+1 \wedge p = 3h'-1 \\ -1 \text{ for } p = 4h-1 \wedge p = 3h'+1 \end{cases}$$

$$\text{altsaa} \quad (\frac{3}{p}) = \begin{cases} 1 & \text{for } p = 12h \pm 1 \\ -1 & \text{for } p = 12h \pm 5 \end{cases}$$

Eksempel 3):

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)^2\cdot\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{for } p = 6h+1 \\ -1 & \text{for } p = 6h-1 \end{cases}$$

Eksempel 4): Vi vil vise, at 1847 er et Primtal.

Det nærmeste Kvadrattal er $1849 = 43^2$, saa det er nok at prøve med Primdivisorer < 43. Men da $p \mid 1847 \Rightarrow$ $43^2 \equiv 2 \pmod{p}$ maa vi have $\left(\frac{2}{p}\right) = 1$, altsaa $p = 8h \pm 1$, saa det er nok at prøve med $p = 7,17,23,31,41$. Ingen af dem gaar op, saa 1847 er et Primtal.

Eksempel 5): Tallet 18074 ønskes primopløst.

Aabenbart er 2 Divisor, $18074 = 2\cdot 9037$. Et Kvadrattal nær 9037 er $9025 = 95^2$. Heraf ses at $p \mid 9037 \Rightarrow \left(\frac{-12}{p}\right) = 1$. Da $\left(\frac{4}{p}\right) = 1$ faas $\left(\frac{-3}{p}\right) = 1$, altsaa (Eks.3)) at $p = 6h+1$. Det viser sig at $p = 7$ gaar op, $9037 = 7\cdot 1291$. Man kan prøve videre (husk, at evt. kunde 7 gaa op en Gang til), men man kan ogsaa bruge at $36^2 = 1296$, altsaa $p \mid 1291$ medfører at $\left(\frac{5}{p}\right) = 1$, derfor $\left(\frac{p}{5}\right) = 1$, som giver at $p = 10h' \pm 1$. Tilsammen ses at det er nok at prøve om 1291 er delelig med 19 eller 31; ingen af dem gaar op.

Altsaa: 18074 primopløses til $2\cdot 7\cdot 1291$.

Eksempel 6): Bestem $\left(\frac{365}{1847}\right)$. (Iflg. Eks.4) er 1847 et Primtal).

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\cdot\left(\frac{73}{1847}\right) = \left(\frac{1847}{5}\right)\cdot\left(\frac{1847}{73}\right) = \left(\frac{2}{5}\right)\cdot\left(\frac{22}{73}\right) =$$

$$\left(\frac{2}{5}\right)\cdot\left(\frac{2}{73}\right)\cdot\left(\frac{11}{73}\right) = (-1)\cdot 1\cdot\left(\frac{11}{73}\right) = -\left(\frac{73}{11}\right) = -\left(\frac{7}{11}\right) = \left(\frac{11}{7}\right) = \left(\frac{4}{7}\right).$$

Da $\left(\frac{4}{7}\right) = 1$ har vi altsaa at $\left(\frac{365}{1847}\right) = 1$.

Eksempel 7): For hvilke Primtal p er $\left(\frac{14}{p}\right) = 1$?

Skrives $\left(\frac{14}{p}\right)$ som $\left(\frac{2}{p}\right)\cdot\left(\frac{7}{p}\right)$ faar man Brug for at opdele p modulo 8, modulo 4 og modulo 7, hvilket kan blive besværligt.

Man kan omgaa det ved at benytte at $(\frac{14}{p}) = (\frac{2}{p})\cdot(\frac{7}{p})$ og bruge Eks.2) og tidligere Bemærkninger. Kravet er aabenbart at $(\frac{2}{p}) = (\frac{7}{p})$ som igen er lig $(\frac{p}{7})$. Følgelig

enten $p = 8h + 1,3 \quad \wedge \quad p = 7h' + 1,2,4$.

eller $p = 8h - 1,3 \quad \wedge \quad p = 7h' - 1,2,4$.

Løsningerne skal samles efter den kinesiske Sætning, og bliver aabenbart ± seks Stk. Restklasser modulo 56.

Man finder $p = 56h \pm 1,9,25,11,43,51$.

Eksempel 8): Hvilke Primtal gaar op i et Tal af Form x^2+7y^2 ?

Muligheder a) p som gaar op i baade x og y.

b) 7, dersom 7 gaar op i x

c) ellers $x^2 \equiv (-7)\cdot y^2$, og da de kvadratiske Rester udgør en Gruppe, maa man have $(\frac{-7}{p}) = 1$.

altsaa (Eks.7)) $p = 7h+1,2,4$ & $p=14h'+1,9,11$.

Taleksempel: Find en Primdivisor i $1000063 = 1000^2+7\cdot 3^2$.

Prøve med 11,23,29,.. giver at 23 gaar op.

Eksempel 9): Det er muligt at bevise endnu nogle Specialtilfælde af Dirichlets Sætning; Beviset løber efter det tidligere Mønster (S.55). Fx Der findes uendelig mange Primtal af Form $p = 8h-1$; vi benytter at et ulige Tal u^2-2 kun kan have Primdivisorer af Form $p = 8h+1$ eller $p = 8h-1$ (2'Suppl) og at det maa have mindst en Divisor af den sidste Art. Saa tages $a_1 = 7$ og $a_n = (a_1\cdot\ldots\cdot a_{n-1})^2-2$, og man ser at ethvert a_n maa indeholde en ny Primdivisor af Type 8h-1. Analogt: Der findes uendelig mange Primtal $p = 8h+3$ (man benytter $a_1 = 3$ og Udtryk u^2+2) og ligeledes uendelig mange $p = 8h-3$ ($a_1=5$ og Udtryk u^2+4). At der er uendelig mange $p = 8h+1$ er tidligere vist (S.84). Metoden kan ogsaa bruges for primiske Restklasser modulo 12, ellers ikke.

Fermat-Tal.

Det er Primtal af Formen

$p = 2^h+1$ (Fermat 1601-1665).

De første er
$2+1 = 3$
$2^2+1 = 5$
$2^4+1 = 17$
$2^8+1 = 257$
$2^{16}+1 = 65537$

Vi har tidligere omtalt dem i Forbindelse med Spørgsmaalet om hvilke regulære Polygoner der er konstruerbare med Passer og Lineal (S.77). Sammesteds vistes at $\varphi(n)$ er en Potens af 2 hvis og kun hvis n er en Potens af 2 gange et Produkt af forskellige Fermattal.

Mersenne-Tal.

Det er Primtal af Formen

$p = 2^h-1$ (Mersenne 1588-1648).

De første er
$2^2-1 = 3$
$2^3-1 = 7$
$2^5-1 = 31$
$2^7-1 = 127$
$2^{13}-1 = 8191$

Vi har tidligere omtalt dem i Forbindelse med Spørgsmaalet om "Fuldkomne Tal" (S.68).

$\delta(n)$ er en Potens af 2 hvis og kun hvis n er et Produkt af forskellige Mersennetal.

Bevis: Da δ er multiplikativ reduceres Spørgsmaalet til at undersøge hvornaar $\delta(p^\alpha) = 2^k$, altsaa $1+p+p^2+\ldots p^\alpha = 2^k$. Da Venstresidens Led er ulige maa Antallet Led være lige, saa at $p+1$ gaar op, og følgelig er af Form 2^h, d.v.s. p er Mersennetal. Kvotienten er af Form $1+p^2+p^4+..$ og hvis større end 1 da ogsaa lige, altsaa delelig med p^2+1. Men p^2+1 er ikke en Potens af 2, da $p^2+1 < (p+1)^2 < 2\cdot(p^2+1)$. □

Dersom 2^h+1 er et Primtal, saa er h en Potens af 2.

Bevis: Hvis h er delelig med et ulige Primtal q, $h = qr$, saa er $2^h+1 = (2^r)^q+1 = (2^r+1)(2^{r(q-1)}-2^{r(q-2)}+..-2^r+1)$ hvori begge Faktorerne er større end 1. □

For saadanne h gælder, at hvis 2^h+1 er delelig med et Primtal p, saa er $p = 2h\cdot hel+1$.

Bevis: Idet $p \nmid 2^h-1$, men $p \mid 2^{2h}-1 = (2^h+1)(2^h-1)$ ses, at i $(\mathbb{Z}_p^*, \cdot)$ vil ord ② $\nmid$ h, men ord ② $\mid$ 2h og følgelig er ord ② = 2h (idet man benytter at h er en Potens af 2). Ifølge Fermats Sætning vil ord ② $\mid$ p-1, hvoraf ses at $p = 2h\cdot hel+1$. □

Af de ifølge foregaaende Sætning mulige Primdivisorer kan Halvdelen forkastes v.Hj.af 2.Supplement til Reciprocitetssætningen, idet man finder at $p \mid 2^h+1$ kun kan indtræffe for $p = 4h\cdot hel+1$ (dog forudsat $h > 2$)

Bevis: Idet h er en Potens af 2 ses at for $h > 2$ er $p \equiv 1 \pmod 8$

Dersom 2^h-1 er et Primtal, saa er h et Primtal.

Bevis: Hvis h er Produkt af to Tal større end 1, $h = qr$, saa er $2^h-1 = (2^r)^q-1 = (2^r-1)(2^{r(q-1)}+2^{r(q-2)}+..+2^r+1)$ hvori begge Faktorerne er større end 1. □

For saadanne h gælder, at hvis 2^h-1 er delelig med et Primtal p, saa er $p = 2h\cdot hel+1$ (dog forudsat $h > 2$).

Bevis: Idet $p \nmid 2-1$, men $p \mid 2^h-1$ ses, at i $(\mathbb{Z}_p^*, \cdot)$ vil ord ② $\nmid$ 1, men ord ② $\mid$ h og følgelig er ord ② = h (idet man benytter at h er et Primtal). Ifølge Fermats Sætning vil ord ② $\mid$ p-1, og da yderligere p er ulige ses at for ulige h er $p = 2h\cdot hel+1$. □

Af de ifølge foregaaende Sætning mulige Primdivisorer kan Halvdelen forkastes v.Hj.af 2.Supplement til Reciprocitetssætningen, idet man finder at $p \mid 2^h-1$ kun kan indtræffe for $p \equiv \pm 1 \pmod 8$.

Bevis: Idet h er ulige ses at $h \mid \frac{p-1}{2}$, altsaa ord ② $\mid \frac{p-1}{2}$, saa

derfor $(\frac{2}{p}) = 1$ som medfører $p \mid 2^{\frac{p-1}{2}}-1$, eller ord $(2) \mid \frac{p-1}{2}$, altsaa $p = 4h\cdot hel+1$. □

Ovenstaaende Sætninger indskrænker Mængden af mulige Primdivisorer p i Tallene 2^h+1.

For h = 32 er det tilstrækkeligt at undersøge om $2^{32}+1$ (10-cifret) er delelig med noget Primtal af Formen $p = 128\cdot hel+1$.

Det blev gjort af Euler, som fandt at p = 641 gaar op. Det er let at kontrollere, thi dels er $641 = 640+1 = 5\cdot 2^7+1$, dels er $641 = 625+16 = 5^4+2^4$, og modulo 641 faas saa $2^{32}+1 \equiv 2^4\cdot(2^7)^4+1 \equiv -5^4\cdot(2^7)^4+1 \equiv -(5\cdot 2^7)^4+1 \equiv -(-1)^4+1 = 0$. Det var heldigt for Euler at der var et saa lille p som gaar op. Den næste h-Værdi er 64 (giver 20-cifret Tal), og en tilsvarende lille Primdivisor findes ikke.

$p \mid 2^{\frac{p-1}{2}}-1$ som medfører at $(\frac{2}{p}) = 1$, hvoraf igen faas at $p \equiv \pm 1 \pmod 8$. □

Ovenstaaende Sætninger indskrænker Mængden af mulige Primdivisorer p i Tallene 2^h-1.

For h = 31 er det tilstrækkeligt at undersøge om $2^{31}-1$ (10-cifret) er delelig med noget Primtal af Formen $p = 62\cdot hel+1 \wedge p \equiv \pm 1 \pmod 8$, d.v.s. $p = 248\cdot hel+\begin{cases}1\\63\end{cases}$.

Det blev gjort af Euler, som fandt at ingen af disse Tal ($< \sqrt{n}$) gaar op, og dermed havde fundet at $2^{31}-1$ er et Primtal. Det havde saa i hundrede Aar Rekorden som det største kendte Primtal. Den næste h-Værdi er 37, og Arbejdet med en tilsvarende Undersøgelse vilde være ti-doblet. Alle de mindre h-Værdier fik han undersøgt; foruden de foran nævnte giver h = 17 og 19 Mersennetal. Euler bemærkede ogsaa, at $h \equiv -1 \pmod 4 \wedge 2h+1 =$ Primtal p medfører at $p \mid 2^h-1$ (ses let, da $(\frac{2}{p}) = 1$).

Pepin-Lucas's Kriterium (ca. 1875): For lige h gælder at 2^h+1 er Primtal hvis og kun hvis $2^h+1 \mid c_h$, hvor $c_2 = 10$ og $c_{r+1} = (c_r-1)^2+1$.

Bevis: Ved Induktion ses direkte at $c_h = 3^{2^{h-1}}+1$.

Dersom 2^h+1 er et Primtal F, ses at $F \equiv 2 (\mathrm{mod}.3), \Rightarrow (\frac{F}{3}) = -1$, og da $F \equiv 1 (\mathrm{mod}.4)$ er $(\frac{3}{F}) = -1$, saa $F \mid 3^{\frac{F-1}{2}}+1$.

Dersom $2^h+1 \mid c_h$, saa lad p være en Primdivisor i 2^h+1. Da nu $p \nmid 3^{2^{h-1}}-1$, men $p \mid 3^{2^h}-1$ ses at i $(\mathbb{Z}_p^*, \cdot)$ er ord $(3) = 2^h$, saa $2^h \mid p-1$ (Fermat !), hvilket kun er muligt med $p = 2^h+1$. □

Kriteriets Anvendelse kræver kun ca. h Kvadreringer mod (2^h+1)

Ved Kriteriet har man undersøgt de mulige h op til og med $2^{14} (\sim 20000)$, og man har ikke fundet flere Fermattal. Man kender altsaa kun de fem nævnte, nemlig for h = 1,2,4,8,16. Det er tvivlsomt om der er flere, og der er neppe uendelig mange, da 2-Potenserne ligger saa spredt i Talrækken. De $2^{2^k}+1$ som er sammensatte er det i nogle Tilfælde lykkedes at faktorisere, helt eller delvis.

Lucas's Kriterium: For ulige h gælder at 2^h-1 er Primtal hvis og kun hvis $2^h-1 \mid c_h$, hvor $c_2 = 2$ og $c_{r+1} = 2c_r^2-1$.

Beviset benytter samme Ideer som Beviset for Lucas-Pepin, men er teknisk lidt sværere, det skal ikke gives her.

Dets Anvendelse kræver kun ca. h Kvadreringer mod. 2^h-1, og ved Haandregning kunde Lucas undersøge fx h = 127 som viste sig at give et Primtal(der indtil ca.1950 (Elektronregnemaskiner) havde Rekorden som det største kendte (Mersenne havde fremsat en Formodning om at h = 31,67, 127,257 skulde give Primtal, smlgn.nedenfor).

Man har nu undersøgt alle h-Værdier op til 20000, og det viser sig at man faar Mersennetal for følgende 24 Stk.: h = 2,3,5,7, 13,17,19,31,61,89,107,127,521, 607,1279,2203,2281,3217,4253, 4423,9689,9941,11213 og 19937. Det sidste (fra 1971) er det største kendte Primtal. Formodentlig er der uendelig mange, da Primtallene ligger ret tæt i Talrækken, men man kan slet ikke bevise det. Og man kender altsaa ogsaa enorme sammensatte Tal (6000 Cifre),Faktorer ukendte.

KAPITEL IX : Haros-Brøker; Diofantisk Approximation; Pell's Ligning.

Vi vil undersøge $\mathbb{Q}$. Ethvert af dens Elementer skrives som en uforkortelig Brøk $\frac{a}{b}$, med $b \in \mathbb{N}$, $a \in \mathbb{Z}$, og $(a,b) = 1$, og denne Fremstilling er entydig.

Vi definerer en Relation $\dashv$ ved

$$\frac{a}{b} \dashv \frac{c}{d} \quad \text{naar} \quad \frac{c}{d} - \frac{a}{b} = \frac{1}{bd}, \text{ d.v.s. naar } bc - ad = 1.$$

Det er klart at Fortegnsskifte vender Relationen: $\frac{a}{b} \dashv \frac{c}{d} \Rightarrow \frac{-a}{b} \vdash \frac{-c}{d}$ (og iøvrigt ogsaa Reciprokning af Brøkerne).

I Relationen kan ens Nævnere kun forekomme hvis de er 1, i hvilket Tilfælde man faar $\ldots \dashv \frac{-1}{1} \dashv \frac{0}{1} \dashv \frac{1}{1} \dashv \frac{2}{1} \dashv \ldots$

Betragter vi en Brøk $\frac{r}{s}$ med $s > 1$, vil der til den netop findes én Brøk $\frac{a}{b}$ saa $\frac{a}{b} \dashv \frac{r}{s}$ og $b < s$.

Bevis: Vi faar Ligningen $rb - sa = 1$ til Bestemmelse af a og b. Da $(r,s) = 1$ findes der en Løsning (a_o, b_o), og samtlige Løsninger er saa $(a_o + t \cdot r, b_o + t \cdot s)$, hvor t gennemløber $\mathbb{Z}$. Det ses at netop én af disse b-Værdier falder i Intervallet $]0,s[$, og da den ikke kan være s (saa kunde Højresiden ikke blive 1) falder den i $]0,s[$. □

Ligeledes findes der til $\frac{r}{s}$ netop én $\frac{c}{d}$ saa $\frac{r}{s} \dashv \frac{c}{d}$ og $d < s$.

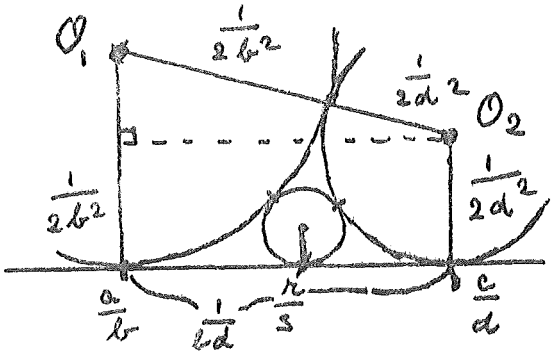
Naar vi har en Situation $\frac{a}{b} \dashv \frac{r}{s} \dashv \frac{c}{d}$ giver Ligningerne $rb - sa = 1$ og $sc - rd = 1$ ved Subtraktion, at $r(b+d) = s(a+c)$ saa at $\frac{r}{s} = \frac{a+c}{b+d}$, altsaa at den midterste Brøk faas af de to yderste ved at addere Tællerne og addere Nævnerne, og saa evt. forkorte.

I den specielle Situation, hvor $\frac{a}{b} \dashv \frac{r}{s} \dashv \frac{c}{d}$ med $b,d < s$ skal vi ikke forkorte, og yderligere gælder $\frac{a}{b} \nvdash \frac{c}{d}$ (i dette Til-

falde virker Relationen altsaa som om den var transitiv, normalt er den det ikke).

Bevis: Da $\frac{r}{s} = \frac{a+c}{b+d}$, og vi har $b+d < 2s$, ses at der ikke kan være nogen Forkortningsfaktor større end 1. Altsaa er $r = a+c$ og $s = b+d$. Endvidere faas $bc - ad = b(a+c) - a(b+d) = br-as = 1$, som viser at $\frac{a}{b} \dashv \frac{c}{d}$. □

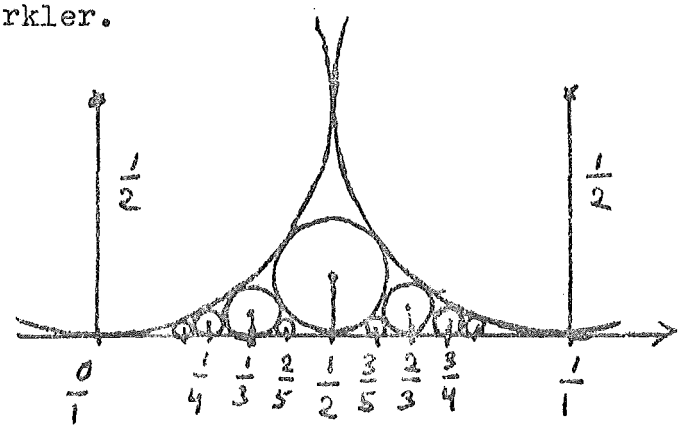
Relationen $\dashv$ har et simpelt geometrisk Billede. Paa en Abscisseakse afbildes Punkterne $\frac{a}{b}$ og $\frac{c}{d}$ og man tegner Cirkler med Radier hhv. $1/2b^2$ og $1/2d^2$



som rører Linien i disse to Punkter; Centrer O_1 og O_2. Centerliniens Længde udregnes: $O_1O_2^2 = (\frac{1}{bd})^2 + \left|\frac{1}{2b^2} - \frac{1}{2d^2}\right|^2 = (\frac{1}{2b^2} + \frac{1}{2d^2})^2$; det viser, at de to Cirkler netop rører hinanden.

Hvis $\frac{a}{b} \dashv \frac{r}{s} \dashv \frac{c}{d}$ med $b,d < s$ og altsaa $r = a+c$ og $s = b+d$ vil Cirklen svarende til $\frac{r}{s}$ røre begge de to foregaaende og Abscisseaksen, og for ethvert rationalt $\frac{r}{s}$ med $s > 1$ kan man altsaa faa en Cirkel som rører Linien og to større Cirkler.

Hvis man nu tegner en Linie og en Række Cirkler med Radius 1/2 som rører den i alle heltallige Punkter (og rører hinanden), og man saa indskyder mindre



Cirkler som rører de allerede forhaanden værende og Linien, og bliver ved med det, saa vil Røringspunkterne paa Linien netop give alle rationale Tal $\frac{r}{s}$, og den tilsvarende Cirkelradius bliver $1/2s^2$.

Denne smukke og simple Konfiguration, "Ford's Cirkler", synes først fremstillet i 1937 (L.R.Ford, 1887-).
Men nedenstaaende Sætninger om rationale Tal er opdaget tidligere, nemlig af Haros 1802 (som, i Anledning af den franske Revolutions Indførelse af Decimalsystemet paa mange nye Felter, udarbejdede Omsætningstabeller fra sædvanlige Brøker til Decimalbrøker); de blev omtalt i en Notits 1816 af en Englænder Farey (hvorfor Brøker opfattet paa denne Maade ofte kaldes Fareybrøker, men burde hedde Harosbrøker), og Sætningerne om dem blev umiddelbart efter bevist af Cauchy (C.1789-1857)./

Vi betragter alle uforkortelige Brøker med Nævnere $\leq n$, og ordner dem efter Størrelse (det betyder altsaa at vi betragter alle Ford'ske Cirkler ned til en vis Størrelse). Saa gælder

1) For to Nabobrøker $\frac{a}{b}$ og $\frac{c}{d}$ er $b+d > n$.

2) For saadanne to Nabobrøker gælder $bc - ad = 1$.

3) Endvidere har man $(b,d) = 1$.

4) For tre Nabobrøker $\frac{a}{b}$, $\frac{c}{d}$ og $\frac{e}{f}$ gælder $\frac{c}{d} = \frac{a+e}{b+f}$.

Beviser: 1) er klart, da Brøken $\frac{r}{s}$ med $s = b+d$ (svarende til den Cirkel som kan indskydes mellem de to Cirkler og Linien) ikke er med (da de var Naboer), og følgelig er $b+d > n$.
2) er klart, da Nabobrøker svarer til rørende Cirkler. 3) er klar Konsekvens af 2). 4) er omtalt foran som Konsekvens af at $\frac{a}{b} \rightarrow \frac{c}{d} \rightarrow \frac{e}{f}$. □

Eksempel: Sæt $n = 7$. De uforkortelige Brøker med Nævnere ≤ 7 ordnet efter Størrelse er

$$\ldots \frac{-1}{7}\ \frac{0}{1}\ \frac{1}{7}\ \frac{1}{6}\ \frac{1}{5}\ \frac{1}{4}\ \frac{2}{7}\ \frac{1}{3}\ \frac{2}{5}\ \frac{3}{7}\ \frac{1}{2}\ \frac{4}{7}\ \frac{3}{5}\ \frac{2}{3}\ \frac{5}{7}\ \frac{3}{4}\ \frac{4}{5}\ \frac{5}{6}\ \frac{6}{7}\ \frac{1}{1} \ldots$$

hvor man kan efterprøve at 1), 2), 3) og 4) er opfyldt.

Diofantisk Approksimation.

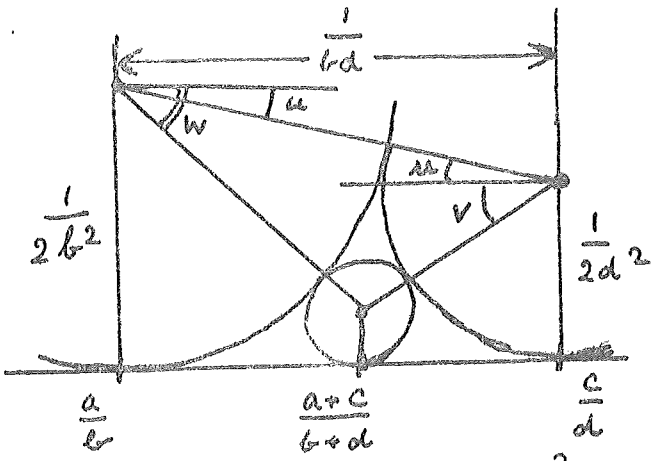
Dermed menes Approximation med rationale Tal. Af den øverste Figur S.165 ses at for $\xi \in \left]\frac{a}{b},\frac{c}{d}\right[$ vil der til ξ findes mindst én Tilnærmelsesbrøk $\frac{x}{y}$, nemlig et af Intervalendepunkterne, for hvilken man har $\left|\xi - \frac{x}{y}\right| \leqq 1/2y^2$. Dersom ξ er irrational vil det ligge indeni en uendelig Følge af saadanne Intervaller, som snævrer sammen om Punktet (baade fra venstre og højre), og vi har derfor at der til ξ findes uendelig mange Tilnærmelsesbrøker $\frac{x}{y}$ for hvilke der gælder $\left|\xi - \frac{x}{y}\right| \leqq 1/2y^2$. Men Resultatet kan forbedres:

Hurwitz's Sætning (H.1859-1919): Til ethvert irrationalt ξ findes uendelig mange rationale Tal $\frac{x}{y}$, saa $\left|\xi - \frac{x}{y}\right| < \frac{1}{\sqrt{5}} \cdot \frac{1}{y^2}$. Konstanten $\frac{1}{\sqrt{5}}$ er bedst mulig (hvoraf følger at Exponenten 2 ved y ogsaa er bedst mulig).

Bevis: Slutparentesen følger af at hvis der kunde bruges en bedre (d.v.s. større) Exponent end 2, vilde man, naar $y \to \infty$, have $\left|\xi - \frac{x}{y}\right| < \frac{1}{y^2} \cdot \varepsilon_y$, i Strid med at $1/\sqrt{5}$ er bedst mulig. Iøvrigt er det bemærkelsesværdigt at der i Sætningen gælder skarpt Ulighedstegn med den bedst mulige Konstant; da det er en Sætning som omhandler en Situation med $y \to \infty$ kunde man vente sig, at den blot gav en Ulighed $\ldots < (1/\sqrt{5} + \varepsilon) \cdot \ldots$, selvom $1/\sqrt{5}$ er bedste Konstant.

Ideen er nu, at dersom man i det ovenfor givne Ræsonnement (referende til Fig. S.165) havde en Situation hvor Fejlvurderingen $1/2y^2$ næsten var bedst mulig, saa maatte det skyldes at baade Centerlinien O_1O_2 dannede en kun lille Vinkel med Abscisseaksen og at ξ laa omtrent midt imellem $\frac{a}{b}$ og $\frac{c}{d}$, men saa maatte ξ ligge nær ved den næste Brøk $\frac{r}{s}$, som saa vilde give en god Approksimation.

Lad os igen betragte Figuren med de tre Cirkler, og lad Centerliniernes Vinkler med vandret hedde u,v og w som angivet paa Figuren. Vi antager b < d (ellers kunde vi blot vende Akseretningen), saa Figuren bliver som tegnet, de to ydre Cirkler har Radier $1/2b^2$ og $1/2d^2$, og da s = b+d har den lille inderste Cirkel Radius lig $1/2(b+d)^2$.

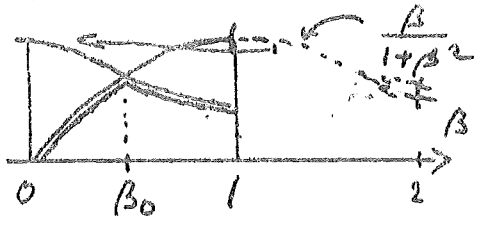


Ved Projektion paa Abscisseaksen faar vi ved at bruge $\frac{a}{b}$ eller $\frac{c}{d}$ som Tilnærmelsesbrøk at $\left|\xi - \frac{x}{y}\right| \leqq \frac{\cos u}{2} \cdot 1/y^2$ og paa tilsvarende Maade faar vi ved at bruge den lille Cirkel sammen med en af de ydre (hvilken af dem afhænger af om ξ er større eller mindre end r/s) at vi har en Tilnærmelsesbrøk $\frac{x}{y}$ med $\left|\xi - \frac{x}{y}\right|$ mindre end eller lig enten $\frac{\cos v}{2} \cdot 1/y^2$ eller $\frac{\cos w}{2} \cdot 1/y^2$. Da nu af Fig. fremgaar at $w > u$, altsaa $\cos w < \cos u$, ses at vi kan bruge den mindste af Størrelserne $\frac{\cos u}{2}$ og $\frac{\cos v}{2}$ som Vurderingsfaktor.

Vi finder

$$\frac{\cos u}{2} = \frac{1}{2} \cdot \frac{\frac{1}{bd}}{\frac{1}{2b^2} + \frac{1}{2d^2}} = \frac{\beta}{1+\beta^2} \quad \text{med} \quad \beta = \frac{b}{d} ;$$

for $\frac{\cos v}{2}$ skal vi foretage samme Regning, men med b erstattet med b+d, d.v.s. β erstattes med $\beta+1$. Som Vurderingsfaktor kan vi altsaa bruge den mindste af disse to Størrelser, $\beta \in]0,1]$. Den afledede af $\beta/(1+\beta^2)$ er $(1-\beta^2)/(1+\beta^2)^2$, og Funktionen er altsaa voksende i $\beta \in]0,1]$. For $\beta > 1$, altsaa naar β er erstattet med $\beta+1$, er Funktionen aftagende;



Vurderingsfaktoren $\min\left\{\beta/(1+\beta^2),\ (1+\beta)/(1+(1+\beta)^2)\right\}$ har en Størsteværdi svarende til Kurvernes Skæringspunkt, altsaa for $\beta/(1+\beta^2) = (1+\beta)/(2+2\beta+\beta^2)$, eller $\beta^2 + \beta - 1 = 0$, som giver $\beta_0 = \frac{-1+\sqrt{5}}{2}$, og indsættes dette faas $\frac{1}{\sqrt{5}}$, som ønsket. Da $\beta \in \mathbb{Q}$ ses, at der gælder skarpt Ulighedstegn, $\sqrt{5}$ idet $\beta \neq \beta_0$.

For at vise at Konstanten er bedst mulig kan vi som det irrationale ξ benytte det nys fundne $\frac{-1+\sqrt{5}}{2}$, som var Rod i $\xi^2 + \xi - 1 = 0$; Polynomiets anden Rod er $\xi - \sqrt{5}$. Vi indsætter et rationalt Tal $\frac{x}{y}$ i Polynomiet og tager numerisk Værdi:

$$\left|\left(\frac{x}{y} - \xi\right)\underbrace{\left(\frac{x}{y} - \xi + \sqrt{5}\right)}\right| = \left|\left(\frac{x}{y}\right)^2 + \left(\frac{x}{y}\right) - 1\right| = \frac{|x^2+xy-y^2|}{y^2} \geqq \frac{1}{y^2};$$

det sidste Ulighedstegn skyldes at den foregaaende Tæller er heltallig og ikke 0, da Polynomiet ikke havde nogen rational Rod. Naar $\left|\frac{x}{y} - \xi\right|$ er lille ses at Parantesen $\underbrace{\ }$ er nær $\sqrt{5}$, og for alle Tilnærmelsesbrøker fra et vist Trin har vi derfor

$$\left|\frac{x}{y} - \xi\right| > \left(\frac{1}{\sqrt{5}} - \varepsilon\right) \cdot \frac{1}{y^2}. \qquad \square$$

Lad os bemærke, at <u>for et rationalt Tal $\frac{a}{b}$ er det ikke muligt at finde en Følge af forskellige Tilnærmelsesbrøker $\frac{x}{y}$ saaledes at Afvigelsen aftager som y^{-2}</u>, thi Differensen kan aabenbart aldrig blive mindre end $\frac{1}{by}$, og aftager altsaa kun proportionalt med $\frac{1}{y}$ (men til Gengæld kan man naturligvis bruge Tallet som rational Tilnærmelse til sig selv).

Det er muligt at angive specielle irrationale Tal ξ for hvilke der findes en Følge af Tilnærmelser $\frac{x}{y}$ hvor Afvigelsen gaar mod 0 meget hurtigere end y^{-2}. Fx vil $\xi = \sum_n 10^{-n!}$ være et saadant. Hvis man som $\frac{x}{y}$ tager det n'te Afsnit af Rækken, saa er $y = 10^{n!}$, og Afvigelsen er $(1+\varepsilon)\cdot 10^{-(n+1)!}$, altsaa mindre end y^{-n}, og for ethvert fast k vil Afvigelsen blive lille i Forhold til y^{-k}.

Dette Tal blev angivet af Liouville som Eksempel paa et Tal der er transcendent (over $\mathbb{Q}$). Dermed blev altsaa Eksistensen af transcendente Tal eftervist; senere viste som bekendt Cantor (C.1845-1918), at Mængden af algebraiske Tal (over $\mathbb{Q}$) er numerabel, medens $\mathbb{R}$ ikke er numerabel, hvoraf ogsaa følger Eksistensen af transcendente Tal. Liouville viste nemlig, at <u>dersom ξ er Rod i Polynomiet $P(t)$ over $\mathbb{Q}$, og deg $P = n$, saa vil for enhver Følge af Tilnærmelsesbrøker $\frac{x}{y}$ til ξ gælde at Afvigelsen $\left|\xi - \frac{x}{y}\right| > C \cdot y^{-n}$, hvor C er en positiv Konstant.</u>

Bevis: Vi kan gerne antage at $P(t)$ har heltallige Koefficienter (ellers gangede vi med Fællesnævneren) og

antage ξ irrational, da vi ovenfor har vist Sætningen for $n = 1$, men iøvrigt vilde det nu følgende Bevis med enkelte verbale Ændringer ogsaa fungere for $n = 1$. Metoden er den samme som blev brugt ved Beviset for at $\sqrt{5}^{-1}$ er bedste Konstant i Hurwitz's Sætning. Vi har

$$\left|P\left(\frac{x}{y}\right)\right| = \left|\left(\frac{x}{y} - \xi\right) \cdot \underbrace{P_{n-1}\left(\frac{x}{y}\right)}\right| = \left|\frac{\text{heltallig}}{y^n}\right| \geqq \frac{1}{y^n},$$

og da Faktoren $\smile$ er begrænset for $\frac{x}{y}$ i Nærheden af ξ ses direkte at $\left|\xi - \frac{x}{y}\right| > C \cdot y^{-n}$. □

Senere fandt man en Række Forbedringer af dette Resultat, idet Eksponenten $n = \deg P$ kunde erstattes med mindre Funktioner af n, og i 1955 lykkedes det Roth (eng.) at vise, at for alle Tal som er irrationale og algebraiske over $\mathbb{Q}$ er den bedst mulige Eksponent lig 2 (altsaa uafhængig af deg P): <u>For enhver Følge af Tilnærmelsesbrøker $\frac{x}{y}$ til et irrationalt algebraisk ξ og ethvert positivt ε er $\left|\frac{x}{y} - \xi\right| > y^{-2-\varepsilon}$ fra et vist Trin.</u>

Ligningen $x^2 - D y^2 = 1$.

Den anførte Ligning, i hvilken D er givet og x,y søges, alt indenfor $\mathbb{Z}$, kaldes "Pells Ligning" (P.1610-1685); Benævnelsen skyldes en Fejltagelse fra Eulers Side, og iøvrigt var allerede Fermat helt klar over Ligningens Forhold, saa man ser den ogsaa lejlighedsvis kaldt "Fermats Ligning".

Den er et Eksempel paa det som man i nyere Tid forstaar ved "Diofantiske Ligninger", d.v.s. Ligninger for hvilke der søges Heltalsløsninger (medens Ligningerne opfattet over $\mathbb{R}$ er "ubestemte", idet man til ethvert y kan finde et x). Diofant (ca. 250 e.Chr.(?)) skrev et Værk om saadanne Ligninger, hvori han dog fortrinsvis søgte Løsninger indenfor $\mathbb{Q}$ (som jo var det da "anerkendte" Talomraade, smlgn. ogsaa den foran benyttede moderne Betegnelse "Diofantisk Approksimation"). Diofant angav dog kun skarpsindige Metoder til at naa frem til specielle Løsninger, om Løsningsmængderne var fuldstændige interesserede ham ikke. Som omtalt (S.90) blev Diofant udgivet 1621 af Bachet (B.1581-1638) med Tilføjelser (en af dem omtales i næste Kapitel), og en Del af Fermats Opdagelser blev skrevet som Randnotater i hans Eksemplar af Bogen, og efter hans Død blev den saa genudgivet af hans Søn med Randnotaterne.

Men lad os først betragte Ligningen $x^2 - Dy^2 = 1$ i en almen Ramme, som omfatter baade Heltals- og Rationaltalssituationen:

Vi ser paa

$$\left.\begin{array}{l} x^2 - Dy^2 = 1\ , \quad \text{med } D \neq 0 \text{ givet} \\ x \text{ og } y \text{ søges} \end{array}\right\} \quad \begin{array}{l} \text{i en Delring } M \\ \text{af } (\mathbb{C}, +, \cdot). \end{array}$$

Man ser, at hvis der er Løsninger, saa vil M indeholde Tallet 1, og følgelig være en Integritetsring.

Vi vælger en fast Værdi for $\sqrt{D} \in \mathbb{C}$, ($\sqrt{D}$ i eller udenfor M), og lad L være Mængden af (x,y) som tilfredsstiller Ligningen. Vi betragter Afbildningen φ: $L \to \mathbb{C}$, givet ved

$$(x,y) \mapsto \varphi(x,y) = x + y\sqrt{D} .$$

Afbildningen er injektiv, thi Ligningen kan skrives som $(x + y\sqrt{D})(x - y\sqrt{D}) = 1$, hvoraf ses at for $\varphi(x,y) = a$ bliver $x - y\sqrt{D} = 1/a$, og derfor $x = (a + \frac{1}{a})/2$ og $y = (a - \frac{1}{a})/2\sqrt{D}$.

Endvidere: Billedmængden $\varphi(L)$ er en Undergruppe i $(\mathbb{C}^*, \cdot)$.

Bevis: 1) Da trivielt $(1,0) \in L$ vil $\varphi(1,0) = 1 \in \varphi(L)$.

2) Trivielt haves: $(x,y) \in L \Rightarrow (x,-y) \in L$, og derfor $a \in \varphi(L) \Rightarrow \frac{1}{a} \in \varphi(L)$.

3) $(x,y) \in L$ giver $(x + y\sqrt{D})(x - y\sqrt{D}) = 1$

$(u,v) \in L$ giver $(u + v\sqrt{D})(u - v\sqrt{D}) = 1$,

som ved Multiplikation (af de to Førstefaktorer og de to Sidstefaktorer) giver

$$((xu+Dyv) + (xv+yu)\sqrt{D})((xu+Dyv) - (xv+yu)\sqrt{D}) = 1 ,$$

som viser at $(xu+Dyv, xv+yu) \in L$ og at φ-Værdien af dette er $\varphi(x,y) \cdot \varphi(u,v)$.

Samtidig havde vi Bijektionen $L \Leftrightarrow \varphi(L)$, og vi ser ved at bruge φ^{-1} at Løsningsmængden L kan organiseres som en Gruppe med Neutralelementet (1,0) og hvor det inverse til (x,y) er (x,-y) og hvor Gruppekompositionen $\circ$ er givet ved

$$(x,y) \circ (u,v) = (xu + Dyv, xv + yu).$$

Det er trivielt, at L foruden (1,0) indeholder (-1,0), men Gruppens Størrelse og Struktur afhænger iøvrigt af det givne M og D, og til Hjælp ved Undersøgelsen af dens Egenskaber kan vi benytte Kendskabet til multiplikative Undergrupper i $(\mathbb{C}^*, \cdot)$.

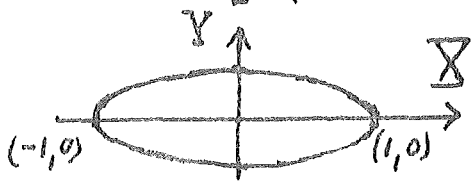
Eksempel: $M = \mathbb{Z}$ og $D = -2$. Ligningen er $x^2+2y^2 = 1$, med eneste Løsninger (1,0) og (-1,0). Gruppen $(\varphi(L), \cdot)$ er blot $(\{\pm 1\}, \cdot)$.

For de umiddelbare Anvendelser er de vigtigste Tilfælde dem hvor M er reel; her kommer en væsentlig Forskel eftersom D er negativ eller positiv.

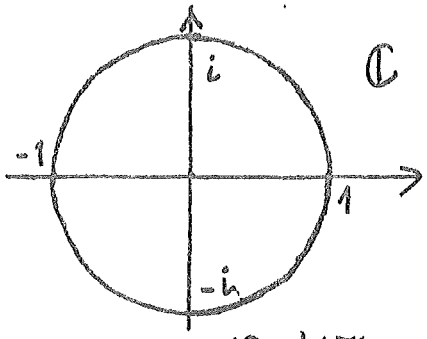
Tilfældet $M \subseteq \mathbb{R}$, D negativ.

Lad os først antage, at $M = \mathbb{R}$. Som $\sqrt{D}$ tages $i\sqrt{|D|}$, det ligger ikke i M, og naar vi adjungerer det faar vi $M[\sqrt{D}] = \mathbb{C}$.

Ligningen er $x^2 - Dy^2 = 1$, som i en XY-Plan fremstiller en Ellipse, og det er altsaa Løsningsmængden L.

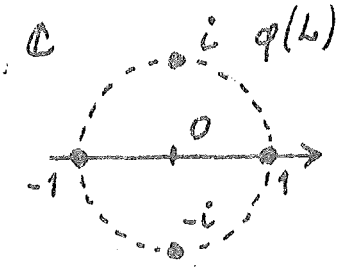


Billedet $\varphi(L)$ bliver bestemt ved at $\varphi(x,y) = x + i\sqrt{|D|}y$, som ses at fremstille Enhedscirklen i $\mathbb{C}$-Planen, og Gruppen $(\varphi(L),\cdot) = (\{e^{2\pi iv}\},\cdot)$ med v reel, altsaa isomorf med Gruppen af Drejninger om et Punkt, d.v.s. en Gruppe af Typen $(\mathbb{R},+)/\mathbb{Z}$, altsaa som de reelle Tal modulo 1.

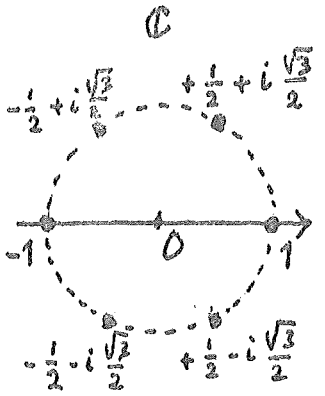


Dette gælder for alle $D < 0$, hvoraf man ser, at dersom vi har et $M \subset \mathbb{R}$, saa vil Gruppen $(\varphi(L),\cdot)$ blive en Undergruppe af den nævnte. Foran blev nævnt et Eksempel paa dette, med $\varphi(L) = \{\pm 1\}$, lad os give endnu et Par Eksempler.

Eksempel [1]): $M = \mathbb{Z}$, $D = -1$ giver Ligningen $x^2 + y^2 = 1$ med Løsningerne $(\pm 1,0)$ og $(0,\pm 1)$; i en $\mathbb{C}$-Plan afbildes $\varphi(L)$ som de 4 Punkter ± 1 og $\pm i$ beliggende paa Enhedscirklen; hvis man afbilder L i en XY-Plan faar man en Figur med de samme 4 Punkter, men nu betegnet $(\pm 1,0)$ og $(0,\pm 1)$.



Eksempel 2): $M = \mathbb{Z}\left[\frac{1}{2}\right]$, $D = -3$. Ligningen er $x^2 + 3y^2 = 1$, og der spørges om Løsninger, der kan skrives som Brøker hvis Nævner er en Potens af 2, altsaa paa Formen $\frac{r}{t}$ hvor r er 0 eller ulige og hvor t er en Potens af 2 ($\geqq 1$). Multipliceres Ligninger med Fællesnævneren faar den Formen $r^2 + 3s^2 = t^2$; her er t en Potens af 2, og mindst et af Tallene r og s er ulige; da et ulige Kvadrat er $\equiv 1 \pmod 8$ ses at $t \geqq 4$ er umulig, og saa bliver der kun Løsningerne (r,s,t) lig $(\pm 1, 0, 1)$ eller lig $(\pm 1, \pm 1, 2)$, d.v.s. (x,y) lig $(\pm 1, 0)$ eller lig $(\pm\frac{1}{2}, \pm\frac{1}{2})$. Der er altsaa 6 Løsninger, og Gruppen $(\varphi(L), \cdot)$ kommer til at bestaa af de 6 paa Fig. viste Punkter paa den komplexe Enhedscirkel.



Rationale Værdier for (cos v, sin v); Pytagoræiske Tal:

Med $M = \mathbb{Q}$, $D = -1$ faas Ligningen $x^2 + y^2 = 1$, og man ser at Problemet kan opfattes som at spørge om rationale Værdisæt for (cos v, sin v).

Idet $\operatorname{tg}\frac{v}{2}$ sættes lig t har man som bekendt Formlerne

$$\cos v = \frac{1-t^2}{1+t^2}, \quad \sin v = \frac{2t}{1+t^2} \quad \text{og} \quad t = \frac{1-\cos v}{\sin v} = \frac{\sin v}{1+\cos v};$$

(i hvilke man paa en selvfølgelig Maade kan regne med $t = \infty$). Man ser at (cos v, sin v) er rationale hvis og kun hvis t er rational. Vi har altsaa dermed at de rationale Løsninger til Ligningen $x^2 + y^2 = 1$ er givet ved $x = \frac{1-t^2}{1+t^2}$, $y = \frac{2t}{1+t^2}$, hvor t er en Parameter som gennemløber $\mathbb{Q}$.

Og $\varphi(L)$ bestaar altsaa af Tallene $x + iy = \cos v + i \sin v$, hvor $\operatorname{tg}\frac{v}{2}$ er rational, og disse udgør med Multiplikation en Gruppe, i Overensstemmelse med at de Vinkler $\frac{v}{2}$ som har en

rational Tangens udgør en Gruppe ved Addition (idet der som bekendt er en rational Formel for tg (u+v) udtrykt ved tgu, tgv).

Ved pytagoræiske Tal (x,y,z) forstaas et Sæt af naturlige Tal som opfylder Ligningen $x^2 + y^2 = z^2$, d.v.s. som kan indgaa som Sider i en retvinklet Trekant. Da Ligningen ogsaa kan skrives $(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1$ føres det over i den ovenfor løste Opgave.

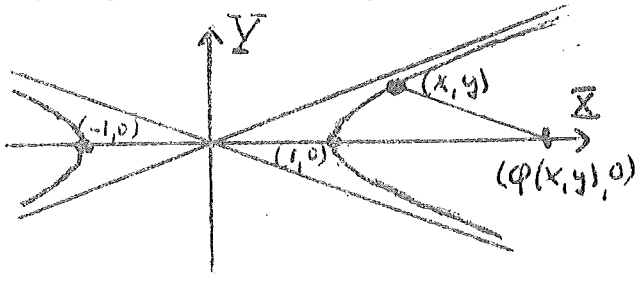
Sættes $t = \frac{r}{s}$ og indsættes det i Formlerne, faar man i den herværende Situation $\frac{x}{z} = \frac{s^2 - r^2}{s^2 + r^2}$, $\frac{y}{z} = \frac{2rs}{s^2 + r^2}$, hvoraf faas at samtlige Løsninger i naturlige Tal til Ligningen $x^2 + y^2 = z^2$ er givet ved Formlerne

$$x = s^2 - r^2 , \quad y = 2rs , \quad z = s^2 + r^2$$

og alt hvad der kan faas ved at multiplicere eller dividere disse tre Tal med en fælles Faktor; i Formlerne betyder r og s naturlige Tal, $r < s$. (Begrænsningerne i Variationsmængderne for r og s følger trivielt af at der ønskes $x,y,z \in \mathbb{N}$).
Det bør bemærkes, at selvom (r,s) = 1, altsaa $\frac{r}{s}$ er uforkortelig, saa kan de anførte Udtryk for x,y og z godt have en fælles Faktor 2 (at der ikke kan være andre fælles Faktorer ses umiddelbart), nemlig hvis r og s begge er ulige.
Eksempel: For $r=1, s=2$ faas $x=3, y=4, z=5$.

Tilfældet $M \subsetneq \mathbb{R}$, D positiv.

Lad os først antage at $M = \mathbb{R}$. Som $\sqrt{D}$ tages den positive Kvadratrod, den er indeholdt i M, saa Adjunktion af den betyder ingen Udvidelse af $M = \mathbb{R}$. Ligningen er $x^2 - Dy^2 = 1$, som i en XY-Plan fremstiller en Hyperbel, og det er altsaa Løsningsmængden L. Billedet $\varphi(L)$ er bestemt ved at $\varphi(x,y)$



$= x + y\sqrt{D}$, som bliver et reelt Tal, der kan faas ved den paa Figuren angivne Konstruktion (gennem (x,y) er trukket en Linie parallel med den anden Asymptote, og dens Skæringspunkt med X-Aksen giver $\varphi(x,y)$), og man ser at $\varphi(L)$ netop bliver $\mathbb{R}^*$.

Dette gælder for alle $D > 0$, hvoraf man ser, at dersom vi har et $M \subset \mathbb{R}$, saa vil Gruppen $(\varphi(L),\cdot)$ blive en Undergruppe af $(\mathbb{R}^*,\cdot)$. Da vi altid har $-1 \in \varphi(L)$ vil Gruppen med t altid indeholde $-t$, og kan derfor skrives som et direkte Produkt $(\varphi(L),\cdot) = (\{\pm 1\},\cdot) \times (\varphi^+(L),\cdot)$, hvor $\varphi^+(L) = \varphi(L) \cap \mathbb{R}^+$. Denne sidste Gruppefaktor som er Undergruppe i $(\mathbb{R}^+,\cdot)$ overføres ved at tage Logaritmen til en Undergruppe i $(\mathbb{R},+)$ og dermed til noget relativ bekendt.

Man ser (smlgn. ogsaa den paa Fig. angivne Konstruktion af $\varphi(x,y)$ udfra (x,y)) at man kan inddele i følgende tre Tilfælde:

I°. Hvis Ligningen kun har Løsningerne $(\pm 1,0)$ vil $\varphi^+(L)$ kun bestaa af det ene Tal 1.

II°. Hvis der findes et mindste $y > 0$ som indgaar i en Løsning (x,y) til Ligningen, saa har $\varphi^+(L)$ et mindste Element a større end 1, og $\varphi^+(L) = \{a^n,\ n \in \mathbb{Z}\}$.

III°. Ellers vil der findes y-Værdier vilkaarlig nær 0 som indgaar i Løsninger (x,y), og Mængden $\varphi^+(L)$ vil blive overalt tæt paa den positive reelle Akse.

Man bemærker, at der er væsentlige Forskelle fra Tilfældet $D < 0$. For det første, at det for $D > 0$ altid er muligt at fraspalte en Gruppefaktor $(\{\pm 1\},\cdot)$, noget saadant er ikke muligt i Eksempel [1]) (S.173), hvor Gruppestrukturen var $\tilde{C}_4$. Endvidere at vi for $D > 0$ kun har Elementerne ± 1 med egl. Potenser som er lig 1, medens der for $D < 0$ kan være mange saadanne ("Torsions-

elementer"). Og at dersom der findes en Løsning (x_1,y_1) med mindste positivt x (y), saa vil Gruppen for $D > 0$ være direkte Produkt af $(\{\pm 1\},\cdot)$ og en uendelig cyklisk Gruppe (hvis Frembringerelement er $x_1+y_1\sqrt{D}$), medens Gruppen for $D < 0$ er endelig cyklisk af lige Orden (med tilsvarende Frembringerelement).

Pell's Ligning.

Vi skal som nævnt betragte $x^2 - Dy^2 = 1$, hvor $D \in \mathbb{N}$ er givet, og hvor (x,y) søges indenfor $\mathbb{Z}$.

Det har kun Interesse at se paa Tilfældet hvor D ikke er Kvadrattal. Thi hvis D er et Kvadrat udtrykker Ligningen at to Kvadrattal skal have Differensen 1, og eneste Løsning bliver $(x,y) = (\pm 1,0)$, altsaa Tilfældet I^o ovenfor.

Det er klart at med heltallige y kan Tilfælde III^o ikke indtræffe, men vi vil vise at Tilfælde II^o altid indtræffer, altsaa følgende Sætning:

Antag D er et positivt helt Tal, ikke et Kvadrattal. Da vil Ligningen $x^2 - Dy^2 = 1$ have uendelig mange Løsningssæt $(x,y) \in \mathbb{N}^2$, og hvis disse ordnet efter Størrelse benævnes $(x_1,y_1),(x_2,y_2),\ldots$, kan (x_n,y_n) faas af Formlen $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$, eller udtrykt induktivt $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

Bemærkninger: Størrelsesordningen er entydig, da større x svarer til større y. Samtlige Løsninger $\in \mathbb{Z}^2$ til Ligningen faas af de ovennævnte ved at skifte Fortegn for x og y, og endvidere medtage $(\pm 1,0)$, og dette kan saa ifølge det tidligere ogsaa udtrykkes ved at $x + y\sqrt{D} = \pm(x_1 + y_1\sqrt{D})^n$, hvor $n \in \mathbb{Z}$; Meningen med denne Formel er at $\pm(x_1 + y_1\sqrt{D})^n$ kan udregnes, hvorved faas et Udtryk $a + b\sqrt{D}$, hvor saa $a = x$ og $b = y$, men

da $\sqrt{D}$ er irrational ses, at alene Talværdien $\in \mathbb{R}$ af $a+b\sqrt{D}$ entydigt bestemmer Værdierne $\in \mathbb{Z}$ af a og b. Den induktive Formel faas af $x_{n+1} + y_{n+1}\sqrt{D} = (x_1+y_1\sqrt{D})(x_n+y_n\sqrt{D})$ ved at udvikle efter $\sqrt{D}$.

Bevis: Problemet er blot at vise, at der findes en Løsning (x,y) med $y \neq 0$, thi saa maa Tilfælde II° indtræffe. Det vil ske som en smuk Anvendelse af Skuffeprincippet.

Vi har

$$|x^2-Dy^2| = |(x+y\sqrt{D})(x-y\sqrt{D})| = \left|\frac{x}{y} - \sqrt{D}\right| \cdot \left|\frac{x}{y} - \sqrt{D} + 2\sqrt{D}\right| \cdot y^2 ,$$

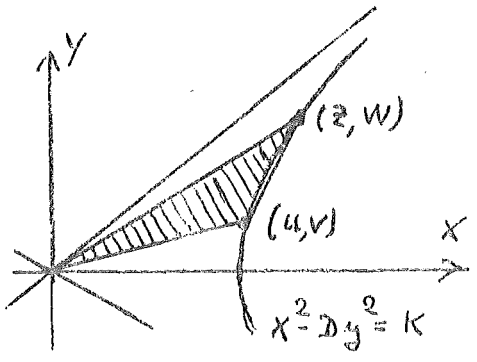
og da $\sqrt{D}$ er irrational vil der ifølge Hurwitz's Sætning findes uendelig mange (x,y) for hvilke dette er mindre end

$$\frac{1}{\sqrt{5}\cdot y^2} \cdot \left|\frac{1}{\sqrt{5}\cdot y^2} + 2\sqrt{D}\right| \cdot y^2 < \sqrt{D} \qquad (\text{da } 2 < \sqrt{5}) .$$

Ifølge Skuffeprincippet findes da et K (med $|K| < \sqrt{D}$), saa Ligningen $x^2 - Dy^2 = K$ har uendelig mange Løsninger. Her er $K \neq 0$ for ellers var jo $\sqrt{D} = \frac{x}{y}$, altsaa rational.

Ifølge Skuffeprincippet findes blandt disse (x,y) en uendelig Delmængde for hvilken alle x-Værdierne er kongruente modulo $|K|$, og ifølge Skuffeprincippet vil der blandt dem igen findes to, for hvilke y-Værdierne er kongruente modulo $|K|$. Lad os kalde disse to Værdisæt for (u,v) og (z,w).

Vi har altsaa $u^2-Dv^2 = z^2-Dw^2 = K$, hvor (u,v) og (z,w) er to forskellige Punkter paa Hyperblen $x^2-Dy^2=K$, og hvor $K|u-z$ og $K|v-w$.



Vi sætter saa

$$x = \frac{uz - Dvw}{K} \quad \text{og} \quad y = \frac{uw - zv}{K} ,$$

og af Figuren ses at $y \neq 0$, thi $uw - zv = \det\begin{pmatrix} u & v \\ z & w \end{pmatrix}$ angiver

jo det dobbelte af det skraverede Trekantsareal. Endvidere er x og y begge heltallige, thi modulo K er Tælleren i x kongruent $u^2-Dv^2 = K$, og Tælleren i y er kongruent $uv-uv = 0$.

Sluttelig skal vi vise, at x og y opfylder $x^2 - y^2 = 1$, og det faas af

$$x^2 - Dy^2 = \frac{(uz-Dvw)^2 - D(uw-zv)^2}{K^2} = \frac{(u^2-Dv^2)(z^2-Dw^2)}{K^2} = 1 ,$$

(i den første Brøk gaar de dobbelte Produkter ud mod hinanden). □

For $n \to \infty$ vil x_n og $y_n \to \infty$, og da $x_n+y_n\sqrt{D} = a$ medfører (S.172) at $x_n = (a + \frac{1}{a})/2$ og $y_n = (a - \frac{1}{a})/2\sqrt{D}$ ses, at x_n vokser som $(x_1+y_1\sqrt{D})^n/2$ og y_n vokser som $x_n/\sqrt{D}$.

"Grundløsningen" (x_1,y_1) afhænger paa meget springende Maade af D. Det hænger sammen med Harosbrøker (og Kædebrøksudviklinger), idet man af Beviset foran ser at x_1/y_1 skal være en god Tilnærmelse til $\sqrt{D}$, da den skal opfylde at $\frac{x}{y} - \sqrt{D} \sim 1/2\sqrt{D}y^2$. Men det er vanskeligt at give ret meget System i det, og der er derfor i Tidens Løb publiceret en Del Tabeller (bl.a. af Degen, 1766-1825, dansk).

Taleksempel: Løs $x^2 - 2y^2 = 1$ indenfor $\mathbb{Z}$.

Ved Forsøg finder man at $3^2 - 2\cdot2^2 = 9 - 8 = 1$, og Grundløsningen er (3,2). Samtlige Løsninger er $(\pm x_n, \pm y_n)$, hvor Følgen kan bestemmes induktivt ved $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

n	x_n	y_n
0	1	0
1	3	2
2	17	12
3	99	70
4	577	408

De første Værdisæt er angivet i Tabellen. Værdierne gaar mod uendelig som Kvotientrækker med Kvotient $3 + 2\sqrt{2} \sim 5{,}8\ldots$. □

Løsningen af Pells Ligning er nært beslægtet med Opgaven: "Indenfor Ringen $\mathbb{Z}[\sqrt{D}]$ ønskes de invertible Elementer bestemt." Thi man ser at $x + y\sqrt{D}$ er invertibel naar og kun naar $(x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2$ er lig $+1$ eller -1. Den første Mulighed er Pells Ligning, og specielt ses altsaa, at der er uendelig mange invertible Elementer i Ringen (saafremt $\sqrt{D}$ er irrational, d.v.s. at Ringen er en ægte Udvidelse af $\mathbb{Z}$). Den anden Mulighed fører til Ligningen $x^2 - Dy^2 = -1$, som man betegner som den Ikke-Pell'ske Ligning (en fra et logisk Synspunkt ejendommelig Betegnelse). Den har sommetider Løsninger, fx for $D = 5$, $(x = 2, y = 1)$, og sommetider har den det ikke, fx for $D = 3$ (da $x^2 \equiv -1$ modulo 3 ikke kan opfyldes), og iøvrigt kan man knap sige at dens Forhold er helt afklaret.

Forbindelsen mellem Approksimationssætninger og diofantiske Ligninger var væsentlig for det foregaaende. En stærkere Approksimationssætning som Roth's Sætning (S.170) er ogsaa af Betydning for diofantiske Ligninger. Fx ses at Ligningen $x^4 - 5y^4 = 1$ kun kan have endelig mange Løsninger, thi

$$x^4 - 5y^4 = \left|\frac{x}{y} - \sqrt[4]{5}\right| \cdot \left|\left(\frac{x}{y}\right)^3 + \ldots\right| \cdot y^4 = 1$$

giver, idet $\left|\left(\frac{x}{y}\right)^3 + \ldots\right| > c$ for et $c > 0$ for $\frac{x}{y}$ nær $\sqrt[4]{5}$ er, at $\left|\frac{x}{y} - \sqrt[4]{5}\right| < \text{konst} \cdot y^{-4}$, hvilket ifølge Roth kun er opfyldt af endelig mange (x,y); Ligningen har ikke-trivielle Løsninger, fx $(x,y) = (3,2)$.

Eksempel paa Teknik:

Opskrives Pascals Trekant (S.37ff) møder man to lige store Binomialkoefficienter, nemlig $\binom{14}{8}$ og $\binom{15}{10}$ som begge er lig 3003. Hvis man ser bort fra Trekantens Symmetri og Randrækkerne $\binom{m}{0} = 1$ og $\binom{m}{1} = m$ synes Fænomenet sjældent forekommende.

Lad os prøve om vi kan finde andre Eksempler paa at

$\binom{m-1}{k-1} = \binom{m}{k+1}$ (det nævnte svarer til m = 15, k = 9).

Hvis man indsætter Udtrykkene for Binomialkoefficienterne kan det meste forkortes bort, og man faar Ligningen $k(k+1) = m(m-k)$, eller $k^2 + mk - m^2 + k = 0$. Der søges Løsninger $m,k \in \mathbb{N}$. Udtrykket kan paa sædvanlig Maade omskrives til en Sum af rene Kvadrater, og man kan faa

$$(\tfrac{5}{2}k + 1)^2 - 5\cdot(m - \tfrac{k}{2})^2 = 1 .$$

(Omskrivningen kan foretages paa mange Maader, men da den kvadratiske Form i den foregaaende Ligning har Determinanten $-\frac{5}{4}$ kan Facit aldrig blive væsensforskelligt fra det her anførte). Vi har altsaa en Ligning $x^2 - 5y^2 = 1$, men har Brug for Løsninger, som gerne maa ligge i $\mathbb{Z}[\frac{1}{2}]$. Paa samme Maade som i Eks.[2]) (S.174) ser man - ved at benytte at et ulige Kvadrat altid er $\equiv 1 \pmod 8$ - at x og y ikke kan have Nævnere større end 2. Følgelig er Tilfælde III° udelukket, og da vi paa den anden Side ved, at Ligningen har ikke-trivielle Heltalsløsninger (naar vi opfatter den som en Pell'sk Ligning), saa maa vi have Tilfælde II°, og der maa være en Løsning med et mindste y. Allerede $y = \frac{1}{2}$ giver en Løsning, nemlig med $x = \frac{3}{2}$.

Samtlige Løsninger med $x,y \in \mathbb{Q}^+$ faas af $x_n + y_n\sqrt{5} = (\frac{3}{2} + \frac{1}{2}\sqrt{5})^n$, eller induktivt udtrykt af

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{pmatrix} \frac{3}{2} & \frac{5}{2} \\ \frac{1}{2} & \frac{3}{2} \end{pmatrix} \cdot \begin{bmatrix} x_n \\ y_n \end{bmatrix} .$$

Naar vi lader n gennemløbe $\mathbb{Z}$ faar vi herved frembragt Gruppen af Løsninger med positivt x. Den skal som Undergruppe indeholde Heltalsløsningerne til den Pell'ske Ligning, og hvis man regner fremad finder man at $x_3 = 9$, $y_3 = 4$, som altsaa er Grundløs-

ningen til Pellligningen, og denne Lignings Løsninger faas saa som (x_{3h}, y_{3h}).

Men vor Opgave er at finde Løsninger $x_n = \frac{5}{2}k + 1$, $y_n = m - \frac{k}{2}$, altsaa med $x_n \equiv 1 \pmod 5$. Af Matrixfremstillingen ses at $x_{n+1} \equiv -x_n \pmod 5$, og da $x_o = 1$ skal vi aabenbart bruge lige Indices $n = 2j$, men saa er det ogsaa godt, thi af $x^2 - 5y^2 = 1$ ses at x og y begge er hele, hhv. ikke-hele, og at det indtræffer for k lige, hhv. ulige. Vi finder

j	x_{2j}	y_{2j}	k	m	ens Binomialkoeffic.
1	7/2	3/2	1	2	$\binom{1}{0} = \binom{2}{2}$
2	47/2	21/2	9	15	$\binom{14}{8} = \binom{15}{10}$
3	161	72	64	104	$\binom{103}{63} = \binom{104}{65}$
		o.s.v			

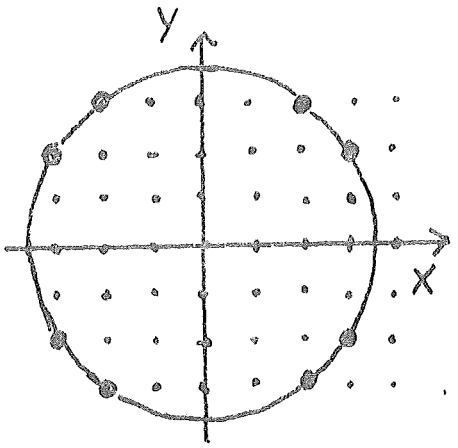
Ved Hjælp af Matricerne kan vi ogsaa finde den lineære Overgang fra et Par (k,m) til det paafølgende (k',m'). Man finder

$$\begin{bmatrix} k' \\ m' \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \cdot \begin{bmatrix} k \\ m \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

Men Ligningen $k(k+1) = m(m-k)$ kan ogsaa løses paa helt anden Maade. Den kan skrives $m^2 = k(m+k+1)$; for et Primtal p vil $p|k \Rightarrow p|m \Rightarrow p \nmid m+k+1$, hvoraf følger at $(k, m+k+1) = 1$, og begge Højresidens Faktorer er derfor Kvadrater, $k = b^2$, $m+k+1 = a^2$ og $m = ab$, og vi skal løse $ab+b^2+1 = a^2$. Her er $a > b$, og vi sætter $a = b+c$. Saa faas $b^2 = bc + c^2 - 1$. Sættes $b = c+d$ faas $cd+d^2+1 = c^2$, altsaa samme Ligning i (c,d) som ovenfor i (a,b), og vi har en "Descente", men ikke "infinie", idet den "vender nede i Bunden" (ved de trivielle Løsninger). Men naar enhver større Løsning faas udfra en mindre, faar man en Kæde af Løsninger. Følgen a,b,c,d,.. er dannet paa samme Maade, men i modsat Retning, som Fibonaccis Følge (S.135), og man kan kontrollere at Bundløsningen svarer til Begyndelsen af Fibonaccifølgen. For de søgte $k = b^2$ og $m = ab$ finder man med det ovenfor brugte Index j og med Benævnelserne fra S.135 at $k = h(2j-2)^2$ og $m = h(2j-2)h(2j-1)$. Da $64 = 8^2$, $104 = 8 \cdot 13$,.. ses at det stemmer.

KAPITEL X: Tals Fremstilling som Sum af Kvadrattal.

Det første Problem som skal løses er: Hvilke Tal kan - og i bekræftende Fald paa hvor mange Maader - skrives som en Sum $n = x^2 + y^2$ af to Kvadrattal ?



Nærmere præciseret skal Antallet af Løsninger $(x,y) \in \mathbb{Z}^2$, for hvilke $x^2+y^2 = n$, betegnes $4F(n)$, og vi skal bestemme dette Antal. Man ser, at det geometrisk kan fortolkes som Antallet af Gitterpunkter i en XY-Plan som ligger paa Cirklen $x^2+y^2 = n$, og af umiddelbare Symmetrigrunde ses at Tallet er deleligt med 4, saa Betegnelsen $4F(n)$ er rimelig.

Til det Formaal skal først bestemmes Antallet $4G(n)$ af primiske Løsninger, d.v.s. Antallet af (x,y) for hvilke $(x,y) = 1$ foruden at $x^2+y^2=n$. Vi har $G(1) = 1$ (nemlig Løsningerne $(\pm 1,0)$ og $(0,\pm 1)$), Og for $n > 1$ ses at $G(n)$ angiver Antallet $(x,y) \in \mathbb{N}^2$ for hvilke $x^2+y^2 = n$ (idet x eller y ikke kan være 0 for disse n hvis de skal være indbyrdes primiske).

Naar G er fundet kan F bestemmes af Formlen $F(n) = \sum G(\frac{n}{k^2})$, hvor der summeres over de k for hvilke $k^2 | n$. Thi Antallet af $x^2+y^2 = n$ med $(x,y) = k$ ses at være det samme som Antallet af primiske Par $(\frac{x}{k},\frac{y}{k})$, for hvilke $(\frac{x}{k})^2+(\frac{y}{k})^2 = \frac{n}{k^2}$. Man ser, at denne Summation kan opfattes som en Foldning $F = G * h$, hvor

$$h(m) = \begin{cases} 1 & \text{saafremt } m = k^2 = \text{et Kvadrat} \\ 0 & \text{ellers} \end{cases};$$

Funktionen h er multiplikativ (et Produkt af to indbyrdes pri-

miske Faktorer er et Kvadrat hvis og kun hvis begge Faktorerne er Kvadrater), og da det skal vise sig at G bliver multiplikativ faar vi dermed ogsaa at F bliver multiplikativ.

Vi vil nemlig bevise, at G(n) er lig Antallet af Restklasser $\textcircled{a} = A \in \mathbb{Z}_n$ for hvilke $A^2 + \textcircled{1} = 0$, og da vi tidligere (S.142) har vist at Antallet af Løsningsrestklasser til en algebraisk Kongruens er en multiplikativ Funktion af Modulen n, faar vi dermed at G og F bliver multiplikative.

Bevis (for paastanden om G(n)): Naar $x^2+y^2 = n$ og $(x,y) = 1$ maa x og y hver for sig være primisk med n.

Følgende Afbildning har saa en Mening:

$$\varphi : (x,y) \mapsto \textcircled{a} = \textcircled{\frac{x}{y}} \in \mathbb{Z}_n .$$

Idet

$$0 = \textcircled{x^2+y^2} = \textcircled{y}^2 \cdot \textcircled{a^2+1}$$

ses at

$$\textcircled{a}^2 + \textcircled{1} = 0.$$

Vi har at φ injektiv. Thi antag $x^2+y^2 = u^2+v^2 = n$ med $x \geqslant u$, hvoraf følger $y \leqslant v$. Da er dels $xv - yu \geqslant 0$, og dels $xv - yu \leqslant xv < \sqrt{n}\cdot\sqrt{n} = n$, hvoraf ses at $xv - yu \not\equiv 0 \pmod{n}$.

Men saa er jo

$$\textcircled{\frac{x}{y}} - \textcircled{\frac{u}{v}} = \textcircled{\frac{xv - yu}{yv}} \not\equiv 0 .$$

Dernæst skal vi vise at φ er surjektiv over paa Mængden af Restklasser $\textcircled{a}$ med $\textcircled{a}^2 = \textcircled{-1}$. Dertil bruger vi følgende:

Thue's Sætning: (Axel Thue, 1863-1922, norsk) Lad n være givet, $n > 1$. Til et vilkaarligt a findes r og s saa $r \equiv as \pmod{n}$ og $|r| \leqslant \sqrt{n}$ og $0 < s \leqslant \sqrt{n}$.

Sætningen er ejendommelig ved at der ikke stilles nogen Krav om at a, r eller s skal være primiske med n, og der paastaas ikke noget om at r og s er entydigt bestemte. Man bemærker ogsaa at Antallet af tilladte Par (r,s) er omtrent 2n.

Bevis: Vi betragter Restklasserne $c - ad$, hvor

$$c \in [0,\sqrt{n}] \text{ , Antallet mulige c er } > \sqrt{n}$$
$$d \in [0,\sqrt{n}[\text{ , Antallet mulige d er } \geqq \sqrt{n} \text{ ;}$$

Antallet Par (c,d) er altsaa større end n, og der findes derfor $(c_1,d_1) \neq (c_2,d_2)$ saa $c_1 - ad_1 \equiv c_2 - ad_2$ (mod.n). Her er $d_1 \neq d_2$, idet $d_1 = d_2$ vilde medføre $c_1 = c_2$ (NB her benyttes at $n > 1$); lad os antage $d_1 > d_2$. Vi tager saa $s = d_1 - d_2$ og $r = c_1 - c_2$, og da $c_1 - c_2 \equiv a(d_1 - d_2)$ har vi $r \equiv as$ som ønsket, og endvidere at r og s opfylder de forlangte Størrelseskrav. Dermed er Thues Sætning bevist. (□)

Lad nu a være saaledes at $\left(\frac{a}{n}\right)^2 = \left(\frac{-1}{n}\right)$. Vi tager r og s fra Thues Sætning, og af Begrænsningerne for deres Størrelse har vi at $0 < r^2 + s^2 < 2n$, og da endvidere $r^2+s^2 \equiv s^2(a^2+1) \equiv 0$ modulo n, maa vi have $r^2+s^2 = n$. Heraf ses, at r og s har ingen fælles Faktor > 1, hvorfra r og s primiske mod n.
Da $r \equiv as$ hvor a er en primisk Restklasse og $s \not\equiv 0$ kan vi ikke have $r = 0$. Dersom $r > 0$ tager vi $x = r$ og $y = s$, og har saa $x^2 + y^2 = n$ med $x,y \in \mathbb{N}$ og $\left(\frac{x}{y}\right) = \left(\frac{a}{n}\right)$ som ønsket. Dersom $r < 0$ tager vi $x = s$ og $y = -r$, og har saa $x^2+y^2 = n$ med $x,y \in \mathbb{N}$ og $\left(\frac{x}{y}\right) = \left(\frac{-1}{a}\right) = \left(\frac{a}{n}\right)$ som ønsket.

Dermed har vi vist en Bijektion mellem Parrene (x,y) og Restklasserne $\left(\frac{a}{n}\right)$, og deres Antal er altsaa ens. □

Tidligere er nævnt at $G(1) = 1$, og vi kan nu angive Værdierne for $G(p^\alpha)$, $\alpha > 0$.

For $p = 2$ har vi $G(2) = 1$ da $a^2+1 \equiv 0$ (mod.2) har én Løsning, og ellers er $G(2^\alpha) = 0$ fordi ethvert ulige Kvadrat er af Form $4h + 1$.

For p af Form 4h+1 har vi $G(p^\alpha) = 2$ (se S.153; vi ved at -1 er kvadratisk Rest for et saadant Primtal).

For $p = 4h-1$ har vi $G(p^\alpha) = 0$ (S.153; -1 er kv.Ikke-Rest mod.p).

Vi kan nu bestemme F, og da vi ved at den bliver multiplikativ skal vi blot udregne $F(p^{\alpha}) = G(p^{\alpha}) + G(p^{\alpha-2}) + G(p^{\alpha-4}) + \ldots$.
For $p = 2$ er alle Led lig 0 undtagen sidste Led som er $G(2)$ eller $G(1)$, i begge Tilfælde lig 1. Følgelig er $\underline{F(2^{\alpha}) = 1.}$

For p af Form 4h+1 faar vi

$$F(p^{\alpha}) = \left\{ \begin{array}{ll} 2 + 2 + \ldots + 2 + 1 & \text{for } \alpha \text{ lige} \\ 2 + 2 + \ldots + 2 & \text{for } \alpha \text{ ulige} \end{array} \right\} = \alpha + 1$$

i begge Tilfælde, altsaa $\underline{F(p^{\alpha}) = \alpha + 1 \text{ for } p = 4h+1.}$

For p af Form 4h-1 faar vi

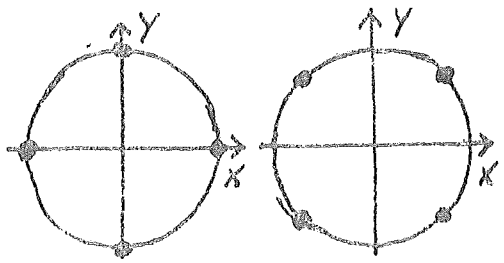
$$F(p^{\alpha}) = \left\{ \begin{array}{ll} 0 + 0 + \ldots + 0 + 1 & \text{for } \alpha \text{ lige} \\ 0 + 0 + \ldots + 0 & \text{for } \alpha \text{ ulige} \end{array} \right.$$

altsaa $\underline{F(p^{\alpha}) = \left\{ \begin{array}{l} 1 \text{ for } \alpha \text{ lige} \\ 0 \text{ for } \alpha \text{ ulige} \end{array} \right\} \text{naar } p = 4h-1.}$

Dermed har vi Sætningen: Et naturligt Tal n kan skrives som $n = x^2 + y^2$ med $4F(n)$ Stk. $(x,y) \in \mathbb{Z}^2$, hvor $F(n)$ er den multiplikative Funktion som er givet ved ovenstaaende Angivelser.
Specielt ses, at nødvendigt og tilstrækkeligt for at n kan skrives som en Sum af to Kvadrater er det, at hvis n indeholder Primfaktorer af Form $p = 4h-1$, da maa disse kun forekomme med lige Eksponenter.

Eksempel: $n = 450 = 2 \cdot 3^2 \cdot 5^2$. $F(450) = F(2)F(3^2)F(5^2) = 1 \cdot 1 \cdot 3$;
Der er altsaa $4 \cdot 3 = 12$ Skrivemaader for $450 = x^2+y^2$. De er $450 = (\pm 3)^2+(\pm 21)^2 = (\pm 21)^2+(\pm 3)^2 = (\pm 15)^2+(\pm 15)^2$.

Eksempel: Et ulige F(n) faas hvis og kun hvis alle de ulige Primfaktorer i n forekommer med lige Eksponent, d.v.s. hvis n er et Kvadrattal eller det dobbelte af et Kvadrattal; det ses at være i Overensstemmelse med at Cirklen $x^2+y^2 = n$ indeholder fire Punkter paa en af de to paa Figurerne viste Maader.



Medens de foregaaende Sætninger først er vist af Gauss, saa var følgende Specialtilfælde af den allerede kendt af Fermat:

Ethvert Primtal $p = 4h+1$ kan paa netop én Maade skrives som en Sum $p = x^2+y^2$ af to Kvadrattal $(x^2 > y^2 > 0)$. At et Primtal $p = 4h-1$ ikke kan skrives saadan er jo trivielt.

En fiks Formulering af Udtrykket for $F(n)$ findes i følgende:

Jacobi's Sætning: Vi har (J.1804-51)

$$F(n) = \sum_{d|n} \chi(d), \text{ hvor } \chi(d) = \begin{cases} 1 \text{ for } d \equiv 1 \pmod 4 \\ -1 \text{ for } d \equiv -1 \pmod 4 \\ 0 \text{ for } d \text{ lige.} \end{cases}$$

Bevis: Da man umiddelbart ser, at χ er en multiplikativ Funktion, vil $\sum_{d|n} \chi(d)$ ogsaa være det, og det er derfor tilstrækkeligt at eftervise Formlens Rigtighed for Primtalpotenser p^α.

Vi skal altsaa vise, at $\chi(1)+\chi(p)+\chi(p^2)+\ldots+\chi(p^\alpha) = F(p^\alpha)$.

For $p = 2$ faar vi $1+0+0+\ldots+0 = 1$, stemmer.

For $p = 4h+1$ faar vi $1+1+1+\ldots+1 = \alpha+1$, stemmer.

For $p = 4h-1$ faar vi $1-1+1-\ldots \pm 1 = \left\{ \begin{matrix} 1 \text{ for } \alpha \text{ lige} \\ 0 \text{ for } \alpha \text{ ulige} \end{matrix} \right\}$, stemmer. □

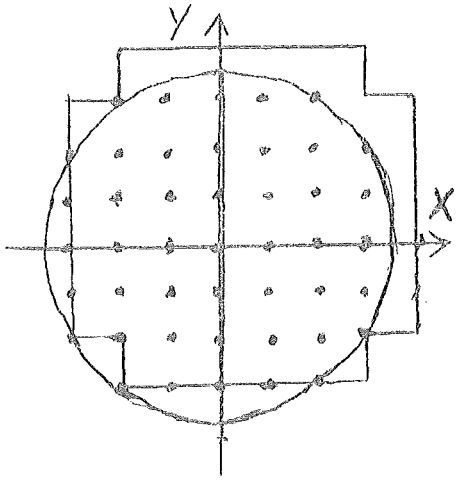
Eksempel: Vi tager igen $n = 450$, og skriver en Tabel over Divisorerne d og deres χ-Værdier (noterer blot +,0 eller -).

d	1	2	3	5	6	9	10	15	18	25	30	45	50	75	90	150	225	450
$\chi(d)$	+	0	-	+	0	+	0	-	0	+	0	+	0	-	0	0	+	0

og Sammentælning giver igen $F(450) = 3$.

Funktionen $\chi(d)$ er en saakaldt "Restkarakter", d.v.s. en Afbildning af $\mathbb{Z}$, hvor for et givet m (i dette Tilfælde $m = 4$) et Tal a først afbildes over i $(\bar{a}) \in \mathbb{Z}_m$, og dernæst Gruppen $(\mathbb{Z}_m^*, \cdot)$ af primiske Restklasser afbildes homomorft over i $(\mathbb{C}^*, \cdot)$, medens de ikke-primiske Restklasser afbildes over i 0. Saadanne Restkarakterer er et vigtigt Hjælpemiddel, fx til at bevise den ofte omtalte"Dirichlets Sætning" (et Bevis for den kunde sagtens indlægges i disse Forelæsninger, men det skal ikke gøres).

"Gennemsnitsværdien" af F(n) er $\frac{\pi}{4}$.



Det ses let, idet $4\sum_{n \leqq K} F(n)$ aabenbart er Antallet af Gitterpunkter i XY-Planen som ligger indenfor eller paa Cirklen $x^2+y^2 = K$; tager man nu sammen med hvert Gitterpunkt Enhedskvadratet (foroven, tilhøjre) ved Punktet faar man overdækket et Omraade, hvis Begrænsning har en Distance paa højst $\sqrt{2}$ til Cirkelperiferiens Punkter, og Arealet er derfor lig Cirklens Areal πK paanær en Afvigelse, hvis Størrelsesorden højst er som $\sqrt{K}$. Lader man $K \to \infty$ viser det sig iøvrigt, at F(n) bliver 0 for "næsten alle" n-Værdier, men at F(n) ogsaa kan antage vilkaarlig store Værdier. □

Dersom man her indsætter Udtrykket fra Jacobis Sætning (og ombytter Summationsordenen) faar man

$$\sum_{n \leqq K} F(n) = \sum_{d} \chi(d) \cdot \left[\frac{K}{d}\right] \sim \frac{\pi}{4} \cdot K ,$$

og hvis man saa benytter at $\left[\frac{K}{d}\right] \sim \frac{K}{d}$ har man (NB med en Del Forsigtighed i ε-Betragtninger og Fortegnsvurderinger) at

$$\frac{\pi}{4} = \sum_{d} \frac{\chi(d)}{d} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots ,$$

altsaa Leibniz's bekendte Formel.

Tal som Summer af fire Kvadrater.

Som nævnt (S.171) blev Diofant udgivet 1621 af Bachet med Tilføjelser. En af dem bestod i en Tabel, i hvilken alle Tal op til 325 blev skrevet som en Sum $n = x^2+y^2+z^2+v^2$ af (højst) fire Kvadrattal. Noget Bavis for at det altid var tilstrækkeligt med fire Kvadrater gav han ikke, men vi vil dog, som man ofte gør (og ogsaa for at have en karakteristisk Betegnelse), knytte hans Navn til Sætningen.

Bachet's Sætning: Ethvert naturligt Tal er en Sum af højst fire Kvadrattal.

Sætningen blev første Gang bevist i 1770 af Lagrange.

Den har faaet fornyet Interesse som et første Skridt til dybtgaaende Undersøgelser over diofantiske Ligninger, inspireret af Nr. 10 blandt Hilberts berømte 23 Problemer (egl. snarere Problemkredse) fra Pariserkongressen i Aar 1900 (" Le .. seuil du vingtième siécle me semble bien choisi pour passer en revue ces problèmes .. attirent notre pensée sur l'avenir inconnu. .. Tant qu'une branche de la Science jouit d'une abondance de problèmes, elle est pleine de vie; le manque de problèmes dénote la mort").

Thi Sætningen angiver jo et Polynomium $x^2+y^2+z^2+v^2$ som for variable $\in \mathbb{Z}$ har Værdimængden $\mathbb{N}_0$; man kan bygge videre, idet fx $(x^2+y^2+z^2+v^2+2)(r^2+s^2+t^2+u^2+2)$ som Værdimængde har netop de sammensatte Tal. I den nyeste Tid er det lykkedes at angive Polynomier (baade Variabelantal og Grad er tocifrede), der som Værdimængde har fx netop Mængden af Primtal; at noget saadant er meget langt fra at være muligt med Polynomier i en Variabel er vist foran (S.30).

Samme Aar som Bachets Sætning blev bevist, 1770, blev den Formodning fremsat af Waring (W.1734-98), at for ethvert $k \in \mathbb{N}$ findes et Tal $g(k)$, saaledes at ethvert naturligt Tal n er Sum af højst $g(k)$ Stk. k'te Potenser af naturlige Tal, altsaa at

$$n = \sum_{j \in]0, g(k)]} a_j^k \quad , \quad \text{alle } a_j \in \mathbb{N}_0 \, .$$

Vi vil naturligvis lade $g(k)$ betegne det mindste Tal med Egenskaben. At $g(1) = 1$ er klart. Bachets Sætning udsiger at $g(2) = 4$. For $g(3)$ har man Værdien 9, idet Talfremstillingen $23 = 8+8+1+1+1+1+1+1+1$ er noget af det værste som kan forekomme. For $g(4)$ har man Værdien 19, idet Talfremstillingen $79 = 16+\ldots+16+1+\ldots+1$ med 4 Addender paa 16 og 15 Addender paa 1 er noget af det værste som kan forekomme.

Det er ikke underligt, at nogle ret smaa Tal giver noget af det værste, længere ude i Talrækken ligger Potenserne paa en vis Maade relativt tættere, og Talfremstillingen gaar faktisk lettere. Derfor har man ogsaa indført Funktionen $G(k) = \lim_{n \to \infty} \sup$ af det nødvendige Antal Addender a^k for at faa Summen n, og man har altsaa, at for et givet k vil fra et vist Trin alle naturlige Tal være Sum af højst $G(k)$ Stk. k'te Potenser.

Det viser sig at for $k \geq 2$ bliver $G(k)$ mindre end $g(k)$ (det er altsaa for saa vidt en uheldig Bogstavbetegnelse man har indført, med lille g og stort G (!)). Man ser at

$G(k)$ endelig $\Leftrightarrow$ $g(k)$ endelig $\Leftrightarrow$ Warings Hypotese rigtig (med k).

Warings Hypotese (eller "Sætning") blev bevist 1909 af Hilbert (H.1862-1943) (med stærk Teknik, bl.a. Brug af 25-dobbelte Integraler !). I de følgende Aar kom der en Del Simplifikationer af Beviset, og ca.1920 gav Hardy-Littlewood (H.1877-1947, L. 1885-1977) et Bevis med Brug af kompleks Funktionsteori; ca.

1930 blev disse Ideer simplificeret ved Overførsel til trigonometriske Rækker af Winogradoff (W. ,russ.), og i 1942 blev der af Linnik (L. ,russ.) givet et Bevis som er "elementært" (d.v.s. nok kompliceret, men principielt anvendeligt som Specialelæsning i Gymnasiet).

Inden vi skrider til Beviset for at $g(2) = G(2) = 4$, saa lad os vise hvorledes Liouville i 1859 ved at benytte dette Resultat kunde vise, at ethvert Tal er en Sum af højst 53 Stk. 4'-Potenser (ogsaa kaldet "Bikvadrater").

Bevis: Det er aabenbart tilstrækkeligt at vise, at ethvert Multiplum af 6 er en Sum af højst 48 Stk. 4'-Potenser, da man saa dertil blot kan føje indtil 5 Stk. Addender $1^4 = 1$. Men naar et Multiplum af 6 kan skrives som $6(m^2+n^2+r^2+s^2)$, saa vil det være tilstrækkeligt at vise, at en Størrelse $6m^2$ kan skrives som en Sum af 12 Stk. 4'-Potenser.

Da $f(x,y) = (x+y)^4 + (x-y)^4 = 2x^4+12x^2y^2+2y^4$, ses at $f(x,y)+f(x,z)+f(x,v)+f(y,z)+f(y,v)+f(z,v) = 6x^4+6y^4+6z^4+6v^4+12x^2y^2+12x^2z^2+\ldots\ldots+12z^2v^2 = 6(x^2+y^2+z^2+v^2)^2$, og naar ethvert Udtryk $6m^2$ kan skrives paa denne sidste Form, har man det ønskede. □

Med Hensyn til Bachets Sætning, saa lad os først bemærke, at ethvert Tal af Form $n = 8h+7$ ikke kan skrives som en Sum af færre end 4 Kvadrattal, hvilket umiddelbart følger af at ethvert Kvadrat modulo 8 er kongruent med 0 eller 1 eller 4. Dermed er altsaa bevist, at $g(2) \geqq G(2) \geqq 4$.

Den svære Del af Sætningen, altsaa at 4 Kvadrater er tilstrækkeligt, vil vi bevise paa den stærke Maade, at vi (i Analogi med Eksponenten 2) for et givet $n \in \mathbb{N}$ vil bestemme Antallet af Talsæt $(x,y,z,v) \in \mathbb{Z}^4$ for hvilke $x^2+y^2+z^2+v^2 = n$, og det vil vise sig, at dette Antal altid er positivt.

Antallet blev bestemt af Jacobi ved analytiske Hjælpemidler (elliptiske Modulfunktioner). Vi skal her give et direkte Bevis.

Bestemmelse af Antallet:

Udgangspunktet er Jacobis Formel: Antallet $(x,y) \in \mathbb{Z}^2$ for hvilke $x^2+y^2 = m$ er lig $4 \sum_d \chi(d)$, hvor der summeres over Divisorerne i m.

Antallet Løsninger til

$$n = \underbrace{x^2 + y^2}_{a} + \underbrace{z^2 + v^2}_{b}$$

faar vi nu ved at lade a og b variere $\in [0,n]$ saaledes at $a + b = n$; det samlede Antal kaldes $8 \cdot H(n)$, og det kommer til at bestaa af tre Bidrag, det første for $a = 0$, $b = n$, det andet for a og $b \in \mathbb{N}$, og det tredie for $a = n$, $b = 0$. Vi faar (idet jo $a = 0$ eller $b = 0$ kun kan fremstilles paa én Maade)

$$8\,H(n) = 4\sum_{d|n}\chi(d) + \sum_{a+b=n}(4\sum_{r|a}\chi(r))\cdot(4\sum_{s|b}\chi(s)) + 4\sum_{d|n}\chi(d)\ .$$

Inden vi gaar videre skal vi minde om at vi strengt holder os til at Summationsvariable er naturlige Tal, og at der ved et $\sum$-Tegn summeres over samtlige Bogstavsæt som opfylder de opskrevne Betingelser. Tallet n er fast. Ved Ændring af en Summation maa vi nøje paase, at der er Bijektion mellem de gamle og de nye Summationsvariable.

I Stedet for at summere over a,b,r,s hvor $a+b = n$ og $r|a$ og $s|b$ kan vi ligesaagodt summere over h,k,r,s med $hr + ks = n$.

Den foregaaende Formel giver saa, efter en nærliggende Division med 8, at

$$H(n) = \sum_{d|n}\chi(d) + 2\cdot\sum_{hr+ks=n}\chi(r)\chi(s)\ ,$$

og det er denne Sum som vi nu skal bestemme (d.v.s. bringe paa en overskuelig Form).

Vi tabellægger $\chi(r)\chi(s)$:

s(mod.4) \ r(mod.4)	0	1	2	3
0	0	0	0	0
1	0	1	0	-1
2	0	0	0	0
3	0	-1	0	1

lig

	0	1	2	3
0	1-1	0-0	0-0	0-0
1	0-0	1-0	0-0	0-1
2	0-0	0-0	1-1	0-0
3	0-0	0-1	0-0	1-0

hvoraf man ser, at

$$\chi(r)\chi(s) = \left\{\begin{matrix} 1 & \text{for } 4\mid r-s \\ 0 & \text{ellers} \end{matrix}\right\} - \left\{\begin{matrix} 1 & \text{for } 4\mid r+s \\ 0 & \text{ellers} \end{matrix}\right\}.$$

Følgelig har vi

$$H(n) = \sum_{d\mid n}\chi(d) + 2\cdot\sum_{\substack{hr+ks=n \\ 4\mid r-s}} 1 - 2\cdot\sum_{\substack{hr+ks=n \\ 4\mid r+s}} 1 \quad .$$

I den midterste Sum vil der være lige mange Led med $r > s$ og $r < s$, og vi vil derfor nedenfor gaa videre med $r > s$ og fordoble; Leddene med $r = s$ kan vi let udregne (de opfylder at $4\mid r-s$), de bliver til $2\cdot\sum 1$, hvor der summeres over $hs+ks = n$, og her maa $h+k$ være en Divisor d fra n, og for givet $d = h+k$ er der $d-1$ mulige Par (h,k), og disse Leds Bidrag er derfor $2\sum(d-1)$, hvor der summeres for $d\mid n$.

Den sidste Sum behandles paa lignende Maade, men her deles op efter $h > k$ (som vi fortsætter med, fordoblet), $h < k$ (som vi derfor bortkaster) og $h = k$, for hvilke vi kan udregne Summen: den bliver $2\cdot\sum 1$, hvor der summeres over $kr+ks = n \wedge 4\mid r+s$; her maa $r+s$ være en med 4 delelig Divisor d fra n, og for givet $d = r+s$ er der $d-1$ mulige Par (r,s), saa Bidraget bliver $2\sum(d-1)$, hvor der summeres for $d\mid n$ og nu med det yderligere Krav at $4\mid d$.

De to udregnede Bidrag kan saa slaas sammen til et Bidrag hvori der summeres for $d\mid n \wedge 4\nmid d$. I første Led i Udtrykket ovenfor

for $H(n)$ summeres $\chi(d)$ for $d \mid n$, og her kan vi ogsaa godt tilføje Ekstrakravet $4 \nmid d$, da jo $\chi(d)$ er 0 for $4 \mid d$.
Naar vi flytter de hidtil udregnede Led over til $H(n)$ paa venstre Side af Lighedstegnet har vi dermed

$$H(n) - \sum_{\substack{d \mid n \\ 4 \nmid d}} \{\chi(d)+2(d-1)\} = 4 \cdot \sum_{\substack{hr+ks=n \\ 4 \mid r-s \wedge r \geqslant s}} 1 - 4 \cdot \sum_{\substack{hr+ks=n \\ 4 \mid r+s \wedge h \geqslant k}} 1 \quad ,$$

og Problemet er at reducere Højresiden.
I begge dens Led skal vi bortset fra Faktoren 4 blot tælle Antallet af Leddene, og Kunsten bliver derfor at jonglere med Summationsvariablene. At i første Sum $r \geqslant s$ kan vi udtrykke ved at skrive $r = s+t$, og at i anden Sum $h \geqslant k$ kan vi udtrykke ved at skrive $h = k+m$. Saa skal der i første og anden Sum summeres over hhv.

$$\left(\begin{array}{c} hs+ht+ks = n \\ 4 \mid t \end{array}\right) \quad \text{og} \quad \left(\begin{array}{c} kr+mr+ks = n \\ 4 \mid r+s \end{array}\right)$$

Vi sætter nu

$$h+k = m \quad \text{hhv.} \quad r+s = t$$

og saa løber Summationerne over

$$(*) \qquad \left(\begin{array}{c} ms+ht = n \\ 4 \mid t \wedge m \geqslant h \end{array}\right) \quad \text{hhv.} \quad \left(\begin{array}{c} mr+kt = n \\ 4 \mid t \wedge t \geqslant r \end{array}\right) .$$

De to Summationsmængder ligner hinanden - bortset fra Bogstavombytninger - , men er ikke ens, da det med 4 deleliget indgaar paa forskellig Maade i Uligheder. Men hvis vender Ulighedstegnene kommer der til at staa det samme (!): at $m \leqslant h$ kan vi udtrykke ved at skrive $h = m+k$ i den første Summationsmængde, og at $t \leqslant r$ kan vi udtrykke ved at skrive $r = s+t$ i den anden Summationsmængde, og derved bliver begge Mængderne til

$$\left(\begin{array}{c} ms + mt + kt = n \\ 4 \mid t \end{array}\right) ,$$

altsaa ens.

Men det betyder jo at den eneste Forskel i de to Summer maa fremkomme ved at vi mangler de Led som vi vilde faa dersom Uligheds-tegnene erstattes med Lighedstegn i (#), og den totale ønskede Højreside bliver derfor lig

$$-4\cdot\sum_{\substack{ms+ht=n\\ 4\mid t\,\wedge\, m=h}} 1 \quad + \quad 4\cdot\sum_{\substack{mr+kt=n\\ 4\mid t\,\wedge\, t=r}} 1 \quad .$$

I den første af disse Summer skal der summeres over hs+ht = n, og her maa s+t være en Divisor d fra n, og for givet d = s+t er der $\left[\frac{d-1}{4}\right]$ mulige Par (s,t) naar t skal være delelig med 4. I den anden af disse Summer skal der summeres over mt+kt = n, men da $4\mid t$ maa m+k være $\frac{d}{4}$, hvor d er en med 4 delelig Divisor fra n, og der er $\frac{d}{4}-1$ Par (m,k). Tilsammen faas

$$-4\cdot\sum_{d\mid n}\left[\frac{d-1}{4}\right] \quad + \quad 4\cdot\sum_{d\mid n\,\wedge\,4\mid d}\left(\frac{d}{4}-1\right) .$$

For $4\mid d$ er $\frac{d}{4}-1=\left[\frac{d-1}{4}\right]$, og derfor kan de to Led trækkes sammen til

$$-4\cdot\sum_{\substack{d\mid n\\ 4\nmid d}}\left[\frac{d-1}{4}\right] .$$

Ialt haves saa

$$H(n)=\sum_{\substack{d\mid n\\ 4\nmid d}}\left\{\chi(d)+2(d-1)-4\left[\frac{d-1}{4}\right]\right\} .$$

Men Resultatet kan blive endnu simplere. Parentesen udregnes:

$$\left.\begin{array}{lllll} d=4h+1 \text{ giver} & 1+8h & -4h & = & 4h+1\\ d=4h+2 \;\;.. & 0+8h+2 & -4h & = & 4h+2\\ d=4h+3 \;\;.. & -1+8h+4 & -4h & = & 4h+3 \end{array}\right\} = d \quad \text{altid.}$$

Altsaa Antallet Løsninger $(x,y,z,v)\in\mathbb{Z}^4$ til $x^2+y^2+z^2+v^2=n$ er lig 8 H(n), hvor H(n) er lig Summen af de Divisorer i n som ikke er delelige med 4.

Da n altid har Divisoren 1 ses at H(n) er positiv, og dermed er Bachets Sætning bevist.

Hvis n er delelig med 8 eller en højere Potens af 2 er $H(n) = H(\frac{n}{4})$, men det er ikke mærkeligt, thi da et ulige Kvadrat altid er $\equiv 1 \pmod 8$ maa n være en Sum af 4 lige Kvadrater, $n = (2x)^2+(2y)^2+(2z)^2+(2v)^2$, og enhver saadan Fremstilling svarer til en Fremstilling $\frac{n}{4} = x^2+y^2+z^2+v^2$.

For $4 \nmid n$ er $H(n) = \delta(n)$ (Summen af Divisorerne), medens man for $4 \mid n$ skal subtrahere nogle Led. Man finder at $H = \delta * c$, hvor Foldningsfaktoren c er Funktionen defineret ved

$$c(n) = \begin{cases} 1 & \text{for } n = 1 \\ -4 & \text{for } n = 4 \\ 0 & \text{ellers} \end{cases}$$

Da c aabenbart er multiplikativ, bliver H multiplikativ, men det maa nærmest siges at være "tilfældigt".

Eksempel: For $n = \prod p^{\alpha}$ er $H(n) = \prod H(p^{\alpha})$. Da nu $H(1) = 1$, $h(2^{\alpha}) = 3$ og $h(p^{\alpha}) = 1+p+p^2+\ldots+p^{\alpha}$ for ulige p, ses at H(n) er ulige hvis og kun hvis n er et Kvadrattal eller det dobbelte af et Kvadrattal. Man kan, i Analogi med Figurerne S.186, forsøge at anskue sig en 4-dimensional Kugle, og se hvorfor det maa være saadan(NB i det 4-dimensionale Rum er der 16 "Sekstentanter").

Iøvrigt kan man bemærke, at i Almindelighed vil en Fremstilling $n = x^2+y^2+z^2+v^2$ ved Symmetri give Anledning til 384 Fremstillinger af samme Art, nemlig 16 Muligheder for Valg af Fortegnene for x,y,z,v og 24 mulige Permutationer af de 4 Kvadrattal.

Taleksempel: Lad os betragte $n = 26$ og $n = 52$.

Tallene har de samme med 4 ikke delelige Divisorer, og vi finder $H(n) = 1+2+13+26 = 42$ for begge. Antallet af Kvadrupler (x,y,z,v) for hvilke $x^2+y^2+z^2+v^2 = n$ er altsaa $8 \cdot 42 = 336$ for dem begge, men det fremkommer paa tilsyneladende ret forskelli-

ge Maader.

Vi vil angive de forskellige Fremstillinger af n som Sum af Kvadrattal, idet vi ved hver angiver hvormange Fortegnsmuligheder der er og hvor mange Permutationsmuligheder, og dermed finder hvordan det skal tælles for at give 8 H(n) = 336.

	Fortegn	Permutationer		Antal
$26 = 25 + 1 + 0 + 0$	4	· 12	=	48
$= 16 + 9 + 1 + 0$	8	· 24	=	192
$= 9 + 9 + 4 + 4$	16	· 6	=	96
			Ialt	336
$52 = 49 + 1 + 1 + 1$	16	· 4	=	64
$= 36 + 16 + 0 + 0$	4	· 12	=	48
$= 25 + 25 + 1 + 1$	16	· 6	=	96
$= 25 + 9 + 9 + 9$	16	· 4	=	64
$= 16 + 16 + 16 + 4$	16	· 4	=	64
			Ialt	336

□

"Gennemsnitsværdien" af H(n) er $\pi^2 n/8$.

Thi vi har tidligere (S.67) vist at Gennemsnitsværdien af $\delta(n)$ er $\pi^2 n/6$, og herfra skal nu trækkes Gennemsnitsværdien af $4\delta(\frac{n}{4})$, men kun for de med 4 delelige n, hvoraf faas det nævnte.

Altsaa er $\sum_{n \leqq K} 8\,H(n) \sim \pi^2 K^2/2$, hvoraf følger at Volumen af den 4-dimensionale Kugle $x^2+y^2+z^2+v^2 \leqq K$ er lig $\pi^2 K^2/2$ ved en Betragtning af samme Art som den 2-dimensionale (S.183).

(Hvis man i Analogi med det 2-dimensionale Tilfælde indsætter Udtrykket for H(n) finder man her at $\pi^2 K^2/16 \sim \sum d \cdot \left[\frac{K}{d}\right]$, hvor der er summeret over de d for hvilke $4 \nmid d$; hvis man i denne rigtige Formel erstatter $\left[\frac{K}{d}\right]$ med $\frac{K}{d}$ bliver Summen uendelig (!), eller hvis man kun gør det for de effektive Led med $d \leqq K$ finder man at π^2 skulde være lig 12 (!)).

Tal som Summer af tre Kvadrater.

Jacobi bestemte ogsaa Udtryk for Antallet af Fremstillinger af et Tal n som Sum af 6 eller 8 Kvadrater, og man er senere gaaet videre med de lige Antal Kvadrataddender. Formlerne bliver dog hurtigt komplicerede og uskønne. Med et ulige Antal Kvadrater er det langt sværere. Vi skal nu undersøge hvilke Tal der kan skrives som Sum af tre Kvadrater (fundet af Gauss), men vi skal kun klare Eksistensspørgsmaalet, og vi vil uden Bevis benytte Dirichlets Sætning om at enhver primisk Restklasse indeholder Primtal.

Nødvendigt og tilstrækkeligt for at et Tal $n \in \mathbb{N}$ kan skrives som Sum af højst 3 Kvadrattal er det at n ikke er af Formen $n = 4^a \cdot (8h + 7)$.

En Konsekvens af Sætningen er det at ethvert naturligt Tal er Sum af højst 3 Trekantstal. Ved Trekantstal forstaar man Tal af Følgen 1,3,6,10,..., altsaa Binomialkoefficienter $\binom{x}{2} = \frac{x(x-1)}{2}$; Navnet hidrører fra at de angiver Antallet Punkter i Figurerne  . Thi Fremstillingen $m = \binom{x}{2} + \binom{y}{2} + \binom{z}{2}$ er ensbetydende med Ligningen $8m + 3 = (2x-1)^2 + (2y-1)^2 + (2z-1)^2$, og naar $8m + 3$ kan skrives som Sum af 3 Kvadrater maa de alle være ulige (da Kvadrat $\equiv 1 \pmod 4$) saa man kan foretage Omskrivningen den modsatte Vej.

Betingelsens Nødvendighed i Sætningen er let at se, thi for det første har vi bemærket (S.191) at 8h+7 ikke kan skrives med mindre end 4 Kvadrater, og for det andet gælder at hvis n kan skrives som Sum af 3 Kvadrater saa kan 4n ogsaa og omvendt; det første er klart, og det andet følger af at hvis $4n = x^2+y^2+z^2$, saa maa x,y og z alle være lige (igen fordi ulige Kvadrat $\equiv 1 \pmod 4$).

*) Bemærk: Bachet: Ethvert n er Sum af 4 "Firkantstal",  .

Problemet er altsaa at vise Betingelsens Tilstrækkelighed. Og af det lige anførte ses at en eventuel Faktor 4 kan bortdivideres, og vi skal derfor blot vise, at saafremt $n \equiv 1 \pmod 4$ eller $n \equiv 2 \pmod 4$ eller $n \equiv 3 \pmod 8$, da kan n skrives som Sum af tre Kvadrattal.

Beviset skal bestaa af to Dele. I den første beviser vi, at dersom der findes naturlige Tal a,b,c saaledes at Ligningen $acn = b^2n + c + 1$ er opfyldt, da kan n skrives som Sum af tre Kvadrater. I den anden skal vi vise, at saadanne a,b,c findes for de ovennævnte Arter af n.

Beviset for første Del skal føres v.Hj.af kvadratiske Former. Læren om disse er velkendt, naar det benyttede Talomraade er $\mathbb{R}$, men da vi her benytter Talomraadet $\mathbb{Z}$ kommer der en Række Modifikationer. Det er det 3-dimensionale Tilfælde vi har Brug for ("ternære" kvadratiske Former), og vi vil derfor kun formulere Teorien for dette, men det er umiddelbart indlysende at alle de første Betragtninger gælder for vilkaarligt Dimensionstal (og naar vi naar det Punkt, hvor det er væsentligt at Dimensionen er 3, skal der blive gjort opmærksom paa det).

Lad M være en symmetrisk 3×3-Matrix med Elementer m_{ij} fra $\mathbb{Z}$. Lad $\underline{v} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ være en Vektor med Elementer fra $\mathbb{Z}$. Saa er $M(\underline{v}) = \underline{v}^{*}\underline{M}\,\underline{v} = m_{11}x^2+m_{12}xy+ \ldots +m_{33}z^2$ en kvadratisk Form over $\mathbb{Z}$, og giver en Afbildning $\mathbb{Z}^3 \to \mathbb{Z}$. Fx er $x^2+y^2+z^2 = E(\underline{v})$, idet $\underline{E}$ er Enhedsmatricen.

Lad L være Mængden af 3×3-Matricer $\underline{A}$ over $\mathbb{Z}$ med det $\underline{A} = \pm 1$. Saa vil L med Matrixmultiplikation udgøre en Gruppe $(L,\cdot)$, thi med $\underline{A}$ og $\underline{B}$ vil L indeholde $^{1)}$ $\underline{E}$, $^{2)}$ $\underline{A}^{-1}$ og $^{3)}$ $\underline{A}\cdot\underline{B}$ (her beror $^{2)}$ paa at den inverse Matrix har Elementer med Nævner $(\det \underline{A})^{-1}$, det øvrige er klart). En Afbildning $\underline{v} \mapsto \underline{w} = \underline{A}\,\underline{v}$

er aabenbart en lineær bijektiv Afbildning $\mathbb{Z}^3 \to \mathbb{Z}^3$, og $(L, \cdot)$ er den generelle lineære Gruppe af disse Afbildninger.

Dersom $\underline{\underline{N}} = \underline{\underline{A}}^* \underline{\underline{M}}\, \underline{\underline{A}}$ sættes $\underline{\underline{N}} \sim \underline{\underline{M}}$. Paa Grund af $^1)$, $^2)$ og $^3)$ bliver Relationen $\sim$ $^1)$ reflexiv, $^2)$ symmetrisk og $^3)$ transitiv, altsaa en Ækvivalensrelation, og vi siger at $\underline{\underline{M}}$ og $\underline{\underline{N}}$ er ækvivalente. Og da $N(\underline{v}) = \underline{v}^* \underline{\underline{N}}\, \underline{v} = \underline{v}^* \underline{\underline{A}}^* \underline{\underline{M}}\, \underline{\underline{A}}\, \underline{v} = \underline{w}^* \underline{\underline{M}}\, \underline{w} = M(\underline{w})$ ses at (naar Vektorerne løber indenfor $\mathbb{Z}^3$) kvadratiske Former med ækvivalente Matricer faar samme Værdimængde.

Da $\det \underline{\underline{N}} = (\det \underline{\underline{A}})^2 \cdot \det \underline{\underline{M}} = \det \underline{\underline{M}}$ haves at ækvivalente Matricer har samme Determinant. Hvis en kvadratisk Form $M(\underline{v})$ kun antager Værdier større end eller lig 0, og kun lig 0 for $\underline{v} = \underline{0}$, siges Formen, og ogsaa dens Matrix $\underline{\underline{M}}$, at være positiv definit, og man ser at Formens ækvivalente har samme Egenskab. Mere generelt ses ogsaa, at ækvivalente Matricer har samme Positivitetsindex (d.e. den maximale Dimension af en lineær Undermodul paa hvilken Formen er positiv definit).

Hvis $\underline{\underline{M}}$ er positiv definit, saa er alle Diagonalelementer m_{ii} større end 0, idet jo Restriktionen af $M(\underline{v})$ til de Vektorer $\underline{v}$ som har højst en Koordinat ulig 0 ogsaa skal være positiv definit.

Enhver positiv definit Matrix er ækvivalent med en Matrix $\underline{\underline{M}}$ i hvilken man for $i \neq j$ har $|m_{ij}| \leqq \frac{1}{2} m_{ii}$.

(Man kan ikke, saaledes som over $\mathbb{R}$, faa den ækvivalent med en ren Diagonalmatrix, men kun med en, i hvilken Diagonalen er "ret fremtrædende" i den angivne Forstand).

Bevis: Blandt Matricens ækvivalente findes nogen hvori Diagonalelementerne er minimale (altsaa at hvis de er $..,m_{ii},..$ og de i en anden Matrix er $..,m_{ii}',..$ saa vil $\bigwedge_i: m_{ii}' \leqq m_{ii}$ medføre at $\bigwedge_i: m_{ii}' = m_{ii}$). Det følger af at alle Diagonal-

elementer tilhører $\mathbb{N}$. Ethvert saadant $\underline{\underline{M}}$ har Egenskaben. Thi lad os tage $\underline{\underline{A}} = \underline{\underline{E}} + \underline{\underline{D}}$, hvor $\underline{\underline{D}}$ er en Matrix som har Tallet 1 paa Pladsen (i,j) og ellers lutter 0. Vi har det $\underline{\underline{A}} = 1$. Saa er $\underline{\underline{A}}^* \underline{\underline{M}}\,\underline{\underline{A}} = \underline{\underline{M}} + \underline{\underline{M}}\,\underline{\underline{D}} + \underline{\underline{D}}^* \underline{\underline{M}} + \underline{\underline{D}}^* \underline{\underline{M}}\,\underline{\underline{D}}$. De tre sidste Led ses ved umiddelbar Udregning at give en Matrix som har 0 overalt undtagen i j'te Række og i j'te Søjle og af følgende Udseende

$$\begin{pmatrix} & & m_{1i} & \\ & 0 & m_{2i} & 0 \\ & & \vdots & \\ m_{i1} \; m_{i2} \; \cdots & & \square & \cdots \\ & 0 & \vdots & 0 \end{pmatrix};$$

hvor Rækken og Søjlen skærer hinanden, altsaa paa Plads (j,j), bliver Elementet $\square$ lig $m_{ii} + 2\,m_{ij}$ (da jo $m_{ji} = m_{ij}$). Foretog man det samme med $\underline{\underline{A}} = \underline{\underline{E}} - \underline{\underline{D}}$ vilde man paa Plads (j,j) faa $m_{ii} - 2\,m_{ij}$. Paa Grund af Minimalegenskaben ved $\underline{\underline{M}}$ maa $m_{ii} \pm 2m_{ij}$ begge være $\geqq 0$, hvoraf Paastanden. □

Nu kommer et Resultat, hvor vi benytter at Dimensionen er 3, det gælder dog ogsaa for lavere Dimension hvor det er næsten trivielt.

Dersom $\underline{\underline{M}}$ er en positiv definit 3×3-Matrix med det $\underline{\underline{M}} = 1$, saa er $\underline{\underline{M}}$ ækvivalent med $\underline{\underline{E}}$.

Ifølge forrige Sætning har $\underline{\underline{M}}$ en ækvivalent af Form

$$\underline{\underline{N}} = \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \quad \text{med} \quad \begin{matrix} 2|d| \leqq a,b \\ 2|e| \leqq a,c \\ 2|f| \leqq b,c \end{matrix}$$

og vi vil vise, at denne maa være lig $\underline{\underline{E}}$.

Vi har det $\underline{\underline{N}} = 1$, og udregnes Determinanten faas

$$abc + 2\,def - af^2 - be^2 - cd^2$$

som viser, at mindst et af Tallene a,b,c maa være ulige. Lad

os antage at a ulige (det kan altid opnaas ved Koordinatskifte, som jo er en speciel Ækvivalens), saa vi kan i de to øverste af Uligheder erstatte a med a-1.

Vi opskriver igen Determinantværdien, og vurderer nedad ledvis:

$$\begin{aligned} & abc + 2\,def - af^2 - be^2 - cd^2 = 1 \\ \geq\; & abc - \tfrac{1}{4}(a-1)bc - \tfrac{1}{4}abc - \tfrac{1}{4}b(a-1)c - \tfrac{1}{4}c(a-1)b = \tfrac{3}{4}bc. \end{aligned}$$

Altsaa maa vi have $b = c = 1$, hvorefter Uligheder giver $d = e = f = 0$, og da det $\underline{\underline{N}} = 1$ faas sluttelig $a = 1$, saa at $\underline{\underline{N}} = \underline{\underline{E}}$. □

Dersom der for et $n \in \mathbb{N}$ findes $a,b,c \in \mathbb{N}$ saa vi har

$$\det \underline{\underline{M}} = 1 \text{ , hvor } \underline{\underline{M}} = \begin{pmatrix} a & b & 1 \\ b & c & 0 \\ 1 & 0 & n \end{pmatrix},$$

saa kan n skrives som en Sum af tre Kvadrater.

(hvor a,b,c intet har at gøre med de ovenfor ligesaabenævnte Størrelser).

Bevis: Paa Underrummet af Vektorer $\begin{pmatrix} 0 \\ y \\ z \end{pmatrix}$ er $M(\underline{v}) = c \cdot y^2 + n \cdot z^2$, hvoraf ses at Positivitetsindex for $\underline{\underline{M}}$ mindst er 2 (hvadenten det opfattes over $\mathbb{R}$ eller $\mathbb{Z}$), og da Produktet af Egenværdierne er lig $\det \underline{\underline{M}} = 1$, er alle 3 Egenværdier positive, altsaa $\underline{\underline{M}}$ positiv definit. Ifølge foregaaende Sætning er $\underline{\underline{M}} \sim \underline{\underline{E}}$, og da n tilhører Værdimængden for $M(\underline{v})$, nemlig for $\underline{v} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, maa n ogsaa tilhøre Værdimængden for $E(\underline{v})$, d.v.s. være en Sum af tre Kvadrater. □

Dermed er første Del af Beviset for Hovedsætningen fuldført. Thi $\det \underline{\underline{M}} = acn - b^2n - c$, og hvis blot vi kan opnaa at dette er lig 1, saa er den ønskede Fremstilling af n mulig.

Saa kommer anden Del af Beviset for Hovedsætningen: Vi skal vise, at for de tidligere angivne Arter af n vil der findes $a,b,c \in \mathbb{N}$ saa

$$acn = b^2n + c + 1 .$$

Ligningen ser meget uskyldig ud, den er lineær i a og c, men at Problemet ikke kan være helt simpelt fremgaar af at vi ved, at for $n = 8h + 7$ er der ingen Løsninger (da disse n ikke er Sum af 3 Kvadrater). (Da man maa have $n \mid c+1$ er det fristende at sætte $c+1 = hn$, hvorved Ligningen bliver til $ahn = b^2 + a + h$, symmetrisk i a og h, men der synes ikke at være vundet noget ved denne Omskrivning).

Problemet kan reduceres, idet Opgaven blot er at bestemme et c som opfylder

I^o: $c \equiv -1 \pmod{n}$

II^o: - n er kvadratisk Rest modulo c.

Thi af I^o følger at c og n er primiske, hvorefter II^o giver at der findes et b (med $b \in \mathbb{Z}_c^*$) saa $(bn)^2 \equiv -n \pmod{c}$, som giver at $c \mid b^2n+1$. Altsaa vil c gaa op i Højresiden, og da ifølge I^o ogsaa n gaar op, saa vil cn gaa op, og vi har dermed et heltalligt a.

Vi skal nu betragte de forskellige Tilfælde for n (se S.199).

For $n \equiv 1 \pmod{4}$ tager vi for c et Primtal p hvor $p \equiv 1 \pmod{4}$ og $p \equiv -1 \pmod{n}$. Da 4 og n er primiske, bliver Kravene ifølge den kinesiske Restklassesætning til at p skal tilhøre en vis primisk Restklasse modulo 4n (det bliver iøvrigt at $p \equiv 2n-1 \pmod{4n}$) og ifølge Dirichlets Sætning findes et saadant p. Kravet I^o er evident opfyldt, ($c = p$), saa det er blot II^o vi skal kontrollere, altsaa at $\left(\frac{-n}{p}\right) = 1$.

Da n er Produkt af ulige Primtal, $n = \prod n_j$, finder vi af Reciprocitetssætningen (med Supplement) at

$$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{n}{p}\right) = \prod\left(\frac{n_j}{p}\right) = \prod\left(\frac{p}{n_j}\right),$$

og da $p \equiv -1 \pmod{n}$ har vi ogsaa $p \equiv -1 \pmod{n_j}$, saa vi faar (igen af første Suppl. til Rec.-Sætn.) at Størrelsen er lig

$$\prod\left(\frac{-1}{n_j}\right) = (-1)^r, \quad \text{med } r = \text{Antallet } n_j \text{ af Form } 4h-1.$$

Men da $n \equiv 1 \pmod{4}$ maa r være lige, og vi har det ønskede. □

For $n \equiv 2 \pmod{4}$ gaar det analogt: For c tager vi et Primtal p, hvor $p \equiv 3 \pmod{8}$ og $p \equiv -1 \pmod{\frac{n}{2}}$. Ifølge den kinesiske Sætning skal p tilhøre en vis Restklasse modulo 4n (det bliver iøvrigt $p \equiv 2n-1 \pmod{4n}$), og ifølge Dirichlets Sætning findes et saadant p. I° er evident opfyldt, og vi skal blot vise at $\left(\frac{-n}{p}\right) = 1$. Dennegang sættes $\frac{n}{2}$ lig $\prod n_j$, og vi benytter at $\left(\frac{-2}{p}\right) = 1$ (S.157), og faar

$$\left(\frac{-n}{p}\right) = \left(\frac{-2}{p}\right)\cdot\left(\frac{\frac{n}{2}}{p}\right) = \prod\left(\frac{n_j}{p}\right) = (-1)^r\cdot\prod\left(\frac{p}{n_j}\right) = (-1)^r\cdot\prod\left(\frac{-1}{n_j}\right) = (-1)^{r+r},$$

altsaa lig +1, saa vi har det ønskede. □

For $n \equiv 3 \pmod{8}$. Dennegang tages $c = 2p$ med $p \equiv 1 \pmod{4}$ og $p \equiv \frac{n-1}{2} \pmod{n}$ (d.v.s. $p \equiv \frac{n-1}{2} \pmod{4n}$). I° er evident, og da $2 \nmid n$ er $-n$ kv.Rest mod.2, saa vi skal blot vise, at $\left(\frac{-n}{p}\right) = 1$. Vi faar

$$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\cdot\prod\left(\frac{n_j}{p}\right) = \prod\left(\frac{p}{n_j}\right) = \prod\left(\frac{4p}{n_j}\right) = \prod\left(\frac{-2}{n_j}\right) = (-1)^s,$$

hvor s angiver Antallet n_j af Form $8h - \begin{cases}1\\3\end{cases}$ (igen S.157). Men naar $n = \prod n_j$ er af Form $8h+3$, saa maa s være lige (indenfor $(\mathbb{Z}_8^*, \cdot)$ er ① og ③ en Undergruppe med ④ og ⑨ som Sideklassen). Dermed er det store Bevis helt afsluttet. □

KAPITEL XI : To gamle Hypoteser og deres indbyrdes Modstrid.

Det drejer sig om to Hypoteser om Primtallenes Fordeling i Talrækken.

Som omtalt i tidligere Kapitler kan Primtallenes Fordeling beskrives ved Primtalfunktionen

$$\pi(x) = (\text{Antallet Primtal mindre end eller lig } x).$$

Vi har (i Kapitel V) vist Primtalsætningen $\pi(x) = \frac{x}{\log x} + R(x)$, hvor Restleddet $R(x)$ bliver forsvindende i Forhold til det første Led for $x \to \infty$. Af Sætningen har vi udledt, at <u>for Tal som i Størrelse ligger nær et stort x vil Afstanden mellem to konsekutive Primtal "gennemsnitlig" være som log x.</u>

En lidt stærkere Form af Sætningen (vist allerede før 1900 af de la Vallée-Poussin) siger at

$$\pi(x) = \int^{x} \frac{1}{\log t}\, dt + R_2(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + R_3(x),$$

hvor baade $R_2(x)$ og $R_3(x)$ er forsvindende i Forhold til $\frac{x}{\log^2 x}$.

Integralet her er den saakaldte "Integrallogaritme", og man ser let ved en partiel Integration at dens Størrelse er som angivet til højre.

Naar man gaar ud i Talrækken vil Primtallene "gennemsnitlig" komme til at ligge mere og mere spredt, og det ytrer sig ved at de angivne Tilnærmelsesfunktioner til $\pi(x)$ er nedad hule, idet fx Integranden $\frac{1}{\log t}$ er aftagende. Denne aftagende Tæthed kan nu udtrykkes i følgende:

<u>Første Hypotese:</u> For alle $x,y \in \mathbb{N} \setminus \{1\}$ gælder

$$\pi(x + y) \leq \pi(x) + \pi(y).$$

I Uligheden er der Symmetri mellem x og y, saa vi kan derfor i alt det følgende antage $x \leq y$. At $x = 1$ maa undtages er klart, da $\pi(1) = 0$, saa Gyldigheden her vilde simpelthen forhindre at π blev en voksende Funktion; iøvrigt er det jo en Definitionssag at 1 ikke medregnes til Primtallene, dersom man gjorde dét blev Venstresiden forøget med 1 og Højresiden med 2, og det er uvæsentligt for Uligheden (og for alt det følgende).
For $x = 2$ siger Uligheden at $\pi(y+2) \leq \pi(y) + 1$, og det er klart, da der højst er ét ulige Tal paa Intervallet $]y,y+2]$; for $x = 3$ eller 4 staar der at $\pi(y+x) \leq \pi(y) + 2$, som er klart, da højst 2 ulige Tal paa Intervallet $]y,y+x]$.
Hypotesen er støttet af vidtgaaende numeriske Undersøgelser, den er saaledes vist at være rigtig for alle $x,y < 10^5$ (Segal,1962).

I 1958 fremsatte A.Schinzel (polsk) en vidtgaaende Hypotese, som løst udtrykt siger, at hvis man har en endelig Mængde Polynomier af en reel Variabel $y \in \mathbb{N}$, da vil der findes uendelig mange y-Værdier for hvilke Polynomierne simultant antager Primtalsværdier, medmindre dette er aabenlyst umuligt.
Præcist: Dersom $f_1(y),\ldots,f_s(y)$ alle tilhører $\mathbb{Z}[y]$, og de har positiv Højestegradskoefficient og de er irreducible og der for ethvert Primtal p findes et $y \in \mathbb{N}$ saa $p \nmid f_1(y)\cdot\ldots\cdot f_s(y)$, da vil der findes uendelig mange $y \in \mathbb{N}$ for hvilke $f_1(y),\ldots,f_s(y)$ simultant er Primtal (ligesom paa S.30 kunde Kravet om heltallige Koefficienter afsvækkes). (Schinzels Hypotese "H").
At de nævnte Betingelser er nødvendige kan let ses: Det første skal blot sikre at der for vilkaarlig store y kan antages positive Værdier, det andet er klart, thi hvis $f_j(y) = g(y)\cdot h(y)$, hvor ingen af Faktorerne er ± 1, da vil $f_j(y)$ for alle tilstrækkelig

store y være et sammensat Tal (NB "irreducibel" betyder jo baade at man ikke kan trække en konstant Talfaktor $\neq \pm 1$ ud, og at Polynomiet ikke kan skrives som Produkt af to ikke-konstante Polynomier); det tredie Krav er nødvendigt, thi hvis det ikke er opfyldt vilde jo altid for alle tilstrækkelig store y mindst et $f_j(y)$ være delelig med et mindre Primtal p (og hvis det paa den anden Side for et givet p er opfyldt af ét y, da er det ogsaa opfyldt af vilkaarlig store y, nemlig af en hel Restklasse modulo p).

Denne vidtrækkende Hypotese er kun bevist i et eneste Specialtilfælde, nemlig for ét Førstegradspolynomium (!), hvor den i det moniske Tilfælde, altsaa et Polynomium $y+b$, er bevist af Euklid (nemlig Sætningen om at der er uendelig mange Primtal), og i det ikke-moniske Tilfælde, altsaa et Polynomium $ay+b$ med $(a,b) = 1$, er bevist af Dirichlet i 1837 (den ofte omtalte Dirichlets Sætning).

Hypotesen vil have mange Konsekvenser. Fx vil der findes uendelig mange Primtal af Form $p = y^2+1$, saa Primtalfølgen 5,17,37,101,.. blev uendelig. Endvidere: Der findes uendelig mange Carmichaeltal (S.146); thi ifølge Hypotesen vil der findes uendelig mange y for hvilke de tre Polynomier $p = 6y+1$, $q = 12y+1$ og $r = 18y+1$ simultant er Primtal, og dermed $pqr - 1 = 1296y^3 + 396y^2 + 36y = 36y\cdot(36y^2 + 11y + 1)$ er delelig med baade p-1, q-1 og r-1, hvilket er tilstrækkeligt til at pqr er et Carmichaeltal.

Man kan sige, at Hypotesen paa en Maade udtrykker, at det virker som om Primtallene er tilfældig fordelt.

Her skal vi dog kun interessere os for et Specialtilfælde af Hypotesen, nemlig hvor den anvendes paa et Sæt af moniske Førstegrads-Polynomier, $f_1(y) = y + b_1$, ... , $f_s(y) = y + b_s$.

Da Polynomierne er irreducible og med positiv Højestegradskoefficient, bliver det kun den tredie af Schinzels Betingelser som faar Interesse. Den udsiger, at for ethvert p skal man kunne finde et $y = y_p$, saa p ikke gaar op i noget $y_p + b_j$, eller med andre Ord at $-y_p \not\equiv b_j$ for $j = 1,\ldots,s$. altsaa at der modulo p findes mindst én Restklasse, nemlig $(-y_p)$, som ikke indeholder noget b_j.

Det udtrykker vi i følgende Definition: Et endeligt Sæt B af hele Tal, $b_1,\ldots,b_s$, kaldes brugbart dersom det for ethvert Primtal p gælder at $\mathbb{Z}_p$ indeholder mindst en Restklasse som er forskellig fra $(b_1),\ldots,(b_s)$. (Definitionen kunde iøvrigt umiddelbart udvides til uendelige Talsæt $b_1,b_2,\ldots$). Vort Specialtilfælde af Schinzels Hypotese udtrykkes saa i følgende:

> Anden Hypotese: For ethvert brugbart Talsæt B skal der findes uendelig mange y hvor $y + B \subseteq$ Primtalmængden P.

Her betyder (som sædvanlig) $y + B$ den forskudte Mængde $\{y+b_j\}$, idet $B = \{b_j\}$.

Det er umiddelbart indlysende, at dersom B er brugbar, da er enhver Delmængde af B ogsaa brugbar, og endvidere at enhver translateret Mængde $a + B$ ogsaa er brugbar.

Det er let at angive Eksempler paa brugbare Talsæt. Fx vil for et fast Primtal p_o Sættet $p_o, p_o^2, \ldots, p_o^s$ være brugbart, thi for $p = p_o$ er alle $(b_j) = (p_o^j) = (0)$, og for $p \neq p_o$ er alle $(b_j) \neq (0)$. Et simpelt Taleksempel er $B = \{2,4\}$, og man ser, at Hypotesen i dette Tilfælde udsiger, at der findes uendelig mange Primtaltvillinger, hvilket er en aarhundredgammel Formodning.

Talsættet $\{1,3,5\}$ er ikke brugbart, thi i $\mathbb{Z}_3$ vil (1), (3) og (5) udgøre samtlige Restklasser, i Overensstemmelse med at tre kon-

sekutive ulige Tal (store) ikke kan være Primtal, idet et af dem vil være deleligt med 3.

Derimod er Sættet $(1,3,7,9)$ brugbart, thi for $p = 2$ eller 5 eller større end 10 er alle (b_j) forskellige fra (0), og for $p = 3$ eller 7 er de forskellige fra (-1). Ifølge Hypotesen skal det give Anledning til uendelig mange Kvadrupler af fire Primtal i samme Dekade i Decimalsystemet (nemlig 5 konsekutive ulige Tal, hvoraf det midterste mangler, og dette maa saa være deleligt med 5). Eksempler paa saadanne er $(11,13,17,19)$ og $(191,193,197,199)$ og $(34841,34843,34847,34849)$ og de findes saa langt ud som Primtaltabellerne gaar, selvom de efterhaanden kommer til at ligge mere spredt.

Hypotesen støttes af følgende Betragtninger: "Sandsynligheden" for at et Tal af Størrelse x er et Primtal er $\frac{1}{\log x}$. "Sandsynligheden" for at $x \pm 1$ simultant er Primtal bliver saa proportional med $(\log x)^{-2}$ (iøvrigt lig $C \cdot (\log x)^{-2}$, thi naar det ene af Tallene er ulige bliver det andet automatisk ogsaa ulige) etc.; "Sandsynligheden" for at $x+1, x+3, x+7, x+9$ simultant er Primtal bliver proportional med $(\log x)^{-4}$ o.s.v.. Og da $\int^{\infty} (\log t)^{-m} dt$ er divergent for alle m maa man vente sig, at saadanne Primtalkonfigurationer gentages i det uendelige.

(Dette er ikke Matematik, Primtallene er jo ikke noget tilfældigt fordelt, men der er hyppigt"noget om det". Et Eksempel som viser baade Styrken og Svagheden i Ideen er følgende: Kravet om at x er et Primtal kan udtrykkes ved at det ikke maa være deleligt med noget $p < x$, hvilket giver "Sandsynligheden" $\prod_{p<x} (1 - \frac{1}{p})$, som kan bevises at være $\frac{0,6..}{\log x}$, hvilket er mindre end det "rigtige" $\frac{1}{\log x}$; men Kravet kan ogsaa udtrykkes ved at x ikke maa være deleligt med noget $p \leqq \sqrt{x}$, hvilket giver "Sandsynligheden"

$\prod_{p \leqq \sqrt{x}} (1 - \frac{1}{p})$, altsaa $\frac{0,6..}{\frac{1}{2}\log x} = \frac{1,2..}{\log x}$, som er større end det rigtige).

At "Sandsynligheden"for at $x \pm 1$ er Primtaltvillinger er proportional med $(\log x)^{-2}$ betyder, at Antallet Primtaltvillinger $\leqslant x$ vokser som $\text{const.} \cdot x \cdot (\log x)^{-2}$, og analogt i de andre Tilfælde; det ses paa samme Maade som at $\pi(x) \sim x \cdot (\log x)^{-1}$ svarer til "Primtalsandsynligheden" $(\log x)^{-1}$. Dette understøttes af flere Resultater. Viggo Brun (norsk,1885-) kunde vise, at Tvillingeantallet er mindre end $\text{const.} \cdot x \cdot (\log x)^{-2}$, men han kunde derimod ikke vise, at Antallet er uendeligt (Bevismetoden var en genial Modifikation af Eratostenes' Si, og blev Oprindelsen til de moderne Anvendelser af "Simetoder" i Talteorien; Resten af Kapitlet her bliver et - relativt simpelt - Eksempel paa Anvendelse af disse). Hardy & Littlewood kunde (1923) - men kun ved at benytte en stadig ubevist Hypotese i Slægt med den berømte "Riemann'ske Formodning" - vise Rigtigheden af de gættede Udtryk, ogsaa med de indgaaende konstante Faktorer, for Antallene af Primtal-Tvillinger, -Kvadrupler, o.s.v. $\leqslant x$, og Resultaterne synes at stemme meget godt med Optællinger i Tabellerne.

Vi definerer

$$\rho(x) = \max_{B} \left| B \cap]0,x] \right|, \quad \text{hvor B brugbar.}$$

Altsaa (ifølge de ovenfor nævnte trivielle Egenskaber for brugbare Mængder): $\rho(x)$ er det maximale Elementtal for et brugbart Sæt paa et Interval af Længde x.

Det er klart, at $\rho(x)$ er en ikke-aftagende Trappefunktion, som opfylder at $\rho(x) \leqq x$, og den vokser med Spring af Størrelsen 1 i visse naturlige Tal. Endvidere gælder at for $y \geqq x$ er $\pi(y+x) - \pi(y) \leqq \rho(x)$, idet Primtallene paa Intervallet $]y,y+x]$

udgør et brugbart Sæt (for $p \leqq y$ vil ingen af dem falde i Nulrestklassen modulo p, og for $p > y$ vil ingen af dem falde i Restklassen (y) modulo p). Af Ræsonnementet ser man fx umiddelbart at Primtallene 11,13,17,19 udgør et brugbart Sæt, som ved Translation giver at (1,3,7,9) er brugbart, benyttet ovenfor. Af Uligheden ses at $\rho(x) \geqq \pi(2x) - \pi(x)$; saa at $\rho(x) - \pi(x)$ er større end eller lig $\pi(2x) - 2 \cdot \pi(x)$; indsætter man heri de la Vallée-Poussins skarpe Tilnærmelser til π faar man at $\rho(x) \gtrsim \pi(x) - 2 \cdot x \cdot \log 2/(\log x)^2$, d.v.s. at $\rho(x)$ kan vurderes nedad ved $\pi(x)$ paanær en Afvigelse, som for $x \to \infty$ bliver forsvindende i Forhold til $\pi(x)$. Ved ret kraftige Midler er det vist (H.L.Montgomery,1971), at $\rho(x) < 2 \cdot \pi(x)$ for store x. Uvæsentligt, men interessant, er det at vi ogsaa har $\rho(x+y) \leqq \rho(x) + \rho(y)$, saa at der for ρ gælder den "Trekantsulighed" som er tvivlsom for π; det følger simpelthen af at et brugbart Sæt paa et Interval af Længde x+y jo umiddelbart kan deles op i et brugbart Sæt paa et Interval af Længde x og et paa et Interval af Længde y.

Den foran fremhævede "anden Hypotese" ses at medføre at

$$\limsup_{y \to \infty} \left(\pi(y+x) - \pi(y) \right) = \rho(x)$$

(Man kan ikke slutte den modsatte Vej; fx er Sættet (2,4,8) brugbart, og det er klart at hvis man skifter Fortegn i et brugbart Sæt faas igen et brugbart Sæt, saa (-2,-4,-8) er ogsaa brugbart og ligger ligesom det forrige paa et Interval af hele Tal af Længde 7; men selvom der findes vilkaarligt store y for hvilke y+2,y+4,y+8 simultant er Primtal, saa er det ikke sikkert at det gælder for Tripler y-2,y-4,y-8).

Det afgørende bliver derfor at sammenligne $\rho(x)$ og $\pi(x)$. Hvis

$\rho(x) \leqq \Pi(x)$, saa viser den for $y \geqq x$ gyldige Ulighed (S.210,nederst) at $\Pi(y+x) \leqq \Pi(y) + \Pi(x)$, og dermed Rigtigheden af"første Hypotese". Men hvis der findes et x for hvilket $\rho(x) > \Pi(x)$, og "anden Hypotese" gælder, saa vil der findes vilkaalig store y for hvilke $\Pi(y+x) > \Pi(y) + \Pi(x)$, og"første Hypotese" maa være forkert; lad os bemærke, at det kan (for store x-Værdier) kun indtræffe hvis x og y er væsentlig forskellige, hvilket fremgaar af Vurderingen (S.211) af $\Pi(2x) - 2\cdot\Pi(x)$. Endvidere maa vi antage $x > 1$, da $\rho(1) = 1$ medens $\Pi(1) = 0$, men det svarer jo netop til at første Hypotese kun omhandler $x,y > 1$. Alt dette er Overvejelser, som - mere eller mindre explicit - er gjort for 50-100 Aar siden. Vi maa derfor undersøge $\rho(x)$ nærmere.

Definitionen af et brugbart Sæt kan aabenbart ogsaa formuleres saaledes: Et brugbart Sæt er et Sæt udtaget blandt de Tal som staar tilbage naar vi for ethvert Primtal p har fjernet en Restklasse modulo p fra Talrækken $\mathbb{Z}$.

Lad $\bar{M}_\infty$ betegne en Foreningsmængde af Restklasser, en for hvert Primtal p; altsaa

$$\bar{M}_\infty = \bigcup_p \{t \equiv a_p \pmod p\}, \text{ét } a_p \text{ for hvert } p.$$

Et Sæt er brugbart hvis det ligger i Komplementærmængden til et $\bar{M}_\infty$, og vi har

$$\rho(x) = \max_{\bar{M}_\infty} \left| \,]0,x] \setminus \bar{M}_\infty \right|.$$

For nærmere at kunne undersøge Fænomenerne definerer vi

$$\bar{M}_z = \bigcup_{p \leqq z} \{t \equiv a_p \pmod p\}, \quad \text{ét } a_p \text{ for hvert } p,$$

og specielt

$$\bar{M}^0_z = \bar{M}_z \text{ hvor alle } a_p = 0.$$

Vi kunde tilsvarende definere $\bar{M}^0_\infty$, det ses at blive lig $\mathbb{Z} \setminus \{\pm 1\}$. Generelt vil der til et større z svare et mere omfattende $\bar{M}_z$, og specielt har vi $\bar{M}^0_1 \equiv \mathcal{O} \subseteq \ldots \subseteq \bar{M}^0_z \subseteq \bar{M}^0_{z+1} \subseteq \cdots \subseteq \bar{M}^0_\infty$.

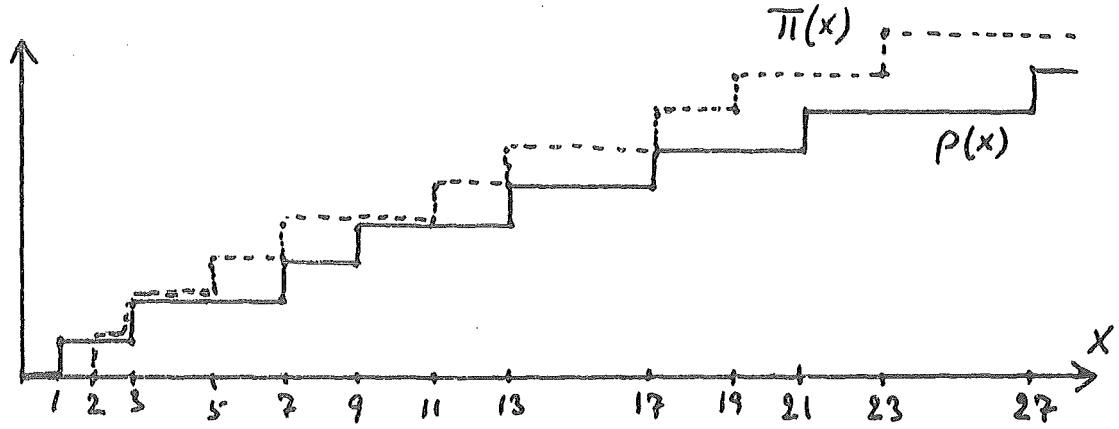
Der er mange forskellige $\bar{M}_z$, men de er ens paanær Translation, thi for givne a_p, $p \leqq z$, findes ifølge den kinesiske Sætning et y saa man for alle disse p har $y \equiv a_p \pmod{p}$, og saa er jo $-y + \bar{M}_z = \bar{M}_z^0$. Da $\bar{M}_{\infty}^0 = \mathbb{Z} \setminus \{\pm 1\}$ ses, at ethvert $\bar{M}_z$ er en ægte Del af $\mathbb{Z}$.

Vi definerer $P_z = \prod_{p \leqq z} p$. Saa er P_z Periode for $\bar{M}_z^0$ og dermed for ethvert $\bar{M}_z$, og Antallet af forskellige $\bar{M}_z$ er altsaa højst lig P_z.

Indskud: Faktisk er P_z den korteste Periode for $\bar{M}_z^0$, og Antallet af forskellige $\bar{M}_z$ er altsaa lig P_z. Dette er ikke trivielt, idet det ikke er umiddelbart indlysende (jf. P. Stk.) at forskellige Sæt $\ldots, a_p, \ldots$ giver forskellige $\bar{M}_z$, men det kan indses saaledes: Antag at q er den korteste Periode for $\bar{M}_z^0$, saa gælder $q \mid P_z$, og q er altsaa Produktet af visse af Primtallene $\leqq z$. Dersom der nu findes et Primtal $p \leqq z$ hvor $p \nmid q$, saa er $(p,q) = 1$ og der findes altsaa et h saa $p \mid hq+1$; men saa er jo $hq+1 \in \bar{M}_z^0$, og naar q er Periode vil ogsaa $1 \in \bar{M}_z^0$, hvilket ikke stemmer. Indskud slut.

For $\bar{M}_{\infty}$ gælder ikke noget tilsvarende. Ovenfor er nævnt at $\bar{M}_{\infty}^0 = \mathbb{Z} \setminus \{\pm 1\}$. Men man kan ogsaa opnaa at et $\bar{M}_{\infty}$ har en uendelig Komplementærmængde, fx omfattende alle Tal $p_0, p_0^2, p_0^3, \ldots$ (S.208, Eksemplet paa brugbar Mængde). Eller et $\bar{M}_{\infty}$ kan omfatte hele $\mathbb{Z}$: Man opskriver alle de hele Tal som en Følge $c_1, c_2, \ldots$ og alle Primtallene som en Følge $p_1, p_2, \ldots$ og tager saa som $\bar{M}_{\infty}$ Foreningsmængden $\bigcup \{t \equiv c_j \pmod{p_j}\}$. Dog gælder det stadig at det translaterede af et $\bar{M}_{\infty}$ igen er et $\bar{M}_{\infty}$.

Det er trivielt at $\rho(1) = 1$ og at $\rho(2) = 1$ (to Nabotal dækker begge Restklasserne modulo 2). Ligesaa ses at $\rho(3) = 2$ (fx var jo (2,4) brugbart, svarende til Primtaltvillingerne) og $\rho(4) = 2$. Iøvrigt ses let at ρ kun kan vokse i de ulige Tal (da en Restklasse mod.2 skal udgaa), hvilket ligner Π-Funktionen.



Figuren viser $\rho(x)$ og (punkteret) $\pi(x)$. Desværre bliver Bestemmelsen af $\rho(x)$ hurtigt kompliceret. Lad os vise, at $\rho(19) = 6$. Af Tallene $]0,19]$ skal først fjernes en Restklasse modulo 2, og det er aabenbart bedst at fjerne de lige Tal, saa at der resterer lo ækvidistante Tal. Dernæst skal fjernes en Restklasse modulo 3; gøres det som paa øverste Figur (eller dermed symmetrisk) med ¬, vil der restere 7 Tal, og naar dernæst fjernes en Restklasse modulo 5 kan man ikke undgaa i bedste Fald, ¬, at fjerne endnu et, saa 6 tilbage, men derefter gaar det glat, idet man modulo 7,11,13,..

altid kan vælge Restklasser som undgaar de 6; modulo 3 kunde man ogsaa have fjernet som paa nederste Figur ¬¬, men saa var man allerede nede paa kun at have 6 tilbage. I bedste Fald er altsaa 6 tilbage af de 19, saa $\rho(19) = 6$.

Paa Figuren ser man at $\pi(x) - \rho(x)$ i det store og hele vokser, omend langsomt. Hardy & Littlewood bestemte (1923) $\rho(x)$ for $x < 100$, og Schinzel & Sierpinski (1882-1970) for $x < 146$ (1961) og Selfridge (ca.1972) for $x < 500$, og den samme Tendens var klar, omend Funktionerne kom nær hinanden for $x = 97$, hvor $\pi(97) = 25$ og $\rho(97) = 23$.

I 1974 er der publiceret et Arbejde af Hensley & Richards (amrk.) hvori det vises, at der findes vilkaarlig store x for hvilke $\rho(x) > \pi(x)$. Dermed er altsaa vist, at de to foran opstillede Hypoteser er uforenelige. Man kan saa fundere over hvilken af dem der er forkert, og det er nok mest sandsynligt at det er første Hypotese, idet anden Hypotese synes bedre underbygget, den har ligesom en mere "matematisk" Baggrund. Endelig er der selvfølgelig ogsaa den Mulighed at begge Hypoteser kan være forkerte.

Faktisk gælder, at $\rho(x) - \pi(x) \to \infty$ for $x \to \infty$, men for at vise det maa man inddrage de la Vallée-Poussins stærke Primtalsvurdering; uden denne kan vi kun vise det ovenfor nævnte, altsaa at $\rho(x) - \pi(x)$ stedvis bliver positiv, men det er jo ogsaa tilstrækkeligt til at vise Hypotesernes Modstrid, og det vil fremgaa, at til det Formaal er Primtalssætningen ikke til nogen Nytte, vi kan klare os med de svagere Tchebycheff-Vurderinger.

Anden Hypotese medfører at der vilkaarligt langt ud i Primtalfølgen findes helt smaa Huller (fx Primtaltvillingerne); det kan man ikke vise, men derimod vil det undervejs i Betragtningerne fremgaa, at der stedvis vil findes konsekutive Primtal af Størrelsesorden x, hvis Differens er vilkaarlig mange Gange større end "Normaldifferensen" log x. Det viser i hvert Fald, at der er Uregelmæssigheder i Primtalfølgen, og er derfor ikke saa fjernt fra vort Formaal.

Som Forberedelse til Beviset vil vi notere et Par Resultater.

I°: Det uendelige Produkt $\prod_p (1 - \frac{1}{p})$ er lig 0, ensbetydende

med at Rækken $\sum \frac{1}{p}$ er divergent. Thi med Stieltjesintegralskrivemaaden har vi

$$\sum_{p \leqq x} \frac{1}{p} = \int_1^x \frac{1}{t}\, d\,\overline{\Pi}(t) = \frac{1}{x}\,\overline{\Pi}(x) + \int_1^x \frac{1}{t^2} \cdot \overline{\Pi}(t)\, dt\ ,$$

og da $\overline{\Pi}(t)$ paanær en begrænset Faktor er lig $t/\log t$ faas at Summen vokser af Størrelsesordenen $\log(\log x)$. (En forfinet Analyse giver iøvrigt at (Summen $-\ \log(\log x)$) konverer mod en Konstant 0,26..).

II°: Vi har $P_z < e^{3z}$ (idet P_z er Produktet af Primtallene $\leqq z$). Det følger umiddelbart af Tchebycheffs Vurdering, idet de enkelte Primtal er $\leqq z$, og deres Antal er $< 3z/(\log z)$.

Beviset for Hovedresultatet skal bestaa af to Dele. I første Del vil vi vise, at $\overline{M}_z$ indeholder et langt ubrudt Interval af konsekutive hele Tal.

Det er trivielt at $\overline{M}_z$ indeholder et Interval af Længde $z-1$, idet $]1,z] \subseteqq \overline{M}_z^0$, men vi vil vise, at for $z \to \infty$ vil $\frac{1}{z} \cdot$(Længden af det største Interval i $\overline{M}_z$) $\to \infty$. Det kan aabenbart ogsaa udtrykkes som:

Til ethvert $\varepsilon > 0$ findes et $K = K_\varepsilon$, saa for alle $x > K$ haves $]0,x] \subseteqq$ et $\overline{M}_{\varepsilon x}$.

Bevis: Vi kan antage $\varepsilon < 1$, og vælger

$$A,\ \text{saa}\ \frac{1}{A} < \frac{\varepsilon}{20}\ , \quad \text{og} \quad B,\ \text{saa}\ \prod_{p \in]A,B]} \left(1 - \frac{1}{p}\right) < \frac{\varepsilon}{20}\ ,$$

(det sidste er muligt p.G.a. I° ovenfor). For $x > AB$ har vi saa Rækkefølgen

Det gælder nu om at bestemme $\overline{M}_{\varepsilon x} = \bigcup_{p \leqq \varepsilon x} \{t \equiv a_p \pmod p\}$ saa det indeholder alle Tallene $]0,x]$.

For $p \in]0,A]$ og for $p \in]B, \frac{x}{A}]$ vælges $a_p = 0$.

Dermed vil $\overline{M}_{\varepsilon x}$ indeholde $]0,x]$ paanær

1) Tal af Formen $p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, hvor $p_j \in]A,B]$ (blandt disse er Tallet 1 med)

2) Primtallene paa $]\frac{x}{A},x]$ (alle ægte Multipla af disse Tal er derimod kommet med i $\overline{M}_{\varepsilon x}$, idet deres øvrige Primfaktorer er mindre end A).

Antallet af resterende Tal er derfor mindre end

$$^{1)}\ (1 + \frac{\log x}{\log A})^B \qquad + \qquad ^{2)}\ \overline{\Pi}(x) - \overline{\Pi}(\tfrac{x}{A})$$

(Vurderingen 1) skyldes at ethvert α_j opfylder $0 \leqq \alpha_j \leqq \frac{\log x}{\log A}$, og Antallet r er jo i hvert Fald mindre end B).

For alle tilstrækkelig store x er dette samlede Antal mindre end $\overline{\Pi}(x)$, thi Bidraget fra 1) vokser højst som en Potens af log x, medens $\overline{\Pi}(\frac{x}{A})$ vokser som $\frac{x}{A}/\log\frac{x}{A}$, altsaa omtrent som $\frac{x}{\log x}$.

Saa lader vi p gennemløbe Primtallene paa $]A,B]$, og vælger hver Gang a_p saaledes at Restklassen (a_p) sluger flest muligt af de resterende Tal; for hvert p vil Restklasserne tilsammen indeholde alle Tallene, og der er derfor mindst en af Restklasserne, som indeholder mindst $\frac{1}{p}$ af dem, og Antallet bliver derfor i hvert Fald nedsat med en Faktor $(1 - \frac{1}{p})$. Ialt bliver Antallet nedsat med en Faktor paa højst $\prod(1 - \frac{1}{p}) < \frac{\varepsilon}{20}$, saa det resterende Antal er nu mindre end $\frac{\varepsilon}{20} \cdot \overline{\Pi}(x)$.

Dem fjerner vi saa, et ad Gangen, idet vi hver Gang vælger et passende a_p for p liggende i Intervallet $]\frac{x}{A}, \varepsilon x]$, saalænge indtil alt er fjernet. Hvis x er tilstrækkelig stor saa gaar det, thi saa har vi $\frac{\varepsilon}{20}\overline{\Pi}(x) < \overline{\Pi}(\varepsilon x) - \overline{\Pi}(\frac{x}{A})$, hvilket følger af Tchebycheffs Vurdering af $\overline{\Pi}$: Dels er $\frac{\varepsilon}{20} \cdot \overline{\Pi}(x) < \frac{\varepsilon}{20} \cdot \frac{3x}{\log x}$, og dels er $\overline{\Pi}(\varepsilon x) - \overline{\Pi}(\frac{x}{A}) > \overline{\Pi}(\varepsilon x) - \overline{\Pi}(\frac{\varepsilon}{20}x)$, og naar man i Vurderingerne af dette benytter at for tilstrækkelig store x er $\frac{\log \varepsilon x}{\log x}$ nær ved 1,

og analogt med $\log \frac{\varepsilon}{20} x \,/ \log x$, finder man at Uligheden er opfyldt (Tallet 20 er valgt saa der bliver et lille Overskud naar man bruger Tchebycheffvurderingerne med $\frac{1}{3}$ og 3). □

Det var første Del af Beviset for Hovedresultatet.

Inden vi gaar videre noterer vi som et Korollar at der findes store Huller i Primtalfølgen, idet <u>for et vilkaarligt stort H gælder det for alle tilstrækkelig store y at Intervallet $]0,y]$ indeholder mindst $H \cdot \log y$ paa hinanden følgende hele Tal, som alle er sammensatte.</u>

Thi lad et G være givet, da vil for alle tilstrækkelig store z gælde at $\overline{M}_z^0$ indeholder et Interval af Længde $> Gz$, og et saadant Interval findes indenfor Perioden $]0,P_z]$ (det kan ikke gaa ud over Enderne af dette Interval, thi vi ved jo at $1 \notin \overline{M}_z^0$). Primtallene i $\overline{M}_z^0$ ligger alle i $]0,z]$, og hvis vi fjerner dette har vi altsaa mindst $(G-1) \cdot z$ konsekutive sammensatte Tal som alle er mindre end P_z, altsaa mindre end e^{3z} (ifølge II° foran). Sættes $y = e^{3z}$ har vi det paastaaede med $H = \frac{1}{3}(G-1)$. □

Det hidtidige er egentlig ældre Resultater, idet de - med det Formaal at bevise de omtalte store Huller i Primtalfølgen - gaar tilbage til Westzynthius (finsk) 1931 og Erdös 1935. Men nu kommer vi til det egentlige Bidrag af Hensley & Richards, altsaa <u>anden Del</u> af Beviset for Hovedresultatet.

For at klarholde Begreberne er det maaske praktisk her at benytte Kvantorer. Vi skal dog et langt Stykke frem holde ε fast, og ligeledes fastholde $x \geqslant K_\varepsilon$ (fra foregaaende Sætning), saa disse Bogstaver vil vi udelade. Nogle Variable skal tilhøre $\mathbb{Z}$, andre skal blot tilhøre $\mathbb{R}$, men det er ret selvfølgeligt, og vil kun blive anført i Teksten. Vi har $x \in \mathbb{R}$; som sædvanlig skal en Intervalbetegnelse $]a,b]$ kun betegne de hele Tal n med $a < n \leqslant b$.

Vi havde

$$\exists_{\overline{M}_{\varepsilon x}} : \;]0,x] \subseteqq \overline{M}_{\varepsilon x} ,$$

og ved Translation kan vi flytte $\overline{M}_{\varepsilon x}$ over i $\overline{M}^{o}_{\varepsilon x}$, saa ($y' \in \mathbb{Z}$)

$$\exists_{y'} : \;]y',y'+x] \subseteqq \overline{M}^{o}_{\varepsilon x} .$$

Vi multiplicerer Konfigurationen med p (p betegner et Primtal, men Operationen her er faktisk gyldig for alle $p \in \mathbb{N}$), hvorved $\overline{M}^{o}_{\varepsilon x}$ afbildes ind i sig selv ; vi sætter $p \cdot y' = y$, og har saa

$$\forall_p \; \exists_y : \{y+p, y+2p, \ldots, y+[x]\,p\} \subseteqq \overline{M}^{o}_{\varepsilon x} .$$

Da $\overline{M}^{o}_{\varepsilon x}$ har Perioden $P_{\varepsilon x}$ kan vi endda vælge y vilkaarlig i en Periodelængde, og vi har, med $k \in \mathbb{R}$,

$$\forall_k \; \forall_p \; \exists_{y \in \,]-k-P_{\varepsilon x},-k]} : \{y+p, \ldots, y+[x]\,p\} \subseteqq \overline{M}^{o}_{\varepsilon x} .$$

Vi har $y \leqq -k$; vi tager nu $k > 0$ og $p > \frac{2k+P_{\varepsilon x}}{x}$, hvormed vi faar $y + xp > y + 2k + P_{\varepsilon x} > k$. Altsaa vil Intervallet $]-k,k]$ være indeholdt i Intervallet $]y,y+xp]$, og den Del af Restklassen (y) modulo p som ligger indeni Intervallet $]-k,k]$ maa være en Delmængde af $\{y+p, \ldots, y+[x]\,p\}$. Altsaa

$$\forall_{k>0} \; \forall_{p > \frac{2k+P_{\varepsilon x}}{x}} \; \exists_y : \{t \equiv y \,(\mathrm{mod}.p)\} \cap]-k,k] \subseteqq \overline{M}^{o}_{\varepsilon x} .$$

Men det betyder jo, at indenfor Intervallet $]-k,k]$ vil $\overline{M}^{o}_{\varepsilon x}$ indeholde en Restklasse modulo ethvert p, der er tilstrækkelig stort, og vil derfor paa dette Interval være identisk med et $\overline{M}_{\infty}$. Præcist: Vi tager et m større end $\frac{2k+P_{\varepsilon x}}{x}$, og hvis vi desuden sørger for at m er større end εx saa er $\overline{M}^{o}_{\varepsilon x} \subseteqq \overline{M}^{o}_{m}$, og vi har ($m \in \mathbb{R}$)

$$\forall_{k>0} \; \forall_{m > \varepsilon x, \frac{2k+P_{\varepsilon x}}{x}} \; \exists_{\overline{M}_{\infty}} : \; \overline{M}_{\infty} \cap]-k,k] = \overline{M}^{o}_{m} \cap]-k,k] .$$

Paa et Interval er et $\overline{M}_{\infty}$ komplementært til et brugbart Sæt, og benytter vi dette paa $]-k,k]$, hvis Længde er 2k, faar vi

$$\forall_{k>0}\,\forall_{m>\varepsilon x,\frac{2k+P_{\varepsilon x}}{x}} : \quad \rho(2k) \geqq \left|\,]-k,k] \setminus \overline{M}_m^o\,\right| .$$

Hidtil har vi holdt x fast, idet blot $x > K_\varepsilon$. Nu lader vi ogsaa x variere,

Vi sætter

$$k = e^{3\varepsilon x} \qquad \text{og} \qquad m = \frac{3k}{x} .$$

Vi har $P_{\varepsilon x} < k$ og dermed er $m > \frac{2k+P_{\varepsilon x}}{x}$ (og endvidere er k positiv), og for tilstrækkelig store x er ogsaa $m > \varepsilon x$, idet

$$m = \frac{3k}{x} = \frac{3\cdot e^{3\varepsilon x}}{x} > \varepsilon x \quad \text{for } x \text{ stor.}$$

Endvidere konstaterer vi at $m < k$ (dersom blot $x > 3$), og at for tilstrækkelig store x er $m > \sqrt{k}$, idet

$$\frac{m}{\sqrt{k}} = \frac{1}{x}\cdot 3 \cdot e^{\frac{3\varepsilon x}{2}} > 1 \quad \text{for } x \text{ stor.}$$

Vi betragter nu $]-k,k] \setminus \overline{M}_m^o$; bortset fra at venstre Endepunkt mangler er der Symmetri omkring 0. Vi havde $\sqrt{k} < m < k$, hvoraf umiddelbart følger at paa den positive Halvakse bestaar denne Mængde netop af Primtallene paa $]m,k]$ suppleret med Tallet 1 (da jo $1 \notin \overline{M}_m^o$). Følgelig har vi

$$\rho(2k) > 2\pi(k) - 2\pi(m) .$$

Da $k = e^{3\varepsilon x}$ ses, at store x-Værdier svarer til store k-Værdier, og idet vi udtrykker m ved k faar vi som Hovedresultat

$$\boxed{\rho(2k) > 2\pi(k) - 2\pi\left(\frac{9\varepsilon k}{\log k}\right) \quad \text{for alle } k > K_\varepsilon^* .}$$

Hvis vi saa benytter de la Vallée-Poussins Vurdering af π er vi færdige. Ved at udvikle, fx $\frac{1}{\log 2k} = \frac{1}{\log k} - \frac{\log 2}{(\log k)^2} + \cdots$ osv.,

finder man

$$\rho(2k) - \overline{\Pi}(2k) \geqq (2 \log 2 - 18\varepsilon) \cdot \frac{k}{(\log k)^2} + R(k) ,$$

hvor Restleddet bliver forsvindende i Fh.t. $k/(\log k)^2$ for $k \to \infty$. Tager man nu blot et passende lille ε (fx lig $\frac{1}{18}$, det er ikke nødvendigt at lade $\varepsilon \to 0$) vil Højresiden gaa mod uendelig for $K \to \infty$, og vort Hovedresultat vil være bevist.

Uden Brug af de la Vallée-Poussins fine Restledvurdering kan vi kun vise, at $\rho(x) - \overline{\Pi}(x)$ stedvis bliver positiv og endda vilkaarlig stor, altsaa at lim sup $(\rho(x) - \overline{\Pi}(x)) = \infty$, medens Resultatet ovenfor sagde at lim $(\rho(x) - \overline{\Pi}(x)) = \infty$. Men til Gengæld kan vi komme igennem blot ved at benytte Tchebycheffvurderingerne (S.34) som udsagde at

$$\frac{1}{3} < f(x) = \frac{\log x}{x} \cdot \overline{\Pi}(x) < 3 .$$

Af skrivemæssige Hensyn vil vi igen benytte $m = (9\varepsilon k)/(\log k)$, idet vi bemærker, at k og m samtidig vil gaa mod uendelig; for $k \to \infty$ vil altsaa ogsaa $\overline{\Pi}(m) \to \infty$, og endvidere vil $\frac{\log m}{\log 2k} \to 1$. Vi vil nu bevise, at Størrelsen

$$\rho(2k) - \overline{\Pi}(2k) - 2\overline{\Pi}(m)$$

kan blive positiv for vilkaarlig store k-Værdier, da deraf følger at lim sup $(\rho(x) - \overline{\Pi}(x)) = \infty$. Ifølge Uligheden foran er Størrelsen større end $2\overline{\Pi}(k) - \overline{\Pi}(2k) - 4\overline{\Pi}(m)$, som altsaa skal vises at blive stedvis positiv. For at faa f ind i Spillet multiplicerer vi med $\frac{\log k}{2k}$, og faar dermed (idet vi betegner det d(k)) at

$$d(k) = f(k) - (1 - \frac{\log 2}{\log 2k}) \cdot f(2k) - 2 \cdot \frac{\log k}{k} \cdot \frac{m}{\log m} \cdot f(m) ,$$

og idet vi spalter den midterste Parentes op, og saa paa de to sidste Led benytter Grænserne for f, og endvidere indsætter

Forholdet $\frac{m}{k}$ i sidste Led faar vi (bruger ogsaa, at $\log 2 > \frac{1}{2}$)

$$d(k) > f(k) - f(2k) + \frac{1}{6}\cdot\frac{1}{\log 2k} - \frac{54\varepsilon}{\log m} \quad .$$

Da nu $\frac{\log m}{\log 2k} \to 1$ kan vi (for tilstrækkelig store k) trække de to sidste Led sammen; hvis blot vi vælger et tilstrækkelig lille ε (fx ε lig 10^{-3}, vi behøver heller ikke her at lade ε gaa mod 0) faar vi

$$d(k) > f(k) - f(2k) + \frac{1}{10}\cdot\frac{1}{\log 2k} \quad .$$

Hvis vi opskriver denne Ulighed med k, med 2k, med 4k,..., med $2^{r-1}k$, og adderer det hele, faas

$$\sum_{j\in[0,r[} d(2^j k) > f(k) - f(2^r k) + \frac{1}{10}\cdot\sum_{j\in]0,r]}\frac{1}{\log 2^j k} \quad .$$

For $r \to \infty$ vil Højresiden gaa mod uendelig, thi f er begrænset, og Summanden under $\sum$-Tegnet er lig $\frac{1}{j\cdot\log 2 + \log k}$ (med j som variabel), og det er Led i en Række der divergerer (af Type som den harmoniske Række). Altsaa maa $d(2^j k)$ være positiv for uendelig mange j. □

Dermed er vort paastaaede Hovedresultat bevist.

Kapitelfortegnelse.

Et Par tværgaaende Emner.

Nogle Trykfejl.

Side 49, Linie 9 for "$(\pm 4)^2 = 16 \equiv 3$" læs "...$16 \equiv 5$"

Side 49, Linie 13 "uforkortelige" skal udgaa

Side 74, midtpaa for "$g = f * \xi$" læs "$g = f * \mu$"

Side 84, Linie 7 t.h. læs "$\phi_2(x) = -\phi_1(-x)$"

Side 108 midtpaa læs
"Dersom $f(t), g(t) \in K$ og er kontinuerte og"

Side 117, Linie 3 f.n. læs "$X, Y, \ldots \neq E$" for hvilke..

Side 128, Linie 3 læs
"Vi betragter nu Antallet af alle Mængder $\mathfrak{M}$ for.."

Side 133, Linie 11 for "ensbetydende med" læs "medfører"

Side 166, Linie 2 Cirkelkonfigurationen
er i hvert Fald beskrevet allerede 1923 af A.Speiser (schweitsisk).

Side 189, Linie 3 f.n. for "som Værdimængde har"
læs "som Værdimængden $\cap N$ har"

Side 191, Linie 3 læs "Linnik (L.1915-72)"

Side 191, Linie 3 f.n. for "Eksponenten"
læs "Addendtallet"