Elementær talteori 2011

Anders Thorup

Matematisk Afdeling
Københavns Universitet

Anders Thorup, e-mail: thorup@math.ku.dk
Elementær talteori, 2011

Matematisk Afdeling
Universitetsparken 5
2100 København Ø

Indhold

Forord.

Elementær talteori handler om vores sædvanlige naturlige tal, først og fremmest om en række spændende egenskaber ved primtallene. Fremstillingen her er elementær i den forstand, at der ikke indgår nogen omfattende teoridannelse: de enkelte resultater opnås med det værktøj, der sådan er for hånden, eller lige kan udvikles. På den anden side vil dette værktøj først og fremmest være resultaterne fra Matematik 2AL/Algebra 2, og i den forstand er kurset bestemt ikke trivielt. Et enkelt kapitel forudsætter i øvrigt at læseren har et kendskab til kompleks analyse, fx fra Matematik 2KF eller KomAn.

Matematisk Afdeling, februar 2006
Anders Thorup

1. Primtallene.

(1.1) Setup. Et tal p kaldes som bekendt et *primtal*, hvis $p \geqslant 2$ og p kun har trivielle divisorer, dvs hvis de eneste (positive) divisorer i p er 1 og p. De første primtal er tallene

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots .$$

Som bekendt gælder:

Sætning (Euklid). *Der er uendelig mange primtal.*

Bevis. En drejning af det velkendte bevis er følgende: Betragt den uendelige følge af tal $a_1, a_2, \dots$, defineret ved $a_1 := 2$ og, induktivt, $a_k = (a_1 \cdots a_{k-1}) + 1$. Øjensynlig gælder, at $2 \leqslant a_1 < a_2 < \cdots$. For $i < k$ er a_i divisor i $a_k - 1$, så a_i og a_k er primiske. Specielt har hvert tal a_k altså sine egne primdivisorer. Da der er uendelig mange tal a_k, er der uendelig mange primtal. □

Korollar. *Det k'te primtal p_k er mindre end eller lig med $2^{2^{k-1}}$.*

Bevis. Med notationen i beviset ovenfor er tallene $a_1, \dots, a_k$ delelige med k forskellige primtal. Specielt er $p_k \leqslant a_k$. Øjensynlig er, for $k \geqslant 2$,

$$a_k = (a_1 \cdots a_{k-2})a_{k-1} + 1 = (a_{k-1} - 1)a_{k-1} + 1 < a_{k-1}^2.$$

Ved induktion følger det let, at $a_k \leqslant 2^{2^{k-1}}$. □

Alle primtal p_k bortset fra det første $p_1 = 2$ er ulige. Specielt er afstanden mellem 2 på hinanden følgende primtal p_k og p_{k+1} (for $k \geqslant 2$) altid mindst 2. *Primtalstvillinger* er par (p_k, p_{k+1}), hvor afstanden er netop 2, fx (3, 5), (5, 7), (11, 13), ... , (347, 349), ... Man ved ikke, om der er uendelig mange primtalstvillinger. Derimod er det klart, at der findes par (p_k, p_{k+1}) med vilkårlig stor afstand. Fx er tallene $l! + 2, l! + 3, \dots, l! + l$ en sekvens af $l - 1$ på hinanden følgende tal, der alle er sammensatte.

(1.2) Primtalsfunktionen. Med $\pi(x)$ betegnes antallet af primtal $p \leqslant x$. Med denne definition, for alle reelle tal x, er $\pi(x)$ en trappefunktion, kontinuert fra højre, og med springet $+1$ præcis i primtallene. A priori er naturligvis værdierne $\pi(n)$ for naturlige tal n de mest interessante. Af overvejelserne i (1.1) følger:

$$\pi(n) \to \infty \quad \text{for } n \to \infty, \quad \log_2 \log_2 n < \pi(n) < n. \tag{1.2.1}$$

Uligheden $\log_2 \log_2 n < \pi(n)$ medfører naturligvis Euklid's resultat, da $\log_2 \log_2 n$ går mod ∞ for $n \to \infty$. Men funktionen $\log_2 \log_2 n$ vokser fortvivlende langsomt: Fx, for $n = 10^{150}$, medfører uligheden kun, at der er 9 primtal mindre end 10^{150}. Det faktiske antal primtal mindre end 10^{150} er naturligvis(?) ikke kendt, men det er større end 10^{147}.

(1.3) Primtalssætningen. En optælling af primtal giver tabellen [Funktionen $A(n)$ i sidste søjle forklares i (1.12)],

n	$\pi(n)$	$n/\pi(n)$	$A(n)$
10^1	4	2,5	−0,2
10^2	25	4,0	0,6
10^3	168	6,0	0,9
10^4	1229	8,1	1,1
10^5	9592	10,4	1,1
10^6	78498	12,7	1,1
10^7	664579	15,0	1,1
10^8	5761455	17,4	1,0
10^9	50847534	19,7	1,0
10^{10}	455052512	22,0	1,0

Multiplikation af n med en faktor 10 svarer altså til forøgelse af $n/\pi(n)$ med en konstant, $\approx 2,3$. Matematikere genkender (genkendte?) naturligvis denne konstant som $\log 10$, og gætter derfor på, at $n/\pi(n)$ kan tilnærmes med $\log n$. Dette resultat er Primtalssætningen: *Asymptotisk gælder relationen,*

$$\pi(n) \sim \frac{n}{\log n}\,, \tag{1.3.1}$$

i den forstand, at vi for kvotienten mellem venstre- og højresiden har

$$\frac{\pi(n)}{n/\log n} \to 1 \quad \textit{for} \quad n \to \infty.$$

Ækvivalent betyder Primtalssætningen, at for alle givne positive $c<1$ og $C>1$ gælder, for $n \gg 0$ (dvs når n er tilstrækkelig stor), ulighederne,

$$\frac{c}{\log n} \leqslant \frac{\pi(n)}{n} \leqslant \frac{C}{\log n}\,. \tag{1.3.2}$$

I det følgende giver vi et elementært bevis for de to uligheder, for *alle* $n \geqslant 2$:

$$\frac{\frac{1}{3}}{\log n} \leqslant \frac{\pi(n)}{n} \leqslant \frac{3}{\log n}\,. \tag{1.3.3}$$

Primtalssætningen blev formodet sidst i 1700-tallet, af Legendre og Gauss (som 15-årig i 1792), på basis af tabeller over primtal. Ulighederne (1.3.3) blev vist omkring 1850 af Chebyshev [1821–1894]. Mere præcist viste Chebyshev, at ulighederne (1.3.2) er opfyldt med $c := 0,89$ og $C := 1,11$ for $n \geqslant n_0$. Primtalssætningen blev først bevist i 1896 af Hadamard [1865–1963] og (uafhængigt) af de la Vallée Poussin [1866–1962].

Det skal understreges, at Primtalssætningen, dvs den asymptotiske relation (1.3.1), alene er et udsagn om *forholdet* mellem de to funktioner $\pi(n)$ og $n/\log n$; resultatet siger ikke, at *forskellen* er lille. Defineres $\varepsilon(n) := \pi(n)/(n/\log n) - 1$, har vi øjensynlig

$$\pi(n) - n/\log n = \varepsilon(n)(n/\log n), \tag{1.3.4}$$

og Primtalssætningen er ækvivalent med, at $\varepsilon(n) \to 0$ for $n \to \infty$. Funktionen $n/\log n$ går mod uendelig. Primtalssætningen siger altså end ikke, at forskellen (dvs venstresiden af (1.3.4)) er begrænset, men snarere, at forskellen går langsommere mod ∞ end $n/\log n$.

Primtalssætningen, altså relationen (1.3.1), er øjensynlig ækvivalent med følgende:

$$\frac{\pi(n)}{n} \sim \frac{1}{\log n}\,.$$

For et givet tal n er brøken $\pi(n)/n$ lig med sandsynligheden for, at et tilfældigt tal $p \leqslant n$ er et primtal. Primtalssætningen udsiger heuristisk, at denne sandsynlighed, når n er stor, er omtrent $1/\log n$. Ifølge Chebyshev's ulighed (1.3.3) er sandsynligheden i hvert fald mindre end $3/\log n$; specielt går sandsynligheden mod 0 for $n \to \infty$, så primtal bliver mere sjældne ude til højre på talrækken. På den anden side er sandsynligheden større end $\frac{1}{3}/\log n$, og den er altså ikke forsvindende: sandsynligheden for, at et tilfældigt tal med 100 decimaler er et primtal, er af størrelsesordenen,

$$1/\log 10^{100} \approx 0,004.$$

(1.4) Sætning. *For alle $n \geqslant 1$ og $n/2 \leqslant k \leqslant n$ er $\binom{n}{k} \geqslant k^{\pi(n)-\pi(k)}$.*

Bevis. For binomialkoefficienten har vi udtrykket,

$$\binom{n}{k} = \binom{n}{n-k} = \frac{n\cdot(n-1)\cdots(k+1)}{1\cdot 2\cdot 3\cdots(n-k)}\,.$$

Blandt faktorerne i tælleren er der $\pi(n) - \pi(k)$ primtal, og de er alle er større end k. Da $k \geqslant n-k$, kan ingen af disse primtal gå op i nævneren. Binomialkoefficienten er derfor delelig med produktet af disse primtal. Heraf følger påstanden. □

(1.5) Korollar. *For alle $n \geqslant 1$ er $n^{\pi(n)} \leqslant 2^{4n}$.*

Bevis. Uligheden vises let for $n \leqslant 3$, og den vises ved fuldstændig induktion for $n > 3$. Sæt $k := \lfloor (n+1)/2 \rfloor$. Tallet $(n+1)/2$ er enten et helt tal eller et helt tal plus $1/2$. Derfor er $n/2 \leqslant k \leqslant (n+1)/2$. Af (1.4) og induktionsantagelsen (og de trivielle vurderinger $\pi(n) \leqslant n-2$ og $\binom{n}{k} \leqslant 2^n$) får vi derfor, at

$$n^{\pi(n)} = (n/k)^{\pi(n)} k^{\pi(n)-\pi(k)} k^{\pi(k)} \leqslant 2^{\pi(n)} \binom{n}{k} 2^{4k} \leqslant 2^{n-2} 2^n 2^{4(n+1)/2} = 2^{4n},$$

som ønsket. [Hvor i induktionsskridtet brugtes, at $n \geqslant 4$?] □

Note. Med en del ekstrabesvær kan man forbedre den anførte vurdering til følgende:

$$n^{\pi(n)} \leqslant 2^{8n/3} \quad \text{for alle } n \geqslant 1. \tag{1.5.1}$$

Lad os prøve at vise ved fuldstændig induktion, som i beviset for Korollaret, en ulighed af den generelle form,

$$n^{\pi(n)} \leqslant 2^{Cn}.$$

I induktionsskridtet sættes $k := \lfloor (n+1)/2 \rfloor$, hvilket via (1.4) giver vurderingen,

$$n^{\pi(n)} \leqslant 2^{\pi(n)} \binom{n}{k} 2^{C(n+1)/2}. \tag{1.5.2}$$

Ovenfor udnyttede vi vurderingerne $\pi(n) \leqslant n-2$ og $\binom{n}{k} \leqslant 2^n$. Den sidste ulighed kan umiddelbart skærpes: Det er let at se, at hvis en vurdering af formen $\binom{n}{k} \leqslant 2^{n-c}$ (for alle k) gælder for $n = n_0$, så gælder den for alle $n \geqslant n_0$. For $n = 9$ er den største binomialkoefficient lig med 127, og altså mindre end $128 = 2^7 = 2^{9-2}$. Følgelig er $\binom{n}{k} \leqslant 2^{n-2}$ for alle $n \geqslant 9$. Altså får vi fra (1.5.2):

$$n^{\pi(n)} \leqslant 2^{\pi(n)+(n-2)+C(n+1)/2}. \tag{1.5.3}$$

Vi kan også forbedre vurderingen af $\pi(n)$. Blandt tallene mindre end eller lig med n som *ikke* er primtal har vi i hvert fald følgende: tallet 1, de lige tal fraregnet tallet 2, tallene delelige med 3 fraregnet tallet 3 og tallene delelige med 6, samt tallet 25, hvis $n \geqslant 25$. Idet vi antager, at $n \geqslant 25$, er antallet af ikke-primtal altså mindst:

$$1 + (\lfloor \tfrac{n}{2} \rfloor - 1) + (\lfloor \tfrac{n}{3} \rfloor - \lfloor \tfrac{n}{6} \rfloor - 1) + 1 = \lfloor \tfrac{n}{2} \rfloor + \lfloor \tfrac{n}{3} \rfloor - \lfloor \tfrac{n}{6} \rfloor.$$

For antallet i komplementærmængden, altså for $\pi(n)$, gælder derfor, at

$$\pi(n) \leqslant n - \lfloor \tfrac{n}{2} \rfloor - \lfloor \tfrac{n}{3} \rfloor + \lfloor \tfrac{n}{6} \rfloor.$$

Udtrykket på højresiden er, for et naturligt tal n, højst $n/3 + 2/3$, hvad der let indses ved at kigge på de 6 muligheder for restklassen af n modulo 6. Herefter er

$$\pi(n) + (n-2) \leqslant \tfrac{n}{3} + \tfrac{2}{3} + n - 2 = \tfrac{4}{3}(n-1).$$

Ved indsættelse i (1.5.3) fås, at

$$n^{\pi(n)} \leqslant 2^{\frac{4}{3}(n-1)+C(n+1)/2}. \tag{1.5.4}$$

Eksponenten på højresiden er mindre end eller lig med Cn, præcis når $C \geqslant 8/3$. Specielt, for $C = 8/3$, fås uligheden (1.5.1).

I udregningerne er det antaget, at $n \geqslant 25$, og yderligere, at uligheden (1.5.1) også gælder for $k := \lfloor (n+1)/2 \rfloor$. Induktionen kommer altså slet ikke i gang med mindre uligheden også vises for nogle værdier af $n = 13, 14, \dots, 24$. For at vise, at uligheden gælder for *alle* $n \geqslant 1$, mangler vi at vise de 24 uligheder for $n = 1, \dots, 24$. For $n = 1, 2, 3$ er det helt trivielt. I almindelighed, for $n \geqslant 2$, er det ækvivalent at vise, med $\kappa(n) := (8/3)n(\log 2)/(\log n)$, at $\pi(n) \leqslant \kappa(n)$. Betragt følgende uligheder:

$$\begin{aligned}
\pi(n) \leqslant \pi(30) = 10 \leqslant \tfrac{32}{3} = \kappa(16) \leqslant \kappa(n), \\
\pi(n) \leqslant \pi(15) = 6 \leqslant \tfrac{64}{9} = \kappa(8) \leqslant \kappa(n), \\
\pi(n) \leqslant \pi(7) = 4 \leqslant \tfrac{16}{3} = \kappa(4) \leqslant \kappa(n).
\end{aligned}$$

Øjensynlig er $\kappa(2^i) = 2^{i+3}/(3i)$ et rationalt tal, let at beregne, og ulighederne mellem de eksplicitte værdier af $\pi(x)$ og $\kappa(y)$ følger ved optælling. Funktionerne $\pi(n)$ og $\kappa(n)$ (for $n \geqslant e$) er voksende. Derfor gælder de yderste uligheder i den første linie for $16 \leqslant n \leqslant 30$, i den 2. linie for $8 \leqslant n \leqslant 15$, og i den 3. linie for $4 \leqslant n \leqslant 7$. Specielt gælder de manglende uligheder for $4 \leqslant n \leqslant 24$.

(1.6) Lemma. *For et primtal p og alle $n \geqslant 1$ og $0 \leqslant k \leqslant n$ gælder, at hvis potensen p^ν er divisor i binomialkoefficienten $\binom{n}{k}$, så er $p^\nu \leqslant n$.*

Bevis. Påstanden vises ved fuldstændig induktion efter n. Lad b være binomialkoefficienten, skrevet som brøk:

$$b := \binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{1 \cdot 2 \cdots k}.$$

Antag, at $p^\nu \mid b$. Det skal vises, at $p^\nu \leqslant n$. Det er trivielt for $\nu = 0$, så vi kan antage, at $\nu > 0$. Specielt er så $n > k \geqslant 1$, og i brøken b er mindst én faktor i tælleren delelig med p.

Lad b' være den brøk, der fremkommer af brøken b ved at fjerne, fra tæller og nævner, alle faktorer, der ikke er multipla af p. Hvis $n'p$ og $k'p$ er de største multipla af p i henholdsvis tæller og nævner, resterer i nævneren faktorerne $1p, 2p, \dots, k'p$. Vi har altså

$$b' = \frac{n'p \cdot (n'-1)p \cdot (n'-2)p \cdots}{1p \cdot 2p \cdot 3p \cdots k'p}.$$

Både tæller og nævner i brøken b er produkter af k på hinanden følgende hele tal, og det er hver p'te faktor, der er delelig med p. I nævneren er der k' faktorer, der er delelige med p, og de første $p - 1$ faktorer ikke delelige med p. Heraf følger, at der i tælleren af b er k' eller $k' + 1$ faktorer, der er delelige med p. De resterer i tælleren for b'. Ved at forkorte k' gange med p får vi i det første tilfælde, at

$$b' = \binom{n'}{k'}, \tag{1}$$

og i det andet tilfælde, at

$$b' = \binom{n'}{k'} \cdot (n' - k')p = \binom{n'-1}{k'} n'p = \binom{n'}{k'+1} \cdot (k'+1)p; \tag{2}$$

de sidste ligninger er blot trivielle omskrivninger af binomialkoefficienten. I begge tilfælde er brøken b' altså et helt tal. Da $p^\nu \mid b$ følger det, at $p^\nu \mid b'$.

I det første tilfælde fås derfor af (1), og induktion, at $p^\nu \leqslant n'$, og så er $p^\nu \leqslant n' < n'p \leqslant n$.

Betragt det andet tilfælde. I de tre udtryk for b' i (2) forekommer faktorerne $n'-k'$, n' og $k'+1$. Mindst én af disse faktorer må være primisk med p. Af det tilsvarende udtryk for b' følger derfor, at $p^{\nu-1}$ er divisor i den tilsvarende binomialkoefficient. Ved induktion følger derfor, at $p^{\nu-1} \leqslant n'$ (hvis n' er primisk med p følger det endda, at $p^{\nu-1} \leqslant n'-1$). Altså er $p^\nu \leqslant n'p \leqslant n$, som ønsket. □

(1.7) Sætning. *For alle $n \geqslant 1$ og $0 \leqslant k \leqslant n$ er $\binom{n}{k} \leqslant n^{\pi(n)}$.*

Bevis. Lad $p_1^{\nu_1} \cdots p_r^{\nu_r}$ være primopløsningen af binomialkoefficienten. Af (1.6) følger så, at $p_i^{\nu_i} \leqslant n$. Specielt er $p_i \leqslant n$, og dermed er $r \leqslant \pi(n)$. Altså er

$$\binom{n}{k} = p_1^{\nu_1} \cdots p_r^{\nu_r} \leqslant n^r \leqslant n^{\pi(n)},$$

hvormed uligheden er eftervist. □

(1.8) Korollar. *For alle $n \geqslant 2$ er $\pi(n)\log n \geqslant \frac{1}{2}(\log 2)n$.*

Bevis. Da $2^n = \sum_k \binom{n}{k}$, følger det af (1.7), at $2^n \leqslant (n+1)n^{\pi(n)}$, hvoraf

$$\pi(n)\log n \geqslant \Big(\log 2 - \frac{\log(n+1)}{n}\Big)n.$$

Brøken på højresiden konvergerer mod 0 for $n \to \infty$, og aftagende for $n \geqslant 2$. For $n \geqslant 7$ er parentesen på højresiden altså mindst $\log 2 - \frac{3}{7}\log 2 = \frac{4}{7}\log 2$. Specielt gælder den påståede ulighed for $n \geqslant 7$. Det er let at se, at den gælder for $n = 2, 3, 4, 5, 6$. Altså gælder uligheden for alle $n \geqslant 2$. □

Bevis for ulighederne (1.3.3). Af (1.5) og (1.8) følger, for $n \geqslant 2$, at vi har ulighederne i (1.3.2) med $c = \frac{1}{2}\log 2$ og $C = 4\log 2$. Da $\log 2 = 0,6931\ldots$, har vi specielt (1.3.3). □

(1.9) Konsekvenser. Af Primtalssætningen følger fx, at

$$\log p_n \sim \log n, \qquad p_n \sim n\log n, \quad p_{n+1} \sim p_n, \tag{1.9.1}$$

hvor p_n det n'te primtal. Af Primtalssætningen følger nemlig først, for $n \to \infty$, at

$$\frac{n\log p_n}{p_n} = \frac{\pi(p_n)}{p_n/\log p_n} \to 1, \tag{1}$$

og dermed at

$$\log\frac{n\log p_n}{p_n} = \log n + \log\log p_n - \log p_n \to 0.$$

Efter division med $\log p_n$ fås, at

$$\frac{\log n}{\log p_n} + \frac{\log\log p_n}{\log p_n} \to 1.$$

Da $(\log x)/x \to 0$ for $x \to \infty$, følger det, at

$$\frac{\log n}{\log p_n} \to 1. \tag{2}$$

Hermed er den første relation i (1.9.1) bevist.

Af (1) og (2) følger, at

$$\frac{n \log n}{p_n} = \frac{\log n}{\log p_n} \cdot \frac{n \log p_n}{p_n} \to 1, \tag{3}$$

hvormed den anden relation er bevist. Endelig er

$$\frac{p_{n+1}}{p_n} = \frac{n \log n}{p_n} \cdot \frac{n+1}{n} \cdot \frac{\log(n+1)}{\log n} \cdot \frac{p_{n+1}}{(n+1)\log(n+1)}.$$

På højresiden konvergerer første og sidste brøk mod 1 ifølge (3). De to midterste brøker konvergerer trivielt mod 1. Heraf følger den sidste relation i (1.9.1).

(1.10) Bertrand's Postulat. *Mellem n og $2n$ ligger altid et primtal.*

Ækvivalent er påstanden, at $\pi(2n) > \pi(n)$ for alle naturlige tal n. Påstanden blev bevist af Chebyshev, essentielt som følger: Antag, for givne positive tal c, C, med $c \leqslant 1$ og $C \geqslant 1$, at ulighederne (1.3.2) gælder for $n \geqslant N_0$. Herefter er, for $n \geqslant N_0$,

$$\pi(2n) - \pi(n) \geqslant \frac{2cn}{\log 2 + \log n} - \frac{Cn}{\log n}. \tag{1.10.1}$$

Det er klart, at hvis $2c > C$, så er højresiden positiv for $n \geqslant N_1$, med et $N_1 \geqslant N_0$. Påstanden i Bertrand's postulat gælder altså for $n \geqslant N_1$. For at vise påstanden for *alle* n kræves en eksplicit bestemmelse af c, C med $c/C > \frac{1}{2}$ og et tilhørende N_0; herefter bestemmes N_1 og Bertrand's Postulat er så bevist for alle n, når det er eftervist for de endelig mange $n \leqslant N_1$.

Bemærk, at de værdier af c, C, hvormed vi har vist Chebyshev's uligheder, er helt utilstrækkelige, idet vi her har $c/C = \frac{1}{9}$. Man kan vise [Rosser og Schoenfeld, 1962], at for alle $n \geqslant 1$ er $\pi(n) \leqslant 1{,}3 \cdot n/\log n$ og for alle $n \geqslant 17$ er $\pi(n) \geqslant n/\log n$, og på den baggrund er det let at vise Postulatet. Vi giver senere et elementært bevis for Postulatet.

(1.11). Det er nærligende at sammenligne fordelingen af primtallene med fordelingen af andre uendelige mængder af tal. Betragt fx kvadrattallene: $q_k = k^2$. For funktionen $\nu(n)$, der tæller antallet af kvadrattal mindre end eller lig med n, får vi trivielt den asymptotiske formel,

$$\nu(n) \sim \sqrt{n};$$

sammenligning med (1.3.1) viser, at kvadrattal er „meget mere sjældne" end primtal. Der er som bekendt så få kvadrattal, at rækken $\sum 1/q$, hvor der summeres over kvadrattal, er konvergent (summen er som bekendt $\pi^2/6$). For primtallene gælder modsætningsvis det efterfølgende resultat, der skyldes Euler (1737).

Sætning. *Rækken* $\sum 1/p$, *over primtal* p, *er divergent.*

Bevis. For $0 < y \leqslant \frac{1}{2}$ er $1/(1-y) \leqslant 2$, så vi får vurderingen,

$$\log \frac{1}{1-y} = \sum_{n \geqslant 1} \frac{1}{n} y^n \leqslant \frac{y}{1-y} \leqslant 2y. \tag{1.11.0}$$

Betragt nu for et tal $x > 1$ produktet, over primtal $p \leqslant x$,

$$\prod_{p \leqslant x} \frac{1}{1 - 1/p}.$$

Faktoren svarende til p er summen $\sum_{\nu \geqslant 0} 1/p^\nu$; når disse summer multipliceres fremkommer summen af alle brøker $1/n$, hvor n har en primopløsning med primfaktorer, der alle er højst x. Heri indgår specielt alle brøker $1/n$, hvor $n \leqslant x$. Vi har altså vurderingen,

$$\sum_{n \leqslant x} \frac{1}{n} \leqslant \prod_{p \leqslant x} \frac{1}{1 - 1/p}.$$

Hvis S er summen på venstresiden har vi øjensynlig $S \geqslant \int_1^x dt/t$, altså $S \geqslant \log x$. Altså er

$$\log x \leqslant \prod_{p \leqslant x} \frac{1}{1 - 1/p}. \tag{1.11.1}$$

Tag nu logaritmen på begge sider af (1.11.1), og brug ulighed (1.11.0) for $y = 1/p$. Det giver uligheden,

$$\log \log x \leqslant 2 \sum_{p \leqslant x} \frac{1}{p}. \tag{1.11.2}$$

Heraf ses specielt, at højresiden går mod ∞ for $x \to \infty$, som påstået. □

(1.12) Andre approksimationer. Primtalssætningen kan formuleres ved hjælp af funktionen $A(x)$ defineret ved følgende ligning:

$$\pi(x) = \frac{x}{\log x - A(x)}.$$

Herefter er $(x/\log x)/\pi(x) = 1 - A(x)/\log x$. Primtalssætningen udsiger altså, at kvotienten $A(x)/\log x$ går mod 0 for $x \to \infty$ eller – ækvivalent – med den såkaldte *lille-o-notation*, at

$$A(x) = o(\log x).$$

Funktionen $A(x)$ er differensen $A(x) = \log x - x/\pi(x)$. Dens værdier for de første 10 potenser af 10 kan altså let fås af tabellen i (1.3), idet $\log 10 = 2,3026$. Det er bemærkelsesværdigt, at værdierne er ganske „tæt“ på 1; primtalssætningen forudsiger jo ikke engang, at funktionen $A(x)$ er begrænset. Man kan vise, at *hvis* grænseværdien $\lim_{x\to\infty} A(x)$ eksisterer, så må den være lig med 1. I lyset af dette resultat kunne man håbe, at tilnærmelsen,

$$\pi(n) \sim \frac{n}{\log n - 1}, \tag{1.12.1}$$

i en eller anden forstand er „bedre“ en (1.3.1). Legendre selv foreslog approksimationen $n/(\log n - 1,08366)$. Som anført, dvs som et udsagn om forholdet mellem de to funktioner, er (1.12.1) trivielt ækvivalent med (1.3.1).

Som nævnt udsiger Primtalssætningen heuristisk, for et stort tal n, at sandsynligheden for at et tal $p \leqslant n$ er et primtal er lig med $1/\log n$. Mere præcist må det forventes, at et „lille“ interval af længde Δ omkring n indeholder $\Delta/\log n$ primtal. [„lille“ skal forstås i betydningen „lille sammenlignet med n, men stort nok til statistiske betragtninger“; fx $n = 10^{100}$, $\Delta = 150.000$.] Forventningen leder til følgende tilnærmelse, foreslået af Gauss,

$$\pi(n) \sim \int_2^n \frac{dt}{\log t}. \tag{1.12.2}$$

Igen er det let at se, at relationen (1.12.2) er ækvivalent med Primtalssætningen. Funktionen på højresiden er, bortset fra (addition af) en konstant, *logaritme-integralet* $\mathrm{Li}(n)$.

Riemann [1826–1866] så, at i tallet $\Delta/\log n$, fortolket som antallet af primtal i et interval af længde Δ omkring n, bør også primtalspotenser indgå, således at k'te potenser vægtes med $1/k$. I stedet for funktionen $\pi(x) = \sum_{p\leqslant x} 1$ betragtes altså funktionen,

$$\Pi(x) = \sum_{p^k\leqslant x} \frac{1}{k} = \sum_{k=1}^{\infty} \frac{1}{k}\pi(\sqrt[k]{x}).$$

Ved hjælp af Möbius-funktionen $\mu(n)$ kan vi omvendt udtrykke $\pi(x)$ ved $\Pi(x)$,

$$\pi(x) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k}\Pi(\sqrt[k]{x}).$$

(Funktionen $\mu(n)$ har værdien $(-1)^r$, når n er et produkt af r forskellige primtal, og værdien 0 ellers. Specielt er $\mu(1) = 1$, idet jo 1 er produktet af ingen primtal.) Riemann's overvejelse leder til approksimationen $\Pi(n) \sim \mathrm{Li}(n)$, og heraf kan formelt udledes, at

$$\pi(n) \sim \sum_{k=1}^{\infty} \frac{\mu(k)}{k}\,\mathrm{Li}(\sqrt[k]{n}) =: R(n). \tag{1.12.3}$$

Funktionen $R(n)$ på højresiden af (1.12.3) kaldes *Riemann's række*. I rækkens k'te led går faktoren $\mathrm{Li}(\sqrt[k]{n})$ mod $-\infty$ for $k \to \infty$, og det er faktisk ækvivalent med Primtalssætningen at vise, at rækken overhovedet er (betinget) konvergent. Riemann selv betragtede kun rækkens afsnitssummer. Hvis vi snyder, og tillægger $\mathrm{Li}(x)$ værdien 0 for $1 < x < 2$, er $R(n)$ blot en endelig sum, og den asymptotiske relation (1.12.3) følger let af (1.12.2).

(1.13) Verdens største tal. Som nævnt gælder for $n \gg 0$ (endda for $n \geqslant 17$) følgende ulighed:

$$n/\log n < \pi(n).$$

Gauss og Riemann formodede, at der for alle n gælder uligheden,

$$\pi(n) < \mathrm{Li}(n).$$

Det skal understreges, at uligheden gælder for *alle* de n, for hvilke $\pi(n)$ overhovedet er beregnet. I tabellen herunder er anført værdierne af $\pi(n)$ for de første 22 potenser af 10 ($\pi(10^{22})$ var den største beregnede værdi i 2000), og de tilsvarende differenser $\mathrm{Li}(n) - \pi(n)$ (afrundet opad).

Tabellen er hentet på nettet fra Sloane's On–Line Encyclopedia of Integer Sequences (Look-Up) `www.research.att.com/~njas/sequences/` ved at indtaste tabellens første tre tal: 4 25 168.

n	$\pi(n)$	$R(n) - \pi(n)$	$\mathrm{Li}(n) - \pi(n)$
10^1	4	−1	2
10^2	25	−1	5
10^3	168	−0	10
10^4	1229	−2	17
10^5	9592	5	38
10^6	78498	−29	130
10^7	664579	−88	339
10^8	5761455	−97	754
10^9	50847534	79	1701
10^{10}	455052511	1828	3104
10^{11}	4118054813	2318	11588
10^{12}	37607912018	1476	38263
10^{13}	346065536839	5773	108971
10^{14}	3204941750802	19200	314890
10^{15}	29844570422669	−73218	1052619
10^{16}	279238341033925	−327052	3214632
10^{17}	2623557157654233	598255	7956589
10^{18}	24739954287740860	3501366	21949555
10^{19}	234057667276344607	−23884333	99877775
10^{20}	2220819602560918840	4891825	222744644
10^{21}	21127269486018731928	86432204	597394254
10^{22}	201467286689315906290	127132665	1932355208

For alle n i tabellen er differensen $\mathrm{Li}(n) - \pi(n)$ positiv, og altså $\pi(n) < \mathrm{Li}(n)$. På baggrund af tabellen kunne man fristes til at tro, at differensen $\mathrm{Li}(n)-\pi(n)$ vokser ubegrænset for $n \to \infty$. Dette er langt fra tilfældet. Littlewood viste allerede i 1914, at differensen $\mathrm{Li}(n) - \pi(n)$ skifter fortegn uendelig mange gange. Beviset er ikke konstruktivt, og angiver ikke en værdi n_0, for hvilken $\pi(n_0) > \mathrm{Li}(n_0)$. Skewes viste i 1934, under forudsætning af Riemann's hypotese (se nedenfor), at et sådant tal findes, med

$$n_0 < 10^{10^{10^{34}}}.$$

Højresiden er Skewes' tal, „verdens største tal". Senere, bl.a. også af Skewes, er der givet øvre grænser for n_0 *uden* forudsætning af Riemann's hypotese.

Det antages i almindelighed, at Riemann's approksimation $R(n)$ er bedre end approksimationerne $\mathrm{Li}(n)$ og $n/\log n$. Antagelsen understøttes numerisk, men som nævnt ovenfor er numeriske data slet ikke overbevisende. Bemærk, at i approksimationen med det andet led medtaget,

$$\pi(n) \sim \mathrm{Li}(n) - \frac{1}{2}\mathrm{Li}(\sqrt{n}),$$

er leddet $\mathrm{Li}(\sqrt{n})$ af størrelsesordenen $\sqrt{n}/\log n$. Det er et dybtliggende spørgsmål, også relateret til Riemann's hypotese, om differensen $\mathrm{Li}(n) - \pi(n)$ overhovedet er af denne størrelsesorden.

(1.14) Riemann's zeta-funktion. I sine undersøgelser inddrog Riemann *zeta-funktionen* $\zeta(s)$, defineret ved rækken,

$$\zeta(s) := \sum_{n\geqslant 1} \frac{1}{n^s}. \tag{1.14.1}$$

Rækken er en såkaldt *Dirichlet-række*. Det er ikke svært at vise, at rækken er absolut konvergent for alle komplekse tal s i området $\mathcal{R}e\, s > 1$, og at funktionen $\zeta(s)$ i dette område er holomorf. Dens sammenhæng med primtallene fremgår af *Euler's produktformel*,

$$\lim_{k\to\infty}\Big(\zeta(s)\prod_{i=1}^{k}\Big(1-\frac{1}{p_i^s}\Big)\Big) = 1, \tag{*}$$

hvor $p_1 < p_2 < p_3 < \cdots$ er følgen af primtal. Vi har nemlig

$$\zeta(s)(1-2^{-s}) = \sum n^{-s} - \sum (2n)^{-s} = \sum{}' n^{-s},$$

hvor summen er over tal $n \geqslant 1$, der ikke er delelige med 2. Med samme argument er

$$\zeta(s)(1-2^{-s})(1-3^{-s}) = \sum{}' n^{-s},$$

hvor summen nu er over tal $n \geqslant 1$, som hverken er delelige med 2 eller 3. Og generelt er

$$\zeta(s)(1-p_1^{-s})\cdots(1-p_k^{-s}) = \sum{}' n^{-s} = 1 + \sum{}'' n^{-s},$$

hvor den sidste sum er over tal $n > 1$, som ikke er delelige med et af primtallene $p_1, \dots, p_k$. Det første af disse tal er p_{k+1}. Idet $\sigma := \mathcal{R}e\, s > 1$, får vi vurderingen,

$$\Big|\sum{}'' \frac{1}{n^s}\Big| \leqslant \sum_{n\geqslant p_{k+1}} \frac{1}{n^\sigma},$$

og her går højresiden mod 0 for $k \to \infty$, da rækken $\sum n^{-\sigma}$ er konvergent. Hermed er (*) bevist. Det følger, for $\mathcal{R}e\, s > 1$, at $\zeta(s) \neq 0$, at det uendelige produkt $\prod_{k=1}^{\infty}(1 - p_k^{-s})$ er konvergent, og at vi har ligningen (hvor p gennemløber primtallene),

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}\,. \tag{1.14.2}$$

Et alternativt bevis for, at $\zeta(s) \neq 0$ for $\mathcal{R}e\, s > 1$ fås ved at bemærke, at rækken $\sum_{n\geqslant 1} \mu(n)/n^s$ er absolut konvergent, og at dens produkt med rækken for $\zeta(s)$ giver konstanten 1. Vi har altså ligningen,

$$\frac{1}{\zeta(s)} = \sum_{n\geqslant 1} \frac{\mu(n)}{n^s}\,. \tag{1.14.3}$$

Formelt har vi for logaritmerne,

$$\log\zeta(s) = \sum_p -\log(1 - p^{-s}) = \sum_{p,m} \frac{1}{m} p^{-sm},$$

og her er højresiden absolut (og majoriseret) konvergent. Ligningen definerer altså en logaritme til $\zeta(s)$. Herefter er det ikke svært at vise ligningen,

$$\log\zeta(s) = s\int_0^\infty \Pi(t)\, t^{-s-1} dt, \tag{1.14.4}$$

der viser sammenhængen mellem Riemann's ζ-funktion og funktionen $\Pi(x)$ fra (1.12).

Riemann viste, at ζ-funktionen kan udvides til en meromorf funktion i hele den komplekse plan, holomorf bortset fra en pol i $s = 1$. I halvplanen, hvor $\mathcal{R}e\, s > 0$, kan den udvidede funktion bestemmes som følger: For $\mathcal{R}e\, s > 1$ gælder øjensynlig, at

$$(1 - 2^{1-s})\zeta(s) = \sum\nolimits_{n=1}^{\infty} \frac{1}{n^s} - \sum\nolimits_{n=1}^{\infty} \frac{2}{(2n)^s} = \sum\nolimits_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}\,.$$

Rækken på højresiden er betinget konvergent for $\mathcal{R}e\, s > 0$ (det er i hvert fald klart, når s er reel), og ligningen ovenfor kan derfor essentielt tages som definition af udvidelsen af $\zeta(s)$ til halvplanen $\mathcal{R}e\, s > 0$. Bemærk dog, at faktoren $1 - 2^{1-s}$ på venstresiden er 0, når $s = 1 + 2\pi i a/\log 2$ med $a \in \mathbb{Z}$. For $a = 0$, dvs for $s = 1$, har højresiden værdien $\log 2$, og

$$(1 - 2^{1-s})^{-1} = (1 - e^{(1-s)\log 2})^{-1} = (\log 2)^{-1}(s-1)^{-1} + \cdots,$$

hvor „$\cdots$" står for en potensrække i $s - 1$. Heraf ses, at $\zeta(s)$ har en simpel pol i $s = 1$, med residuet 1.

Endelig beviste Riemann, at den udvidede funktion $\zeta(s)$ tilfredsstiller følgende funktionalligning:

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\Gamma(s)\zeta(s), \tag{1.14.5}$$

hvor $\Gamma(s)$ er *gamma-funktionen*. De to argumenter, s og $1-s$, i funktionalligningen ligger symmetrisk omkring punktet $s=\frac{1}{2}$. Specielt, på linien, hvor $\mathcal{R}e\,s=\frac{1}{2}$, er $1-s$ det konjugerede af s.

Af særlig interesse er nulpunkterne for $\zeta(s)$. For $\mathcal{R}e\,s>1$ har $\zeta(s)$ som nævnt ingen nulpunkter, og af faktorerne på højresiden af (1.14.5) er det kun faktoren $\cos\pi s/2$, der kan være nul, svarende til $s=3,5,7,\ldots$. I området $\mathcal{R}e\,s<0$ har $\zeta(s)$ derfor kun de *trivielle* nulpunkter $-2,-4,-6,\ldots$. Riemann viste, at Primtalsætningen er ækvivalent med, at $\zeta(s)$ ikke har nulpunkter på de to linier $\mathcal{R}e\,s=0$ og $\mathcal{R}e\,s=1$. Det var faktisk ved hjælp af denne ækvivalens, at Primtalssætningen blev bevist.

Tilbage bliver spørgsmålet om eventuelle nulpunkter i den *kritiske strimmel* $0<\mathcal{R}e\,s<1$. Man kan vise, at $\zeta(s)$ har uendelig mange nulpunkter på „symmetrilinien“ $\mathcal{R}e\,s=\frac{1}{2}$. Derimod har man ikke bevist den berømte:

Riemann's hypotese. *Alle nulpunkter s for zeta-funktionen $\zeta(s)$ i den kritiske strimmel $0<\mathcal{R}e\,s<1$ ligger på linien, hvor $\mathcal{R}e\,s=\frac{1}{2}$.*

Riemann beviste en eksakt formel for $\pi(n)$. Med brug af funktionen $R(n)$ er formlen ækvivalent med følgende: *For alle $n>1$ er*

$$\pi(n)=R(n)-\sum\nolimits_{\rho}R(n^{\rho}), \tag{1.14.6}$$

hvor ρ gennemløber nulpunkterne for $\zeta(s)$ i den kritiske strimmel.

Tallet n^{ρ} er komplekst, $n^{\rho}=e^{\rho\log n}$, og det har som bekendt numerisk værdi $|n^{\rho}|=n^{r}$, hvor $r=\mathcal{R}e\,\rho$. Riemann's hypotese betyder, at alle tallene n^{ρ} har numerisk værdi lig med $n^{1/2}=\sqrt{n}$. Man kan i øvrigt vise, at Riemann's hypotese er ækvivalent med relationen,

$$\pi(n)-\mathrm{Li}(n)=O(\sqrt{n}\log n), \tag{1.14.7}$$

hvor „*store-O-notationen*“ indikerer, at differensen $\pi(n)-\mathrm{Li}(n)$ numerisk er begrænset af en konstant gange $\sqrt{n}\log n$. Det skal understreges, at de asymptotiske relationer i (1.12) er ækvivalente med Primtalssætningen. Derimod er Riemann's hypotese, og altså (1.14.7), ikke er bevist.

(1.15) Logaritme-integral og eksponential-integral. I Riemann's formel (1.14.6) indgår værdier af $R(w)$, og dermed af $\mathrm{Li}(w)$, også for komplekse tal w (af formen $w=n^{\rho}$). Når $x>1$ og $\rho\neq 0$ *definerer* vi $\mathrm{Li}(x^{\rho}):=\mathrm{Ei}(\rho\log x)$, hvor $\mathrm{Ei}(z)$ er *eksponential-integralet*, defineret for komplekse $z\neq 0$ ved udtrykket,

$$\mathrm{Ei}(z)=\int_{-\infty}^{z}\frac{e^{t}\,dt}{t}+i\pi. \tag{1.15.1}$$

Når z er negativ reel eller i den øvre halvplan, er kurveintegralet langs en kurve, der begynder i $-\infty$ (og ender i z), og som ikke kommer i den nedre halvplan. For reelle positive z kan kurven forløbe langs den negative reelle akse, cirkle rundt om 0 i den øvre halvplan, og fortsætte langs den positive halvakse. For punkter i den nedre halvplan forudsættes, at kurven krydser den reelle akse på den positive del; alternativt kan der integreres langs en kurve i den nedre halvplan, idet konstanten $i\pi$ så skal erstattes af $-i\pi$.

Funktionen $\mathrm{Ei}(z)$ er holomorf i $\mathbb{C}$ opskåret langs den negative reelle akse; værdierne for negative reelle z er grænseværdier for værdierne i den øvre halvplan. Kurveintegralet definerer en funktion, der lokalt er holomorf med den afledede $e^z/z = 1/z + \sum_{m\geqslant 1} z^{m-1}/m!$. Med en konstant γ har vi har altså ligningen,

$$\mathrm{Ei}(z) = \gamma + \log z + \sum_{m=1}^{\infty} z^m/(m\, m!) \tag{1.15.2}$$

(også når z er negativ reel, hvor vi sætter $\log z := \log|z| + i\pi$). Øjensynlig er γ grænseværdien for $z \to 0$ af $\mathrm{Ei}(z) - \log z$. Når u er positiv reel, er

$$\mathrm{Ei}(-u) - \log(-u) = \int_{\infty}^{-u} \frac{e^t\, dt}{t} - \log|u| = -\int_u^{\infty} \frac{e^{-t}\, dt}{t} + \int_u^1 \frac{dt}{t},$$

hvoraf

$$\gamma = \int_0^1 \frac{(1-e^{-t})dt}{t} - \int_1^{\infty} \frac{e^{-t}\, dt}{t}.$$

At γ faktisk er *Euler's konstant* følger af udregningerne,

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n = \int_0^1 \frac{1-u^n}{1-u} du - \int_1^n \frac{1}{t} dt$$
$$= \int_0^n \frac{1-(1-t/n)^n}{t} dt - \int_1^n \frac{1}{t} dt = \int_0^1 \frac{1-(1-t/n)^n}{t} dt - \int_1^n \frac{(1-t/n)^n}{t} dt\,;$$

Euler's konstant er grænseværdien, for $n \to \infty$, af venstresiden, og som bekendt er e^{-t} grænseværdien af $(1-t/n)^n$.

(1.16) Om konvergens af Riemann's række. Med logaritme-integralet defineret via eksponential-integralet får vi følgende udtryk for rækken, der definerer $R(n)$:

$$R(e^z) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \mathrm{Ei}(z/k).$$

Indsæt, i rækken på højresiden, udtrykket (1.15.2) for $\mathrm{Ei}(z/k)$, og brug at $\gamma + \log(z/k) = (\gamma + \log z) - \log k$. Resultatet bliver en sum af tre rækker. De to første er rækkerne

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k}(\gamma + \log z) \quad \text{og} \quad -\sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log k. \tag{1.16.1}$$

Man kan vise, at der gælder ligningerne,

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k} = 0, \qquad \sum \frac{-\mu(k)\log k}{k} = 1. \tag{1.16.2}$$

De to venstresider opstår formelt, når man sætter $s = 1$ i rækken $1/\zeta(s) = \sum \mu(k)/k^s = 1/\zeta(s)$ fra (1.14.3) og i $(1/\zeta(s))' = -\sum \mu(k) \log k/k^s$. Da $\zeta(s)$ har en simpel pol med residuet 1 i $s = 1$, gælder, for $s \to 1$, at $1/\zeta(s) \to 0$ og $(1/\zeta(s))' \to 1$, og dette kan tages som en vag indikation for ligningerne i (1.16.2), men langtfra som bevis. Det er ikke så svært at vise, at den første ligning i (1.16.2) er ækvivalent med primtalssætningen.

Det følger af ligningerne (1.16.2), at de to rækker i (1.16.1) blot bidrager med konstanten 1 til $R(e^z)$. Det tredie bidrag har formen,

$$\sum_{k=1}^{\infty} \sum_{m=1}^{\infty} \frac{\mu(k)}{k} \frac{z^m}{k^m m m!}.$$

Det er nemt at se, at denne dobbeltrække er absolut konvergent. Ved ombytning af summationerne bliver den indre sum til rækken $\sum_k \mu(k) k^{-m-1} = 1/\zeta(m+1)$. Vi har således vist, at rækken $R(e^z)$ er (betinget) konvergent, og at vi for summen har udtrykket,

$$R(e^z) = 1 + \sum_{m \geqslant 1} \frac{z^m}{\zeta(m+1) m\, m!}.$$

(1.17) Opgaver.

U1 **1.** Möbius-funktionen $\mu(n)$ har værdien 1 for $n = 1$, værdien $(-1)^r$ når n er et produkt af r *forskellige* primtal, og værdien 0 ellers. Vis, at Möbius-funktionen $\mu(n)$ kan karakteriseres som den eneste funktion $\mu \colon \mathbb{N} \to \mathbb{C}$ som opfylder: $\mu(1) = 1$ og $\sum_{d|n} \mu(d) = 0$ for $n > 1$.

H1 **2.** Bevis formlen $\pi(n) = \sum_k (\mu(k)/k) \Pi(\sqrt[k]{n})$, hvor $\Pi(n)$ er defineret i (1.12).

H1 **3.** Vis, at de tre asymptotiske formler, $\pi(n) \sim \mathrm{Li}(n)$, $\Pi(n) \sim \mathrm{Li}(n)$, $\pi(n) \sim R(n)$, alle er ækvivalente med Primtalssætningen. Her fortolker vi $R(n)$ som den (endelige) sum der fremkommer af højresiden i (1.12.3), når logaritme-integralet sættes til 0 for $1 < x < 2$.

H1 **4.** Tegn på millimeterpapir graferne for funktionerne $300\pi(x)$ og $300\nu(x)$ på intervallet $0 \leqslant x \leqslant N$, hvor $N := 10^{130}$, idet interval-endepunkterne på x-aksen anbringes med en afstand på 10 cm. Du må gerne antage, at $\pi(x) = x/\log x$ for $x > 2$ (og $\nu(x)$ er antallet af kvadrattal, der højst er x), og du må gerne tegne med en blyant, hvis spids er ca 1mm tyk. Men du skal kunne forsvare din tegning. [Vink: $300 \approx \log 10^{130}$.]

H1 **5.** Vis, at (3, 5, 7) er det eneste sæt primtalstrillinger.

H1 **6.** Bestem, med $A(n)$ fra (1.12), $A(10^{18})$ med 2 decimaler. Værdien $\pi(10^{18})$ er givet i (1.13).

U1 **7.** *Fermat-primtallene* er (ulige) primtal af formen $p = 2^k + 1$. Vis, at hvis $2^k + 1$ (med $k > 0$) er et primtal, så er k nødvendigvis en potens af 2. Fermat-primtallene er altså af formen $F_n = 2^{2^n} + 1$. De første 5 Fermat-primtal er følgende

n	0	1	2	3	4
F_n	3	5	17	257	65.537

Man kender ikke andre Fermat-primtal. Euler beviste, at 641 går op i F_5. Check lige udregningen: Det er let at se, at $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$. Modulo 641 gælder derfor, at

$$2^{32} = 2^4 \cdot 2^{28} \equiv -5^4 \cdot (2^7)^4 \equiv -(-1)^4 = -1, \text{ altså er } F_5 = 2^{32} + 1 \equiv 0 \pmod{641}.$$

U2 **8.** *Mersenne-primtallene* er primtal af formen $M_p = 2^p - 1$. Vis, at hvis M_p er et primtal, så er p et primtal. Vis, at det omvendte ikke gælder. Her er de første Mersenne-primtal:

p	2	3	5	7	13	17	19	31
M_p	3	7	31	127	8.191	131.071	524.287	2.147.483.647

Der kendes (i 2008) ialt 46 Mersenne-primtal. Det største, svarende til $p = 43.112.609$, har 12.978.189 ciffre.

U3 **9.** Med $\sigma(n)$ betegnes summen af divisorerne i n, altså $\sigma(n) = \sum_{d|n} d$. Bestem $\sigma(p^\nu)$, når p er et primtal. Vis, at når $n = n_1 n_2$, hvor faktorerne n_1, n_2 er primiske, så er $\sigma(n) = \sigma(n_1)\sigma(n_2)$.

U2 **10.** Et tal n kaldes *fuldkomment*, hvis det er lig med summen af sine ægte divisorer (divisoren 1 medregnet), altså hvis $\sigma(n) = 2n$. Vis Euklid's resultat: Hvis $2^\nu - 1$ er et primtal, så er tallet $n = 2^{\nu-1}(2^\nu - 1)$ fuldkomment.

*Vis Euler's resultat: ethvert lige, fuldkomment tal n er af Euklid's form.

U2 **11.** Vis, at alle tal af formen $n = 6k$ for $k > 1$ er *abundante* tal, dvs opfylder $\sigma(n) > 2n$.

U3 **12.** Vis, at alle tal af formen $n = 3^\alpha 5^\beta$ $(n > 1)$ er *deficiente* tal, dvs opfylder $\sigma(n) < 2n$.

U3 **13.** Lad $\alpha(n)$ betegne antallet af løsninger til den diofantiske ligning $n = x^2 - y^2$, dvs løsninger med $x, y \in \mathbb{Z}$. Vis, at når n er ulige, så er $\alpha(n) = 2\tau(n)$, hvor $\tau(n)$ er antallet af divisorer i n (som bekendt kan $\tau(n)$ bestemmes ud fra primopløsningen $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ som $\tau(n) = (\nu_1 + 1) \cdots (\nu_r + 1)$). Find en tilsvarende formel for $\alpha(2^\nu u)$, når u er ulige. [Vink: Pas på, der er noget lusk omkring $\nu = 1$.]

U1 **14.** Vis, at tallene $l! + 2, l! + 3, \ldots, l! + l$ en sekvens af $l - 1$ på hinanden følgende tal, der alle er sammensatte. Kan du, med en betingelse på l, sikre dig, at også $l! + 1$ er sammensat?

U1,U8 **15.** Har kongruensen $23x \equiv 17 \pmod{41}$ en løsning? Har kongruensen $x^2 \equiv -8 \pmod{41}$ en løsning?

U1 **16.** Hvordan bestemmer man antallet af cifre i Fermat-tallet $F_5 = 2^{2^5} + 1$?

U1 **17.** Gauss beviste, at n-kanten er konstruerbar, hvis og kun hvis n er et produkt, $n = 2^\nu p_1 \cdots p_r$, af en potens af 2 og *forskellige* Fermat-primtal p_i. Vis, at n-kanten er konstruerbar, hvis og kun hvis $\varphi(n)$ er en potens af 2.

18. For hvert polynomium $f \in \mathbb{Z}[X]$ betegnes med $\mathcal{R}(f)$ det polynomium, der fremkommer, når hver koefficient i f erstattes med sin principale rest modulo 2. Sæt $R_m := \mathcal{R}((1 + X)^m)$ for $m = 1, 2, \ldots$. Fx, for $m = 3$, er $(1 + X)^3 = 1 + 3X + 3X^2 + X^3 \equiv 1 + X + X^2 + X^3$, og R_3 er det sidste polynomium. Bestem tallene $R_m(2)$ for $m = 1, \ldots, 6$.

Følgende er et *bemærkelsesværdigt resultat. Den ulige n-kant er konstruerbar, hvis og kun hvis n er et af tallene i følgen $R_1(2), R_2(2), R_3(2), R_4(2), \ldots$.*

Men resultatet er nu heller ikke helt korrekt! Forklar sammenhængen. [Vink: Det er klart, at $(1 + X)^{l+m} = (1 + X)^l (1 + X)^m$, men deraf følger vel ikke, at $R_{l+m} = R_l R_m$?]

19. Stirling's formel udsiger, at $n! \sim \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n}$. Lad b_n betegne den største værdi af binomialkoefficienterne $\binom{n}{k}$. Vis ved hjælp af formlen, at der findes en konstant C således, at

$b_n \leqslant C2^n/\sqrt{n}$. Vis, at for hvert positivt tal c er $b_n \leqslant 2^{n-c}$ for $n \gg 0$. Vis, at hvis $b_n \leqslant 2^{n-c}$ for $n = n_0$, så er $b_n \leqslant 2^{n-c}$ for alle $n \geqslant n_0$. [Vink til det sidste spørgsmål: Har intet at gøre med det foregående.]

20. Tilføj til tabellen over $\pi(n)$ nogle af differenserne $\pi(n) - n/\log n$, fx for $n = 10^k$ med $k = 6, 7, 8$. Sammenlign med tabellens andre differenser.

U2 **21.** Bestem, med $c = 1$ og $C = 1{,}3$ et naturligt tal N således, at højresiden i (1.10.1) er positiv for $n \geqslant N$. Gennemfør et bevis for Bertrand's postulat.

U1 **22.** Antag, at n ikke er den k'te potens af et helt tal. Vis, at tallet $\sqrt[k]{n}$ er irrationalt.

U1 **23.** Antag, at n ikke er en potens af 10. Vis, at 10-talslogaritmen $\log_{10} n$ er irrational. Hvad gælder, hvis grundtallet 10 erstattes med et mere generelt helt grundtal g, $g \geqslant 2$?

24. Antag, at for naturlige tal x, y gælder ligningen $y^2 = 1 + x + x^2 + x^3 + x^4$. Vis, at $(x, y) = (3, 11)$. [Vink: Det er klart, at $x > 1$. Tænk nu på naturlige tal fremstillet i x-tal-sxstemet. Ligningens højreside er så tallet 11111 (med fem ciffre). Overvej, at i x-tal-systemet må y være 3-ciffret, og det ledende ciffer (koefficienten til x^2) må være 1. Bestem så de sidste to ciffre (og x og y).]

25. Vis for $Q := X^2 - X + 41$, at alle tallene $Q(1), Q(2), \dots, Q(40)$ er primtal. [Vink: det kræver vist gruppearbejde! – eller en henvisning til Mat2AL/Alg2.]

Vis, at der ikke findes noget ikke-konstant polynomium $P \in \mathbb{Z}[X]$ således, at følgen $P(1), P(2), P(3), \dots$ består af lutter primtal. [Vink: hvis $p := P(1)$, så er $P(np+1) \equiv P(1) \equiv 0 \pmod{p}$.]

U6 **26.** Lad $v_p(k)$ betegne den eksponent primtallet p forekommer med i primopløsningen af k. Vis, at $v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$ (det er en endelig sum!). Brug princippet, fx med $p = 2, 3$ og 5, til at primopløse $100!$.

U6 **27.** Vis, at et vilkårligt produkt af r på hinanden følgende hele tal altid er deleligt med $r!$.

U8 **28.** I noterne er det vist, at rækken $\sum \frac{1}{p}$, hvor summen er over primtal p, er divergent. Vis, at divergensen også følger af primtalssætningen $\pi(x) \sim x/\log x$. (*Det kræver omhyggelighed at vise, at divergensen alene følger af en vurdering af formen $\pi(x) \geqslant cx/\log x$.)

Lad os her definere *en primtalstvilling* som et par af primtal (q, q'), hvor $q' = q + 2$. Som nævnt ved man ikke, om der er uendelig mange primtalstvillinger. Man kan vise, at rækken $\sum(\frac{1}{q} + \frac{1}{q'})$, hvor summen er over primtalstvillinger (q, q'), er konvergent (værdien er Brun's konstant), og man kan vise, at der for antallet $\pi_2(x)$ af primtalstvillinger (q, q') med $q \leqslant x$ gælder en vurdering af formen $\pi_2(x) \leqslant Kx/(\log x)^2$.

Det er en formodning (slet ikke bevist), at der gælder en assymptotisk formel af formen $\pi_2(x) \sim Kx/(\log x)^2$. Vis, at konvergensen vil være en følge af formodningen.

29. Lad Q være en given delmængde af $\mathbb{N}$, og lad $\pi_Q(x)$ betegne antallet af tal $q \leqslant x$ i delmængden Q. Betragt for en given talfølge α_n summen $\sum_{a \leqslant q \leqslant b}^{Q} \alpha_q$, hvor notationen indikerer, at der summeres over $q \in Q$ med $a \leqslant q \leqslant b$. Af og til kan man have gavn af følgende omskrivninger (hvor n gennemløber naturlige tal):

$$\sum_{a\leqslant q\leqslant b}^{Q} \alpha_p = \sum_{a\leqslant n\leqslant b} \alpha_n\big(\pi_Q(n) - \pi_Q(n-1)\big)$$
$$= \alpha_{b+1}\pi_Q(b) - \alpha_a\pi_Q(a-1) + \sum_{a\leqslant n\leqslant b} (\alpha_n - \alpha_{n+1})\pi_Q(n);$$

den sidste forudsætter, at a og b er hele tal. Eftervis omskrivningerne. Vis, at divergensen af rækken $\sum \frac{1}{p}$ over primtal p alene følger af en vurdering af formen $\pi(x) \geqslant cx/\log x$. Vis, at konvergensen af rækken $\sum \frac{1}{q}$ over primtalstvillinger q er en konsekvens af en vurdering af formen $\pi_2(x) \leqslant Kx/(\log x)^2$. [Vink: benyt, og begrund, at $\sum 1/(n(\log n)^s)$ (over $n \geqslant 2$) er konvergent, præcis når $s > 1$.]

30. Check lige, at definitionen i (1.15), $\mathrm{Li}(x) = \mathrm{Ei}(\log x)$, harmonerer med, at logaritmeintegralet er en stamfunktion til $1/\log x$, jfr (1.12.2).

31. Vis, at rækkerne (1.14.1) og (1.14.3) er „hinandens reciprokke“.

32. Vis ligningen (1.14.4). [Vink: funktionen $\Pi(x)$ i (1.12) er givet ved

$$\Pi(x) = \sum_{p,m} \frac{1}{m} 1_{[p^m,\infty)}(x),$$

hvor $1_I(x)$ betegner den karakteristiske funktion for intervallet I.]

33. Det er vel klart, at eksponential-integralet $\mathrm{Ei}(x)$ er reelt, når x er reel og positiv? Og at $\mathrm{Ei}(x) = \lim_{\varepsilon\to 0}\big(\int_{-\infty}^{-\varepsilon} + \int_{\varepsilon}^{x}\big)e^t t^{-1}dt$.

34. Lad b_n betegne den midterste af binomialkoefficienterne $\binom{n}{l}$ (eller de midterste), altså $b_n = \binom{n}{k}$, hvis $n = 2k$ eller $n = 2k-1$. Brug Stirling's formel herunder til at vise følgende formel:

$$b_n = \sqrt{\tfrac{2}{\pi}}\, 2^n \frac{1}{\sqrt{n}} e^{\frac{\theta}{n}}, \quad \text{hvor } |\theta| \leqslant 1.$$

Ifølge (1.7) er $b_n \leqslant n^{\pi(n)}$. Hviken vurdering af $\pi(n)$ kan herved opnås? Sammenlign med (1.8). Du kender vel den lidt mere kvantitative udgave af Stirling's formel:

$$k! = \sqrt{2\pi}\, k^{k+\frac{1}{2}} e^{-k+\frac{\theta}{12k}}, \text{ hvor } 0 < \theta < 1.$$

35. Et naturligt tal er som bekendt *kvadratfrit*, hvis intet kvadrat (bortset fra 1) er divisor i tallet, eller, ækvalent, hvis det er et produkt af indbyrdes forskellige primtal. Bestem, udtrykt ved antallet af primdivisorer i n, antallet af kvadratfri divisorer i n.

2. Gruppen af primiske restklasser.

(2.1) Setup. I det følgende betegner n et naturligt tal større end 1. Den additive gruppe af restklasser modulo n betegnes $\mathbb{Z}/n$, og den multiplikative gruppe af primiske restklasser modulo n betegnes $(\mathbb{Z}/n)^*$. Gruppen $\mathbb{Z}/n$ er en additiv udgave af den cykliske gruppe af orden n. Gruppen $(\mathbb{Z}/n)^*$ har orden $\varphi(n)$, hvor $\varphi(n)$ er *Euler's φ-funktion*, dvs $\varphi(n)$ er antallet af tal a med $0 \leqslant a < n$ og $(a, n) = 1$.

For en endelig gruppe G findes eksponenter $l \geqslant 1$ således, at $g^l = 1$ for alle $g \in G$. Mere præcist betyder ligningen $g^l = 1$, at l er et multiplum af ordenen af g. Ligningen $g^l = 1$ er altså opfyldt for alle g, hvis og kun hvis l er et multiplum af alle elementordener. Heraf ses, mere præcist, at den mindste mulige eksponent l er det mindste fælles multiplum af elementordenerne. Denne mindste eksponent kaldes også *gruppens eksponent*. Det følger af Lagrange's Indexsætning, at $g^{|G|} = 1$ for alle $g \in G$. Ordenen $|G|$ er altså et multiplum af eksponenten.

Det er velkendt (men ikke helt trivielt), at for en endelig *kommutativ* gruppe er enhver elementorden divisor i den maksimale elementorden. Med andre ord: eksponenten for en kommutativ gruppe er netop den maksimale elementorden.

Med $\lambda(n)$ betegnes eksponenten for gruppen $(\mathbb{Z}/n)^*$, dvs det mindste positive tal l således, at $a^l \equiv 1 \pmod{n}$ for alle tal a primiske med n. Det følger af det foregående, at $\lambda(n)$ er divisor i $\varphi(n)$.

Fra en primopløsning af n:

$$n = p_1^{\nu_1} \cdots p_r^{\nu_r},$$

fås, ved brug af Den kinesiske Restklassesætning, isomorfier,

$$\mathbb{Z}/n \xrightarrow{\sim} \mathbb{Z}/p_1^{\nu_1} \times \cdots \times \mathbb{Z}/p_r^{\nu_r}, \qquad (\mathbb{Z}/n)^* \xrightarrow{\sim} (\mathbb{Z}/p_1^{\nu_1})^* \times \cdots \times (\mathbb{Z}/p_r^{\nu_r})^*.$$

Af den sidste isomorfi følger, at

$$\varphi(n) = \varphi(p_1^{\nu_1}) \cdots \varphi(p_r^{\nu_r}).$$

For et primtal p har vi $\varphi(p) = p - 1$, idet alle tal $a = 1, \dots, p-1$ er primiske med p. Mere generelt, for en primtalspotens p^ν har vi

$$\varphi(p^\nu) = (p-1)p^{\nu-1}.$$

Et tal a er nemlig primisk med p^ν, netop når p ikke går op i a. Af de p^ν tal a med $0 \leqslant a < p^\nu$ er det altså de $p^{\nu-1}$ tal af formen $a = bp$ for $0 \leqslant b < p^{\nu-1}$, der ikke er primiske med p. Antallet af resterende, dvs $p^\nu - p^{\nu-1}$, er altså antallet $\varphi(p^\nu)$.

(2.2) Sætning. *Den multiplikative gruppe $(\mathbb{Z}/p^\nu)^*$, af primiske restklasser modulo en ulige primtalspotens, er cyklisk.*

Bevis. For $\nu = 1$ er påstanden velkendt: Restklasseringen $\mathbb{Z}/p$ er et legeme, sædvanligvis betegnet $\mathbb{F}_p$, med p elementer, og gruppen $(\mathbb{Z}/p)^*$ er den multiplikative gruppe $\mathbb{F}_p^*$ bestående af elementerne forskellige fra 0 i dette legeme. Lad $l := \lambda(p)$ være eksponenten for gruppen $\mathbb{F}_p^*$. Specielt er så l divisor i gruppens orden $p-1$. Polynomiet $X^l - 1$ i $\mathbb{F}_p[X]$ har hvert af de $p-1$ elementer i $\mathbb{F}_p^*$ som rod, så for graden har vi $l \geqslant p-1$. Derfor er $l = p-1$. Tallet $p-1$ er altså den maksimale elementorden, så der findes i $\mathbb{F}_p^*$ et element af orden $p-1$. Altså er $\mathbb{F}_p^*$ cyklisk.

Antag nu, at $\nu \geqslant 2$. Betragt ringhomomorfien,

$$\mathbb{Z}/p^\nu \to \mathbb{Z}/p,$$

der afbilder restklassen af a modulo p^ν på restklasen af a modulo p. Ringhomomorfien inducerer er gruppehomomorfi mellem grupperne af invertible elementer. Vi får altså en induceret homomorfi,

$$(\mathbb{Z}/p^\nu)^* \to (\mathbb{Z}/p)^*.$$

Denne homomorfi er surjektiv, thi når a er primisk med p (og dermed med p^ν) vil restklassen af a modulo p på højresiden komme fra restklassen af a modulo p^ν på venstresiden. Lad U være kernen for homomorfien. Gruppen $(\mathbb{Z}/p^\nu)^*$ har orden $(p-1)p^{\nu-1}$, og billedgruppen har orden $p-1$. Af Lagrange's Indexsætning følger derfor, at U har orden $p^{\nu-1}$.

Det påstås først, at der findes en restklasse z i $(\mathbb{Z}/p^\nu)^*$ af orden $p-1$. Vælg hertil et tal a, hvis restklasse modulo p frembringer gruppen $(\mathbb{Z}/p)^*$, dvs hvis restklasse modulo p har orden $p-1$. Restklassen $w := [a]$, af a modulo p^ν, har da i gruppen $(\mathbb{Z}/p^\nu)^*$ en orden, der er et multiplum af $p-1$ og divisor i gruppens orden, dvs i $(p-1)p^{\nu-1}$. Ordenen af w er derfor $(p-1)p^\mu$, med $0 \leqslant \mu \leqslant \nu - 1$. Det følger, at restklassen $z := w^{p^\mu}$ har orden $p-1$.

Herefter er det nok at vise, at U er cyklisk, altså at der findes element $u \in U$ af orden $p^{\nu-1}$. Med et sådant element har nemlig z og u primiske ordener, og produktet zu har derfor orden $(p-1)p^{\nu-1}$. Produktet zu er altså en frembringer for $(\mathbb{Z}/p^\nu)^*$.

Eksistensen af u er klar, hvis $\nu = 2$, idet U så har orden p og derfor er cyklisk. I det almindelige tilfælde $\nu \geqslant 2$ viser vi, mere præcist, at restklassen $u := [1+p]$ i U er brugbar.

Først bemærkes, at for $\mu \geqslant 1$ og alle k gælder kongruensen,

$$(1+kp)^{p^{\mu-1}} \equiv 1 + kp^\mu \pmod{p^{\mu+1}}. \tag{*}$$

Kongruensen er nemlig en lighed for $\mu = 1$. Antag, induktivt, at (*) er opfyldt for et $\mu \geqslant 1$. Venstresiden har altså formen $1+a$, hvor $a \equiv kp^\mu \pmod{p^{\mu+1}}$. Af binomialformlen får vi en ligning,

$$(1+kp)^{p^\mu} = (1+a)^p = 1 + pa + \tbinom{p}{2}a^2 + \cdots + a^p\,.$$

På højresiden er $pa \equiv kp^{\mu+1} \pmod{p^{\mu+2}}$. De efterfølgende led på højresiden er enten delelige med pa^2 eller med a^3 (her udnyttes, at $p \geqslant 3$); da $p^\mu \mid a$, er leddet i begge tilfælde altså deleligt med $p^{\mu+2}$. Følgelig gælder (*) for $\mu + 1$.

Betragt nu restklassen $u := [1+p]$ modulo p^ν. Den tilhører gruppen U, som har orden $p^{\nu-1}$. Ordenen af u er altså divisor i $p^{\nu-1}$. Af (*), med $k := 1$ og $\mu := \nu - 1$, fremgår, at ordenen af u ikke kan være en ægte divisor i $p^{\nu-1}$. Derfor er ordenen lig med $p^{\nu-1}$. Altså er u brugbar. $\square$

(2.3) Bemærkning. Gruppen $(\mathbb{Z}/2^\nu)^*$ har orden $2^{\nu-1}$. For $\nu = 1$ har vi $(\mathbb{Z}/2)^* = \{1\}$, altså den trivielle gruppe. For $\nu = 2$ har vi $(\mathbb{Z}/4)^* = \{\pm 1\}$, som er den cykliske gruppe af orden 2. For $\nu = 3$ har vi gruppen $(\mathbb{Z}/8)^*$, med de fire restklasser ± 1 og ± 3. For hver af de fire restklasser a har vi øjensynlig $a^2 = 1$. Gruppen $(\mathbb{Z}/8)^*$ er altså Klein's Vierer-gruppe $C_2 \times C_2$, og specielt er den ikke cyklisk. For $\nu \geqslant 3$ har vi, som i beviset for (2.2), en surjektiv homomorfi,

$$(\mathbb{Z}/2^\nu)^* \to (\mathbb{Z}/8)^*.$$

Da højresiden ikke er cyklisk, kan venstresiden heller ikke være cyklisk.

Tilsvarende kan vi betragte den surjektive homomorfi,

$$(\mathbb{Z}/2^\nu)^* \to (\mathbb{Z}/4)^*.$$

Lad U være kernen. Billedgruppen har orden 2, så U har orden $2^{\nu-2}$. Som i beviset for (2.2) vises, for alle $\mu \geqslant 1$, kongruensen,

$$(1+4)^{2^{\mu-1}} \equiv 1 + 2^{\mu+1} \pmod{2^{\mu+2}}. \tag{*}$$

Øjensynlig ligger restklassen [5] i U, og restklassens orden er derfor divisor i $2^{\nu-2}$. Af kongruensen, for $\mu := \nu - 2$, følger, at restklassens orden ikke er divisor i $2^{\nu-3}$. Restklassens orden er derfor $2^{\nu-2}$. Gruppen U er derfor cyklisk, frembragt af [5]. Restklassen -1 frembringer den cykliske undergruppe $\{\pm 1\}$ af orden 2. Øjensynlig er -1 ikke i U, så fællesmængden $U \cap \{\pm 1\}$ består kun af 1. Da ordenen af $(\mathbb{Z}/2^\nu)^*$ er produktet af ordenerne af U og $\{\pm 1\}$ fås:

Gruppen $(\mathbb{Z}/2^\nu)^*$, for $\nu \geqslant 3$, er produktet af undergruppen $\{\pm 1\}$ og undergruppen U frembragt af [5]*:*

$$\{\pm 1\} \times U = (\mathbb{Z}/2^\nu)^*,$$

altså et produkt af cykliske grupper af orden 2 og $2^{\nu-2}$.

Korollar. Gruppen $(\mathbb{Z}/n)^*$ er cyklisk, hvis og kun hvis $n = q^\nu$ eller $n = 2q^\nu$ med et ulige primtal q, eller $n = 4$.

Bevis. Ifølge Den kinesiske Restklassesætning er gruppen isomorf med produktet af grupperne $(\mathbb{Z}/p^\nu)^*$ svarende primtalspotenserne i primopløsningen af n. I tilfældene bortset fra de nævnte er der enten mindst to faktorer af denne form (og så kan gruppen ikke være cyklisk, da faktorerne $(\mathbb{Z}/p^\nu)^*$ har lige orden, når $p^\nu > 2$) eller der er kun én faktor $(\mathbb{Z}/2^\nu)$ med $\nu \geqslant 3$ (og så er gruppen ikke cyklisk ifølge det lige viste). ∎

(2.4) Definition. Af Fermat's lille Sætning følger, når n er et primtal, at

$$(a, n) = 1 \implies a^{n-1} \equiv 1 \pmod{n}. \tag{2.4.1}$$

Ækvivalent, udtrykt ved eksponenten af $(\mathbb{Z}/n)^*$, betyder betingelsen (2.4.1), at $\lambda(n) \mid n-1$. Et tal $n > 1$, der er sammensat og opfylder betingelsen (2.4.1) kaldes et *Carmichael-tal*.

(2.5) Sætning. *Et tal n er et Carmichael-tal, hvis og kun hvis $n = p_1 \cdots p_r$ er et produkt af (mindst tre) ulige, forskellige primtal p_i, som opfylder, at $p_i - 1 \mid n - 1$.*

Bevis. Lad $n = 2^\nu p_1^{\nu_1} \cdots p_r^{\nu_r}$ være primopløsningen af n, hvor primtallene p_i er ulige.

Antag først, at n er et Carmichael-tal. Hvis n er lige, er $n - 1$ ulige. Betingelsen (2.4.1) medfører derfor, at alle elementer i $(\mathbb{Z}/n)^*$ har ulige orden. Gruppens orden, dvs $\varphi(n)$, må derfor være ulige. Af udregningerne af $\varphi(n)$ i (2.1) fremgår, at dette kun kan være tilfældet for $n = 2$. Da et Carmichael-tal er sammensat, følger det, at n er ulige.

For $\mu \leqslant \nu_i$ kan vi betragte den kanoniske homomorfi,

$$(\mathbb{Z}/n)^* \to (\mathbb{Z}/p_i^\mu)^*.$$

Den er surjektiv. Ifølge Den kinesiske Restklassesætning kan vi nemlig, for et givet a primisk med p_i, finde et helt tal x således, at $x \equiv a \pmod{p_i^{\nu_i}}$ og $x \equiv 1 \pmod{p_j^{\nu_j}}$. Restklassen af x modulo n er da en primisk restklasse, og den afbildes på restklassen af a modulo p_i^μ ved homomorfien.

Da n er et Carmichael-tal, har alle elementer på homomorfiens venstreside en orden, der er divisor i $n - 1$. Følgelig har alle elementer på højresiden en orden, der er divisor i $n - 1$. Tag $\mu := 1$. Højresiden er da cyklisk, dvs indeholder et element af orden $p_i - 1$. Altså er $p_i - 1$ divisor i $n - 1$. Hvis $\nu_i \geqslant 2$, kunne vi tage $\mu := 2$; højresiden indeholder så et element af orden p_i, men så er $p_i \mid n - 1$ i modstrid med at $p_i \mid n$.

Hermed er vist, for primopløsningen af n, at $\nu = 0$ og at $\nu_1 = \cdots = \nu_r = 1$, og at $p_i - 1 \mid n - 1$. Antallet r af primfaktorer er mindst 2, da et Carmichael-tal er sammensat. Hvis $r = 2$, altså $n = p_1 p_2$, har vi,

$$n - 1 = (p_1 - 1)p_2 + (p_2 - 1);$$

da $p_i - 1 \mid n - 1$ følger det, at $p_1 - 1 \mid p_2 - 1$ og (tilsvarende) $p_2 - 1 \mid p_1 - 1$. Derfor er $p_1 = p_2$, en modstrid. Altså er $r \geqslant 3$.

Antag omvendt, at betingelserne er opfyldt. Da er

$$(\mathbb{Z}/n)^* = (\mathbb{Z}/p_1)^* \times \cdots \times (\mathbb{Z}/p_r)^*.$$

Da $p_i - 1 \mid n - 1$, vil den $(n - 1)$'te potens af et r-sæt på højresiden være det neutrale element i produktgruppen. Følgelig er $a^{n-1} = 1$ for alle a på venstresiden. Altså er n et Carmichael-tal. □

(2.6) Eksempel. Carmichael–tal blev betragtet af Carmichael i 1912. Som vi senere skal se, spiller tallene en rolle i forbindelse med primtalstestning. Det er først i 1992 blevet bevist, at der er uendelig mange Carmichael-tal [Alford–Granville–Pomerance].

For et tal med 3 primfaktorer, $n = p_1 p_2 p_3$, har vi

$$n - 1 = (p_1 - 1)p_2 p_3 + (p_2 p_3 - 1).$$

Vi har altså $p_1 - 1 \mid n - 1$, hvis og kun hvis $p_1 - 1 \mid p_2 p_3 - 1$, og tilsvarende betingelser med p_2 og p_3.

Betragt et Carmichael-tal af formen $3p_1p_2$, hvor $3 < p_1 < p_2$. Betingelsen for primtallet 3 er altid opfyldt, da $p_1p_2 - 1$ er lige. De øvrige betingelser er

$$\text{(i)} \quad p_1 - 1 \mid 3p_2 - 1, \qquad \text{(ii)} \quad p_2 - 1 \mid 3p_1 - 1.$$

Da $p_2 > p_1$, følger af (ii), at $3p_1 - 1 = p_2 - 1$ eller $3p_1 - 1 = 2(p_2 - 1)$. Det første tilfælde er udelukket, da $p_2 \neq 3p_1$. Altså er $3p_1 - 1 = 2(p_2 - 1)$, og dermed er

$$\text{(iii)} \quad 3(p_1 - 1) = 2p_2 - 4;$$

specielt er $p_1 - 1 \mid 6p_2 - 12$. At (i) følger, at $p_1 - 1 \mid 6p_2 - 2$. Tilsammen fås, at $p_1 - 1$ er divisor i $(6p_2 - 2) - (6p_2 - 12) = 10$. Yderligere er $p_1 > 3$ et primtal, så derfor er $p_1 = 11$. Af (iii) følger nu, at $p_2 = 17$. Omvendt er det klart, med $p_1 = 11$ og $p_2 = 17$, at betingelserne (i) og (ii) er opfyldt. Tallet $n = 3 \cdot 11 \cdot 17 = 561$ er altså et Carmichael tal.

(2.7) Opgaver.

U3 **1.** Vis, at 561 er det mindste Carmichael-tal.

U3 **2.** Vis, at et sammensat tal $n > 1$ er et Carmichael–tal, hvis og kun hvis der for alle hele tal a gælder $a^n \equiv a \pmod{n}$.

U3 **3.** Vis, at et tal $n > 1$ er et primtal, hvis og kun hvis der for alle a med $1 \leqslant a < n$ gælder $a^{n-1} \equiv 1 \pmod{n}$.

H2 **4.** Bestem alle Carmichael-tal af formen $5p_1p_2$, hvor p_1 og p_2 er primtal.

U3 **5.** Vis, at $(\mathbb{Z}/n)^*$ er en 2-gruppe, hvis og kun hvis $n = 2^\nu p_1 \cdots p_r$, hvor $p_1, \dots, p_r$ er indbyrdes forskellige Fermat-primtal.

U3 **6.** Gruppen $(\mathbb{Z}/11^4)^*$ er cyklisk af orden 13.310. Vis, at restklassen af 2 er en frembringer. [Vink: Anvend (2.2)(*) med $1 + kp = 2^{10}$.]

H2 **7.** Lad p være et ulige primtal, og lad z være et helt tal således, at $[z]_p$, dvs z's restklasse modulo p, frembringer gruppen $(\mathbb{Z}/p)^*$. Betragt de p tal $z_i := z + ip$ for $0 \leqslant i < p$; de har alle den samme restklasse modulo p, men restklasserne $[z_i]_{p^2}$ er forskellige.

(i) Vis, at af de p restklasser $[z_i]_{p^2}$ er der $p - 1$, som frembringer den cykliske gruppe $(\mathbb{Z}/p^2)^*$.

(ii) Vis, at hvis restklassen $[z]_{p^2}$ frembringer gruppen $(\mathbb{Z}/p^2)^*$, så vil restklassen $[z]_{p^\nu}$ frembringe gruppen $(\mathbb{Z}/p^\nu)^*$ for alle ν.

[Vink: Ifølge Fermat findes en fremstilling $z^{p-1} = 1 + kp$. Vis, at $[z]_{p^2}$ frembringer $(\mathbb{Z}/p^2)^*$, hvis og kun hvis $p \nmid k$. Bestem den tilsvarende fremstilling for z_i. For at vise (ii) kan man udnytte kongruensen $(1 + kp)^{p^{\mu-1}} \equiv 1 + kp^\mu \pmod{p^{\mu+1}}$, jfr (2.2)(*).]

U1 **8.** Beskriv for en divisor d i n den naturlige homomorfi $(\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*$. Vis, at homomorfien er surjektiv, og bestem ordenen af kernen $U(d)$. Betragt $n = 24$ og $d = 8$ og restklassen $b := [3]_8$ i $(\mathbb{Z}/8)^*$. Bestem en primisk restklasse i $(\mathbb{Z}/24)^*$ som ved homomorfien afbildes på b. Angiv restklasserne i $U(8)$ og i $U(6)$ (stadig med $n = 24$).

U1 **9.** Vis, for $m > 2$, at hvis kongruensen $x^{2^k} \equiv -1 \pmod{m}$ kan løses, så er 2^{k+1} divisor i $\varphi(m)$. Vis, at der er uendelig mange primtal p med $p \equiv 1$ modulo 4. [Vink: Antag, at $p_1, \dots, p_n$ er givne, og vælg en primdivisor p i $(2p_1 \cdots p_n)^2 + 1$ som p_{n+1}.] Hvad sker modulo 8? – og modulo 16?

U2 **10.** Vis, at der er uendelig mange primtal p med $p \equiv 3 \pmod{4}$. [Vink: Antag, at $p_1, \dots, p_n$ er givne. Vis, at tallet $4p_1 \cdots p_k - 1$ må have en primdivisor p med $p \equiv 3 \pmod{4}$, og vælg sådan en som p_{n+1}.]

H1 **11.** Vis, at der er uendelig mange primtal p med $p \equiv 2 \pmod{3}$. Vis for hvert $n > 2$, at der er uendelig mange primtal p med $p \not\equiv 1 \pmod{n}$. (Resultatet er i øvrigt en konsekvens af Dirichlet's sætning: *I enhver primisk restklasse findes uendelig mange primtal, dvs at for hvert givet* a *med* $(a, n) = 1$ *er der uendelig mange primtal* p *med* $p \equiv a \pmod{n}$.)

U4 **12.** Vis, for $n > 1$, at $\sum_{(a,n)=1} a = \frac{1}{2}n\varphi(n)$, hvor summen er over tal a, med $1 \leqslant a \leqslant n$ og primiske med n.

U1 **13.** For hvilke n er $\varphi(n) = 6$? Og for hvilke k er $\varphi(\varphi(k)) = 6$.

U2 **14.** Vis, at for $p \geqslant 2$ gælder: p er et primtal, hvis og kun hvis p går op i $(p-1)! + 1$ (Wilson's sætning).

U2 **15.** Vis, at for $p \geqslant 2$ gælder: p er et primtal, hvis og kun hvis $p \mid (p-2)! - 1$. For hvilke p gælder $p \mid 2(p-3)! + 1$?

U2 **16.** Vis, at for $a \geqslant 3$ gælder: $a - 1$ og $a + 1$ er primtalstvillinger, hvis og kun hvis $a^2 - 1$ går op i $4(a-2)! + a + 3$.

U3 **17.** Angiv den fuldstændige løsning til kongruensen $x^2 \equiv 1 \pmod{p^\nu}$, hvor p er et primtal. [Vink: Antallet af løsninger er 2 når p er ulige, og 4 når $p = 2$ og $\nu \geqslant 3$.]

U3 **18.** (Gauss's generalisering af Wilson's sætning). Lad w være produktet af alle naturlige tal mindre end n og primiske med n. Antag $n > 2$. Vis, at $w \equiv (-1)^{N/2} \pmod{n}$, hvor N er antallet af løsninger modulo n til kongruensen $x^2 \equiv 1 \pmod{n}$. [Vink: $[w]$ er produktet af samtlige elementer i gruppen $(\mathbb{Z}/n)^*$. Faktorerne a og a^{-1} forekommer i produktet, og de spiser hinanden, når de er forskellige, dvs når $a^2 \neq 1$. Tilbage bliver produktet over alle a med $a^2 = 1$. I det sidste produkt forekommer med a også faktoren $-a$, og den er forskellig fra a.]

*Vis, at $w \equiv -1 \pmod{n}$, når $n = 4$ eller $n = p^\nu$ eller $n = 2p^\nu$ (et ulige primtal p), og at $w \equiv 1$ i alle andre tilfælde.

U3 **19.** Bestem en frembringer for gruppen $(\mathbb{Z}/17)^*$. Og for gruppen $(\mathbb{Z}/289)^*$.

H2 **20.** Bestem for hvert af primtallene $p = 17, 19, 23, 29, 31$ det mindste naturlige tal z således, at $[z]_p$ frembringer gruppen $(\mathbb{Z}/p)^*$.

H2 **21.** Bestem for hvert af tallene $n = 16, 18, 20, 21, 24, 26, 27, 28, 30$ et element af den maksimale elementorden i $(\mathbb{Z}/n)^*$.

H2 **22.** Lad $p < q < r$ være ulige primtal. Vis, at tallet $n := pqr$ er et Carmichael-tal, hvis og kun hvis

$$(1)\quad p-1 \mid qr-1, \qquad (2)\quad q-1 \mid pr-1, \qquad \text{og } (3)\quad r-1 \mid pq-1.$$

Antag, at (3) er opfyldt. Vis, at så er $pq - 1 = d(r-1)$ med $2 \leqslant d \leqslant p-1$ og

$$(4) \quad q-1 \mid d(r-1)-p+1.$$

Vis, at hvis også (2) er opfyldt, så er $q-1$ divisor i $(d+p)(p-1)$. Slut heraf, at der for et givet primtal p kun er endelig mange Carmichael-tal af formen pqr.

U6 **23.** Antag om tallet h, at de tre tal $p := 6h+1$, $q := 12h+1$, og $r := 18h+1$, alle er primtal. Vis, at tallet pqr er et Carmichael-tal.

3. Cirkeldelingspolynomier. Endelige legemer.

(3.1) Definition. Lad n være et naturligt tal. Et element ζ i et legeme L kaldes en n'te *enhedsrod*, hvis $\zeta^n = 1$ (hvor 1 er et-elementet i L). Ækvivalent er ζ altså en n'te enhedsrod, hvis ζ er rod i polynomiet $X^n - 1$. Ligningen $\zeta^n = 1$ medfører øjensynlig, at $\zeta \neq 0$, og at ζ i legemets multiplikative gruppe L^* har en orden, der er divisor i n. Hvis ζ har *orden* n, dvs hvis $\zeta^n = 1$ og $\zeta^j \neq 1$ for $1 \leqslant j < n$, kaldes ζ en *primitiv* n'te enhedsrod.

Hvis legemet er de komplekse tals legeme $\mathbb{C}$, har polynomiet $X^n - 1$ netop n rødder. Det er velkendt, at de komplekse n'te enhedsrødder er tallene af formen,

$$\zeta = e^{2\pi i a/n}, \quad \text{hvor} \quad 0 \leqslant a < n.$$

Sættes $\zeta_n := \exp 2\pi i/n$, er det altså tallene af formen $\zeta = \zeta_n{}^a$, altså potenserne af tallet ζ_n. De komplekse n'te enhedsrødder udgør derfor den cykliske gruppe frembragt af den specielle enhedsrod ζ_n. Øjensynlig har ζ_n orden n. Heraf følger, at ζ_n^a har orden lig med $n/(a, n)$. Specielt ses, at ζ_n^a har orden n, hvis og kun hvis a er primisk med n. Antallet af primitive komplekse n'te enhedsrødder er altså $\varphi(n)$, hvor φ er Euler's φ-funktion. I legemet $\mathbb{R}$ er de eneste enhedsrødder naturligvis 1 og -1 (af ordener 1 og 2).

(3.2) Definition. Polynomiet,

$$\Phi_n := \prod_{\zeta}(X - \zeta),$$

hvor ζ gennemløber de $\varphi(n)$ primitive, komplekse n'te enhedsrødder, kaldes det n'te *cirkeldelingspolynomium*. Polynomiet Φ_n er øjensynligt et normeret polynomium af grad $\varphi(n)$.

(3.3) Sætning. *Cirkeldelingspolynomierne Φ_n tilfredsstiller ligningerne,*

$$X^n - 1 = \prod_{d|n} \Phi_d, \tag{3.3.1}$$

hvor produktet på højresiden er over alle positive divisorer d i n.

Bevis. Polynomiet på venstresiden af ligningen kan faktoriseres:

$$X^n - 1 = \prod_{\xi}(X - \xi),$$

hvor ξ gennemløber de n komplekse rødder i polynomiet, dvs de n'te enhedsrødder. Grupperes i produktet faktorerne $X - \xi$ svarende til at ξ har en bestemt orden d (nødvendigvis med $d \,|\, n$), fremkommer polynomiet Φ_d. Heraf fås den ønskede formel. □

Korollar. *Cirkeldelingspolynomiet Φ_n har koefficienter i $\mathbb{Z}$.*

Bevis. Formlen i Sætningen kan skrives:

$$X^n - 1 = \Phi_n \Pi_n, \quad \text{hvor } \Pi_n = \prod_{d\,|\,n,\, d<n} \Phi_d.$$

Heraf ses, at Φ_n fremkommer som kvotient, når polynomiet $X^n - 1$ divideres med polynomiet Π_n. Polynomiet Π_n er øjensynlig normeret. Idet Korollarets påstand vises ved fuldstændig induktion efter n, kan det antages, at Π_n har hele koefficienter. Heraf følger, at kvotienten Φ_n også har hele koefficienter. □

(3.4) Eksempel. Øjensynlig er

$$\Phi_1 = X - 1, \quad \Phi_2 = X + 1, \quad \Phi_4 = X^2 + 1,$$
$$\Phi_3 = X^2 + X + 1 \quad \text{og} \quad \Phi_6 = X^2 - X + 1.$$

Ifølge Sætning (3.3), jfr. beviset for Korollaret, fremkommer Φ_n ved at dividere polynomiet $X^n - 1$ med produktet af førstegradspolynomierne $X - \xi$, hvor ξ er en n'te enhedsrod af orden strengt mindre end n. Hvis $n = p^r$ er en primtalspotens, så har en n'te enhedsrod ξ orden strengt mindre end n, netop når $\xi^{p^{r-1}} = 1$. Følgelig er

$$\Phi_{p^r} = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1.$$

Specielt fås for et primtal p, at

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

og for potenser af 2:

$$\Phi_{2^r} = X^{2^{r-1}} + 1.$$

Betragt $n = 48$. Hvis $\xi^{48} = 1$, og ξ ikke har orden 48, så har ξ orden d, hvor d er en ægte divisor i 48. Enten er altså d divisor i 24, eller $d = 16$. Følgelig er

$$\Phi_{48} = \frac{X^{48} - 1}{(X^{24} - 1)\Phi_{16}} = \frac{X^{24} + 1}{X^8 + 1} = X^{16} - X^8 + 1.$$

(3.5) Karakteristik. Betragt et vilkårligt legeme L. Den kanoniske ringhomomorfi $\mathbb{Z} \to L$ er som bekendt afbildningen $k \mapsto k1$, der afbilder k på den k'te (additive) potens af et-elementet 1 i L. For $k \in \mathbb{N}$ er altså

$$k1 = \overbrace{1 + \cdots + 1}^{k}.$$

Kernen er et ideal i $\mathbb{Z}$, altså af formen $\mathbb{Z}p$, hvor $p \geqslant 0$. Tallet p kaldes som bekendt *karakteristikken* af L. Karakteristikken kan være 0, svarende til at homomorfien $\mathbb{Z} \to L$ er injektiv; i dette tilfælde kan vi opfatte $\mathbb{Z}$ som en delring af L,

$$\mathbb{Z} \hookrightarrow L.$$

Hvis karakteristikken af et legeme ikke er 0, må den som bekendt være et primtal. I dette tilfælde giver Isomorfisætningen for ringe en naturlig isomorfi mellem kvotienten $\mathbb{Z}/p$ og billedringen. Vi kan altså opfatte legemet $\mathbb{F}_p = \mathbb{Z}/p$ (med p elementer) som delring af L,

$$\mathbb{F}_p \hookrightarrow L.$$

Karakteristik kan som bekendt defineres for en vilkårlig kommutativ ring R. I primtalskarakteristik gælder følgende nyttige resultat:

Freshman's Dream. *Når karakteristikken af R er et primtal p, så er, for alle $x, y \in R$,*

$$(x+y)^p = x^p + y^p, \ (xy)^p = x^p y^p, \ 1^p = 1. \tag{3.5.1}$$

De to sidste ligninger er blot almindelige potensregler, den første følger ved at anvende binomialformlen: da p er et primtal, er binomialkoefficienterne $\binom{p}{i}$ for $0 < i < p$ delelige med p, og leddene $\binom{p}{i}x^i y^{p-i}$ er derfor 0 i R.

Et polynomium f i $\mathbb{Z}[X]$ giver via den kanoniske homomorfi et polynomium i $L[X]$. I karakteristik 0 fremkommer det via inklusionen $\mathbb{Z}[X] \hookrightarrow L[X]$. I positiv karakteristik p reduceres først koefficienterne i f modulo p; det reducerede polynomium ligger så i delringen $\mathbb{F}_p[X] \subseteq L[X]$. Det fører sædvanligvis ikke til misforståelser, hvis det reducerede polynomium også betegnes med f. I alle tilfælde kan vi, for et element $\xi \in L$, indsætte ξ i f, og specielt undersøge, om ξ er rod i f.

(3.6) Sætning. *Lad p være karakteristikken af legemet L. Da gælder, for $\zeta \in L$ og $n \in \mathbb{N}$, at ζ har orden n i L^*, hvis og kun hvis $\Phi_n(\zeta) = 0$ og p ikke går op i n.*

Bevis. Den sidste betingelse, $p \nmid n$, er naturligvis altid opfyldt, hvis $p = 0$. Hvis p er et primtal, og n er ordenen af et element ζ i L, er den også opfyldt. Antag nemlig, indirekte, at ζ har orden n, hvor $n = dp$. Da er

$$0 = \zeta^n - 1 = \zeta^{dp} - 1 = (\zeta^d - 1)^p,$$

hvor den sidste ligning følger af (3.5.1). Følgelig er også $\zeta^d = 1$, i modstrid med at ordenen n er den mindste positive eksponent med $\zeta^n = 1$.

Vi kan altså, i resten af beviset, antage, at $p \nmid n$. Af (3.3.1) får vi, eventuelt ved at reducere koefficienterne, følgende ligning i $L[X]$:

$$X^n - 1 = \prod_{d \mid n} \Phi_d. \tag{3.6.1}$$

Af (3.6.1) følger umiddelbart, at hvis ζ er rod i Φ_n, så er ζ rod i $X^n - 1$, altså $\zeta^n = 1$, og omvendt, hvis $\zeta^n = 1$, så er ζ rod i et af polynomierne Φ_d for $d \mid n$.

Antag, at ζ har orden n. Da er $\zeta^n = 1$, og ζ er dermed rod i et polynomium Φ_d for $d \mid n$. Specielt er også $\zeta^d = 1$. Da ζ har orden n, er det udelukket, at $d < n$. Altså er ζ rod i Φ_n.

Antag omvendt, at ζ er rod i Φ_n. Da er $\zeta^n = 1$, så ζ's orden er en divisor e i n. Da $\zeta^e = 1$ fås, ved at betragte (3.6.1) for $n := e$, at ζ må være rod i et Φ_d, hvor $d \mid e$. Antag, indirekte, at $e < n$. Da er $d < n$, og ζ er altså rod i to forskellige faktorer på højresiden af (3.6.1). Vi får derfor en ligning $X^n - 1 = (X - \zeta)^2 g$ med et polynomium $g \in L[X]$. Ved differentiation fås ligningen,

$$nX^{n-1} = (X - \zeta)\big(2g + (X - \zeta)g'\big).$$

Ved indsættelse af ζ fås $n\zeta^{n-1} = 0$, og videre, ved multiplikation med ζ, fås $n1 = 0$, i modstrid med at karakteristikken p ikke var divisor i n. $\square$

(3.7) Bemærkning. Hvis G er en endelig undergruppe af den multiplikative gruppe L^*, så er G cyklisk. Dette er velkendt (og vi brugte det i (2.2), hvor vi udnyttede, at den multiplikative gruppe $\mathbb{F}_p^*$ er cyklisk). Alternativt kan vi udnytte Sætningen ovenfor.

Lad n være ordenen af G. Da er $\xi^n = 1$ for alle elementer $\xi \in G$. Polynomiet $X^n - 1$ er normeret af grad n, og det har n forskellige rødder i L, nemlig de n elementer $\xi_1, \dots, \xi_n$ i G. Altså gælder i $L[X]$ ligningen,

$$X^n - 1 = (X - \xi_1) \cdots (X - \xi_n). \tag{3.7.1}$$

Det skal vises, at et af elementerne ξ_i i G har orden n. Hertil bruges Sætningen.

Ved differentiation og indsættelse af ξ_1 i (3.7.1) fås ligningen,

$$n\xi_1^{n-1} = (\xi_1 - \xi_2) \cdots (\xi_1 - \xi_n).$$

Højresiden er forskellig fra 0. Altså kan n, som indgår i venstresiden, ikke være delelig med karakteristikken af L.

Af (3.7.1) og (3.6.1) sluttes, at hver faktor Φ_d på højresiden af (3.6.1) må være et produkt af visse af førstegradsfaktorerne $X - \xi_j$ (lige så mange som graden af Φ_d). Specielt må Φ_n være et sådant produkt, og heraf fremgår videre, at Φ_n har en rod ξ_i blandt elementerne ξ_j. Ifølge Sætningen har ξ_i orden n. Den cykliske undergruppe frembragt af ξ_i har altså orden n, og ξ_i må derfor være en frembringer for G. Altså er G cyklisk.

(3.8) Sætning. *Lad p være et primtal, primisk med n. Betragt i $\mathbb{F}_p[X]$ cirkeldelingspolynomiet $\Phi_n(X)$, og i Φ_n en irreducibel divisor $f \in \mathbb{F}_p[X]$ af grad r. Da er kvotientringen $K := \mathbb{F}_p[X]/(f)$ et legeme med p^r elementer, som omfatter $\mathbb{F}_p$, og restklassen $\xi := (X \bmod f)$ er en primtiv n'te enhedsrod i K. Yderligere er r lig med ordenen af restklassen $[p]_n$ i $(\mathbb{Z}/n)^*$.*

Bevis. Det er en velkendt beskrivelse af en polynomiumskvotient $K := \mathbb{F}_p[X]/(f)$, at når f har grad r, så er $\mathbb{F}_p \subseteq K$ og elementerne i K kan entydigt skrives

$$\alpha = a_0 + a_1\xi + \cdots a_{r-1}\xi^{r-1} \tag{3.8.1}$$

med $a_i \in \mathbb{F}_p$. Der er p muligheder for a_i, og altså p^r muligheder for α. Derfor er $|K| = p^r$. Yderligere er det velkendt, når f er irreducibel, at hovedidealet (f) er et maksimalideal, og at kvotienten $K := \mathbb{F}_p[X]/(f)$ derfor er et legeme.

Homomorfien $\mathbb{F}_p[X] \to \mathbb{F}_p[X]/(f)$ er bestemt ved $F(X) \mapsto F(\xi)$. Specielt er $f(\xi) = 0$, og $\Phi_n(\xi) = 0$, fordi f er divisor i Φ_n. Af Sætning (3.6) fremgår, at ξ har orden n i K^*.

Den multiplikative gruppe K^* har orden $p^r - 1$. Derfor er ordenen n divisor i $p^r - 1$. Med andre ord er $p^r \equiv 1 \pmod{n}$, eller $[p]_n^r = 1$ i $(\mathbb{Z}/n)^*$. Restklassen $[p]_n$ i $(\mathbb{Z}/n)^*$ har altså en orden, som er divisor i r. Det påstås, at ordenen må være lig med r. Antag hertil for et naturligt tal s, at $[p]_n^s = 1$ i $(\mathbb{Z}/n)^*$; det skal vises, at $s \geqslant r$. Af antagelsen følger, at n er divisor i $p^s - 1$, og derfor er $\xi^{p^s-1} = 1$. Følgelig er $\xi^{p^s} = \xi$. Heraf følger videre, at $(\xi^i)^{p^s} = \xi^i$. Af Fermat's lille sætning følger, for $a \in \mathbb{F}_p$, at $a^p = a$, og så er er også $a^{p^s} = a$. Af Freshman's Dream følger så, at højresiden i (3.8.1) ikke ændres, når den opløftes til potensen p^s. Derfor er $\alpha^{p^s} = \alpha$ for alle $\alpha \in K$. Polynomiet $X^{p^s} - X$ har derfor de p^r elementer i K som rødder. Da graden mindst er antallet af rødder, følger det, at $p^s \geqslant p^r$. Altså er $s \geqslant r$, som ønsket. □

(3.9) Korollar. *For hver primtalspotens $q = p^r$ findes et legeme K med q elementer, fx bestemt som kvotienten,*

$$K := \mathbb{F}_p[X]/(f),$$

hvor f i $\mathbb{F}_p[X]$ er en irreducibel divisor i Φ_{q-1}. I denne beskrivelse er sideklassen $\xi := (X \bmod f)$ en frembringer for den cykliske gruppe K^*. Yderligere gælder, at alle legemer med q elementer er isomorfe med K. Mere generelt gælder, at hvis L er et legeme med p^s elementer, så findes en homomorfi $K \hookrightarrow L$, hvis og kun hvis $r \,|\, s$.

Bevis. Med $n := p^r - 1$ er det klart, at restklassen af p modulo n har orden r i $(\mathbb{Z}/n)^*$. Derfor kan (3.8) anvendes. Det følger, at f har grad r. Derfor er $|K| = p^r$. Yderligere har ξ orden $n = p^r - 1$, og da $|K^*| = p^r - 1$, må ξ være en frembringer for gruppen K^*.

Lad nu L være et legeme med p^s elementer. Antag først, at der findes en homomorfi $K \to L$. En homomofi mellem legemer er som bekendt altid injektiv (antydet med skrivemåden $K \hookrightarrow L$), så vi kan opfatte K som dellegeme af L. Specielt kan L opfattes som vektorrum over K, idet multiplikation af en vektor $u \in L$ med en skalar $\alpha \in K$ blot er produktet αu i legemet L. Hvis d er dimensionen af L som vektorrum over K, kan elementerne i L, efter valg af basis, beskrives ved koordinatsæt med d koordinater fra K. Derfor er $|L| = |K|^d$, altså $p^s = (p^r)^d$. Derfor er $r \,|\, s$.

Antag omvendt, at $r \,|\, s$. Så er $n = p^r - 1$ divisor i $p^s - 1$. Da L^* har orden $p^s - 1$, er alle $p^s - 1$ elementer i L^* rødder i polynomiet $X^{p^s-1} - 1 \in L[X]$. Polynomiet $X^{p^s-1} - 1$ er derfor lig med produktet af de $p^s - 1$ faktorer $X - \alpha$ svarende til elementerne $\alpha \in L^*$. På den anden side er f divisor i Φ_n, som er divisor i $X^n - 1$, som er divisor i $X^{p^s-1} - 1$. Derfor må f (efter normering) være lig med produktet af r af faktorerne $X - \alpha$. Specielt har f altså en rod i L. Betragt nu ringhomomorfien,

$$\mathbb{F}_p[X] \to L \qquad \text{bestemt ved } F(X) \mapsto F(\alpha).$$

Da $f(\alpha) = 0$, ligger f i kernen, og derfor er hovedidealet (f) indeholdt i kernen. Kernen er et ægte ideal, og da hovedidealet er et maksimalideal, må ringhomomorfiens kerne være lig med hovedidealet (f). Isomorfisætningen giver nu en isomorfi af $K = \mathbb{F}_p[X]/(f)$ på billedringen, og dermed den ønskede homomorfi $K \hookrightarrow L$.

I specialtilfældet, hvor $s = r$, dvs hvor L er et legeme med q elementer, må denne injektive homomorfi være en isomorfi. Alle legemer med q elementer er altså isomorfe med K. $\square$

(3.10) Korollar. *Lad p være et primtal. For primopløsningen af $X^{p^k} - X$ (for $k \geqslant 1$) i $\mathbb{F}_p[X]$ gælder da, at primfaktorerne er samtlige (normerede) irreducible polynomier i $\mathbb{F}_p[X]$ af en grad, som går op i k, og hver af faktorerne forekommer præcis én gang.*

Bevis. Hvis en primfaktor g indgik to gange, ville vi have en ligning $X^{p^k} - X = g^2 h$ i $\mathbb{F}_p[X]$, og ved differentiation ville vi få:

$$-1 = g(2g'h + gh'),$$

hvilket er en modstrid, da g ikke kan være konstant.

Lad f være et normeret, irreducibelt polynomium i $\mathbb{F}_p[X]$, og lad r betegne graden af f. Det skal vises, at

$$f \mid X^{p^k} - X \iff r \mid k.$$

Betragt hertil kvotienten $K := \mathbb{F}_p[X]/(f)$ og ækvivalensklassen $\xi := (X \bmod f)$. Da er K et legeme med p^r elementer og ξ er rod i f. Hvis $\xi \neq 0$, så ligger ξ i gruppen K^*, der har orden $p^r - 1$, og så er $\xi^{p^r-1} = 1$; specielt er $\xi^{p^r} - \xi = 0$. Den sidste ligning gælder trivielt, hvis $\xi = 0$. Polynomiet $X^{p^r} - X$ afbildes altså i 0 ved homomorfien $F(X) \mapsto F(\xi)$; det ligger altså i hovedidealet (f). Derfor er f divisor i $X^{p^r} - X$.

Antag først, at $r \mid k$. Da er $p^r - 1 \mid p^k - 1$. Følgelig er $X^{p^r-1} - 1 \mid X^{p^k-1} - 1$, og ved multiplikation med X fås $X^{p^r} - X \mid X^{p^k} - X$. Da vi har set, at $f \mid X^{p^r} - X$, følger det, at $f \mid X^{p^k} - X$.

Antag omvendt, at $f \mid X^{p^k} - X$, altså at $\xi^{p^k} - \xi = 0$. Det skal vises, at $r \mid k$. Det er klart, hvis $r = 1$, så vi kan antage, at $r > 1$. Specielt er så $f \neq X$, og derfor er $\xi \neq 0$. Da $\xi^{p^k} = \xi$, følger det, at $\xi^{p^k-1} = 1$. Lad n være ordenen af ξ. Så er $\Phi_n(\xi) = 0$, og derfor er f divisor i Φ_n. Af Sætning (3.8) følger så, at r er ordenen af restklassen $[p]_n$ i $(\mathbb{Z}/n)^*$. På den anden side er n divisor i $p^k - 1$. Men så er $p^k \equiv 1 \pmod{n}$, og derfor et k et multiplum af ordenen af $[p]_n$, dvs et multiplum af r, som ønsket. □

(3.11) Eksempel. For at konstruere et legeme $\mathbb{F}_{16}$ med $2^4 = 16$ elementer, og heri en frembringer for gruppen $\mathbb{F}_{16}^*$, betragtes cirkeldelingspolynomiet Φ_{15}. Man finder:

$$\Phi_{15} = \frac{X^{15} - 1}{(X^5 - 1)(X^2 + X + 1)} = \frac{X^{10} + X^5 + 1}{X^2 + X + 1} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

Korollar (3.9) forudsiger, at dette polynomium modulo 2, dvs i $\mathbb{F}_2[X]$, er et produkt af irreducible polynomier af grad 4. Det er let at se, at der modulo 2 gælder:

$$X^8 + X^7 + X^5 + X^4 + X^3 + X + 1 = (X^4 + X^3 + 1)(X^4 + X + 1).$$

De to polynomier på højresiden er altså irreducible i $\mathbb{F}_2[X]$. Det søgte legeme kan altså fx beskrives som $\mathbb{F}_{16} := \mathbb{F}_2[X]/(X^4 + X + 1)$. Ved denne beskrivelse er restklassen ξ, af X modulo $(X^4 + X + 1)$, en frembringer for den multiplikative gruppe $\mathbb{F}_{16}^*$.

Bemærk, hvordan man regner i det således konstruerede legeme $\mathbb{F}_{16}$: Elementerne har formen

$$r = r_0 + r_1\xi + r_2\xi^2 + r_3\xi^3,$$

og de svarer til 4-sæt (r_0, r_1, r_2, r_3) af restklasser modulo 2. Addition af 4-sæt er blot koordinatvis addition. Multiplikation er bestemt ved ligningen,

$$\xi^4 = \xi + 1;$$

heraf følger fx, at $\xi^5 = \xi + \xi^2$, at $\xi^6 = \xi^2 + \xi^3$, at $\xi^7 = \xi^3 + \xi^4 = \xi^3 + \xi + 1$, osv.

Det skal understreges, at det i almindelighed er en ikke-triviel opgave at faktorisere cirkeldelingspolynomierne modulo p. I det simpleste tilfælde, $r = 1$ (altså $q = p$), af (3.9), vides, at de irreducible divisorer i Φ_{p-1} er førstegradsfaktorer. Det er førstegradsfaktorerne $X - a$, hvor restklassen a er *primitiv rod modulo* p, dvs en frembringer for den cykliske gruppe $\mathbb{F}_p^*$, og det er ikke-trivielt at bestemme primitive rødder modulo p (når $p \gg 0$).

(3.12) Eksempel. Betragt $q = 49$, hvor altså $p = 7$. Vi har

$$\Phi_{48} = X^{16} - X^8 + 1.$$

Sætningen forudsiger, at dette polynomium modulo 7 er et produkt af (nødvendigvis 8) andengradspolynomier.

Et legeme med 49 elementer kan naturligvis konstrueres som en kvotient $\mathbb{F}_7[X]/(g)$ for et vilkårligt irreducibelt andengradspolynomium g. Fx er $g = X^2 + 1$ et sådant polynomium, idet polynomiet modulo 7 øjensynlig ikke har rødder. Lad i betegne restklassen af X i kvotientringen $L := \mathbb{F}_7[X]/(X^2+1)$. Da har elementerne i L formen $a + ib$, hvor $a, b \in \mathbb{F}_7$; regning foregår ved at udnytte, at $i^2 = -1$. Specielt har i orden 4. For at bestemme et element $a + ib$ af orden 8, løses ligningen $(a + ib)^2 = i$, altså

$$a^2 - b^2 = 0, \quad 2ab = 1;$$

en løsning er $(a, b) = (2, 2)$, så $2 + 2i$ har orden 8. Et element af orden 16 bestemmes ved at løse $(c + id)^2 = 2 + 2i$, altså

$$c^2 - d^2 = 2, \quad 2cd = 2.$$

En løsning er $(c, d) = (5, 3)$. Elementet $5 + 3i$ har altså orden 16. Endelig, da 2 øjensynlig har orden 3, følger det, at $2(5 + 3i) = 3 - i$ har orden 48. Dette element er den ene rod i

$$f = X^2 - 6X + 10 = X^2 + X + 3 \in \mathbb{F}_7[X].$$

Vi kan altså også opfatte L som kvotienten $\mathbb{F}_{49} := \mathbb{F}_7[X]/(X^2 + X + 3)$: elementerne har formen $a + b\xi$, med $a, b \in \mathbb{F}_7$, og regning i $\mathbb{F}_{49}$ er bestemt ved $\xi^2 = -3 - \xi$. Elementet ξ har orden 48.

(3.13) Korollar. *Lad $\alpha_p(r)$ betegne antallet af irreducible normerede polynomier af grad r i $\mathbb{F}_p[X]$. Da er $p^r = \sum_{d\,|\,r} d\alpha_p(d)$, og følgelig er*

$$\alpha_p(r) = \frac{1}{r}\sum_{d\,|\,r} p^{r/d}\mu(d),$$

hvor μ er Möbius-funktionen.

Bevis. Produktet af samtlige irreducible polynomier af grad $d\,|\,r$ er ifølge Korollar (3.10) lig med $X^{p^r} - X$. Den første anførte ligning følger nu ved sammenligne graderne, og heraf følger den anden ligning ved Möbius-inversion. □

(3.14) Bemærkning. Af (3.8) fremgår, hvordan man undersøger, om polynomiet $\bar{\Phi}_n$ (fremkommet ved at reducere koefficienterne i Φ_n modulo p) er irreducibelt i $\mathbb{F}_p[X]$, hvor $p \nmid n$. Det fremgår mere præcist, hvordan man bestemmer graden af de irreducible faktorer f, der indgår i primopløsningen af $\bar{\Phi}_n \in \mathbb{F}_p[X]$.

I primopløsningen af $\bar{\Phi}_n$ i $\mathbb{F}_p[X]$ som produkt af irreducible, normerede polynomier er faktorerne i øvrigt indbyrdes forskellige. Antag nemlig indirekte, for et irreducibelt polynomium $f \in \mathbb{F}_p[X]$, at f^2 er divisor i $\bar{\Phi}_n$. Konstruktionen i Sætning (3.8) giver et legeme $K \supseteq \mathbb{F}_p$, hvori f har en rod ξ. Da f^2 er divisor i $\bar{\Phi}_n$, er ξ dobbeltrod i $\bar{\Phi}_n$. Men det er i modstrid med, at ξ er en primitiv n'te enhedsrod, hvorfor polynomiet $\bar{\Phi}_n$ i K har $\varphi(n)$ forskellige rødder, nemlig potenserne ξ^a med $(a, n) = 1$.

Det er et fundamentalt resultat i algebraisk talteori, at Φ_n altid er irreducibelt i $\mathbb{Q}[X]$.

Betragt hertil i $\mathbb{Q}[X]$ en normeret, irreducibel divisor F i Φ_n. Det skal vises, at $F = \Phi_n$. Da $F \mid \Phi_n$, er enhver (kompleks) rod i F også rod i Φ_n, altså en primitiv n'te enhedsrod. Det skal altså omvendt vises, at enhver primitiv n'te enhedsrod er rod i F. Ud fra en given primitiv n'te enhedsrod ζ fås de øvrige som potenserne ζ^a, med $a \geqslant 1$ primisk med n. Eksponenten a kan skrives som produkt af primtal p med $p \nmid n$. Det er derfor nok at vise følgende påstand:

Hvis ζ er rod i F og p er et primtal med $p \nmid n$, så er ζ^p også rod i F.

I beviset for påstanden bruges, at ethvert polynomium i $\mathbb{Q}[X]$ med ζ som rod er et multiplum af F. Det følger af at polynomiumsringen $\mathbb{Q}[X]$ er et hovedidealområde: Polynomierne i $\mathbb{Q}[X]$ med ζ som rod er et ideal; derfor findes et normeret polynomium F_0 således, at dette ideal består af samtlige multipla af F_0. Da $F(\zeta) = 0$, er F et multiplum af F_0; da F er irreducibel, og altså kun har trivielle divisorer, er $F = F_0$. Idealet består derfor af alle multipla af F.

Antag nu, indirekte, at ζ^p ikke er rod i F. Polynomiet $\Phi_n \in \mathbb{Q}[X]$ er et produkt af irreducible, normerede faktorer, og en af dem er F. Da ζ^p er rod i Φ_n, må ζ^p så være rod i en af de andre irreducible faktorer; lad os kalde den G. Fra primopløsningen i $\mathbb{Q}[X]$ af $\Phi_n(X)$ får vi så specielt en faktorisering i $\mathbb{Q}[X]$:

$$\Phi_n = FGH. \tag{*}$$

Da polynomierne er normerede og venstresiden har hele koefficienter, følger det af et korollar til Gauss's Lemma, at F, G, H har koefficienter i $\mathbb{Z}$. Da ζ^p er rod i G, er ζ rod i polynomiet $G(X^p)$. Altså er $G(X^p)$ et multiplum af F. Derfor findes en faktorisering $G(X^p) = QF$. At Q har koefficienter i $\mathbb{Z}$ følger fx af Sætningen om division med rest.

Nu reduceres koefficienterne modulo p. Af (*) fås $\bar{\Phi}_n = \bar{F}\bar{G}\bar{H}$. Videre er koefficienterne i $\bar{G}$ elementer i $\mathbb{F}_p$, og for $a \in \mathbb{F}_p$ gælder $a^p = a$ ifølge Fermat's lille sætning. Derfor følger det af Freshman's Dream, at $\big(\bar{G}(X)\big)^p = \bar{G}(X^p)$. Af $QF = G(X^p)$ følger derfor, at $\bar{F}\bar{Q} = \bar{G}^p$. Vi har altså følgende faktoriseringer i $\mathbb{F}_p[X]$:

$$\bar{\Phi}_n = \bar{F}\bar{G}\bar{H}, \qquad \bar{Q}\bar{F} = \bar{G}^p. \tag{**}$$

Betragt nu i $\mathbb{F}_p[X]$ en irreducibel, normeret divisor f i $\bar{F}$. Af den anden faktorisering følger, at f er divisor i $\bar{G}^p$, og heraf følger, da f er irreducibel, at f er divisor i $\bar{G}$. I den første faktorisering er f altså divisor i både $\bar{F}$ og $\bar{G}$, og derfor er f^2 divisor i $\bar{\Phi}_n$. Men det er en modstrid, idet primdivisorerne i primopløsningen af $\bar{\Phi}_n$ som nævnt er indbyrdes forskellige.

Hermed er påstanden ovenfor bevist, og det er godtgjort, at Φ_n er irreducibelt i $\mathbb{Q}[X]$.

(3.15) Bemærkning. Cirkeldelingspolynomier har mange anvendelser. Lad os her vise, for et naturligt tal $n > 1$, at der er uendelig mange primtal p med $p \equiv 1 \pmod{n}$. Lad der være givet k primtal $p_1, \dots, p_k$. Vi viser, at der eksisterer et primtal p, forskelligt fra de givne, med $p \equiv 1 \pmod{n}$.

Vi bemærker først, at for hvert naturligt tal h er værdien $\Phi_n(h)$ et helt tal (fordi Φ_n har hele koefficienter), og når $h \geqslant 2$ er $\Phi_n(h) > 1$. Mere præcist gælder uligheden,

$$(h-1)^{\varphi(n)} < \Phi_n(h), \text{ når } h \geqslant 1. \tag{3.15.1}$$

Tallet $\Phi_n(h)$ er nemlig produktet af faktorerne $h - \xi$ for primitive n'te enhedsrødder ξ. For hver sådan er også $\bar{\xi} = \xi^{-1}$ en primitiv n'te enhedsrod. Idet (3.15.1) er triviel for $n = 2$, antager vi $n > 2$, og så er $\bar{\xi} \neq \xi$. Med $h - \xi$ forekommer altså også $h - \bar{\xi}$ som faktor, og produktet af disse to faktorer er positivt. Altså er $\Phi_n(h)$ positiv (endda for *alle* reelle tal h, når $n > 2$).

Numerisk er $|h - \xi|$ lig med afstanden fra h til ξ. Da ξ ligger på enhedscirklen, og $\xi \neq 1$, er $|h - \xi| > |h - 1|$. Altså gælder (3.15.1).

Vælg nu, for de givne primtal, $h := np_1 \cdots p_k$. Tallet $\Phi_n(h)$ er større end 1, så der findes et primtal p, med $p \mid \Phi_n(h)$. Da $\Phi_n(h)$ er divisor i $h^n - 1$, er p divisor i $h^n - 1$. Specielt kan p ikke være divisor i h. Altså er p forskellig fra de givne primtal, og p er ikke divisor i n. Modulo p er restklassen $[h] \in \mathbb{F}_p$ rod i Φ_n. Følgelig har $[h]$ orden n i gruppen $\mathbb{F}_p^*$. Altså er n divisor i $p - 1$, dvs $p \equiv 1 \pmod{n}$, som ønsket.

Det er en sætning af Dirichlet, at der i enhver primisk restklasse findes uendelig mange primtal, altså at der for hvert a primisk med n findes uendelig mange primtal p med $p \equiv a \pmod{n}$. Ovenstående viser resultatet for $a = 1$.

(3.16) Bemærkning. Lad os som yderligere anvendelse vise, at ethvert endeligt skævlegeme Λ er kommutativt [*Wedderburn's Sætning*, 1905].

Hertil betragtes *centret* L i Λ, bestående af de elementer $\alpha \in \Lambda$, som kommuterer med alle $\lambda \in \Lambda$. Øjensynlig er L et kommutativt dellegeme af Λ. Specielt er elementantallet i L en primtalspotens q. Som i (3.9) kan vi opfatte Λ som vektorrum over L. Specielt følger det, at elementantallet i Λ er en potens q^r af q. Det skal vises, at $r = 1$.

Den multiplikative gruppe Λ^* har orden $q^r - 1$. Det er klart, at L^* er centret i gruppen Λ^*. Klasseligningen har altså formen,

$$q^r - 1 = q - 1 + \sum\nolimits' |\Lambda^* : C^*(\alpha_j)|, \tag{3.16.1}$$

hvor $C^*(\alpha)$ er centralisatoren i Λ^* af α, og summen er over repræsentanter for konjugeretklasser uden for centret. Specielt er hvert led i summen strengt større end 1. Centralisatoren $C^*(\alpha)$ består af de elementer $\lambda \in \Lambda^*$, for hvilke $\lambda\alpha = \alpha\lambda$. Føjes hertil nul-elementet, fremkommer øjensynlig et delskævlegeme $C(\alpha)$ af Λ. Da $L \subseteq C(\alpha)$, følger det at $|C(\alpha)|$ er en potens q^d. Altså er $|C^*(\alpha)| = q^d - 1$.

Klasseformlen giver altså en ligning af formen,

$$q^r - 1 = q - 1 + \sum \frac{q^r - 1}{q^{d_j} - 1}.$$

Hvert led i summen er et helt tal, så $q^{d_j} - 1 \mid q^r - 1$. Heraf følger let, at $d_j \mid r$. Endvidere er d_j en ægte divisor i r, da leddene i summen var større end 1. Det følger nu af (3.3.1), at tallet $\Phi_r(q)$ er divisor i hvert led i summen. Videre er $\Phi_r(q)$ divisor i $q^r - 1$. Af ligningen følger derfor, at $\Phi_r(q)$ er divisor i $q - 1$. Vurderingen (3.15.1) giver nu en modstrid, med mindre $r = 1$.

(3.17) Opgaver.

H2 **1.** Vis, at konstantleddet i Φ_n, for $n > 1$, er lig med 1. Vis, at koefficienterne i Φ_n ikke altid er ± 1 eller 0. [Vink: bestem nogle koefficienter i Φ_{105}.]

U4 **2.** Vis for $\zeta \in \mathbb{C}$ og et ulige tal u, at ζ har orden $2u$, hvis og kun hvis $-\zeta$ har orden u. Slut heraf, at $\Phi_{2u}(X) = \Phi_u(-X)$.

U4 **3.** For et polynomium f af grad k defineres $c(f) := -f_{k-1}$, hvor f_{k-1} er koefficienten til leddet at næsthøjeste grad. Vis, for normerede polynomier f, g, at $c(fg) = c(f) + c(g)$. Vis, at næsthøjestegradskoefficienten i Φ_n er lig med $-\mu(n)$, hvor $\mu(n)$ er Möbius-funktionen. [Vink: Brug Opgave Kap1: 1.]

U4 **4.** Vis formlen $\Phi_n = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}$, hvor μ er Möbius-funktionen.

5. Det fremgår af Eksempel (3.12), at i $\mathbb{F}_7[X]$ er $f := X^2 + X + 3$ divisor i Φ_{48}. Bestem kvotienten Φ_{48}/f.

U4 **6.** Angiv, i $\mathbb{F}_7[X]$, primopløsningen af Φ_{48} (eller i hvert fald nogle af primfaktorerne).

U5 **7.** Diskuter for hvilke n og primtal $p \nmid n$ polynomiet Φ_n er irreducibelt i $\mathbb{F}_p[X]$. (Fx: Findes der for et givet n altid sådanne primtal p? Eventuelt uendelig mange?)

8. Bestem Φ_{28}.

U4 **9.** Vis, når p er et primtal og $p \nmid n$, at $\Phi_{np}(X) = \Phi_n(X^p)/\Phi_n(X)$.

U4 **10.** Vis, når p er et primtal og $p \nmid n$, at i $\mathbb{F}_p[X]$ er $\Phi_{np} = \Phi_n^{p-1}$.

U5 **11.** Vis, at der for $\mathbb{F}_p[X]$ gælder, at brøkdelen af irreducible polynomier blandt alle polynomier af grad n asymptotisk er lig med $1/n$.

U9 **12.** *Vis „primtalssætningen“ for $\mathbb{F}_p[X]$: Nummerér polynomierne i $\mathbb{F}_p[X]$, således at først kommer konstanterne, dernæst polynomierne af grad 1, dernæst polynomierne af grad 2, osv; polynomierne af samme grad nummereres tilfældigt. Lad $\pi_p(n)$ være antallet af irreducible blandt de første n polynomier. Da gælder asymptotisk: $\pi_p(n) \sim Cn/\log n$, med konstanten $C = \log p$.

U4 **13.** Vis, at hvis $q^d - 1$ er divisor i $q^s - 1$, så er $d \mid s$. [Vink: skriv $s = hd + r$, med $r < d$, og regn modulo $q^d - 1$.]

U4 **14.** Vis, for enhedsrødderne $\zeta_5 := e^{2\pi i/5}$ og $\zeta_{10} := e^{2\pi i/10}$, at

$$\zeta_5 = \frac{\sqrt{5} - 1}{4} + i\frac{\sqrt{10 + 2\sqrt{5}}}{4}, \qquad \zeta_{10} = \frac{\sqrt{5} + 1}{4} + i\frac{\sqrt{10 - 2\sqrt{5}}}{4}.$$

[Vink: $\zeta := \zeta_5$ er rod i Φ_5, så $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. Efter division med ζ^2 fås $0 = (\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1$, hvoraf $\zeta + \zeta^{-1} = \frac{-1+\sqrt{5}}{2}$. Tilsvarende er ζ_{10} rod i $\Phi_{10} = X^4 - X^3 + X^2 - X + 1$.]

U6 **15.** Der er velkendte „pæne“ udtryk for de primitive n'te enhedsrødder ζ_n for $n = 3, 4$ og 5. Ud fra et udtryk $\zeta_n = a+ib$ ($b > 0$) får man et udtryk for ζ_{2n} ved at løse andengradsligningen $z^2 = a + ib$; det giver

$$\zeta_{2n} = \sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} = \sqrt{\frac{1+a}{2}} + i\sqrt{\frac{1-a}{2}}\,.$$

Bestem herved pæne udtryk for $\zeta_6, \zeta_8, \zeta_{10}, \zeta_{12}, \zeta_{16}, \zeta_{20}, \zeta_{24}$. Hvorfor kan man ikke tilsvarende få et udtryk for ζ_9, og mere generelt for ζ_{3n}, ved at bruge, at $z = \zeta_{3n}$ opfylder $z^3 = a+ib$? – det er jo en simpel trediegradsligning, og Cardano's formel fortæller, hvordan sådan en skal løses.

U6 **16.** Vis, når p er et primtal og $p\,|\,m$, at $\Phi_{p^\nu m}(X) = \Phi_m(X^{p^\nu})$. Vis, når $p \nmid n$ og $\nu > 0$, at $\Phi_{p^\nu n}(X) = \Phi_n(X^{p^\nu})/\Phi_n(X^{p^{\nu-1}})$.

U6 **17.** Principielt kan n'te enhedrødder defineres i en vilkårlig (kommutativ) gruppe G: Det er de elementer $g \in G$, som opfylder, at $g^n = 1$. Lad $\alpha_G(n)$ betegne antallet af n'te enhedsrødder. Hvordan bestemmer man antallet af elementer af orden n ud fra funktionen α_G?

Hvordan bestemmer man $\alpha_G(n)$, når G er cyklisk? Hvordan bestemmes antallet $\alpha_{G\times H}(n)$ for en produktgruppe ud fra α_G og α_H?

U8 **18.** Lad K være et endeligt legeme af karakteristik p. Vis, at elementantallet q i K er en potens $q = p^r$ af p. Vis, at $\alpha^q = \alpha$ for alle $\alpha \in K$.

19. Lad L være et legeme af positiv karakteristik p. Afbildningen $\sigma(\xi) := \xi^p$ er så en ringhomomorfi $\sigma\colon L \to L$, og den inducerer en ringhomomorfi $L[X] \to L[X]$, hvor billedet ${}^\sigma f$ af et polynomium $f \in L[X]$ fås ved at anvende σ på koefficienterne i f.

Lad f være et normeret polynomium med koefficienter i $\mathbb{F}_p$. Vis, at hvis f i L har en rod ξ, så er også ξ^p rod i f.

Antag, at $f \in \mathbb{F}_p[X]$ er irreducibelt, med roden ξ i L, og at $f \neq X$ (altså at $\xi \neq 0$). Lad r være graden af f og lad n være ordenen af ξ. Da gælder som bekendt, at r er ordenen af restklassen af p modulo n. Vis, at rødderne i f er potenserne ξ^{p^i} for $i = 0, \dots, r-1$.

U6 **20.** Antag, at $p \equiv 3 \pmod 4$ er et primtal. Vis, at legemet $\mathbb{F}_{p^2}$, med p^2 elementer, så kan defineres som kvotienten $\mathbb{F}_p[X]/(X^2+1)$. Idet i betegner restklassen af X, har elementerne α i $\mathbb{F}_{p^2}$ altså fremstillinger $\alpha = a + ib$ med entydigt bestemte koefficienter $a, b \in \mathbb{F}_p$. Regning i $\mathbb{F}_{p^2}$ er bestemt ved $i^2 = -1$.

Vis, at $\alpha = a + ib$ er rod i polynomiet $(X-a)^2 + b^2 \in \mathbb{F}_p[X]$. Sæt $\bar\alpha := a - ib$. Vis, at $\alpha \mapsto \bar\alpha$ er en ringhomomorfi $\mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$. Vis, at $\bar\alpha = \alpha^p$ for alle $\alpha \in \mathbb{F}_{p^2}$.

U6 **21.** Legemet $\mathbb{F}_{49}$ er beskrevet i (3.12): Elementerne har formen $a + ib$, hvor $a, b \in \mathbb{F}_7$ og $i^2 = -1$. For elementet $\xi = 5 + 3i$ er $\xi^2 = 2 + 2i$, og $\xi^4 = i$. Specielt er $\xi^8 = -1$ og ξ har orden 16. Elementet $\zeta = 2\xi = 3 - i$ har så orden 48.

Bestem de 8 potenser ζ^a for $a = 1, 5, 11, 13, 17, 19, 25, 41$, og de 8 normerede andengradspolynomier i $\mathbb{F}_7[X]$, hvori potenserne er rødder. Hvad kan du sige om disse polynomier i relation til cirkeldelingspolynomiet Φ_{48}.

22. *Lad p være et ulige primtal. Vis, at der findes en ring med præcis p enheder, hvis og kun hvis p er et Mersenne-primtal.

23. Vis, at Sætning (3.8) gælder, når $\mathbb{F}_p$ erstattes med et vilkårligt endeligt legeme L med q elementer: Antag $(n, q) = 1$. Betragt i $L[X]$ en irreducibel divisor f i Φ_n. Så er f's grad lig med ordenen af $[q]_n$ i $(\mathbb{Z}/n)^*$.

24. Vis, at Φ_{17} er irreducibel i $\mathbb{F}_3[X]$.

4. Reciprocitetssætningen.

(4.1) Definition. Lad p være et primtal. Et helt tal a kaldes en *kvadratisk rest* modulo p, hvis a er primisk med p og kongruensen $x^2 \equiv a \pmod p$ har en løsning. Ofte kaldes a en *kvadratisk ikke-rest*, hvis a er primisk med p og kongruensen ikke har løsninger. Det er klart, at spørgsmålet om hvorvidt a er en kvadratisk rest modulo p kun afhænger af a's restklasse modulo p: Tallet a er kvadratisk rest, netop når a's restklasse $[a]_p$ i $\mathbb{Z}/p$ tilhører delmængden af kvadrater på de primiske restklasser. Tilfældet $p = 2$ er uinteressant. For et ulige primtal p defineres *Legendre-symbolet*,

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{hvis } a \text{ er kvadratisk rest modulo } p, \\ -1, & \text{hvis } a \text{ er kvadratisk ikke-rest modulo } p, \\ 0, & \text{hvis } p \text{ går op i } a. \end{cases}$$

(4.2) Euler's kriterium. *For et ulige primtal p bestemmer Legendre-symbolet $\left(\frac{a}{p}\right)$ en ikke-triviel homomorfi $(\mathbb{Z}/p)^* \to \{\pm 1\}$. Yderligere gælder Euler's Kriterium:*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p. \tag{4.2.1}$$

Bevis. Vi bemærker først, at de kvadratiske restklasser udgør en undergruppe af index 2 i gruppen $(\mathbb{Z}/p)^*$ af primiske restklasser; specielt er det netop halvdelen af de primiske restklasser, der er kvadratiske. De kvadratiske restklasser udgør nemlig billedmængden Q ved afbildningen $(\mathbb{Z}/p)^* \to (\mathbb{Z}/p)^*$ bestemt ved $x \mapsto x^2$. Denne afbildning er øjensynlig en homomorfi, og dens kerne består af de restklasser x modulo p, som opfylder $x^2 = 1$. Da p er et ulige primtal, er denne ligning opfyldt for præcis to restklasser, nemlig 1 og -1. Kernen er derfor en undergruppe af orden 2. Det følger, at billedet Q er en undergruppe, hvis orden er halvdelen af ordenen af $(\mathbb{Z}/p)^*$. Men det betyder netop, at Q har index 2.

Da Q er en undergruppe af index 2 i gruppen $(\mathbb{Z}/p)^*$, har kvotientgruppen af $(\mathbb{Z}/p)^*$ modulo Q orden 2, og den kan derfor identificeres med gruppen $\{\pm 1\}$. Den kanoniske homomorfi på kvotienten er så bestemt ved at værdien på a er lig med 1, når $a \in Q$, og lig med -1, når a ligger i den anden sideklasse, dvs i komplementærmængden til Q.

Værdien af Legendre-symbolet $\left(\frac{a}{p}\right)$ afhænger øjensynlig kun af a's restklasse modulo p. Det er klart, at $\left(\frac{a}{p}\right)$ som funktion af de primiske restklasser, netop er den kanoniske homomorfi $(\mathbb{Z}/p)^* \to \{\pm 1\}$. Specielt er det en surjektiv homomorfi, og altså ikke-triviel, dvs ikke konstant lig med 1.

For at eftervise Euler's Kriterium noterer vi følgende ligning i $\mathbb{F}_p[X]$:

$$X^{p-1} - 1 = \big(X^{\frac{p-1}{2}} - 1\big)\big(X^{\frac{p-1}{2}} + 1\big).$$

Ifølge Fermat's lille Sætning gælder for hvert $x \neq 0$ i $\mathbb{F}_p$, at $x^{p-1} = 1$. Hvert $x \neq 0$ er altså rod i $X^{p-1} - 1$, og dermed også rod i et af de to polynomier på højresiden. For $a \in Q$ er $a = x^2$, og altså $a^{(p-1)/2} = x^{p-1} = 1$. Hvert af de $(p-1)/2$ elementer $a \in Q$ er derfor rod i den første faktor. Da graden er $(p-1)/2$, kan den første faktor ikke have yderligere rødder. De resterende elementer i $(\mathbb{Z}/p)^*$, dvs de kvadratiske ikke-rester, må derfor være rødder i den anden faktor. Heraf følger (4.2.1). $\square$

(4.3) Den generelle Reciprocitetssætning. *Legendre-symbolet har en udvidelse til et symbol $\left(\frac{a}{b}\right)$, defineret, når nævneren b enten er ulige og positiv, eller er en diskriminant, dvs et tal forskelligt fra 0 som modulo 4 er kongruent med 0 eller 1. Symbolet har følgende egenskaber:*

(1) *Værdien $\left(\frac{a}{b}\right)$ afhænger kun af restklassen af a modulo b. Værdien er 0, hvis a ikke er primisk med b. Som funktion af tal a, der er primiske med b, er symbolet en homomorfi $(\mathbb{Z}/b)^* \to \{\pm 1\}$.*

(2) *For en diskriminant D og et ulige positivt tal u gælder reciprocitetsformlen,*

$$\left(\frac{u}{D}\right) = \left(\frac{D}{u}\right). \tag{4.3.1}$$

Symbolet $\left(\frac{a}{b}\right)$ kaldes *Jacobi-symbolet*, når nævneren b er ulige og positiv, og *Kronecker-symbolet*, når nævneren er en diskriminant. De tilladte „nævnere" b kan naturligvis være både positive og ulige, og diskriminanter; det sker præcis, når $b > 0$ og $b \equiv 1 \pmod 4$. For sådanne værdier af b har de to symboler altså samme værdi, og når $b = p$ er et primtal med $p \equiv 1 \pmod 4$, så er begge symboler lig med Legendre-symbolet $\left(\frac{a}{p}\right)$.

For et helt tal $b \neq 0$ kaldes en funktion $\chi : \mathbb{Z} \to \mathbb{C}$ en (restklasse-)*karakter (eller en Dirchlet-karakter) modulo* b, hvis der gælder: (i) værdien $\chi(a)$ afhænger kun af a's restklasse modulo b, (ii) værdien er 0 netop hvis a ikke er primisk med b, og (iii) χ er multiplikativ: $\chi(a_1a_2) = \chi(a_1)\chi(a_2)$. Den sidste betingelse er ensbetydende med at χ, som funktion af de primiske restklasser, er en homomorfi $(\mathbb{Z}/b)^* \to \mathbb{C}^*$. Hvis værdierne kun er 0, 1, og -1, dvs hvis $\chi(a)^2 = 1$ når a er primisk med b, kaldes χ en *kvadratisk karakter*. Egenskaben (1) udtrykker altså, at symbolet $\left(\frac{a}{b}\right)$ som funktion af a er en kvadratisk karakter modulo b.

Ofte betragtes restklassekarakterer med værdier i andre legemer end $\mathbb{C}$. For kvadratiske karakterer er der ingen essentiel forskel, bortset fra at det er uinteressant, hvis legemet har karakteristik 2.

(4.4) Bemærkning. Inden vi beviser Den generelle Reciprocitetssætning, vil vi udlede en række konsekvenser, og vi vil vise, at et symbol med egenskaberne (1) og (2) i sætningen er entydigt fastlagt alene ved værdien $\left(\frac{3}{8}\right)$. Med den sidste værdi lig med $+1$ bestemmes det trivielle symbol, med værdien -1 bestemmes altså udvidelsen af Legendre-symbolet. Som vi skal se, er det nemt ud fra egenskaberne nævnt i sætningen at angive en algoritme, der *beregner* det udvidede symbol $\left(\frac{a}{b}\right)$, men det skal understreges, at algoritmen er aldeles uegnet som *definition* af symbolet; der er næsten ingen af symbolets egenskaber, der direkte fremgår af algoritmen. Fx er det ikke muligt ud fra algoritmen at indse for et ulige primtal p, at det udvidede symbol $\left(\frac{a}{p}\right)$ er lig med Legendre-symbolet. Det udvidede symbol defineres i Afsnit (4.11), og beviserne for Reciprocitetssætningen gives først i de følgende afsnit. De resultater, vi udleder inden, bygger altså alene på *antagelsen* om, at $\left(\frac{a}{b}\right)$ er et symbol med Reciprocitetssætningens egenskaber og med værdien $\left(\frac{3}{8}\right) = -1$.

Generelt gælder, at $\left(\frac{a}{b}\right) = 0$, når a, b ikke er primiske. Derfor er det nok at betragte værdierne $\left(\frac{a}{b}\right)$, når a er primisk med b. Da symbolet er en homomorfi $(\mathbb{Z}/b)^* \to \{\pm 1\}$, gælder altid, at $\left(\frac{aq}{b}\right) = \left(\frac{a}{b}\right)$, når q er et kvadrat (dvs af formen $q = c^2$) primisk med b. Specielt er naturligvis $\left(\frac{1}{b}\right) = 1$ for ethvert „tilladt" b.

For $b = 8$ får vi, under brug af egenskaberne, $\left(\frac{1}{8}\right) = 1$ og $\left(\frac{7}{8}\right) = \left(\frac{8}{7}\right) = \left(\frac{1}{7}\right) = 1$. Da $\left(\frac{a}{8}\right)$ definerer en homomorfi $(\mathbb{Z}/8)^* \to \{\pm 1\}$, og restklassen af 1 og 7 ligger i kernen, må de to andre restklasser, af 3 og af 5, give samme værdi. Da vi antager, at $\left(\frac{3}{8}\right) = -1$, gælder $\left(\frac{3}{8}\right) = \left(\frac{5}{8}\right) = -1$. Med andre ord gælder ligningen $\left(\frac{a}{8}\right) = \chi_8(a)$, hvor $\chi_8(a)$ er homomorfien $(\mathbb{Z}/8)^* \to \{\pm 1\}$ bestemt i tabelllen herunder.

a	1	3	5	7
χ_8	1	-1	-1	1

Videre fremhæver vi, at for *ulige* diskriminanter D gælder ligningen,

$$\left(\frac{a}{D}\right) = \left(\frac{a}{|D|}\right). \tag{4.4.1}$$

Ligningen er naturligvis triviel, hvis D er positiv, så vi antager $D < 0$. Tallet D er en ulige diskriminant, så $D \equiv 1 \pmod 4$. Derfor er $-D > 0$ og $-D \equiv 3 \pmod 4$. Vi kan eventuelt til a lægge et passende multiplum af $-D$, så vi kan antage, at a er positiv og $a \equiv 1 \pmod 4$. Herefter er $\left(\frac{-1}{a}\right) = \left(\frac{-4}{a}\right) = \left(\frac{a}{-4}\right) = \left(\frac{1}{-4}\right) = 1$, og vi får den søgte lighed,

$$\left(\frac{a}{D}\right) = \left(\frac{D}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{-D}{a}\right) = \left(\frac{-D}{a}\right) = \left(\frac{a}{-D}\right).$$

Betragt nu symbolet $\left(\frac{2}{b}\right)$. Hvis b er lige, er værdien 0. Hvis b er ulige og positiv, har vi $\left(\frac{2}{b}\right) = \left(\frac{8}{b}\right) = \left(\frac{b}{8}\right) = \chi_8(b)$, som blev bestemt ovenfor. Hvis b er ulige og negativ, er b nødvendigvis en diskriminant, og derfor er $\left(\frac{2}{b}\right) = \left(\frac{2}{|b|}\right) = \chi_8(|b|)$ ifølge (4.4.1). Øjensynslig gælder for alle a, at $\chi_8(-a) = \chi_8(a)$. Derfor gælder i alle tilfælde, at $\left(\frac{2}{b}\right) = \chi_8(b)$.

Nu er det nemt at se, at følgende algoritme bestemmer symbolet $\left(\frac{a}{b}\right)$ ud fra symbolet $\left(\frac{2}{b}\right)$.

Algoritme. Algoritmen initialiseres med $\mathbf{s} := 1$, $\mathbf{a} := a$ og $\mathbf{b} := b$, hvor b enten er en diskriminant, eller ulige og positiv; registret $\mathbf{s}$ indeholder, når algoritmen stopper, værdien af symbolet $\left(\frac{a}{b}\right)$.
(0) Hvis $\mathbf{a}$ og $\mathbf{b}$ begge er lige, så sæt $\mathbf{s} := 0$ og STOP.
(1) Hvis $\mathbf{b} = 1$, så STOP.
(2) Bestem den principale rest r af $\mathbf{a}$ ved division med $\mathbf{b}$, altså $\mathbf{a} = q\mathbf{b} + r$ med $0 \leqslant r < |\mathbf{b}|$. Hvis $r = 0$, så sæt $\mathbf{s} := 0$ og STOP. Ellers sættes $\mathbf{a} := r$.
(3) Faktoriser den største potens af 2: skriv $\mathbf{a} = 2^\nu u$, hvor u er ulige (og positiv). Sæt $\mathbf{a} := u$. Hvis ν er ulige, så sæt $\mathbf{s} := \mathbf{s} * \left(\frac{2}{\mathbf{b}}\right)$.
(4) Hvis $\mathbf{b} \equiv 3 \pmod 4$, så sæt $\mathbf{b} := -\mathbf{b}$.
(5) Ombyt og gentag: Sæt $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a})$, og GOTO (1).

Bemærk, at algoritmen, bortset fra særbehandlingen af primtallet 2, essentielt er Euklid's algoritme til bestemmelse af den største fælles divisor for a og b.

(4.5) Formler. Symbolet i Reciprocitetssætningen er ikke-trivielt, og det medfører som nævnt, at $\left(\frac{2}{b}\right)$ må antage værdien -1. Ifølge udregningen i (4.4) er det ækvivalent med, at $\left(\frac{3}{-4}\right) = -1$. Herefter er $\left(\frac{a}{-4}\right)$ den ikke-trivielle homomorfi $(\mathbb{Z}/4)^* \to \{\pm 1\}$. For ulige, positive tal u har vi $\left(\frac{-1}{u}\right) = \left(\frac{-4}{u}\right) = \left(\frac{u}{-4}\right)$, altså

$$\left(\frac{-1}{u}\right) = \left(\frac{u}{-4}\right) = \begin{cases} 1 & \text{hvis } u \equiv 1 \pmod 4, \\ -1 & \text{hvis } u \equiv 3 \pmod 4. \end{cases} \tag{4.5.1}$$

Videre er $\left(\frac{2}{u}\right) = \left(\frac{8}{u}\right) = \left(\frac{u}{8}\right)$, og, som vi har set i (4.4),

$$\left(\frac{2}{u}\right) = \left(\frac{u}{8}\right) = \begin{cases} 1, & \text{hvis } u \equiv \pm 1 \pmod 8, \\ -1, & \text{hvis } u \equiv \pm 3 \pmod 8. \end{cases} \tag{4.5.2}$$

Endelig fremhæver vi, at for primiske, positive, ulige tal u, v er

$$\left(\frac{v}{u}\right) = \begin{cases} \left(\frac{u}{v}\right), & \text{når } u \text{ eller } v \text{ er } \equiv 1 \pmod 4, \\ -\left(\frac{u}{v}\right), & \text{når } u \text{ og } v \text{ er } \equiv 3 \pmod 4. \end{cases} \tag{4.5.3}$$

I det første tilfælde kan vi nemlig antage, at $u \equiv 1 \pmod 4$, og så følger resultatet direkte af (4.3.1). I det andet tilfælde er $u \equiv 3 \pmod 4$. Følgelig er $-u \equiv 1 \pmod 4$, så $-u$ er en ulige diskriminant. Af (4.4.1) ses, at $\left(\frac{v}{u}\right) = \left(\frac{v}{-u}\right)$, og så er

$$\left(\frac{v}{u}\right) = \left(\frac{v}{-u}\right) = \left(\frac{-u}{v}\right) = \left(\frac{-1}{v}\right)\left(\frac{u}{v}\right) = -\left(\frac{u}{v}\right),$$

idet det sidste lighedstegn følger af (4.5.1), da $v \equiv 3 \pmod 4$.

(4.6) Eksempel. Af (4.5.2) fås $\left(\frac{2}{15}\right) = 1$, $\left(\frac{2}{7}\right) = 1$, og $\left(\frac{2}{3}\right) = -1$; algoritmen giver altså

$$\begin{aligned} \left(\frac{15}{89}\right) &= \left(\frac{89}{15}\right) = \left(\frac{14}{15}\right) = \left(\frac{2}{15}\right)\left(\frac{7}{15}\right) = 1 \cdot \left(\frac{-15}{7}\right) \\ &= \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = 1 \cdot \left(\frac{-7}{3}\right) = \left(\frac{2}{3}\right) = -1. \end{aligned}$$

Inddrages (4.5.1) fås mere direkte: $\left(\frac{15}{89}\right) = \left(\frac{89}{15}\right) = \left(\frac{-1}{15}\right) = -1$.

(4.7) Bemærkning. Det skal understreges, at de tre formler i (4.5) er udledt som konsekvenser af egenskaberne ved det generelle symbol $\left(\frac{a}{b}\right)$. Vi har endnu ikke defineret symbolerne, og altså slet ikke bevist formlerne. De tre formler, for ulige primtal $u = p$ og $v = q$, udgør *Gauss's Reciprocitetsformler*. De vedrører alene Legendre-symbolet, og vi giver et af beviserne for dem inden vi definerer det generelle symbol; de er essentielle i det første bevis for Den generelle Reciprocitetssætning, men ikke i det andet.

(4.8) Bemærkning. Det fremgår af (4.2), at for et ulige primtal p er Legendre-symbolet $\left(\frac{a}{p}\right)$ en ikke-triviel, kvadratisk karakter modulo p. Den betegnes også χ_p. Det er i øvrigt den eneste ikke-trivielle, kvadratiske karakter modulo p. For en kvadratisk karakter $\chi : (\mathbb{Z}/p)^* \to \{\pm 1\}$ er jo $\chi(x^2) = \chi(x)^2 = 1$. Kernen for χ vil derfor indeholde alle kvadrater. Da kvadraterne udgør en undergruppe af index 2, vil kernen for χ altså enten bestå af kvadraterne (og så er $\chi = \chi_p$) eller den vil være hele $(\mathbb{Z}/p)^*$ (og så er $\chi = \chi_1$ den trivielle karakter modulo p).

For $n = 2$ er der kun én kvadratisk karakter modulo n, idet der kun er én primisk restklasse modulo 2. For $n = 4$ har vi to primiske restklasser, nemlig 1 og -1, så der er én ikke-triviel karakter. Det er øjensynlig karakteren defineret ved højresiden af (4.5.1); vi betegner den χ_{-4}. For $n = 8$ er der fire primiske restklasser, ± 1 og ± 3. Gruppen $(\mathbb{Z}/8)^*$ er Klein's Vierer-gruppe, idet alle ulige kvadrater modulo 8 er kongruente med 1. Udover den trivielle karakter χ_1 er der er altså 3 ikke-trivielle karakterer modulo 8. Den ene er øjensynlig χ_{-4}. En anden er karakteren defineret ved højresiden af (4.5.2); den betegnede vi χ_8. Den tredie er herefter produktet $\chi_{-4}\chi_8$, som vi betegner χ_{-8}. De fire karakterer er bestemt ved tabellen,

a	1	3	5	7
χ_1	1	1	1	1
χ_{-4}	1	-1	1	-1
χ_8	1	-1	-1	1
χ_{-8}	1	1	-1	-1

(4.9) Gauss's Lemma. *Lad p være et ulige primtal, og antag, at p ikke går op i a. Da er*

$$\left(\frac{a}{p}\right) = (-1)^n, \tag{4.9.1}$$

hvor n er antallet af negative blandt de numerisk mindste rester modulo p af tallene xa for $1 \leqslant x \leqslant (p-1)/2$.

Bevis. Tallene xa for $1 \leqslant x \leqslant (p-1)/2$ er ikke delelige med p, så deres numerisk mindste rester er tal r med $1 \leqslant |r| \leqslant (p-1)/2$. Betragt to tal x_1 og x_2 med $1 \leqslant x_1, x_2 \leqslant (p-1)/2$, og lad r_1 og r_2 være de numerisk mindste rester af $x_1 a$ og $x_2 a$. Antag, at $|r_1| = |r_2|$. Modulo p er så $0 = r_1 \pm r_2 \equiv (x_1 \pm x_2)a$; da $|x_1 \pm x_2| \leqslant p - 1$, følger det først, at $x_1 \pm x_2 = 0$, og dernæst, at $x_1 = x_2$.

De numeriske værdier af de numerisk mindste rester af tallene xa for $1 \leqslant x \leqslant (p-1)/2$ er altså forskellige. Der er $(p-1)/2$ tal og $(p-1)/2$ muligheder for de numeriske værdier. De numeriske værdier må derfor være tallene $1, 2, \ldots, (p-1)/2$. Produktet af de numerisk mindste rester er derfor $1 \cdot 2 \cdots (p-1)/2$ multipliceret med $(-1)^n$, hvor n er antallet af negative faktorer. Modulo p har vi derfor kongruensen,

$$1a \cdot 2a \cdots \tfrac{p-1}{2}a \equiv (-1)^n 1 \cdot 2 \cdots \tfrac{p-1}{2},$$

og heraf følger $a^{(p-1)/2} \equiv (-1)^n$. Ligning (4.9.1) følger nu af Euler's Kriterium (4.2.1). ◻

(4.10) Gauss's Reciprocitetsformler. *For ulige primtal p, q gælder følgende formler for Legendre-symbolet:*

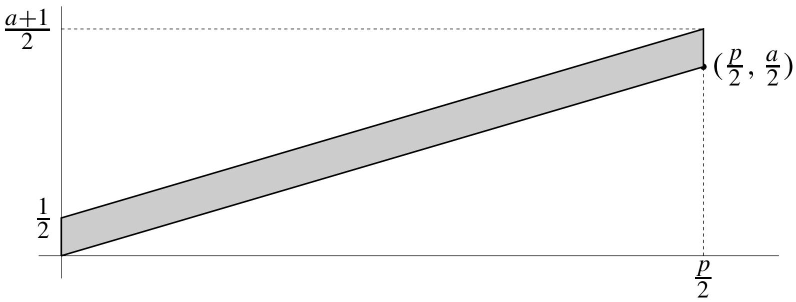
$$\left(\frac{-1}{p}\right) = \chi_{-4}(p) = \bigl(-1\bigr)^{(p-1)/2}, \quad \left(\frac{2}{p}\right) = \chi_8(p) = \bigl(-1\bigr)^{(p^2-1)/8}, \quad \left(\frac{p}{q}\right) = \pm\left(\frac{q}{p}\right);$$

fortegnet i den sidste formel er -1, hvis $p \equiv q \equiv 3 \pmod 4$, og ellers $+1$ (og i øvrigt bestemt ved $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$).

Bevis. En geometrisk fortolkning af tallet n i Gauss's Lemma (4.9) fås på følgende måde: Øjensynlig er n antallet af tal x, med $1 \leqslant x \leqslant (p-1)/2$, for hvilke der findes et tal y med $-(p-1)/2 \leqslant xa - yp \leqslant -1$. Et sådant y er entydigt bestemt. Da p er ulige, er ulighederne for y ensbetydende med at $-p/2 < xa - yp < 0$. Tallet n er altså antallet af heltalspar (x, y) (gitterpunkter), som opfylder ulighederne,

$$0 < x < \tfrac{p}{2}, \qquad \tfrac{a}{p}x < y < \tfrac{a}{p}x + \tfrac{1}{2}.$$

Ulighederne bestemmer et parallellogram i planen:

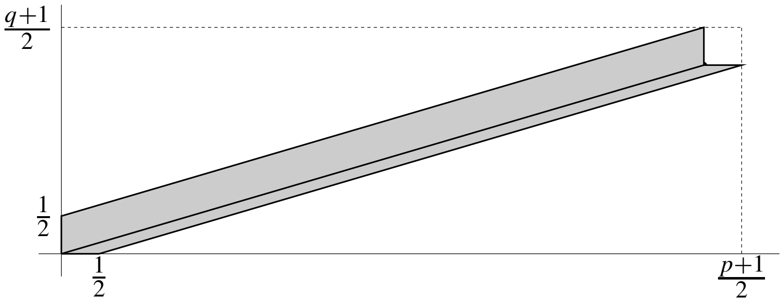


og tallet n er altså antallet af gitterpunkter i det indre af parallellogrammet.

Den sidste reciprocitetsformel er ækvivalent med ligningen,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \bigl(-1\bigr)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{4.10.1}$$

Ifølge Gauss's Lemma er venstresiden $(-1)^{n+m}$, hvor n er antallet af gitterpunkter i parallellogrammet ovenfor, med $a := q$, og m er antallet af gitterpunkter i et tilsvarende parallellogram. Spejles dette sidste parallellogram i linien $x = y$ ses, at $n + m$ er antallet af gitterpunkter i det indre af den markerede figur herunder (da p og q er primiske, er der ingen gitterpunkter på linien fra $(0, 0)$ til $(p/2, q/2)$).

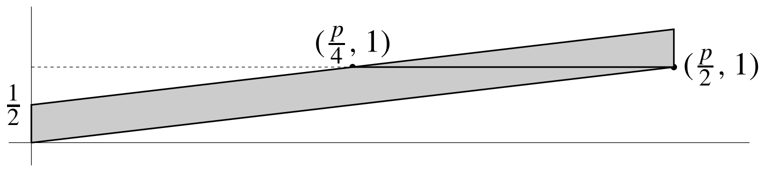


Det (åbne) rektangel består af den markerede figur, to trekanter, og et kvadrat med sidelængde $\frac{1}{2}$. I kvadratet findes ingen gitterpunkter. De to trekanter er kongruente, og indeholder derfor samme antal gitterpunkter. Modulo 2 er antallet, $n+m$, af gitterpunkter i den markerede figur altså lig med antallet af gitterpunkter i det åbne rektangel, dvs lig med $\frac{p-1}{2}\frac{q-1}{2}$. Heraf følger øjensynlig Formel (4.10.1).

Den mellemste reciprocitetsformel er ligningen,

$$\left(\frac{2}{p}\right) = \chi_8(p). \tag{4.10.2}$$

Ifølge Gauss's Lemma er $\left(\frac{2}{p}\right) = (-1)^n$, hvor n er antallet af gitterpunkter i det indre af parallellogrammet (med $a := 2$):



I parallellogrammet er der øjensynlig kun gitterpunkter på linien, hvor $y = 1$, og antallet er $n = [\frac{p}{2}] - [\frac{p}{4}]$. Øjensynlig er

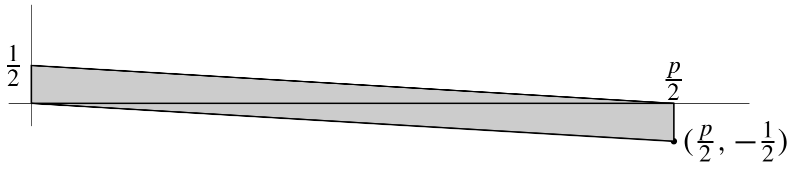
$$\left[\frac{p}{2}\right] - \left[\frac{p}{4}\right] = \begin{cases} 4h - 2h = 2h, & \text{hvis } p = 8h+1, \\ (4h-1) - (2h-1) = 2h, & \text{hvis } p = 8h-1, \\ (4h+1) - 2h = 2h+1, & \text{hvis } p = 8h+3, \\ (4h-2) - (2h-1) = 2h-1, & \text{hvis } p = 8h-3. \end{cases}$$

Heraf ses, at $(-1)^n = \chi_8(p)$, hvormed (4.10.2) er bevist.

Betragt endelig den første reciprocitetsformel,

$$\left(\frac{-1}{p}\right) = \chi_{-4}(p). \tag{4.10.3}$$

Da p er ulige, er $\chi_{-4}(p) = (-1)^{(p-1)/2}$. Formlen følger derfor umiddelbart af Euler's Kriterium (4.2.1). Dette kriterium indgik også i beviset for Gauss's Lemma. Lad os alligevel bemærke, at Gauss's Lemma medfører (4.10.3). Vi har $\left(\frac{-1}{p}\right) = (-1)^n$, hvor n antallet af gitterpunkter i det indre af parallellogrammet (med $a := -1$):



Her er der kun gitterpunkter på linien hvor $y = 0$, og antallet er $n = [\frac{p}{2}] = (p-1)/2$.

Hermed er Gauss's reciprocitetsformler bevist. ▯

(4.11) Definition. Legendre-symbolet udvides til det generelle symbol $\left(\frac{a}{b}\right)$ nævnt i Sætning (4.3) på følgende måde: *Jacobi-symbolet* $\left(\frac{a}{u}\right) = \chi_u(a)$ (hvor u er ulige og positiv) gives værdien 0, hvis a, u ikke er primiske. I almindelighed betragtes en „primopløsning" af u:

$$u = (\text{kvadrat}) \cdot p_1 \cdots p_r, \tag{4.11.1}$$

med forskellige ulige primtal p_j. Når $(a, u) = 1$, defineres $\left(\frac{a}{u}\right)$ som produktet af værdierne af Legendre-symbolerne $\left(\frac{a}{p_j}\right)$.

Et tal D kaldes en *primdiskriminant*, hvis enten $D = p$ er et primtal kongruent med 1 modulo 4, eller $D = -p$, hvor p er et primtal kongruent med 3 modulo 4, eller D er et af tallene -4, 8, -8. For et ulige tal u sætter vi $u^* = (-1)^{(u-1)/2}u$. De ulige primdiskriminanter er altså tallene af formen p^*, hvor p er et ulige primtal, og de lige primdiskriminanter er tallene 2^*, hvor 2^* (aldeles upræcist) betegner et af tallene -4, 8, -8.

Kronecker-symbolet $\left(\frac{a}{D}\right) = \chi_D(a)$ (hvor D er en diskriminant) gives værdien 0, hvis a, D ikke er primiske. For en primdiskriminant p^* defineres symbolet ved ligningerne,

$$\left(\frac{a}{p^*}\right) := \chi_p(a), \quad \left(\frac{a}{-4}\right) := \chi_{-4}(a), \quad \left(\frac{a}{8}\right) := \chi_8(a), \quad \left(\frac{a}{-8}\right) := \chi_{-8}(a).$$

I den første ligning er p et ulige primtal, og $\chi_p(a)$ er Legendre-symbolet. Karaktererne $\chi_{-4}, \chi_8, \chi_{-8}$ er beskrevet i (4.8) for ulige a; de gives værdien 0, når a er lige. Enhver diskriminant D kan entydigt faktoriseres:

$$D = (\text{kvadrat}) \cdot p_1^* \cdots p_t^*, \tag{4.11.2}$$

hvor faktorerne p_i^* er forskellige primdiskriminanter og højst én er lige. Når $(a, D) = 1$, defineres $\left(\frac{a}{D}\right)$ som produktet af værdierne af symbolerne $\left(\frac{a}{p_i^*}\right)$.

(4.12) Første bevis for Den generelle Reciprocitetssætning. Det skal vises, at det udvidede symbol har egenskaberne (1) og (2) i (4.3). Egenskaben (1) er triviel, idet $\left(\frac{a}{b}\right)$, ud fra primopløsningen af b, er defineret som et produkt af karakterer. Betragt Reciprocitetsformlen (4.3.1). Skriv D som produkt på formen i (4.11.2), og skriv u som produkt af formen i (4.11.1). Begge sider af formlen er 0, hvis D og u ikke er primiske, så vi kan antage, at D og u er primiske. Under brug af de multiplikative egenskaber ses, at det er nok at vise formlen når $u = p$ er et ulige primtal og $D = q^*$ er en primdiskriminant. Det skal altså vises, når p ikke går op i q^*, at

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q^*}\right).$$

Denne ligning følger let af Gauss's tre Reciprocitetsformler: Med $q^* = -4$ er $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = \chi_{-4}(p)$; med $q^* = 8$ er $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right) = \chi_8(p)$; med $q^* = -8$ er $\left(\frac{-8}{p}\right) = \left(\frac{-4}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \chi_{-4}(p)\chi_8(p) = \chi_{-8}(p)$. og med et ulige primtal q er $\left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{(q-1)/2}q}{p}\right) = \left(\frac{-1}{p}\right)^{(q-1)/2}\left(\frac{q}{p}\right) = \left((-1)^{(p-1)/2}\right)^{(q-1)/2}\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \chi_q(p)$. □

(4.13) Tilføjelse. *Jacobi-symbolet $\left(\frac{a}{u}\right)$, for ulige positive u, er også multiplikativt i u, og der gælder formlerne:*

$$\left(\frac{-1}{u}\right) = \chi_{-4}(u) = \left(-1\right)^{(u-1)/2},$$
$$\left(\frac{2}{u}\right) = \chi_8(u) = \left(-1\right)^{(u^2-1)/8},$$
$$\left(\frac{u_1}{u_2}\right) = \pm\left(\frac{u_2}{u_1}\right),$$

hvor fortegnet i den sidste formel er -1, hvis $u_1 \equiv u_2 \equiv 3 \pmod 4$, og ellers $+1$.

Kronecker-symbolet $\left(\frac{a}{D}\right)$, for diskriminanter D, er også multiplikativt i D, og der gælder formlerne:

$$\left(\frac{-1}{D}\right) = \begin{cases} 1 & \text{når } D > 0, \\ -1 & \text{når } D < 0. \end{cases} \tag{4.13.1}$$
$$\left(\frac{2}{D}\right) = \chi_8(D) = \left(-1\right)^{(D^2-1)/8}, \quad \text{når } D \text{ er ulige}, \tag{4.13.2}$$
$$\left(\frac{D_1}{D_2}\right) = \pm\left(\frac{D_2}{D_1}\right), \tag{4.13.3}$$

hvor fortegnet i den sidste formel er -1, hvis D_1 og D_2 begge er negative, og ellers $+1$.

Bevis. Det følger umiddelbart af definitionen, at Jacobi-symbolet er multiplikativt i u, og formlerne for Jacobi-symbolet blev vist i (4.5).

For at vise, at Kronecker-symbolet er multiplikativt,

$$\left(\frac{a}{D_1 D_2}\right) = \left(\frac{a}{D_1}\right)\left(\frac{a}{D_2}\right), \tag{4.13.4}$$

bemærkes, at opløsningen (4.11.2) for $D_1 D_2$ fås udfra de tilsvarende opløsninger af D_1 og D_2. Det skal vises, at hver primdiskriminant p^*, som forekommer i D_1 og/eller D_2, bidrager med samme faktor på begge sider af (4.13.4). Det er trivielt for en ulige primdiskriminant. For en lige primdiskriminant reduceres til tilfældet, hvor D_1 og D_2 er lige og forskellige primdiskriminanter. Mulighederen for $D_1 D_2$ er så essentielt følgende:

$$(-4)\cdot 8 = (2^2)\cdot(-8), \qquad (-4)\cdot(-8) = (2^2)\cdot 8, \qquad 8\cdot(-8) = 4^2\cdot(-4);$$

den påståede ligning (4.13.4) reduceres til definitionen: $\chi_{-8} = \chi_{-4}\chi_8$.

Betragt ligning (4.13.1). Begge sider er multiplikative i D, så det er nok at vise ligningen, når D er en primdiskriminant. Når $D = p \equiv 1 \pmod 4$, er begge sider 1. Når $D = -p \equiv 3 \pmod 4$, er begge sider lig med -1. Endelig, for en lige primdiskriminant følger påstanden af at $\chi_8(-1) = 1$ og $\chi_{-4}(-1) = \chi_{-8}(-1) = -1$.

I (4.13.2) er D en ulige diskriminant. Under brug af (4.4.1) får vi,

$$\left(\frac{2}{D}\right) = \left(\frac{8}{D}\right) = \left(\frac{8}{|D|}\right) = \left(\frac{|D|}{8}\right) = \chi_8(|D|) = \chi_8(D);$$

i den sidste ligning er det brugt, at $\chi_8(a) = \chi_8(-a)$ for alle a.

Endelig, i ligning (4.13.3) er begge sider 0, hvis D_1 og D_2 ikke er primiske. Antag altså, at D_1 og D_2 er primiske. Specielt er så et af tallene D_1 og D_2 ulige. Af symmetrigrunde kan vi antage, at D_2 er ulige. Under brug af (4.4.1) får vi,

$$\left(\frac{D_1}{D_2}\right) = \left(\frac{D_1}{|D_2|}\right) = \left(\frac{|D_2|}{D_1}\right).$$

Hvis D_2 er positiv, er dette den søgte formel. Hvis $D_2 < 0$, er højresiden lig med $\left(\frac{-D_2}{D_1}\right) = \left(\frac{-1}{D_1}\right)\left(\frac{D_2}{D_1}\right)$, og nu følger den søgte formel af (4.13.1). □

(4.14) Alternativt bevis. I det foregående har vi set, hvordan Gauss's Reciprocitetsformler, der kun vedrører Legendre-symbolet $\left(\frac{a}{p}\right)$, næsten umiddelbart medfører Den generelle Reciprocitetssætning (4.3), så snart det generelle symbol $\left(\frac{a}{b}\right)$ er defineret,

I det følgende giver vi et alternativt bevis for Den generelle Reciprocitetssætning, hvor det fundamentale skridt er et direkte bevis for følgende ligning (hvor p er et ulige primtal, og D er en „kvadratfri" diskriminant (dvs af formen $D = q_1^* \cdots q_t$, hvor $q_1^*, \dots, q_t^*$ er parvis primiske primdiskriminanter):

$$\left(\frac{D}{p}\right) = \chi_D(p); \tag{4.14.1}$$

venstresiden er altså Legendre-symbolet og højresiden er Kronecker-symbolet. Med valgene $D = -4$, $D = 8$, og $D = q^*$ med et ulige primtal q, følger Gauss's reciprocitetsformler af (4.14.1). Det er altså nok at vise (4.14.1). Beviset bygger på egenskaber ved Gauss-summer dannet i endelige legemer.

(4.15) Gauss-summer. Vi betragter et helt generelt 'setup': Der er givet et naturligt tal n, og et legeme L, hvis karakteristik ikke er divisor i n; i den klassiske sitation er $L = \mathbb{C}$, men i vores anvendelse vil L faktisk være et endeligt legeme af karakteristik p, hvor $p \nmid n$. Videre er der givet en generel Dirichlet-karakter (dvs en homomorfi) $\chi\colon (\mathbb{Z}/n)^* \to L^*$ og en n'te enhedsrod $\zeta \in L$.

Under disse generelle forudsætninger defineres den tilhørende *Gauss-sum* $\tau := \tau(\chi, \zeta)$ som summen,

$$\tau(\chi, \zeta) := \sum_{a \bmod^* n} \chi(a)\zeta^a,$$

hvor notationen indikerer, at index a gennemløber et repræsentantsystem for de *primiske* restklasser modulo n. Gauss-summen τ er naturligvis element i det givne legeme L.

For hver divisor $d \mid n$ har vi en veldefineret homomorfi,

$$(\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*, \tag{4.15.1}$$

der afbilder restklassen af a modulo n på restklassen af a modulo d. Homomorfiens kerne $U = U(d) \subseteq (\mathbb{Z}/n)^*$ består af de primiske restklasser af a modulo n, som opfylder $a \equiv 1 \pmod{d}$. Det er ikke svært at vise, at homomorfien er surjektiv. De to grupper har ordner $\varphi(n)$ og $\varphi(d)$, så homomorfiens kerne har orden $\varphi(n)/\varphi(d)$.

Karakteren $\chi\colon (\mathbb{Z}/n)^* \to L^*$ siges at være *induceret* af en karakter modulo d, hvis der findes en karakter $\widehat{\chi}\colon (\mathbb{Z}/d)^* \to L^*$ således, at $\chi([a]_n) = \widehat{\chi}([a]_d)$ for tal a, der er primiske med n. Fx er den *trivielle karakter* $\chi_1\colon (\mathbb{Z}/n)^* \to L^*$, bestemt ved $\chi_1(a) = 1$ for alle tal a primiske med n, induceret af en karakter modulo 1. Da homomorfien $(\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*$ er surjektiv, følger det af Homomorfisætningen, at χ induceres af en karakter modulo d, hvis og kun hvis $\chi(a) = 1$ for alle restklasser $a \in U(d)$. Karakteren χ kaldes *primitiv*, hvis den ikke induceres af en karakter modulo d med en divisor $d < n$.

(4.16) Lemma. (1) *Antag, at $\chi\colon (\mathbb{Z}/n)^* \to L^*$ er en Dirichlet-karakter. Da er*

$$\sum_{a \bmod^* n} \chi(a) = \begin{cases} \varphi(n), & \text{hvis } \chi(a) = 1 \text{ for alle } a \in (\mathbb{Z}/n)^*, \\ 0, & \text{ellers.} \end{cases} \tag{4.16.1}$$

(2) *Antag, at $\zeta \in L^*$ har orden n. Lad h være et helt tal, og sæt $k := (n, h)$. Da er*

$$\sum_{a \bmod^* n} \zeta^{ah} = \frac{\varphi(n)}{\varphi(n/k)} \mu(n/k) = \sum_{d\,|\,k} \mu(n/d)\, d. \tag{4.16.2}$$

Bevis. (1) Den første ligning gælder for en vilkårlig homomorfi $\chi\colon G \to L^*$, hvor G er en endelig kommutativ gruppe:

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{hvis } \chi(g) = 1 \text{ for alle } g \in G, \\ 0, & \text{ellers.} \end{cases}$$

Tallet $|G|$ på højresiden skal naturligvis fortolkes som tallet gange et-elementet i legemet; det er øjensynlig lig med summen på venstresiden, når χ er den trivielle homomorfi $\chi(g) = 1$ for alle $g \in G$. Hvis χ er ikke-triviel, findes et element $g_0 \in G$ med $\chi(g_0) \neq 1$. Når g gennemløber G, vil også $g_0 g$ gennemløbe G, og derfor er $\sum_g \chi(g) = \sum_g \chi(g_0 g) = \chi(g_0) \sum_g \chi(g)$. Altså er $(1 - \chi(g_0)) \sum_g \chi(g) = 0$. I legemet L gælder specielt nulreglen. Følgelig er $\sum_g \chi(g) = 0$.

(2) Enhedsroden ζ har orden n, og frembringer derfor i L^* en cyklisk undergruppe af orden n. Heraf følger som bekendt, at ζ^h har orden $e := n/k$, hvor $k := (n, h)$. Når a gennemløber de primiske restklasser modulo n, vil ζ^a gennemløbe de primitive n'te enhedsrødder, og $(\zeta^h)^a$ vil gennemløbe de primitive e'te enhedsrødder, idet hver rammes $\varphi(n)/\varphi(e)$ gange. Derfor er $\sum_{a \bmod^* n} \zeta^{ha}$ lig med $\varphi(n)/\varphi(e)$ gange summen af de primitive e'te enhedsrødder; den sidste sum er som bekendt lig med $\mu(e)$. Hermed er den første ligning i (4.16.2) bevist.

Den anden ligning i (4.16.2) er en ligning mellem hele tal. Ligningen gælder for naturlige tal n, k med $k\,|\,n$. Med $n = ek$ har ligningen følgende form:

$$\frac{\varphi(ek)}{\varphi(e)} \mu(e) = \sum_{d\,|\,k} \mu\Big(e\, \frac{k}{d}\Big) d. \tag{4.16.3}$$

Vi omformer ligningens venstreside (vs) og højreside (hs) hver for sig. I argumentet skal vi gentagne gange udnytte, at $\mu(m) = 0$, hvis argumentet m *ikke* er *kvadratfrit*, dvs når m er deleligt med et kvadrat større end 1.

Betragt for de givne tal k, e den naturlige fremstilling af k som et produkt $k = e'm$, bestemt ved at alle primdivisorer i e' går op i e og ingen primdivisorer i m går op i e. Af egenskaben ved e' følger, at $\varphi(ee') = e'\varphi(e)$, og af egenskaben ved m følger, at m er primisk med e og med e'. Specielt, da $\varphi(n)$ er multiplikativ, følger det, at $\varphi(ek) = \varphi(ee'm) = e'\varphi(e)\varphi(m)$. Altså får vi for venstresiden:

$$\text{vs} = \frac{\varphi(ek)}{\varphi(e)}\mu(e) = e'\varphi(m)\mu(e).$$

På højresiden i (4.16.3) er summen over divisorerne d i $k = e'm$. Da e', m er primiske, har divisorerne formen $d = bc$, hvor $b \,|\, e'$ og $c \,|\, m$. Altså er

$$\text{hs} = \sum_{d\,|\,k} \mu\Big(e\,\frac{k}{d}\Big)d = \sum_{b\,|\,e',\,c\,|\,m} \mu\Big(e\,\frac{e'}{b}\,\frac{m}{c}\Big)bc.$$

Tallet e'/b er divisor i e', og hver primdivisor i e' er divisor i e. Heraf følger, at produktet $e(e'/b)(m/c)$ kun kan være kvadratfrit, når $b = e'$. I den sidste sum ovenfor er det altså kun leddene svarende til $b = e'$, der kan være forskellige fra 0. Medtages kun disse led, får vi forenklingen:

$$\text{hs} = \sum_{c\,|\,m} \mu\Big(e\,\frac{m}{c}\Big)e'c = e'\mu(e)\sum_{c\,|\,m}\mu\Big(\frac{m}{c}\Big)c;$$

det sidste lighedstegn følger af, at μ er multiplikativ og e er primisk med m/c. Det følger af Möbius's Inversionsformel, at summen ovenfor er lig med $\varphi(m)$. Følgelig er vs = hs, som ønsket. □

(4.17) Sætning. *Antag, at karakteren $\chi : (\mathbb{Z}/n)^* \to L^*$ er primitiv og at den n'te enhedsrod $\zeta \in L^*$ er primitiv. Betragt Gauss-summerne $\tau := \tau(\chi, \zeta)$ og $\tau^* := \tau(\chi^{-1}, \zeta^{-1})$. Da gælder $\tau\tau^* = n$.*

Bevis. Betragt produktet $\tau\tau^*$ af de to Gauss-summer. Når a, b gennemløber alle par af primiske restklasser, vil ba, b gennemløbe de samme par. Derfor kan vi omforme:

$$\tau\tau^* = \sum_{a,b \bmod^* n} \chi(a)\chi(b)^{-1}\zeta^{a-b} = \sum_{a,b \bmod^* n} \chi(ab)\chi(b)^{-1}\zeta^{ba-b} = \sum_{a \bmod^* n}\chi(a)\sum_{b \bmod^* n}\zeta^{b(a-1)}.$$

Den inderste sum for fast a kan vi beregne ved hjælp af (4.16.2) med $h := a - 1$. Vi får

$$\sum_{b \bmod^* n} \zeta^{b(a-1)} = \sum_{d\,|\,n,\,d\,|\,a-1} \mu(n/d)\,d.$$

Altså er

$$\tau\tau^* = \sum_{a \bmod^* n} \chi(a) \sum_{d\,|\,n,\,d\,|\,a-1} \mu(n/d)\,d.$$

Vi ombytter summationsrækkefølgen og summerer yderst over $d\,|\,n$ og inderst, for fast d, over de primiske restklasser a modulo n, som opfylder, at $d\,|\,a-1$, altså at $a \equiv 1 \pmod{d}$. Disse restklasser udgør netop kernen $U(d)$ for den naturlige homomorfi $(\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*$. Derfor får vi:

$$\tau\tau^* = \sum_{d|n} \sum_{a \in U(d)} \chi(a)\mu(n/d)\, d.$$

For fast d bestemmes summen $\sum_{a\in U(d)} \chi(a)$ ved hjælp af (4.16.1): Restriktionen af χ til $U(d)$ er en homomorfi $U(d) \to L^*$; da χ er antaget primitiv, kan restriktionen kun være triviel, hvis $d = n$. Derfor er summen lig med 0 med mindre $d = n$. I summen ovenfor er der altså kun bidrag for $d = n$; her er $U(n) = \{1\}$, og det giver øjensynlig ligningen $\tau\tau^* = n$. ▯

(4.18) Korollar. *Antag under forudsætningerne i* (4.17)*, at karakteren χ er kvadratisk, dvs at χ^2 er konstant* 1*. Da gælder for kvadratet på Gauss-summen $\tau := \tau(\chi, \zeta)$, at $\tau^2 = \chi(-1)n$.*

Antag specielt, at $\chi = \chi_D$ er Kronecker-symbolet hørende til en diskriminant D, der er et produkt af parvis primiske primdiskriminanter, og at L er et legeme, som indeholder en primitiv n'te enhedsrod ζ, hvor $n = |D|$. Da gælder for kvadratet på Gauss-summen $\tau := \tau(\chi_D, \zeta) \in L$, at $\tau^2 = D$.

Bevis. Da χ er kvadratisk, er $\chi(a)^{-1} = \chi(a)$. Når a gennemløber de primiske restklasser modulo n, vil $-a$ gennemløbe de samme restklasser, og $\chi(-a) = \chi(-1)\chi(a)$. Altså er

$$\tau^* = \sum_{a \bmod^* n} \chi(a)\zeta^{-a} = \sum_{a \bmod^* n} \chi(-1)\chi(a)\zeta^{a} = \chi(-1)\,\tau,$$

og dermed er $\tau = \chi(-1)\tau^*$. Af Sætningen fås så, at $\tau^2 = \chi(-1)\tau\tau^* = \chi(-1)n$.

Det er let at se, under forudsætningerne om D, at Kronecker-symbolet χ_D er en primitiv karakter modulo $n = |D|$. Videre er $\chi_D(-1) = \operatorname{sign} D$. Dette er indholdet af ligning (4.13.1); af beviset i (4.13) fremgår, at ligningen alene følger af Euler's Kriterium (og et blik på karaktererne χ_{-4}, χ_8, χ_{-8}. Altså er $\chi_D(-1)n = (\operatorname{sign} D)\,|D| = D$. Den sidste ligning i Korollaret er altså et specialtilfælde af den første. ▯

(4.19) Bemærkning. En karakter χ er en homomorfi fra en endelig gruppe, så hver værdi $\chi(a)$ er enhedsrod (fordi a har endelig orden).

Betragt det komplekse tilfælde, altså $L = \mathbb{C}$. Af $z^n = 1$ følger $|z|^n = 1$, så hver enhedsrod har numerisk værdi 1. Den inverse til en enhedsrod er altså det komplekst konjugerede tal. Det følger specielt, at $\chi(a)^{-1} = \overline{\chi(a)}$ og $\zeta^{-1} = \overline{\zeta}$. Gauss-summen τ^* er altså det komplekst konjugerede tal $\bar{\tau}$. Derfor er $\tau\tau^* = |\tau|^2$. Under forudsætningerne i (4.17) gælder altså, at $|\tau| = \sqrt{n}$.

For en kvadratisk karakter χ gælder, under forudsætningerne i (4.18), at $\tau^2 = \chi(-1)n$. Hvis $\chi(-1) = 1$, må der altså gælde $\tau = \pm\sqrt{n}$ og hvis $\chi(-1) = -1$ må der gælde $\tau = \pm i\sqrt{n}$. Fortegnene afhænger af valget af enhedsrod. For den „kanoniske" n'te enhedsrod $\zeta_n := e^{2\pi i/n}$, og Kronecker-karakteren χ_D hørende til en primdiskriminant, kan man vise, at fortegnet altid er $+1$. For de lige primdiskrimanenter -4, 8 og -8 er det naturligvis en triviel udregning. For en ulige primdiskriminant $p^* = (-1)^{(p-1)/2}p$ er karakteren Legendresymbolet χ_p, og resultatet er ganske dybtliggende:

$$\tau(\chi_p, \zeta_p) = \begin{cases} \sqrt{p} & \text{når } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{når } p \equiv 3 \pmod 4. \end{cases}$$

(4.20) Andet bevis for Reciprocitetssætningen. Som nævnt i (4.14) er det nok at vise, for et ulige primtal p og en diskriminant D, der er et produkt af parvis primiske primdiskriminanter, at $\chi_D(p) = \left(\frac{D}{p}\right)$. Begge sider i ligningen er nul, hvis $p \mid D$. Det kan derfor antages, at $p \nmid D$.

Sæt $n := |D|$ og vælg et legeme L af karakteristik p som indeholder en primitiv n'te enhedsrod ζ. Et sådant legeme kan som bekendt konstrueres som en endelig udvidelse af $\mathbb{F}_p$. Betragt i L Gauss-summen $\tau = \tau(\chi_D, \zeta)$, og dens kvadrat τ^2. Af resultatet i (4.18) fås:

$$\tau^2 = D. \tag{4.19.1}$$

Da $p \nmid D$, er $D \neq 0$ i legemet L; ligningen medfører derfor specielt, at $\tau \neq 0$.

Betragt på den anden side den p'te potens τ^p. Elementet τ er en sum i karakteristik p og $\chi_D(a)^p = \chi_D(a)$, da p er ulige. Derfor får vi,

$$\tau^p = \sum_{a \bmod^* n} \chi_D(a)\zeta^{ap} = \sum_{a \bmod^* n} \chi_D(p)\chi_D(pa)\zeta^{ap} = \chi_D(p)\tau.$$

Da $\tau \neq 0$, kan τ bortforkortes, så vi får ligningen

$$\tau^{p-1} = \chi_D(p). \tag{4.19.2}$$

Tilsammen får vi i L ligningerne,

$$D^{(p-1)/2} = (\tau^2)^{(p-1)/2} = \tau^{p-1} = \chi_D(p).$$

Det to yderste sider i ligningerne er hele tal, opfattet i legemet L. Da legemet har karakteristik p, må disse tal altså være kongruente modulo p. Via Euler's Kriterium opnås derfor,

$$\chi_D(p) \equiv D^{(p-1)/2} \equiv \left(\frac{D}{p}\right) \pmod{p}.$$

De to yderste sider i kongruenserne er ± 1, så deres differens er numerisk højst 2. Da differensen er delelig med det ulige primtal p, må differensen altså være 0. Derfor gælder ligningen $\chi_D(p) = \left(\frac{D}{p}\right)$, som ønsket. □

(4.21) Bemærkning. Som en anvendelse af reciprocitetssætningen viser vi følgende om Mersenne-tallene $M_q = 2^q - 1$.

Sætning. *Lad q være et ulige primtal. Da er $2q+1$ divisor i M_q, hvis og kun hvis $2q+1$ er et primtal og $q \equiv 3 \pmod 4$.*

Bevis. Sæt $p := 2q+1$. Da er p ulige, $p > 3$, og $p-1 = 2q$.

„kun hvis“: Antag, at $p \mid M_q$, altså $p \mid 2^q - 1$. Idet vi regner modulo p, er altså $2^q \equiv 1$. Følgelig er $(-2)^q \equiv -1$, og dermed er $(-2)^{2q} \equiv 1$. Den sidste kongruens viser, at modulo p har -2 en orden, som er divisor i $2q$, og den første viser, at orden ikke kan være q. Da q er et primtal, og vi trivielt har $(-2)^2 \not\equiv 1$, følger det, at restklassen af -2 i gruppen $(\mathbb{Z}/p)^*$ har orden $2q$. Denne gruppe indeholder altså (mindst) $2q = p-1$ elementer. Restklassen af 0 er derfor den eneste restklasse i $\mathbb{Z}/p$, som ikke er invertibel. Altså må p være et primtal. Yderligere følger det af kongruensen $(-2)^q \equiv -1$, at -2 ikke kan være et kvadrat modulo p. Værdien af Legendre-symbolet $\left(\frac{-2}{p}\right)$ er altså -1. Modulo 8 er p derfor kongruent med 5 eller 7. Da $p = 2q+1$, med q ulige, følger det, at $q \equiv 3 \pmod 4$.

„hvis“: Antag, at p er et primtal og at $q \equiv 3 \pmod 4$. Da er $p \equiv 7 \pmod 8$. Følgelig er 2 et kvadrat modulo p, altså $2 \equiv x^2 \pmod p$. Heraf ses, at $2^q = x^{2q} \equiv 1 \pmod p$. Følgelig går p op i $2^q - 1$. $\square$

Af sætningen følger, at Mersenne-tallene $M_{11}, M_{23}, M_{83}, \dots$ er delelige med, henholdsvis, $23, 47, 167, \dots$. Det første sammensatte Mersenne-tal, som ikke står i denne liste er i øvrigt M_{29}.

(4.22) Opgaver.

U5 **1.** Betragt Jacobi-symbolet $\left(\frac{a}{u}\right)$, hvor u er positiv og ulige, og $(a,u) = 1$. Vis, at hvis kongruensen $x^2 \equiv a \pmod u$ kan løses, så er $\left(\frac{a}{u}\right) = 1$. Vis, at det omvendte ikke nødvendigvis gælder.

U6 **2.** Bestem værdierne af $\left(\frac{3}{D}\right)$ for alle diskriminanter D med $-20 \leqslant D \leqslant 20$.

U5 **3.** Indsæt resten af værdierne i nedenstående tabel over Legendre-symbolet $\chi(a) = \left(\frac{a}{13}\right)$:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\chi(a)$	1			1					1			

U5 **4.** Vis påstanden i (4.11) om entydig faktorisering af diskriminanter.

U6 **5.** Vis, for et ulige primtal p og $(a,p) = 1$, at a er kvadratisk rest modulo p^ν, hvis og kun hvis $\left(\frac{a}{p}\right) = 1$.

6. Vis, for et ulige primtal p, formlen $\sum_a \left(\frac{a(a+1)}{p}\right) = -1$, hvor summen er over restklasser a primiske med p. [Vink: Med $ab \equiv 1 \pmod p$ er $a(a+1) \equiv a^2(1+b)$.]

U5 **7.** For hvilke b er $\left(\frac{a}{b}\right)$ den trivielle karakter $(\mathbb{Z}/b)^* \to \{\pm 1\}$?

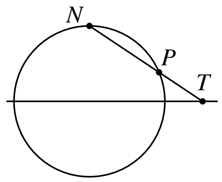
U5 **8.** Vis, at følgende algoritme bestemmer symbolet $\mathbf{s} = \left(\frac{a}{b}\right)$ uden at faktorisere potenser af 2. Initialiser med $\mathbf{a} := a$, $\mathbf{b} := b$, $\mathbf{s} := 1$.
(0) Hvis $\mathbf{b} \equiv 3 \pmod 4$, så sæt $\mathbf{b} := -\mathbf{b}$.
(1) Hvis $\mathbf{b} = 1$, så STOP.
(2) Bestem den principale rest r af $\mathbf{a}$ ved division med $\mathbf{b}$, altså $\mathbf{a} = q\mathbf{b} + r$ med $0 \leqslant r < |\mathbf{b}|$. Hvis $r = 0$, så sæt $\mathbf{s} := 0$ og STOP. Ellers sættes $\mathbf{a} := r$.

(3) Hvis $\mathbf{a} \equiv 3 \pmod 4$, så sæt $\mathbf{a} := -\mathbf{a}$. Hvis $\mathbf{a} \equiv 2 \pmod 4$: Hvis $\mathbf{b} > 0$, så sæt $\mathbf{a} := \mathbf{a} - \mathbf{b}$ og hvis $\mathbf{b} < 0$, så sæt $\mathbf{s} := -\mathbf{s}$ og $\mathbf{a} := -\mathbf{a} - \mathbf{b}$.

(4) Ombyt og gentag: Sæt $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a})$, og GOTO (1).

[Vink: Løkke-invarianter (strengt taget for (2)+(3)): „$\mathbf{b}$ er en diskriminant", og $\mathbf{s} \cdot \left(\frac{\mathbf{a}}{\mathbf{b}}\right)$. Vedr (3): Brug, at $\mathbf{a} > 0$, og brug bogens ligninger for Kronecker-symbolet. I de manglende tilfælde i (3) er $\mathbf{a}$ en positiv diskriminant.]

U5 **9.** For et primtal p sættes $S(\mathbb{F}_p) := \{\, (x, y) \in \mathbb{F}_p^2 \mid x^2 + y^2 = 1 \,\}$; det er „enhedscirklen" modulo p. Øjensynlig er $|S(\mathbb{F}_2)| = 2$. Vis for $p > 2$, at $|S(\mathbb{F}_p)| = p - (-1)^{(p-1)/2}$. Hvad sker der, når man mere generelt betragter et „keglesnit" $ax^2 + y^2 = 1$ modulo p, hvor $p \nmid a$?



[Vink: Punkterne $P = (x, y)$ på den sædvanlige enhedscirkel $S(\mathbb{R})$, fraregnet nordpolen $N = (0, 1)$, parametriseres ved at man lader punktet P svare til skæringspunktet $T = (t, 0)$ mellem linien NP og x-aksen. Beskriv parametriseringen, og overvej, hvordan regningerne forløber, hvis man i stedet regner modulo p.]

H3 **10.** Vis, at der er uendelig mange primtal p med $p \equiv 3 \pmod 8$. [Vink: Kig, for givne ulige $p_1, \dots, p_n$ på en primdivisor p i $u^2 + 2$, hvor $u := p_1 \cdots p_n$. Vis, at -2 er et kvadrat modulo p, og slut at modulo 8 er $p \equiv 1$ eller $p \equiv 3$. Det sidste må indtræffe for mindst ét p (ja, hvorfor?); vælg sådan et p som p_{n+1}.]

Vis tilsvarende, at der er uendelig mange primtal p med $p \equiv 7 \pmod 8$. Hvad med $p \equiv 5 \pmod 8$? [Vink: Kig på primdivisorer i $(2u)^2 + 1$, hvor u er ulige.] Hvad med $p \equiv 1 \pmod 6$? [Vink: Kig på $(2u)^2 + 3$.] Og hvad med $p \equiv a \pmod{12}$, for $a = 5, 7, 11$?

U7 **11.** Hvad betyder „kubisk karakter"? For hvilke primtal p kunne det være af interesse at studere kubiske karakterer modulo p?

U7 **12.** Lad D være en diskriminant. Vis, at hvis D er en „kvadratfri" diskriminant, altså et produkt af parvis primiske primdiskriminanter, så bestemmer Kronecker-symbolet $\left(\frac{a}{D}\right)$ en primitiv karakter $\chi_D \colon (\mathbb{Z}/D)^* \to \{\pm 1\}$. Vis omvendt, at hvis Kronecker-symbolet bestemmer en primitiv karakter, så er D „kvadratfri".

U7 **13.** Lad p være et ulige primtal. Vis, at for alle $\nu \geqslant 1$ er der præcis én ikke-triviel kvadratisk karakter $(\mathbb{Z}/p^\nu)^* \to \{\pm 1\}$. Er det karakteren bestemt ved Jacobi-symbolet $\left(\frac{a}{p^\nu}\right)$?

14. Vis, modulo et primtal $p > 3$, at summen af de kvadratiske rester er kongruent med 0.

15. *Vis, at for hver primdivisor p i Fermattallet $F_m = 2^{2^m} + 1$ er $p \equiv 1 \pmod{2^{m+2}}$. [Vink: kig på ordenen af 2 modulo p; det giver i hvert fald umiddelbart $p \equiv 1 \pmod{2^{m+1}}$.]

U7 **16.** Vis, at tallet $q_k = 2^k + 1$ for $k \geqslant 2$ er et primtal, hvis og kun hvis $3^{(q_k-1)/2} \equiv -1 \pmod{q_k}$. Hvorfor er det i øvrigt kun tilfældet, hvor k er en potens af 2, der er interessant? [Vink. „hvis": Brug kongruensen til at bestemme ordenen af 3 modulo q_k, og videre ordenen af $(\mathbb{Z}/q_k)^*$. „kun hvis": her er q_k er primtal, altså et Fermat-primtal, så specielt er k lige. Så er øjensynlig $q_k \equiv 1 \pmod 4$, og $q_k \equiv 2 \pmod 3$, og potensen $3^{(q_k-1)/2}$ modulo q_k kan bestemmes via „Euler" og reciprocitet.]

17. Antag, at $n = n_1 n_2$ er produktet af to primiske faktorer n_1, n_2. Antag, for $j = 1, 2$, at ζ_j er en n_j'te enhedsrod og at χ_j er en karakter modulo n_j. Vis, at $\zeta := \zeta_1 \zeta_2$ er en

n'te enhedsrod. Under hvilke omstændigheder bliver ζ en primitiv n'te enhedsrod? Vis, at enhver n'te enhedsrod kan skrives på denne form, $\zeta = \zeta_1\zeta_2$, med passende ζ_j. Vis, at $\chi := \chi_1\chi_2$, defineret ved $\chi(a) = \chi_1(a)\chi_2(a)$ når $(a, n) = 1$, er en karakter modulo n. Vis for Gauss-summerne, at $\tau(\chi, \zeta) = \tau(\chi_1, \zeta_1)\tau(\chi_1, \zeta_2)$.

U7 **18.** Lad χ være en karakter modulo n, og lad ζ være en n'te enhedsrod. Vis, når $(b, n) = 1$, at $\chi(b)\tau(\chi, \zeta^b) = \tau(\chi, \zeta)$.

U9 **19.** Betragt Gauss-summen $\tau = \tau(\chi, \zeta)$, hvor $\chi \colon (\mathbb{Z}/n)^* \to L^*$ er en karakter og $\zeta \in L$ er en k'te enhedsrod (hvor $k \,|\, n$). Vis, at hvis χ induceres af en karakter $\widehat{\chi} \colon (\mathbb{Z}/k)^* \to L^*$, så er $\tau(\chi, \zeta) = (\varphi(n)/\varphi(k))\tau(\widehat{\chi}, \zeta)$. Vis, at hvis χ ikke er induceret af en karakter modulo k, så er $\tau = 0$.

20. Antag, at $\zeta \in L^*$ er en primitiv n'te enhedsrod og at $\chi \colon (\mathbb{Z}/n)^* \to L^*$ er en primitiv karakter. Sæt $\chi^*(a) = \chi(a)^{-1}$ når $(a, n) = 1$, og giv $\chi(a)$ og $\chi^*(a)$ værdien 0, når a ikke er primisk med n. Specielt er så $\varphi(n) = \sum_{c \bmod n} \chi(c)\chi^*(c)$. Desuden er $\chi^*(a)\tau(\chi, \zeta) = \tau(\chi, \zeta^a)$ for alle a. Betragt Gauss-summerne $\tau = \tau(\chi, \zeta)$ og $\tau^* = \tau(\chi^*, \zeta^{-1})$. Gennemgå de enkelte skridt i følgende udregning (hvor summerne er over alle restklasser modulo n):

$$\varphi(n)\tau\tau^* = \sum_c \chi^*(c)\tau(\chi, \zeta)\chi(c)\tau(\chi^*, \zeta^{-1}) = \sum_c \tau(\chi, \zeta^c)\tau(\chi^*, \zeta^{-c})$$
$$= \sum_{a,b,c} \chi(a)\chi^*(b)\zeta^{ac-bc} = \sum_{a,b} \chi(a)\chi^*(b) \sum_c \zeta^{ac-bc} = \sum_a \chi(a)\chi^*(a)n = \varphi(n)n.$$

Ved division med $\varphi(n)$ fås $\tau\tau^* = n$. Der er en karakteristisk lille fejl i argumentet. Hvilken?

21. *Antag, at $\zeta \in L^*$ har orden n og at karakteren $\chi \colon (\mathbb{Z}/n)^* \to L^*$ induceres af en primitiv karakter modulo f, hvor $f \,|\, n$. Vis, at hvis n/f er kvadratfri og $(f, n/f) = 1$, så er $\tau\tau^* = f$. I alle andre tilfælde er $\tau = 0$. [Vink: reducer til tilfældet, hvor f er en primtalspotens.]

22. *Lad $\xi \colon (\mathbb{Z}/n)^* \to L^*$ være en karakter modulo n. Vis, at der findes en divisor $f \,|\, n$ med følgende egenskab: χ induceres af en karakter modulo f, og enhver anden divisor $d \,|\, n$ således, at χ induceres af en karakter modulo d, er et multiplum af f. Tallet f kaldes *føreren for* χ.

23. Bestem de komplekse Gauss-summer $\tau(\chi, \zeta_n)$ (hvor $\zeta_n = e^{2\pi i/n}$), når (1) $n = 4$, $\chi = \chi_{-4}$, og (2) $n = 8$, $\chi = \chi_8$, og når (3) $n = 8$, $\chi = \chi_{-8}$.

24. Betragt for et ulige primtal p den komplekse Gauss-sum $\tau_p = \tau(\chi_p, \zeta_p)$, hvor χ_p er Legendre-karakteren og $\zeta_p = e^{2\pi i/p}$. Bestem τ_p for $p = 3, 5, 7$. [Vink: Ifølge resultatet i noterne er det nok at bestemme fortegnet, men for $p = 3$ og $p = 5$ kan du da beregne Gauss-summen direkte.]

25. Betragt legemet $L = \mathbb{F}_{11}$ med 11 elementer. Vis, at restklassen af 2 er en frembringer for gruppen $\mathbb{F}_{11}^*$. Restklassen $\zeta := [4]$ er derfor en primitiv 5'te enhedsrod i $\mathbb{F}_{11}$. Lad χ_5 være Legendre-karakteren modulo 5. Bestem, i $\mathbb{F}_{11}$, Gauss-summen $\tau(\chi_5, \zeta)$. Check lige, at $\tau^2 = 5$.

26. Betragt et element $\xi \neq 0$ i legemet $L = \mathbb{F}_{29}$. Vis, at hvis $\xi^4 \neq 1$, så har ξ^4 orden 7. Vis, at $\zeta := [16]$ har orden 7 i L^*. Bestem, i $\mathbb{F}_{29}$, Gauss-summen $\tau(\chi_7, \zeta)$. Check lige, at $\tau^2 = -7$.

27. Vis, at der bestemmes en karakter $\chi : (\mathbb{Z}/5)^* \to \mathbb{C}^*$ ved $\chi(1) = 1, \chi(2) = i, \chi(3) = -i$, $\chi(4) = -1$. [Vink: $(\mathbb{Z}/5)^*$ er cyklisk, frembragt af restklassen af 2.] Bestem Gauss-summen $\tau = \tau(\chi, \zeta_5)$. Check lige, at $|\tau| = \sqrt{5}$.

U8 **28.** Lad der være givet et legeme L. Ved en *karakter* på G, hvor G er en endelig abelsk gruppe, forstås en homomorfi $\chi : G \to L^*$. Vis, at karaktererne på G udgør en kommutativ gruppe. Vis, at hver værdi $\chi(g)$, for $g \in G$, er en enhedsrod i L.

29. *Lad G være en endelig gruppe og lad l være den maksimale elementorden i G. Antag, at legemet L indeholder en primitiv l'te enhedsrod. Vis, at gruppen af alle karakterer $\chi : G \to L^*$ er isormorf med G. (Isomorfien er ikke kanonisk.) [Vink: Vis først påstanden for en cyklisk gruppe; brug struktursætningen i det almindelige tilfælde.]

30. Er karaktererne χ_{12} og χ_{-12}, svarende til Kronecker-symbolerne $\left(\frac{a}{12}\right)$ og $\left(\frac{a}{-12}\right)$, primitive karakterer modulo 12? Vis, at der er 4 karakterer modulo 12. Hvorfor kan de naturligt betegnes χ_1, χ_3, χ_{-4} og χ_{12}?

31. Vis, at restklassen $\zeta := [2]_{13}$ har orden 12 i $\mathbb{F}_{13}^*$. Bestem med denne enhedsrod Gauss-summerne i $\mathbb{F}_{13}$ svarende til de 4 karakterer (χ_1, χ_3, χ_{-4} og χ_{12}) modulo 12.

32. Bestem for $n = 5$ de komplekse Gauss-summer $\tau(\chi_5, \zeta_5)$ og $\tau(\chi_1, \zeta_5)$, hvor $\chi_5(a) = \left(\frac{a}{5}\right)$ og χ_1 er den trivielle karakter modulo 5. Lad x_1 og x_2 betegne realdelene af ζ_5 og ζ_5^2. Udtryk Gauss-summerne ved x_1 og x_2, og brug resultatet til at bestemme x_1 (og dermed ζ_5).

Besvar de samme spørgsmål for $n = 12$.

H3 **33.** Legemet $\mathbb{F}_{49}$ er beskrevet i (3.12): Elementerne har formen $a + ib$, hvor $a, b \in \mathbb{F}_7$ og $i^2 = -1$. Vis, at $\zeta := 2i$ er en primitiv 12'te enhedsrod i $\mathbb{F}_{49}$. Bestem Gauss-summen $\tau = \tau(\chi_{12}, \zeta)$ (hvor $\chi_{12}(a)$ er Kronecker-symbolet $\left(\frac{a}{12}\right)$), og dens kvadrat τ^2.

H3 **34.** Legemet $\mathbb{F}_{16}$ er beskrevet i (3.11): Elementerne har formen $a + b\xi + c\xi^2 + d\xi^3$, hvor $a, b, c, d \in \mathbb{F}_2$ og $\xi^4 = 1 + \xi$. Vis, at $\zeta := \xi^3$ er en primitiv 5'te enhedsrod. Bestem Gauss-summen $\tau = \tau(\chi_5, \zeta)$ (hvor $\chi_5(a)$ er Legendre-symbolet $\left(\frac{a}{5}\right)$), og dens kvadrat τ^2.

Kan du, når du har besvaret opgaven, tilføje en besvarelse på én linie?

H4 **35.** Lad $p > 2$ være et primtal. Vis, at hvis $[a]_p$ frembringer $(\mathbb{Z}/p)^*$, så er $\left(\frac{a}{p}\right) = -1$. Vis, at hvis p er et Fermat-primtal, så gælder også det omvendte. Vis, at hvis p ikke er et Fermat-primtal, så findes et tal a således, at $\left(\frac{a}{p}\right) = -1$ og $[a]_p$ *ikke* frembringer $(\mathbb{Z}/p)^*$.

H4 **36.** Tabellen herunder er uddrag af en tabel med søjler svarende til tallene $n = 2, 3, 4, \ldots, 21$. Under n i første rækkke står i anden række primopløsningen af $M_n = 2^n - 1$, og i tredie række de primtal p, for hvilke restklassen $[2]_p$ har orden n i $(\mathbb{Z}/p)^*$. Forklar, hvordan man kan få tredie række ud fra tabellens anden række.

Kompleter tabellen, så den indeholder resultaterne for alle $n = 2, 3, 4, \ldots, 21$. Du må gerne overspringe de n, for hvilke M_n er et Mersenne-primtal. Det er nok, at du anfører tabellens tredie række.

2	3	4	5	6	......	11	......	21
3	7	$3{\cdot}5$	31	$3^2 \cdot 7$	......	$23 \cdot 89$	......	
3	7	5	31		......	23, 89	......	337

[Vink: Du behøver i hvert fald ikke at beregne potenser af 2 større end 2^{10}. Ultimativt kan du faktorisere $2^n - 1$ ved at bruge, at $2^n - 1 = \prod_{d\,|\,n} \Phi_d(2)$, men du kan såmænd nøjes med at bruge, at hvis $n = qd$ er sammensat, så er $2^d - 1$ divisor i $2^{qd} - 1$.]

Bestem det mindste primtal p, for hvilket der gælder, at $\left(\frac{2}{p}\right) = -1$ og $[2]_p$'s orden er mindre end $p - 1$.

U8 **37.** Hvad er det for en „Homomorfisætning", der omtales i (4.15)?

38. Betragt for $a \neq 0$ ligningen $\left(\frac{a}{p}\right) = 1$ for ulige primtal p med $p \nmid a$. Vis, at hvis ligningen gælder for alle p, så er a et kvadrat.

Vis, når a er en diskriminant, at det er nok at kræve ligningen opfyldt for alle $p < |a|$. Vis i almindelighed, at det er nok at kræve ligningen opfyldt for $p < 4|a|$.

39. Vis, at for hvert helt tal $a \neq 0$ findes der uendelig mange primtal $p > 2$ således, at a er et kvadrat modulo p, og, når a ikke er et kvadrattal, uendelig mange primtal p således, at a er et ikke-kvadrat modulo p. Du må gerne bruge Dirichlet's Sætning om primtal i restklasser.

*Vis påstanden uden at bruge Dirichlet's sætning.

5. Primtalstestning.

(5.1) Setup. I det følgende betegner m et ulige tal større end 1. Vi beskriver en række tests til afgørelse af om m med en given sandsynlighed er et primtal. I praksis er m et tilfældigt tal med et stort antal cifre frembragt på en computer. Hvis m passerer de nedenfor angivne tests, så er m med stor sandsynlighed et primtal. Hvis derimod m ikke passerer blot en enkelt af disse tests, så er m med sikkerhed ikke et primtal. I praksis vil man altså efter testningen enten vide med sikkerhed, at m er et sammensat tal, eller vide med stor sandsynlighed, at m er et primtal. Det er værd at bemærke, at en computer således ofte ganske let kan bevise, at et givet stort tal m er sammensat uden at computeren kan finde blot én ikke-triviel divisor i tallet.

Sandsynligheden for at et tilfældigt tal med fx 100 cifre er et primtal er naturligvis ikke stor. At denne sandsynlighed på den anden side ikke er forsvindende følger af Primtalssætningen: Idet $\pi(n)$ betegner antallet af primtal mindre end eller lig med n gælder for $n \to \infty$, at

$$\frac{\pi(n)}{n} \sim \frac{1}{\log n}\;.$$

Sandsynligheden for at et tilfældigt tal med 100 cifre er et primtal er efter denne approksimation af størrelsesordenen $(100 \log 10)^{-1} \approx 0{,}0043$. Der findes mange mere kvantitative vurderinger af sandsynligheden $\pi(n)/n$. En elementær vurdering, der gælder for alle $n \geqslant 2$, er Chebyshev's vurdering:

$$\frac{1/3}{\log n} < \frac{\pi(n)}{n} < \frac{3}{\log n}.$$

(5.2) Definition. For hvert naturligt tal b betegnes med psp_b, eller $\mathrm{psp}_b(m)$, udsagnet:

$$b^{m-1} \equiv 1 \pmod{m}. \qquad (\mathrm{psp}_b)$$

Hvis psp_b er opfyldt for m, siges m at *passere testen* psp_b, eller at være et *basis-b pseudoprimtal* (eller kort: et psp_b-tal). (Ofte kræves yderligere, at m er sammensat, men vi vil medregne ulige primtal til pseudoprimtallene.) Tilfældet $b = 1$ er naturligvis uinteressant, idet udsagnet psp_1 altid er sandt. I forbindelse med testen antager vi altid, at $b \geqslant 2$.

Observation. *Tallet m er et primtal, hvis og kun hvis det passerer psp_b for alle $b < m$.*

'kun hvis' følger nemlig af Fermat's „lille“ sætning, og 'hvis' er trivielt: af $\mathrm{psp}_b(m)$ følger jo specielt at b må være primisk med m, og hvis det er tilfældet for alle $b < m$, må m være et primtal.

Tallet m er selvfølgelig et primtal, netop når ingen af tallene $\leqslant \sqrt{m}$ er divisorer i m, så den oplagte primtalstest er at prøve med alle tal $d \leqslant \sqrt{m}$, om d går op i m. De tal m, der skal primtalstestes, vil ved de praktiske anvendelser være store, dvs med 100 eller flere cifre. For et sådant tal er $\sqrt{m}$ som bekendt større end antallet af atomer her på jorden. Den oplagte test er altså med sikkerhed absolut uanvendelig. Observationen ovenfor, at teste om m passerer psp_b for alle $b < m$, er om muligt endnu mere uanvendelig.

Bemærk, at det er den del af udsagnet, der vedrører „for alle $b < m$“, som gør udsagnet uanvendeligt. Et tal med m med 100 cifre fylder blot 100 tegn, og altså næsten ingen plads i en computers hukommelse. En computer kan let – og hurtigt – regne med tal af denne størrelsesorden. Heller ikke potensopløftningen i testen psp_b (hvor der skal regnes modulo m) er afskrækkende, selv om potensen a priori kræver $N = m - 1$ multiplikationer: det kan faktisk gøres med $\log_2 N$ multiplikationer (hvordan?).

Hvis m passerer psp_b for alle tal b, der er primiske med m, vil vi sige, at m er et *pseudoprimtal*. Glosen er i og for sig overflødig, thi af definitionen fremgår, at m er et pseudoprimtal, hvis og kun hvis m er enten et primtal eller et Carmichael-tal. Af karakteriseringen af Carmichael-tal i (2.5) følger derfor, at m er et pseudoprimtal, hvis og kun hvis m er et produkt, $m = p_1 \cdots p_r$, af forskellige ulige primtal p_i, som opfylder at $p_i - 1 \mid m - 1$.

(5.3) Sætning. *Antag, at m ikke er et pseudoprimtal. Blandt restklasserne b modulo m er brøkdelen af de b, for hvilke m passerer* psp_b, *højst lig med $\frac{1}{2}$.*

Bevis. Det er klart, at hvis m passerer psp_b, altså hvis $b^{m-1} = 1$ i $\mathbb{Z}/m$, så er b en primisk restklasse. Restklasserne b, for hvilke $b^{m-1} = 1$ udgør øjensynlig en undergruppe H af gruppen $G = (\mathbb{Z}/m)^*$ af alle primiske restklasser. Den søgte brøkdel er $|H|/m$, som med sikkerhed er mindre end $|H|/|G| = 1/|G{:}H|$. Ifølge antagelsen om m er H ægte undergruppe. Index $|G{:}H|$ er derfor mindst 2. Brøkdelen er derfor mindre end $\frac{1}{2}$. □

(5.4) Korollar. *Antag, at m er tilfældigt valgt blandt tallene $1, \dots, N$, og at m passerer* psp_b *for k tilfældigt valgte værdier af b. Sandsynligheden for at m ikke er et pseudoprimtal er da mindre end $2^{-k} \log N$.*

Bevis. Betragt mængden $\mathcal{X}$ af $(k+1)$-sæt $(m, b_1, \dots, b_k)$ af tal $\leqslant N$, med diskret sandsynlighedsmål, og heri følgende hændelser (delmængder): $\mathcal{I}$: m er ikke et pseudoprimtal; $\mathcal{Y}$: m passerer psp_b for $b = b_1, \dots, b_k$; $\mathcal{P}$: m er et primtal.

Den søgte sandsynlighed er den relative sandsynlighed $P(\mathcal{I}|\mathcal{Y})$. Som bekendt er

$$P(\mathcal{I}|\mathcal{Y}) = \frac{P(\mathcal{I} \cap \mathcal{Y})}{P(\mathcal{Y})} = \frac{P(\mathcal{Y}|\mathcal{I})P(\mathcal{I})}{P(\mathcal{Y})}.$$

I tælleren på højresiden er $P(\mathcal{Y}|\mathcal{I}) \leqslant 2^{-k}$ ifølge sætningen, og $P(\mathcal{I}) \leqslant 1$. I nævneren er $P(\mathcal{Y}) \geqslant P(\mathcal{P})$, og $P(\mathcal{P}) = \pi(N)/N$. Endelig er $N/\pi(N) \sim \log N$ ifølge Primtalssætningen (man kan faktisk vise, at der altid (for $N \geqslant 17$) gælder $N/\pi(N) \leqslant \log N$).

Heraf følger vurderingen. [I beviset er der foretaget nogle tilnærmelser: tilfældige valgte $b \leqslant N$ giver ikke nødvendigvis tilfældige restklasser modulo m; og et primtal m vil ikke passere psp_b, når b er et multiplum af m. I øvrigt er selve formuleringen af påstanden tvivlsom: Når et bestemt m *er* valgt, giver det ingen mening at tale om sandsynligheden for at m fx er et primtal. Formuleringen bør altså snarere være: Sandsynligheden for at den beskrevne metode resulterer i et ikke-pseudoprimtal . . . .] □

(5.5) Bemærkning. Resultatet kan anvendes på et tilfældigt fundet tal m, fx med 100 cifre ($N = 10^{100}$), til at fastslå, enten at m med sikkerhed ikke er et pseudoprimtal eller at m

med stor sandsynlighed er et pseudoprimtal. Hvis m har passeret psp_b for $18 = 10 + 8$ tilfældigt valgte tal b, er m med 99,9% sandsynlighed et pseudoprimtal ($2^{-10} < 0,001$ og $2^{-8} \cdot 100 \log 10 < 1$). En væsentlig vanskelighed i praksis er naturligvis at frembringe et *tilfældigt* tal mindre end N.

Tallet 2, der indgår i faktoren $\frac{1}{2}$ i vurderingen, kan teoretisk erstattes med index af den undergruppe H, der indgår i beviset for sætningen, og det vil ofte være meget større end 2. Det viser sig i praksis ved, at når man underkaster et stort tal m testen, så vil det enten blive afsløret i første forsøg, at m ikke passerer testen (og så er m med sikkerhed ikke et primtal), eller også passerer m testen, så længe man gider teste.

I det såkaldte RSA–system, som vi beskriver senere, indgår som et vigtigt element at producere tal n, der er produkter af to store primtal m_1 og m_2. Det er værd at bemærke, at af hensyn til kodning og dekodning behøver det blot at forudsættes, at m_1 og m_2 er to primiske pseudoprimtal. Kravet om at m_1 og m_2 skal være primtal er således et krav, der stilles af hensyn til kodens sikkerhed.

(5.6) Definition. For hvert naturligt tal b betegnes med e-psp_b, eller e-$\mathrm{psp}_b(m)$, udsagnet:

$$b^{(m-1)/2} \equiv \left(\frac{b}{m}\right) \neq 0 \pmod m, \qquad (\text{e-psp}_b)$$

hvor $\left(\frac{b}{m}\right)$ betegner Jacobi-symbolet. (Den sidste betingelse, at Jacobi-symbolet ikke er 0, betyder blot, at b og m er primiske.) Hvis e-psp_b er opfyldt for m, siges m at *passere testen* e-psp_b, eller at være et *basis-b Euler-pseudoprimtal* (eller kort: et e-psp_b-tal). Vi antager sædvanligvis, at $b \geqslant 2$.

Højresiden i kongruensen i (e-psp_b) er ± 1, når b er primisk med m, og 0 ellers. Følgelig gælder, at e-$\mathrm{psp}_b \implies \mathrm{psp}_b$. Et basis-$b$ Euler-pseudoprimtal er altså et basis-b pseudoprimtal.

(5.7) Sætning. *Tallet m passerer testen* e-psp_b *for alle alle b, som er primiske med m, hvis og kun hvis m er et primtal. Antag, at m er tilfældigt valgt blandt tallene $\leqslant N$, og at m passerer* e-psp_b *for k tilfældigt valgte værdier af b. Sandsynligheden for at m er et primtal er da større end $1 - 2^{-k} \log N$.*

Bevis. „hvis" følger umiddelbart af Euler's kriterium, (4.7). Antag omvendt, at m er passerer e-psp_b (og dermed psp_b) for alle b, der er primiske med m og mindre end m. Da er m specielt et pseudoprimtal. Antag, indirekte, at m ikke er et primtal. Af Sætning (5.3) følger så specielt, at m har formen $m = pd$, hvor p er et primtal og d er større end 1 og primisk med p. Vælg et tal g, der er kvadratisk ikke-rest modulo p, altså med $\left(\frac{g}{p}\right) = -1$. Ifølge den kinesiske restklassesætning findes et tal b, så at $b \equiv 1 \pmod d$ og $b \equiv g \pmod p$. Af definitionen på Jacobi-symbolet følger let, at $\left(\frac{b}{m}\right) = -1$. Af e-$\mathrm{psp}_b(m)$ fås derfor modulo m, at $b^{(m-1)/2} \equiv -1$. Følgelig gælder denne kongruens også modulo divisoren d i m. Men det er i modstrid med at $b \equiv 1 \pmod d$.

Sætningens sidste påstand følger som i beviset for Korollar (5.4), idet mængden af restklasser af de tal b, for hvilke e-psp_b gælder, øjensynlig er en undergruppe i gruppen $G = (\mathbb{Z}/m)^*$ af primiske restklasser. □

Den foregående sætning kan anvendes på det givne (store) tal m til at fastslå, enten at m ikke er et primtal eller at m med stor sandsynlighed er et primtal. Testen kaldes *Soloway–Strassen's primtalstest.*

(5.8) Definition. Skriv $m-1$ på formen $m-1=u2^s$, hvor u er ulige. (Da m er ulige, er $s\geqslant 1$.) For hvert naturligt tal b betegnes med s-psp$_b$ eller s-psp$_b(m)$ udsagnet (modulo m):

$$\begin{cases} \text{Enten:} & b^u \equiv 1 \pmod m \\ \text{Eller:} & b^u \equiv -1 \text{ eller } b^{u2} \equiv -1, \text{ eller } b^{u2^2} \equiv -1, \text{ eller } \dots, b^{u2^{s-1}} \equiv -1. \end{cases} \qquad (\text{s-psp}_b)$$

Hvis s-psp$_b$ er opfyldt for m, siges m at *passere* s-psp$_b$, eller at være et *basis-b stærkt pseudoprimtal* (eller kort: et s-psp$_b$-tal).

Betingelsen i anden linie er, at der eksisterer et $t=1,\dots,s$ således, at $b^{u2^{t-1}}\equiv -1 \pmod m$. I praksis udføres testen på følgende måde: Først dannes $x_0:=b^u$. Hvis $x_0\equiv \pm 1 \pmod m$, så gælder s-psp$_b$. Er $x_0\not\equiv \pm1$, så kvadrerer vi successivt: $x_{t+1}:=x_t^2$. Fremkommer herved et t med $1\leqslant t<s$ således, at $x_t\equiv -1 \pmod m$, så gælder s-psp$_b$. I modsat fald er s-psp$_b$ falsk.

Det er let at se, at s-psp$_b$ $\implies$ psp$_b$. Et basis-b stærkt pseudoprimtal er altså et basis-b pseudoprimtal.

(5.9) Sætning. *Hvis* $m\equiv 3 \pmod 4$, *så gælder:* s-psp$_b$ $\iff$ e-psp$_b$.

Bevis. Antag, at $m\equiv 3 \pmod 4$, altså at $m-1=2u$, hvor u er ulige. Det kan antages, at b er primisk med m. Ifølge definitionen betyder e-psp$_b$, at $b^u\equiv\left(\frac{b}{m}\right)$, og s-psp$_b$, at $b^u\equiv\pm1$. Det er således klart, at e-psp$_b$ $\implies$ s-psp$_b$. Antag omvendt, at $b^u\equiv\pm1$. Da $m\equiv 3 \pmod 4$, gælder ifølge (4.4.1), at $\left(\frac{\pm1}{m}\right)=\pm1$. Af $b^u\equiv\pm1$ følger derfor, at $\left(\frac{b^u}{m}\right)=b^u$. Og så er

$$\left(\frac{b}{m}\right)=\left(\frac{b}{m}\right)^u=\left(\frac{b^u}{m}\right)=b^u,$$

som ønsket. □

(5.10) Lemma. *Antag, at m har primopløsningen $m=p_1^{\mu_1}\cdots p_k^{\mu_k}$. Skriv*

$$m-1=u2^s \quad \text{og} \quad p_i-1=u_i2^{s_i} \text{ for } i=1,\dots,k,$$

hvor u og u_i er ulige. Lad s_0 betegne det mindste af tallene s_i for $i=1,\dots,k$. Da gælder: Blandt de primiske restklasser b modulo m er brøkdelen af de b, for hvilke s-psp$_b$ *gælder, givet ved udtrykket,*

$$C\prod_i \frac{1}{p_i^{\mu_i-1}}\prod_i\frac{(u,u_i)}{u_i}\prod_i\frac{1}{2^{s_i-s_0}}\;, \qquad (5.10.1)$$

hvor faktoren $C=C_{k,s_0}$ er bestemt ved

$$C=\frac{1}{2^{ks_0}}\left(1+\frac{2^{ks_0}-1}{2^k-1}\right)=\frac{1}{2^k-1}+\frac{1}{2^{ks_0}}\left(1-\frac{1}{2^k-1}\right).$$

Yderligere gælder, at s-psp$_b$ $\implies$ e-psp$_b$.

Bevis. Vi betragter gruppen $G := (\mathbb{Z}/m)^*$ af primiske restklasser, og heri delmængden K bestående af b, for hvilke s-psp$_b$ gælder. Det påstås altså, at brøken $|K|/|G|$ (hvor jo $|G| = \varphi(m)$) er bestemt ved det anførte udtryk.

I G (såvel som i enhver anden kommutativ gruppe) kan hvert element b entydigt skrives $b = ac$, hvor a har ulige orden og c's orden er en potens af 2. Det er let at se, at s-psp$_b$ gælder, hvis og kun hvis følgende udsagn begge er opfyldt,

$$a^u = 1, \tag{1}$$

$$c = 1 \text{ eller } c^{2^{t-1}} = -1 \text{ for passende } t = 1, \dots, s. \tag{2}$$

Elementantallet i delmængden K fås derfor ved at multiplicere antallet af a'er, der opfylder (1), med antallet af c'er, som opfylder (2).

Ifølge Den kinesiske Restklassesætning er $G = (\mathbb{Z}/m)^*$ lig med produktet af grupperne $G_i := (\mathbb{Z}/p_i^{\mu_i})^*$. Hver restklasse i G definerer altså en restklasse i hver af grupperne G_i, og hver af ligningerne i (1) og i (2) ensbetydende med at den tilsvarende ligning gælder i G_i for $i = 1, \dots, k$. Først bestemmes derfor for hver af ligningerne antallet af løsninger til ligningen i gruppen G_i. Da m er ulige, er p_i et ulige primtal, og gruppen G_i er derfor cyklisk. Dens orden er $\varphi(p_i^{\mu_i}) = p_i^{\mu_i-1}(p_i - 1) = p_i^{\mu_i-1}u_i 2^{s_i}$.

Betragt først ligningen $a^u = 1$ i den i'te gruppe G_i. Da G_i er cyklisk, er antallet af løsninger lig med den største største fælles divisor for u og ordenen af G_i. Her er u ulige og divisor i $m - 1$, og p_i er divisor i m. Det følger, at den søgte største fælles divisor er den største fælles divisor (u, u_i). Af Den kinesiske Restklassesætning fås derfor, at antallet af løsninger i G til ligningen, dvs antallet af løsninger a til ligningen (1), er lig med produktet,

$$\prod_i (u, u_i). \tag{1'}$$

Betragt dernæst ligningen $c^{2^{t-1}} = -1$. Gruppen G_i er cyklisk af lige orden. Der er specielt netop ét element $z \neq 1$ af orden 2 i G_i, nemlig $z = -1$. Heraf følger, at $c^{2^{t-1}} = -1$, hvis og kun hvis c i G_i har orden lig med 2^t. Antallet af løsninger i G_i er altså antallet af elementer af orden 2^t. Dette antal er 2^{t-1}, hvis $t \leqslant s_i$, og 0 ellers. Antallet af løsninger til ligningen i G er derfor 0, hvis $t > s_0$, og lig med $\prod_i 2^{t-1} = 2^{k(t-1)}$ ellers.

Antallet af de c i G, som tilfredsstiller en af ligningerne i (2), er derfor $1 + \sum_t 2^{k(t-1)}$, hvor der summeres over tal t (med $1 \leqslant t \leqslant s$), som er mindre end eller lig med ethvert s_i, dvs $t \leqslant s_0$. Vi viser om lidt, med $s \geqslant s_0$. Derfor er summen over $0 < t \leqslant s_0$, og antallet er

$$1 + \sum_{t=1}^{s_0} 2^{k(t-1)} = 1 + \frac{2^{ks_0} - 1}{2^k - 1}. \tag{2'}$$

Som nævnt er antallet af elementer b i G, der opfylder s-psp$_b(m)$ lig med produktet af tallene (1') og (2'). Den søgte brøkdel fås derfor ved at dividere dette produkt med ordenen $\varphi(m)$ af

G. Øjensynlig er

$$\varphi(m) = \prod_i p_i^{\mu_i - 1} u_i 2^{s_i} = 2^{ks_0} \prod_i p_i^{\mu_i - 1} \prod_i u_i \prod_i 2^{s_i - s_0}. \tag{3'}$$

Det er nu klart, at det ønskede udtryk for for brøkdelen fremkommer ved at multiplicere (1') med (2') og dividere med (3'). Borset fra den ikke-viste ulighed $s \geqslant s_0$ er Lemma'ets første påstand altså bevist.

For at vise den sidste påstand antages om b, at s-$\mathrm{psp}_b(m)$ gælder. Det er klart, at b så må være primisk med m. Det skal vises, at følgende ligning gælder i gruppen $G = (\mathbb{Z}/m)^*$:

$$b^{(m-1)/2} = \left(\frac{b}{m}\right). \tag{4}$$

Skrives som ovenfor $b = ac$, er det nok at vise ligningen (4) for $b := a$ og for $b := c$. For $b := a$ er antagelsen, at (1) er opfyldt, altså at $a^u = 1$. Tallet u var en ulige divisor i $m-1$, og derfor divisor i $(m-1)/2$. Venstresiden i (4) er derfor 1. Jacobi-symbolet er multiplikativt, med værdierne ± 1; ligningen $a^u = 1$ med ulige u medfører derfor, at $\left(\frac{a}{m}\right) = 1$. Altså gælder (4).

For $b := c$ er antagelsen, at (2) er opfyldt. Hvis $c = 1$, er (4) trivielt opfyldt, så vi antager, at $c^{2^{t-1}} = -1$ for et t med $0 < t \leqslant s$. Vi har endnu ikke bevist uligheden $s \geqslant s_0$, og betragter derfor mere generelt et element c, der opfylder ligningen $c^{2^{t-1}} = -1$ for et vilkårlig $t > 0$. Ligningen er ækvivalent med at c har orden 2^t i hver af grupperne G_i, så specielt eksisterer et sådant element c, hvis og kun hvis $t \leqslant s_0$. Regn nu modulo 2^{t+1} og udnyt, at for et ulige tal v er $v2^t \equiv 2^t \pmod{2^{t+1}}$. Lad l være antallet af primtal p_j (talt med multiplicitet μ_j) for hvilke $t = s_j$ (øjensynlig er $l = 0$, når $t < s_0$). For disse primtal er $p_j - 1 = 2^t u_j \equiv 2^t$, altså $p_j \equiv 1 + 2^t$, og for de øvrige primtal p_i gælder $p_i \equiv 1 \pmod{2^{t+1}}$. Da $m = \prod p_i^{\mu_i}$ følger det, at

$$m \equiv \prod_j (1 + 2^t) \equiv 1 + l\,2^t \pmod{2^{t+1}}, \tag{5}$$

idet der er l faktorer i produktet. Da $m - 1 = 2^s u$, ses af (5), at $t \leqslant s$; specielt, med $t := s_0$, fås uligheden $s \geqslant s_0$, dvs den søgte ulighed.

Betragt nu de to sider af (4) for $b := c$. Venstresiden er $c^{(m-1)/2}$. Af kongruensen (5) følger, at $(m-1)/2 \equiv l2^{t-1} \pmod{2^t}$. Da $c^{2^{t-1}} = -1$, følger det, at

$$c^{(m-1)/2} = (-1)^l. \tag{6}$$

Betragt dernæst højresiden af (4). I den cykliske gruppe G_i er c af orden 2^t, så c er et kvadrat, hvis og kun hvis $t < s_i$. Altså er $\left(\frac{c}{p_j}\right) = -1$, hvis og kun hvis $t = s_j$. Da Jacobi-symbolet er produktet af $\left(\frac{c}{p_i}\right)$ over p_i med multiplicitet, følger det, at $\left(\frac{c}{m}\right) = (-1)^l$. Af (6) fremgår nu den søgte ligning. $\square$

Bemærkning. Brøkerne, der indgår i udtrykket (5.10.1), er stambrøker, dvs af formen $1/l$, hvor l er et naturligt tal. Det ses, at alle disse brøker er lig med 1, hvis og kun hvis m er kvadratfri, og $u_i \,|\, u$ og $s_i = s_0$ for $i = 1, \dots, k$. At det sidst indtræffer betyder, at s_i'erne er ens og at $p_i - 1 \,|\, m - 1$ for $i = 1, \dots, k$. Brøkerne er således alle lig med 1, hvis og kun hvis $m = p_1 \cdots p_k$ er et primtal ($k = 1$), eller et Carmichael tal ($k \geqslant 3$) hvor alle s_i'erne er ens. Et eksempel på det sidste er $13 \cdot 37 \cdot 61 = 29.341$.

Faktoren $C = C_{k,s_0}$ er mindre end eller lig med 1, da $s_0 \geqslant 1$, og den er kun lig med 1 for $k = 1$. For hver fast værdi af k er faktoren størst for $s_0 = 1$. Disse største værdier er $C_{k,1} = 1/2^{k-1}$.

(5.11) Sætning. *Tallet m passerer* s-psp$_b$ *for alle b, som er primiske med m, hvis og kun hvis m er et primtal. Antag, at m er tilfældigt valgt blandt tallene $\leqslant N$, og at m passerer* s-psp$_b$ *for k tilfældigt valgte værdier af b. Sandsynligheden for at m er et primtal er da større end* $1 - 4^{-k} \log N$.

Bevis. Den første påstand følger umiddelbart af det foregående Lemma: brøkdelen er lig med 1, hvis og kun hvis m er et primtal (Alternativ: da s-psp$_b$ $\Longrightarrow$ e-psp$_b$ følger påstanden af Sætning (5.7)). Et elementært bevis for den første påstand er følgende:

„hvis“: Antag, at m er et primtal. Lad b være primisk med n. Det skal vises, at s-psp$_b$ er sandt. Hvis $b^u \equiv 1 \pmod{m}$, er dette klart, så det kan antages, at $x_0 := b^u \not\equiv 1$. Betragt kvadraterne $x_{j+1} := x_j^2$. For $j = 0$ er $x_0 \not\equiv 1$, og for $j = s$ er $x_s = x_0^{2^s} = b^{u2^s} = b^{m-1} \equiv 1$ ifølge Fermat's „lille“ sætning. Der findes derfor en værdi $j < s$, så at $x_j \not\equiv 1$ og $x_j^2 = x_{j+1} \equiv 1$. For denne værdi er $x_j \equiv -1$, idet kongruensen $y^2 \equiv 1$ kun har løsningerne ± 1, da m er et primtal.

„kun hvis“: Antag omvendt, at m passerer s-psp$_b$ for alle b primiske med m og (indirekte) ikke er et primtal. Da er m som nævnt et pseudoprimtal. Af Sætning (5.3) følger derfor specielt, at m har formen $m = pd$, hvor p er et ulige primtal og d er større end 1 og primisk med p. Vælg et tal b med $b \equiv 1 \pmod{d}$ og $b \equiv -1 \pmod{p}$. Da u er ulige, gælder de samme kongruenser for b^u. Specielt er $b^u \not\equiv \pm 1 \pmod{m}$, Da $b^{2u} \equiv 1 \pmod{m}$ (og dermed $b^{2^t u} \equiv 1 \pmod{m}$), er betingelsen i (5.8) altså ikke opfyldt, i modstrid med antagelsen.

Sætningens sidste påstand følger af, at brøkdelen angivet i Lemma'et, når m ikke er et primtal, højst er $1/4$ (Det er ikke helt korrekt, tilfældet $m = 3^2 = 9$ kræver faktisk en særbehandling, hvor man må udnytte, at 9 heller ikke passerer s-psp$_b$ når $b = 3, 6$). ☐

Bemærkning. Den foregående sætning kan anvendes på det givne (store) tal m til at fastslå, enten at m ikke er et primtal eller at m med stor sandsynlighed er et primtal. Denne test kaldes også *Miller–Rabin's primtalstest*. Som vist i Lemma (5.10) gælder, at s-psp$_b$ $\Rightarrow$ e-psp$_b$, altså at ethvert basis-b stærkt pseudoprimtal er et basis-b Euler-pseudoprimtal. I tilfældet $m \equiv 3 \pmod{4}$ er det endda let, jfr. (5.9), at se, at s-psp$_b$ $\Leftrightarrow$ e-psp$_b$.

(5.12) Bemærkning. De anførte primtalstests er såkaldte probabilistiske tests: de viser i polynomial tid, enten med en vis sandsynlighed, at m er et primtal, eller med sikkerhed, at m ikke er et primtal. Det er nærliggende at overveje, om disse tests ikke kan gøres effektive ved at vælge b'erne systematisk snarere end tilfældigt. I den forbindelse er det nødvendigt at inddrage den såkaldte *generaliserede Riemann-hypotese*. Generaliseringer af Riemann's zeta-funktion er funktioner af formen,

$$L_\chi(s) = \sum\nolimits_{n\geqslant 1} \frac{\chi(n)}{n^s},$$

hvor $\chi\colon \mathbb{Z} \to \{0, \pm 1\}$ er en kvadratisk karakter, dvs χ fås ved at udvide en homomorfi $\chi\colon (\mathbb{Z}/m)^* \to \{\pm 1\}$ med værdien 0 på restklasser, der ikke er primiske med m. Riemann's zeta-funktion fremkommer, når $\chi(n) = 1$ for alle n. Den generaliserede Riemann-hypotese er påstanden om at der også for disse generaliserede „zeta-funktioner" gælder, at nulpunkterne i den kritiske strimmel har realdel lig med $\frac{1}{2}$.

Under forudsætning af den generaliserede Riemann-hypotese kan man vise, at Miller–Rabin testen er deterministisk i polynomial tid. Mere præcist kan man under denne forudsætning vise, at *hvis m passerer* s-psp$_b$ *for alle $b < 2(\log m)^2$, så er m et primtal.*

(5.13) Opgaver.

H3 **1.** Bestem for de første primtal $p = 3, 5, 7, \dots, 31$ ordenen af 2 i $(\mathbb{Z}/p)^*$. [Vink: værdien af Legendre-symbolet $\left(\frac{2}{p}\right)$ fortæller ganske meget om ordenen.] Angiv det mindste sammensatte basis-2 pseudoprimtal; — og basis-2 Euler-pseudoprimtal.

H3 **2.** Lad p være et ulige primtal. Vis, at $m = M_p := 2^p - 1$ er et basis-2 stærkt pseudoprimtal. Tallet $M_{11} = 2.047$ er faktisk det mindste sammensatte basis-2 stærke pseudoprimtal.

H3 **3.** Antag, at $m - 1 = 2^s u$, hvor u er ulige og $\leqslant 2^s + 1$. Vis, at hvis der findes et tal b således, at $b^{2^{s-1}} \equiv -1 \pmod{m}$, så er m et primtal. [Vink: kongruensen bevares modulo en primdivisor p i m, og den bestemmer ordenen af restklassen af b.] Vis omvendt, at hvis m er et primtal, så er det „let" at finde et sådant b.

U8 **4.** For hvilke b er tallet 15 et psp$_b$-tal? Og for hvilke b er tallet 21 et psp$_b$-tal? Generaliser til tal af formen $3p$, hvor p er et primtal.

U8 **5.** Antag, at p og $q := 2p - 1$ er primtal, og sæt $m = pq$. Vis, at m er et psp$_b$-tal, hvis og kun hvis b er primisk med m og en kvadratisk rest modulo q. For hvor stor en del af b'erne (modulo m) sker det?

U9 **6.** Antag, at m er ulige og sammensat, at p er en primdivisor i m, og at $(b, m) = 1$.
(1) Vis, at hvis m er et psp$_b$-tal, så er $b^{m/p-1} \equiv 1 \pmod{p}$.
(2) Vis, at hvis $m = 3p$ (hvor $p > 3$), så er m ikke et psp$_b$-tal for $b = 2, 5, 7$.
(3) Vis, at hvis $m = 5p$ (hvor $p > 5$), så er m ikke et psp$_b$-tal for $b = 2, 3, 7$.
(4) Bestem det mindste sammensatte psp$_3$-tal.

7. Et *at-primtal* er et ulige tal m, der passerer følgende test for alle b:

$$\text{at-p}_b(m): \quad m = 3 \text{ eller } m = 5 \text{ eller } m = 7 \text{ eller } b \text{ er ulige.}$$

Vis, at hvis m *ikke* er et at-primtal, så er sandsynligheden for at m passerer testen at-p$_b$ mindre end $\frac{1}{2}$. Hvad er sandsynligheden for at et tal m, tilfældigt frembragt med N ciffre, og testet k gange „yes" med at-p, ikke er et at-primtal.

6. RSA, og andre public key systemer.

(6.1). A skal sende en meddelelse til B. Denne situation forekommer naturligvis utallige gange i vores dagligdag: vi kommunikerer, vi signalerer, vi meddeler os til hinanden. I en kryptologisk sammenhæng er det naturligvis nogle specielle aspekter af situationen, der er interessante. En del af disse aspekter kan sammenfattes i en række nøgleord: *hemmelighed, autenticitet/ægthed (integritet og signatur)*, og *simpelhed*. Disse aspekter vil være hovedemnet i det følgende. Bemærk, at meddelelsens *indhold* overhovedet ikke er medregnet blandt de interessante.

Hemmelighed er naturligvis ønsket om, at meddelelsen skal kunne sendes uden at udenforstående får information om indholdet. Tænk fx på

en spion, der vil sende meddelelser til udenrigsministeriet,
en repræsentant, der vil sende sine salgstal til hovedkontoret,
en bank, der vil sende kontooplysninger til en kunde,
en dankort-terminal, der skal videregive en transaktions-besked til hovedterminalen,
en student, der vil betale et køb af noter via internettet,

eller et utal af lignende situationer. Ofte vil hemmelighed søges opnået ved en kombination af mange metoder. Man kan bruge usynligt blæk. Man kan skjule selve udvekslingen af meddelelsen (A og B kan mødes hemmeligt, eller bruge en hemmelig telefonledning, eller brevduer, eller . . .). Man kan sløre udvekslingen (A kan hviske til B). Endelig kan man sløre selve meddelelsen: den kan *krypteres*, dvs kodes med henblik på hemmelighedsholdelse. Det sidste er naturligvis et hovedemne for kryptologi.

Autenticitet (eller *ægthed*) er nøgleord for ønsket om at kunne fastslå, at en modtagen meddelelse er autentisk. Der er forskellige grader vægt, det kan tillæges et sådant ønske. *Integritet* er i denne forbindelse B's ønske om vide med sikkerhed, at det modtagne virkelig kom fra A, og er identisk med det som blev afsendt. B skal altså kunne overbevises om, at A var afsenderen, og at ingen udenforstående har ændret, fjernet eller tilføjet noget. *Signatur* er A's underskrift på meddelelsen. I sin yderste konsekvens er det ønsket om, at det kan fastslås overfor trediemand, om en meddelelse B har modtaget, faktisk er blevet afsendt af A. Det er her ikke nok, at B føler sig overbevist om, at A var afsenderen. Det skal også kunne bevises i en retssal; specielt skal det også kunne udelukkes, at det var B selv, der havde produceret meddelelsen. Ønsket om integritet og/eller signatur er et spørgsmål om ægthed. Det er principielt uafhængigt af ønsket om hemmelighed. Eksemplerne ovenfor kan illustrere varierende ønsker om ægthed. Som yderligere eksempel kan anføres en flerbruger-datamat, hvor den enkelte bruger fastslår sin ægthed ved hjælp af et 'password'.

Simpelhed er (delvist) selvforklarende: Det skal være så simpelt at kryptere en meddelelse, at selv en computer kan gøre det (i rimelig tid). Hvis det ønskes, skal den retmæssige modtager af en hemmelig meddelelse kunne rekonstruere det originale indhold i rimelig tid.

(6.2). Når der anvendes kryptering, sender A ikke selve meddelelsen (den såkaldte *klartekst*) til B. I stedet sendes en *krypteret* version, som vi her vil kalde h-teksten (h for „hemmelig“). Det forudsættes, at B ud fra den modtagne h-tekst er i stand til at forstå den information, der lå i klarteksten. Mere præcist forudsættes, at B kan rekonstruere klarteksten, altså at B kan *dekryptere* (dekode, decifrere) h-teksten. En model af denne situation er følgende: Idet $\mathcal{K}$ betegner mængden af klartekster og $\mathcal{H}$ betegner mængden af h-tekster, er kryptering en transformation, dvs en afbildning,

$$E : \mathcal{K} \to \mathcal{H},$$

og dekryptering er en transformation,

$$D : \mathcal{H} \to \mathcal{K}.$$

Det forudsættes, at DE er den identiske afbildning på mængden af klartekster. Afsendelse af klarteksten t fra A til B foregår altså i tre skridt. Først krypterer A klarteksten t til h-teksten $\tau = E(t)$. Dernæst sendes h-teksten τ fra A til B. Endelig dekrypterer B den modtagne h-tekst τ til klarteksten $D(\tau) = DE(t) = t$.

Vi vil oftest forudsætte, at $\mathcal{K} = \mathcal{H}$. I praksis er hver klartekst blot en sekvens af tegn, og h-teksterne antages altså at være (mystisk udseende) sekvenser bestående af den samme slags tegn. Vi vil yderligere forudsætte, at $\mathcal{K}$ er en endelig mængde. Som nævnt vil meddelelserne i praksis være sekvenser af tegn, og det forudsættes altså specielt, at hver klartekst har en på forhånd fastlagt længde. Større tekster sendes så blot ved at sende flere mindre klartekster. Under disse antagelser følger det af forudsætningerne, at E og D er bijektive afbildninger, og „hinandens inverse“.

I praksis kan vi altid tænke på $\mathcal{K}$ som en mængde af tal $1, 2, \dots, n$, eller som restklasserne i $\mathbb{Z}/n$. En tekststreng med k tegn, hvor hvert tegn er et af 256 mulige (i en udvidet ASCII-kodning), kan identificeres med et tal skrevet i 256-talssystemet. Når $n \geqslant 256^k$, kan sådanne tekststrenge altså identificeres med tal i intervallet $[0, n-1]$, og dermed med restklasser i $\mathbb{Z}/n$.

(6.3) Eksempel. I de helt klassiske krypteringer er $\mathcal{K} = \mathcal{H}$ blot mængden bestående af de 26 bogstaver i det engelske(!?) alfabet. Krypteringstransformationen er altså her en af de mulige 26! permutationer. Identificeres bogstaverne på oplagt måde med restklasser i $\mathbb{Z}/26$, kan fx *Cæsar's kodning* beskrives som permutationen $x \mapsto x + 3$. Herefter krypteres

SEND MORE MONEY til VHQG PRUH PRQHB.

Krypteringer, hvor mængden $\mathcal{K}$ er lille, kan ofte brydes. Fx kan man anvende frekvensanalyse: bogstavet E er det hyppigst forekommende bogstav, så ud fra h-teksten ovenfor ville man gætte på, at E $\mapsto$ H. Med kendskab til, at krypteringstransformationen er af formen $x \mapsto x + b$, er koden altså allerede brudt: $b = 3$.

(6.4). Med computere kan man let anvende krypteringstransformationer af mængder $\mathcal{K}$, der er store. Et eksempel er DES (Data Encryption Standard). Her består $\mathcal{K}$ af bit-følger af længde 64; der er altså 2^{64} „klartekster“. Krypteringstransformationerne, der indgår i DES, er permutationer af denne mængde. Hver transformation (og dens inverse) bestemmes ved en *nøgle*. Hver nøgle κ bestemmer en tilhørende transformation E_κ og dens inverse D_κ. I

DES er der 2^{56} mulige nøgler. Permutationerne i DES udgør altså en beskeden brøkdel af samtlige $(2^{64})!$ mulige permutationer.

Kryptografiske transformationer, der anvendes i praksis, indgår altid i hele familier af transformationer; de udgør, i lighed med DES, et *kryptosystem*, bestemt ved brugen af et bestemt princip for kryptering. Dette er bekvemt, hvis flere brugere skal sende meddelser til hinanden, eller hvis to brugere ønsker at kunne skifte krypterings-transformation med mellemrum. I en sådan familie af transformationer (og deres inverse) er den enkelte transformation bestemt ved en såkaldt *nøgle*. Kendskab til nøglen fastlægger altså den pågældende transformation fra familien. I et *klassisk krypto-system* fastlægger nøglen også den inverse transformation. I et sådant system kommunikerer to brugere ved at aftale hvilken nøgle, de vil benytte. Vanskeligheden er her at hemmeligholde nøglen for uvedkommende.

I praksis vil $\mathcal{K}$ være stor, fx med 10^{200} elementer. Her er det ikke svært at tro på, at man kan vælge (simple) krypteringsafbildninger, der undrager sig en analyse, som den der er skitseret i (6.3). Mere overraskende er måske følgende:

(6.5) Påstand. *Der findes (simple) bijektive afbildninger E (af endelige mængder), der har (simple) inverse afbildninger D, men alligevel er så komplicerede, at man ikke alene ud fra kendskab til afbildningen E kan bestemme den inverse afbildning.*

Set i et matematisk lys er påstanden forhåbentlig rystende. Vi er vant til, at hvis E er en bijektiv afbildning, så er den inverse afbildning D jo „blot" afbildningen E^{-1}. Alligevel vil vi bygge en hel teori på eksistensen af sådanne *envejs-afbildninger* ('one-way functions'). Denne teori hviler således på et grundlag, der kan forekomme foruroligende spinkelt.

En envejs-afbildning E kan bruges til hemmelighedsholdelse. Antag, at B er i besiddelse af afbildningen E og at kun B kender den inverse afbildning D. Afbildningen E kan da gøres offentlig kendt. Herefter kan A meddele klarteksten t til B ved at sende h-teksten $\tau = E(t)$. Da B er den eneste, der kender den inverse afbildning D, er B den eneste, der kan dekryptere den modtagne h-tekst τ tilbage til klarteksten $D(\tau) = DE(t) = t$.

En envejs-afbildning E kan også bruges i forbindelse med ægthed. Antag her, at A er den eneste, der kender den inverse afbildning D til E. A's *signatur* er så $\sigma = D(s)$, hvor s er en simpel tekst, der indeholder fx navn, personnummer, et tidsstempel (dato og klokkeslet) og lignende. At signaturen σ kommer fra A kontrolleres med den offentlige afbildning E ved, at $E(\sigma) = ED(s) = s$ er denne simple tekst. Og det er kun A, der kan have frembragt signaturen, idet kun A har kendskab til D.

(6.6). Anvendelsen af envejs-afbildninger i forbindelse med kryptosystemer blev først foreslået af Diffie og Hellman (1976). Resultatet er et såkaldt *public key system*. Et 'public key' system opfattes nu som et system, hvor der for hver bruger A er en sådan (offentlig kendt) envejs-afbildning E_A (fastlagt ved en simpel nøgle), og hvor kun brugeren A har kendskab til den inverse afbildning D_A. Brugeren A kan så sende klarteksten t hemmeligt til B ved at sende h-teksten $\tau = E_B(t)$. Ægthed opnås ved at A inkluderer sin signatur $\sigma_A = D_A(s_A)$ i sin klartekst, altså ved at A afsender h-teksten $E_B(t\sigma_A)$ til B. Integritet opnås ved at A i stedet sender h-teksten $\tau = E_B(tD_A(t\sigma_A))$ til B. Afsendelsen er hemmelig, idet kun B kan dekryptere med sin hemmelige afbildning D_B til $D_B(\tau) = tD_A(t\sigma_A)$; herved fremkommer dels klarteksten t, dels h-teksten $D_A(t\sigma_A)$. På denne h-tekst kan B anvende den offentlig nølge E_A og derved frembringe klarteksten ts_A; herved kan B kontrollere integriteteten (de to modtagne eksemplarer af t er identiske) og A's underskrift s_A.

(6.7). I det følgende vil vi hovedsagelig betragte et enkelt 'public key' system, *RSA-systemet* fra 1978. Det er opkaldt efter fædrene Rivest, Shamir og Adleman. Vi vil omtale både teoretiske og praktiske spørgsmål i forbindelse med RSA.

I systemet indgår en beskrivelse af en række envejs-afbildninger. De indgående mængder er restklasseringe af formen $\mathbb{Z}/n$. Tallet n er i det følgende et fast, stort (ulige) naturligt tal (der opfylder en række nærmere angivne betingelser). Med $\lambda(n)$ betegnes eksponenten for gruppen $(\mathbb{Z}/n)^*$. Når n er kvadratfri, altså et produkt $n = p_1 \cdots p_r$ af forskellige primtal p_i, er $\lambda(n)$ det mindste fælles multiplum af tallene $p_i - 1$. Den elementære talteori, der ligger til grund for systemet, er det efterfølgende resultat.

(6.8) Sætning. *Antag, at n er kvadratfri, $n = p_1 \cdots p_r$. For hvert naturligt tal e gælder da, at afbildningen $E_e\colon \mathbb{Z}/n \to \mathbb{Z}/n$, bestemt ved*

$$E_e\colon x \mapsto x^e, \tag{6.8.1}$$

er bijektiv, hvis og kun hvis e er primisk med hvert af tallene $p_i - 1$. De bijektive afbildninger af formen (6.8.1) *udgør en undergruppe $\mathcal{E}$ af permutationsgruppen for $\mathbb{Z}/n$.*

Antag, at $l \geqslant 1$ er et multiplum af tallene $p_i - 1$. Når e er primisk med l, er den inverse afbildning $D = E_e^{-1}$ bestemt ved

$$D = E_d\colon y \mapsto y^d, \quad \text{hvor } d \geqslant 1 \text{ opfylder, at } de \equiv 1 \pmod{l}. \tag{6.8.2}$$

Yderligere gælder, at afbildningen, der til et tal e primisk med l knytter afbildningen E_e, er en veldefineret, surjektiv gruppehomomorfi $(\mathbb{Z}/l)^* \twoheadrightarrow \mathcal{E}$. Den er en isomorfi, hvis og kun hvis $l = \lambda(n)$ er det mindste fælles multiplum af tallene $p_i - 1$; specielt har $\mathcal{E}$ orden $\varphi(\lambda(n))$.

Bevis. Vi bemærker først, at under antagelsen om l gælder, for alle hele tal $c \geqslant 1$ og $k \geqslant 0$ (og $x \in \mathbb{Z}$), følgende kongruens:

$$x^{c+kl} \equiv x^c \pmod{n}. \tag{*}$$

Da n er kvadratfri, er kongruensen (*) nemlig opfyldt, hvis den er opfyldt modulo p_i for alle i. Modulo p_i er begge sider 0, hvis $p_i \mid x$ (idet eksponenterne er positive). Hvis $p_i \nmid x$ benyttes Fermat's lille sætning: Modulo p_i er $x^{p_i - 1} \equiv 1$, og da l, og dermede også kl, er et multiplum af $p_i - 1$, følger det at $x^{kl} \equiv 1$; altså er $x^{c+kl} = x^c x^{kl} \equiv x^c$.

Afbildningen E_e er naturligvis defineret for alle eksponenter $e \geqslant 1$, og det er klart, at $E_{ce} = E_c E_e$ for alle naturlige tal c, e. Af (*) fremgår, at afbildningen E_e kun afhænger af e's restklasse modulo l.

Antag først, at e ikke er primisk med hvert af tallene $p_i - 1$. Så har e en (prim-)divisor $h > 1$ fælles med et af tallene $p_j - 1$. Gruppen $(\mathbb{Z}/p_j)^*$ er cyklisk af orden $p_j - 1$, og indeholder derfor et element af orden h. Specielt findes et helt tal a_0 således, at der modulo p_j gælder

$a_0 \not\equiv 1$ og $a_0^h \equiv 1$; da $h \mid e$, er $a_0^e \equiv 1$. Vælg nu, ifølge Den kinesiske Restklassesætning, et tal a med $a \equiv a_0 \pmod{p_j}$ og $a \equiv 1 \pmod{p_i}$ for $i \neq j$. Modulo n er $a \not\equiv 1$, men $a^e \equiv 1$, thi modulo p_j er $a^e \equiv a_0^e \equiv 1$, og modulo p_i med $i \neq j$ er $a^e \equiv 1^e = 1$. Kongruensen $x^e \equiv 1$ har altså modulo n de to forskellige løsninger 1 og a. Afbildningen E_e er derfor ikke injektiv.

Øjensynlig er e er primisk med tallene $p_i - 1$, hvis og kun hvis e er primisk med $\lambda(n)$, og det er opfyldt, når e er primisk med et multiplum l af $\lambda(n)$. Antag, at e er primisk med l. Da har kongruensen i (6.8.2) en løsning $d \geqslant 1$. Det påstås, at $E = E_e$ er bijektiv, med $D = E_d$ som den inverse. Det skal altså vises, at $ED = DE$ er den identiske afbildning af $\mathbb{Z}/n$, altså at der for alle hele tal x gælder kongruensen,

$$x^{de} \equiv x \pmod{n}.$$

Ifølge antagelsen findes en ligning $de = 1 + kl$, nødvendigvis med $k \geqslant 0$. Den søgte kongruens følger derfor umiddelbart af (*).

Hermed er sætningens først påstand bevist. Af det foregående følger videre, at afbildningen, der til $e \geqslant 1$ primisk med l knytter permutationen E_e, er en veldefineret homomorfi fra gruppen $(\mathbb{Z}/l)^*$ ind i gruppen af alle permutationer af $\mathbb{Z}/n$. Når $l = \lambda(n)$ er billedemængden netop $\mathcal{E}$, så $\mathcal{E}$ er en undergruppe af permutationsgruppen. Når $\lambda(n)$ er divisor i l, er homomorfien $(\mathbb{Z}/l)^* \to (\mathbb{Z}/\lambda(n))^*$ som bekendt surjektiv. Derfor er homomorfien $(\mathbb{Z}/l)^* \to \mathcal{E}$ altid surjektiv.

Antag, at restklassen af $e \geqslant 1$ modulo l ligger i kernen, altså at kongruensen $x^e \equiv x$ gælder modulo n for alle x. Da gælder kongruensen også modulo p_i for alle x. Når x er primisk med p_i, så følger af $x^e \equiv x \pmod{p_i}$, at $x^{e-1} \equiv 1 \pmod{p_i}$. Da gruppen $(\mathbb{Z}/p_i)^*$ er cyklisk af orden $p_i - 1$, følger det, at $e - 1$ er et multiplum af $p_i - 1$. Altså er $e - 1$ et multiplum af $p_i - 1$ for hvert i, og dermed et multiplum af $\lambda(n)$. Kernen er altså lig med kernen for homomorfien $(\mathbb{Z}/l) \to (\mathbb{Z}/\lambda(n))^*$. Kernens orden er derfor $\varphi(l)/\varphi(\lambda(n))$, og homomorfien er injektiv, hvis og kun hvis $\varphi(l) = \varphi(\lambda(n)$. Den sidste ligning, for en lige divisor $\lambda(n)$ i l, gælder, hvis og kun hvis $l = \lambda(n)$. □

(6.9) RSA-transformationerne. En-vejs-afbildningerne i RSA-systemet kan nu beskrives som følger: Tallet n vælges som et produkt af to store (forskellige) primtal, $n = pq$. Så er $l = \lambda(n)$ bestemt som

$$l := \text{mindste fælles multiplum for } p - 1, q - 1. \tag{6.9.1}$$

Videre bestemmes tallene e og d større end 1 således, at

$$de \equiv 1 \pmod{l}; \tag{6.9.2}$$

specielt er så e (og d) primisk med l. Hertil hører afbildningerne,

$$E\colon x \mapsto x^e \pmod{n}, \quad \text{og} \quad D\colon y \mapsto y^d \pmod{n},$$

der ifølge (6.8) er permutationer af $\mathbb{Z}/n$, og „hinandens inverse“. Permutationerne af denne form udgør en gruppe $\mathcal{E}$ isomorf med $(\mathbb{Z}/l)^*$; specielt er antallet af mulige transformationer lig med $\varphi(l)$.

Afbildningen E er den offentligt kendte krypteringstransformation, og D er den hemmelig inverse. De to afbildninger kan kort beskrives ved RSA-*nøglen* (n, e, d). Af denne nøgle er parret (n, e) den *offentlige del*, som beskriver krypteringstransformationen $E\colon x \mapsto x^e$. Tallet d er den *hemmelige del* af nøglen. Det er offentligt kendt, at n er et produkt af to store primtal, men selve primtallene holdes hemmelige.

Påstanden er nu, at det er muligt at vælge n, e, d således, at krypteringstransformationen $x \mapsto x^e$ er en envejs-funktion, dvs således, at d ikke (i praksis) kan bestemmes alene ud fra (n, e). Bemærk, at d umiddelbart kan bestemmes ud fra n, e og $l = \lambda(n)$ ved hjælp af (6.9.2). Det er altså en del af påstanden, at $\lambda(n)$ ikke (i praksis) kan bestemmes ud fra n. Specielt er det en del af påstanden, at man, på trods af en viden om, at n er et produkt af to primfaktorer, ikke kan bestemme disse to faktorer.

Som nævnt i (6.9) er afbildningerne $E = E_e$ og $D = E_d$ „hinandens inverse", hvis det blot forudsættes, at l er et fælles multiplum af $p - 1$ og $q - 1$. I forbindelse med RSA kan det være naturligt fx at vælge

$$l = (p-1)(q-1). \tag{6.9.3}$$

Det skal understreges, at beskrivelsen i (6.8) af gruppen $\mathcal{E}$ af alle RSA-transformationer, og specielt at antallet af transformationer er bestemt som $\varphi(l)$ kun gælder, når $l = \varphi(n)$, dvs når l er bestemt ved 6.9.1.

Antag, mere generelt, at $n = pq$ er et produkt af to primiske faktorer p, q, hvor både p og q er pseudoprimtal, dvs et primtal eller et Carmichael-tal. Af karakteriseringen af Carmichael-tal følger specielt, at n er kvadratfri. Hver primdivisor p_i i n divisor i p eller i q, og så følger det videre, at $p_i - 1$ divisor i $p - 1$ eller i $q - 1$. Derfor vil tallet l defineret ved (6.9.1) (eller ved (6.9.3)) opfylde betingelserne i (6.9), og under de givne forudsætninger om e og d vil afbildningerne E_e og E_d være hinandens inverse. Men det skal understreges, at hvis en af de to faktorer p, q er et Carmichael-tal (og altså ikke et primtal), så vil tallet l defineret ved (6.9.1) sædvanligvis ikke være lig med $\lambda(n)$.

(6.10) RSA-systemet. RSA-systemet kan nu kort beskrives således: Hver bruger A af systemet vælger som ovenfor en nøgle (n_A, e_A, d_A). Meddelelser til brugeren B krypteres som angivet i (6.6) ved at bruge krypteringstransformationen E_B svarende til den offentlige del (n_B, e_B) af B's nøgle. Her forudsættes altså, at de klartekster, der skal sendes til B, består af et (eller flere) tal, der er mindre end n_B (og derfor kan opfattes som element i restklasseringen $\mathbb{Z}/n_B$). En afsender A underskriver ved at anvende sin hemmelig dekryptering D_A på sin signatur s_A. En modtager kontrollerer signaturen ved at anvende A's offentlige kryptering E_A på den modtagne signatur $D_A(s_A)$.

(6.11) Angreb på RSA. I det følgende omtales en række forhold, der har betydning for sikkerheden i RSA-systemet. Som nævnt er det en forudsætning, at krypteringstransformationerne i systemet, dvs de bijektive afbildninger af formen

$$E\colon x \mapsto x^e \pmod{n}$$

hørende til RSA-nøgler (n, e, d), er envejs-afbildninger. Det er således en nødvendig forudsætning, at tallenene n er store – så store, at man ikke ved at tabellægge afbildningen E, eller ved udtømmende søgning, kan bestemme den inverse afbildning $D\colon y \mapsto y^d$.

Hvornår er et tal stort? Det er en god tommelfingerregel, at alle i naturen forekommende (naturlige) tal (antal) er mindre end 10^{50}. Universets alder er $10^{18}\,sec$, dets diameter er $10^{22}\,m$. Jordens rumfang $10^{22}\,m^3$. Et atom fylder $10^{-30}\,m^3$. En øvre grænse for antallet af atomer i universet (i sig selv et ret unaturligt antal) er således 10^{70}. I denne forstand er 10^{50} altså et stort tal, og tal med fx det dobbelte antal cifre er endog meget store. Bemærk, at angivelsen af et enkelt bestemt tal af denne størrelsesorden ikke fylder særlig meget. Fx er tallet n herunder:

403973053172146480004640109925029870946484075995819629605478298423496995260211882781424365195345494425377235497204137003,

et tal med 120 cifre. Vi kan sagtens regne med tal af denne størrelsesorden, fx multiplicere tallet n ovenfor med sig selv, men vi kan ikke drømme om at få en computer til at gennemløbe alle tallene mindre end n. Sandsynligheden for at et tilfældigt tal med 120 cifre netop er tallet n, er naturligvis forsvindende.

Sikkerheden i en given RSA-nøgle (n, e, d) hviler på påstanden om man ikke alene med kendskab til den offentlige del (n, e) kan bestemme den inverse afbildning D til afbildningen $E\colon x \mapsto x^e \pmod n$ — på trods af en viden om at n er et produkt af to primtal, og på trods af en viden om at den inverse afbildning D har formen $y \mapsto y^d$ med et passende tal d. [Jeg kan i øvrigt fortælle, at tallet n herover indgår i en RSA-nøgle (n, e, d), hvor e er følgende tal:

242383831903287888002784065955017922567890445597491777763286181173909355814409107124533522394028213426536142542190639885,

men jeg røber selvfølgelig ikke mit hemmelige d.]

(6.12). I det følgende betragtes en RSA-nøgle (n, e, d), med den offentlige del (n, e). Det mest oplagte angreb på nøglen er naturligvis at forsøge at faktorisere n i de to primfaktorer p og q. Hvis fjenden F kender p og q, så kan F umiddelbart beregne $\varphi(n) = (p-1)(q-1)$ eller $\lambda(n)$; herefter kan F ud fra e bestemme (et brugbart) d, og dermed den inverse afbildning $D\colon y \mapsto y^d$. Vi har altså:

Angreb. *Nøglen er brudt, hvis fjenden F kan faktorisere n.*

Forholdsregel. Den primære sikkerhed ved RSA-systemet bygger som sagt på troen på, at det er ikke er muligt at faktorisere n, når de to primfaktorer p og q er store (og passende valgte). Denne tro hviler på, at alle kendte metoder til faktorisering har et tidsforbrug, der vokser eksponentielt med størrelsen af det tal n, der skal faktoriseres. Troen rokkes ikke af, at der konstrueres hurtigere computere. Antag, at et givet RSA-system opererer med nøgler af en størrelse, som det med dagens hurtigste computere vil tage tusind år at faktorisere (i praksis opereres med en endnu større sikkerhedsmargin). Hvis regnekraften forøges med en faktor 10^{10} (det svarer vist til forskellen mellem en kugleramme og en PC), kan disse nøgler brydes på 3 sekunder. Men en simpel forøgelse af nøglelængden til det 10-dobbelte vil gøre nøglerne ubrydelige for de nye computere.

Det bemærkes, at „umuligheden" af at faktorisere n ikke alene sikres af, at p og q er store. Specielle (uheldige) egenskaber ved p og q vil gøre faktorisering mulig i overkommelig tid. Vi vil senere skitsere nogle få metoder til faktorisering. Herunder omtales yderligere nogle forhold i forbindelse med angreb på RSA.

Bemærkning. Som anført ovenfor afhænger brydningen ved faktorisering af, at F ud fra primfaktorerne p og q i n umiddelbart kan bestemme $\varphi(n) = (p-1)(q-1)$. Omvendt, hvis F kender tallet $k = \varphi(n)$, så er $n - k = pq - (p-1)(q-1) = p + q - 1$ kendt af F, og herefter kan p og q umiddelbart bestemmes som rødderne i polynomiet $X^2 - (n-k+1)X + n$; F kan altså bryde nøglen. For en RSA-nøgle svarer faktorisering af n altså til at bestemme $\varphi(n)$.

(6.13) Angreb. *Hvis fjenden har fundet to tal z og w, så at der modulo n gælder: $z^2 \equiv w^2$ og $z \not\equiv \pm w$, så kan fjenden faktorisere n.*

Bevis. Ifølge forudsætningen gælder, at

$$n \mid z^2 - w^2 = (z-w)(z+w).$$

Hvert af primtallene p og q går derfor op i højresiden, og dermed i en af faktorerne $z - w$ og $z + w$. Hvis p og q begge er divisorer i $z - w$, så ville n være divisor i $z - w$, i modstrid med at $z \not\equiv w$. Tilsvarende udelukkes, at både p og q er divisor i $z + w$. Præcis ét af primtallene p og q er derfor divisor i $z - w$, og dette primtal må være den største fælles divisor $(z - w, n)$. Beregning af denne største fælles divisor giver altså umiddelbart den ene primfaktor i n. ∎

Bemærkning. Ifølge Den kinesiske Restklassesætning er

$$\mathbb{Z}/n = \mathbb{Z}/p \times \mathbb{Z}/q,$$

så restklasser x modulo n svarer til par $x = (x_1, x_2)$ af restklasser modulo henholdsvis p og q. Ligningen $z^2 = w^2$ i $\mathbb{Z}/n$ svarer herved til et par af ligninger, $z_i^2 = w_i^2$ for $i = 1, 2$, i restklasseringene modulo p og q. Heraf følger, at ligningen $z^2 = w^2$ gælder, hvis og kun hvis $z = (z_1, z_2)$ er et af de 4 par (w_1, w_2), $(-w_1, -w_2)$, $(-w_1, w_2)$ eller $(w_1, -w_2)$. De 4 par er naturligvis kun forskellige, når $w_1 \neq 0$ og $w_2 \neq 0$, dvs når w er en primisk restklasse modulo n. Restklasserne z og w fra angrebet må altså være primiske restklasser; specielt ses, at F i stedet for z og w i angrebet kan anvende zw^{-1} og 1.

Forholdsregel. Hvis det er „umuligt" at faktorisere n, må det jo specielt være umuligt at finde z og w med egenskaben i angrebet. Som nævnt i bemærkningen ovenfor er det nok at sikre, at fjenden ikke kan finde et tal z, som modulo n opfylder, at $z \not\equiv \pm 1$ og $z^2 \equiv 1$. Det fremgår ovenfor, at der er præcis 2 tal z med denne egenskab, så det kan i hvert fald udelukkes, at F finder et sådant z „tilfældigt". ∎

(6.14). Specielt i forbindelse med RSA spiller såkaldte *probabilistiske algoritmer* en rolle. Det er jo ikke nok at tro på, at der ikke findes nogen effektiv metode, der med sikkerhed faktoriserer n. Hvis F har en metode, der med en sandsynlighed på blot én procent faktoriserer et naturligt tal af den optrædende størrelsesorden i rimelig tid, så skal det jo nok vise sig, at den RSA-nøgle, som vi har konstrueret, kan brydes af F på ingen tid.

Angreb. *Antag, at F har fundet et tal $f \geqslant 1$ således, at der for alle x, der er primiske med n gælder:*

$$x^f \equiv 1 \pmod{n}. \tag{6.14.1}$$

Da kan F med vilkårlig stor sandsynlighed faktorisere n.

Bevis. Tallet f må nødvendigvis være lige, thi ellers fås en modstrid ved at sætte $x := -1$ i (6.14.1). Nu erstattes f med $f/2$, og det undersøges, om (6.14.1) er opfyldt med den nye værdi af eksponenten f. Ved denne undersøgelse må F erklære sig tilfreds med en sandsynlighed: betingelsen efterprøves med en række tilfældige værdier af x. Det er klart, at hvis betingelsen ikke er opfyldt for alle x, så vil den ikke være opfyldt for mindst halvdelen af x'erne. Enten findes altså et x, hvor betingelsen ikke er opfyldt, eller også er betingelsen opfyldt for så mange x'er, at den med stor sandsynlighed er opfyldt for alle x.

Hvis betingelsen er opfyldt for den nye værdi af f gentages proceduren. Efter endelig mange skridt nås herved en værdi g, for hvilken betingelsen (6.14.1) er opfyldt med eksponenten $f = 2g$, men ikke med eksponenten g.

Betragt nu gruppen $G := (\mathbb{Z}/n)^*$ og den ved $x \mapsto x^g$ bestemte afbildning $G \to G$. Denne afbildning er klart en homomorfi. Ifølge Den kinesiske Restklassesætning er $G = (\mathbb{Z}/p)^* \times (\mathbb{Z}/q)^*$, og herved svarer elementerne i G, dvs de primiske restklasser x modulo n, til par $x = (x_1, x_2)$ af primiske restklasser modulo henholdsvis p og q. Specielt svarer homomorfien $x \mapsto x^g$ til homomorfien,

$$(x_1, x_2) \mapsto (x_1^g, x_2^g).$$

Valget af g sikrer, at billedgruppen består af mere end $(1, 1)$ og at der for alle (y_1, y_2) i billedgruppen gælder, at $y_1^2 = 1$ og $y_2^2 = 1$. Modulo et primtal gælder, at hvis $y^2 = 1$, så er $y = \pm 1$. De mulige par i billedgruppen er derfor $(1, 1)$, $(1, -1)$, $(-1, 1)$ og $(-1, -1)$. De to par $(1, 1)$ og $(-1, -1)$ udgør øjensynlig en undergruppe i G, og originalmængden hertil udgør derfor en undergruppe H i G. Øjensynlig består H af de elementer x i G, for hvilke $x^g = \pm 1$. Undergruppen H er en ægte undergruppe af G. Ifølge antagelsen findes nemlig et par (x_1, x_2), så at billedet (x_1^g, x_2^g) ikke er $(1, 1)$. Det kan fx antages, at $x_1^g = -1$. Og så er $(x_1, 1)$ et element, der ikke tilhører H.

Da H ifølge ovenstående er en ægte undergruppe i G, har komplementærmængden til H mindst lige så mange elementer som H. Fjenden F tager nu modulo n et tilfældigt tal x, og betragter $z := x^g$. Modulo n er $z^2 \equiv 1$. Hvis x ikke tilhører H, er $z \not\equiv \pm 1$, og tallene z og 1 opfylder derfor betingelserne i Angreb (6.13). Da et tilfældigt tal x med sandsynlighed $\frac{1}{2}$ ikke tilhører H, kan F derfor opnå en ikke-triviel divisor i n med enhver ønsket sandsynlighed. □

Forholdsregel. Hvis det er „umuligt“ at faktorisere n, må det jo specielt være „umuligt“ at finde f med egenskaben i angrebet. At f har egenskaben betyder, at hvert element i gruppen $(\mathbb{Z}/n)^*$ har en orden, der er divisor i f. Ifølge Den kinesiske Restklassesætning har vi ligningen $(\mathbb{Z}/n)^* = (\mathbb{Z}/p)^* \times (\mathbb{Z}/q)^*$. De to grupper på højresiden er som bekendt cykliske grupper af orden $p - 1$ og $q - 1$. Tallet f har derfor egenskaben, hvis og kun hvis f er delelig med både $p - 1$ og $q - 1$. Specielt må f være et stort tal, så sandsynligheden for at F „tilfældigt“ finder et sådant f, er forsvindende. □

Bemærkning. En nærmere analyse af Angreb (6.14) viser, at det må udelukkes, at F kan bestemme f, så at (6.14.1) er opfyldt for bare en ikke-forsvindene brøkdel af x'er. For et givet f ses ved brug af Den kinesiske Restklassesætning, at antallet af x'er, der er primiske med n og opfylder (6.14.1), er bestemt som produktet $(f, p-1)\cdot(f, q-1)$. Antallet er således lille, med mindre f er meget speciel (og det er et „tilfældigt" tal f ikke).

(6.15) Angreb. *Hvis F for et givet n kan bryde en RSA-nøgle (n, e) for bare én værdi $e > 1$ (fx for en værdi af e som F selv har fundet), da kan F med vilkårlig stor sandsynlighed faktorisere n.*

Bevis. At bryde nøglen svarer til at bestemme d, så at $x^{ed} \equiv x \pmod n$ for alle x. Når x er primisk med n følger det, at $x^{ed-1} \equiv 1$. Med $f := ed - 1$ er betingelsen i Angreb (6.14) derfor opfyldt. □

Forholdsregel. Det følger, at man ikke i et RSA-system kan bruge nøgler (n, e_A, d_A) med samme n til en hel familie af brugere. Enhver bruger ville nemlig så ud fra sin hemmelig del af nøglen kunne bryde alle de andre nøgler i systemet.

(6.16). Da tallet n er sammensat, vil n næppe passere ret mange af de såkaldte primtalstests, der for et tilfældigt (eller måske velvalgt) tal $b < n$ undersøger visse kongruenser modulo n. Hvis et sådant b ikke er primisk med n, kan F øjensynlig bestemme p eller q som den største fælles divisor for b, n. Det er udelukket, at F tilfældigt finder et sådant b, idet brøkdelen af tal $b < n$, som ikke er primiske med n, er givet ved

$$\frac{n-\varphi(n)}{n} = \frac{pq-(p-1)(q-1)}{pq} = \frac{1}{p} + \frac{1}{q} - \frac{1}{pq};$$

når p og q er store, er brøkdelen altså forsvindende.

Som bekendt har disse tests forskellig styrke. A priori kan følgende angreb derfor ikke udelukkes:

Angreb. *Antag, at F kan finde et tal b, således at n passerer „Fermat-testen"* psp_b *og ikke Miller–Rabin's test* s-psp_b*. Da kan F faktorisere n.*

Bevis. Antag, at b opfylder betingelsen i angrebet. Som bekendt betyder psp_b, at

$$b^{n-1} \equiv 1 \pmod{n}. \tag{6.16.1}$$

Skriv $n - 1 = u2^s$, hvor u er ulige. At n ikke passerer s-psp_b betyder så, modulo n, at $x_0 := b^u \not\equiv 1$ og at kvadraterne $x_j := x_{j-1}^2$ for $j = 1, \dots, s-1$ aldrig er $\equiv -1$. Da $x_s = b^{n-1} \equiv 1$, kan F derfor bestemme det første j, for hvilket $x_{j+1} \equiv 1$. For $z := x_j$ er $z \not\equiv \pm 1$ og $z^2 \equiv 1$. Betingelserne for Angreb (6.13) er derfor opfyldt, og følgelig kan F faktorisere n. □

Forholdsregel. Sørg for, at F slet ikke kan finde et $b < n$ således, at n passerer psp_b. Antallet af sådanne tal b er, som det let ses, lig med produktet $(n-1, p-1)\cdot(n-1, q-1)$. Nu er $n - 1 = pq - 1 = q(p-1) + q - 1$, så den første faktor er lig med $(q-1, p-1)$. Tilsvarende ses, at den anden faktor er lig med $(p-1, q-1)$. Antallet er altså kvadratet,

$$(p-1\,, q-1)^2,$$

på den største fælles divisor for $p - 1$ og $q - 1$. Det ønskede kan derfor opnås ved at sørge for at denne fælles divisor er lille.

(6.17) Angreb. *Hvis F ved iteration af krypteringstransformationen $E: x \mapsto x^e$ kan bestemme en potens E^i, som er den identiske afbildning (dvs opfylder $E^i(x) = x$ for alle x), så kan F bryde nøglen.*

Bevis. Af $E^{i-1}E = E^i = \mathrm{id}$ følger, at dekrypteringstransformationen er $D = E^{i-1}$. Herved er nøglen brudt. ∎

Bemærkning. Dekrypteringstransformationen D bestemt ved angrebet ovenfor har formen $y \mapsto y^d$, hvor $d = e^{i-1}$. Dette d vil normalt være betydeligt større end det d, der hørte til den hemmelige del af nøglen.

Forholdsregel. Krypteringstransformationerne er de bijektive afbildninger $E: x \mapsto x^e$. De udgør gruppen $\mathcal{E}$. Tallet i fra angrebet (eller rettere sagt det mindste i med egenskaben i angrebet) er ordenen af transformationen E i gruppen $\mathcal{E}$. Det er således nødvendigt at sikre, at „alle“ krypteringstransformationer har „stor“ orden.

Ifølge Sætning (6.8) er gruppen $\mathcal{E}$ isomorf $(\mathbb{Z}/l)^*$, hvor l er det mindste fælles multiplum af $p-1$ og $q-1$. Det skal altså sikres, at „alle“ elementer i gruppen $(\mathbb{Z}/l)^*$ har stor orden. Denne gruppe har orden $\varphi(l)$. For at sikre, at alle elementer har stor orden er det ifølge nedenstående Lemma (6.18) nok at sikre, at gruppens orden indeholder en stor primfaktor r. Hertil er det igen nok at sikre, at følgende betingelse er opfyldt: $p-1$ indeholder en stor primfaktor s således at $s-1$ indeholder en stor primfaktor r. Antag nemlig, at den sidste betingelse er opfyldt. Da $p-1$ er divisor i l, vil s så være divisor i l. Følgelig vil $s-1$ være divisor i $\varphi(l)$. Da r er divisor i $s-1$, vil r så være (en stor) primdivisor i $\varphi(l)$, som påstået.

(6.18) Lemma. *Lad G være en (endelig) kommutativ gruppe, og lad r være en primdivisor i ordenen af G. Da vil højst $1/r$ af elementerne i G have en orden, som ikke er et multiplum af r.*

Bevis. Af Struktursætningen for kommutative grupper følger specielt, at G er et produkt,

$$G = G' \times G'' \tag{6.18.1}$$

af undergrupperne G' og G'', hvor G' består af de elementer i G, hvis orden går op i en potens af r, og G'' består af de elementer, hvis orden er primisk med r. Yderligere er G' ikke triviel, idet r var divisor i ordenen af G. Svarende til fremstillingen (6.18.1) består G af par $z = (z', z'')$, hvor $z' \in G'$ og $z'' \in G''$. Det er klart $z^h = 1$, hvis og kun hvis både z' og z'' har ordener, der er divisorer i h. Hvis $z' \neq 1$, så har z' en orden, der er en potens af r og større end 1; specielt er ordenen så et multiplum af r. Det er således kun elementerne af formen $z = (1, z'')$, dvs kun elementerne i G'', hvis orden ikke er delelig med r. Brøkdelen af disse elementer er

$$|G''|/|G| = 1/|G'|,$$

som med sikkerhed højst er $1/r$. Hermed er Lemma'et bevist. ∎

(6.19). Bemærk, at sikkerheden af en given krypteringstransformation E ikke kun afhænger af at den inverse $D = E^{-1}$ ikke kan bestemmes. Det skal også sikres, at fjenden F ikke udfra en eneste funktionsværdi $y = E(x)$ er i stand til at „gætte" x. Det sidste kan sædvanligvis ikke opfyldes: For en transformation $E\colon x \to x^e$, der kommer fra en RSA-nøgle (n, e, d) er e nødvendigvis er ulige, så for $x = 0, 1, n-1$ er $E(x) = x$. Mere præcist gælder den sidste ligning, når den gælder modulo hver af de to primfaktorer i n. Den gælder altså i hvert fald for hver af de $3 \cdot 3 = 9$ værdier af x, der både modulo p og modulo q er kongruente med et af tallene $0, 1, -1$. Med henblik på sikkerheden må E altså opfylde, at der kun for meget få værdier af x gælder $E(x) = x$.

Modulo p gælder kongruensen $x^e \equiv x$, hvis og kun hvis enten $x \equiv 0$ eller $x^{e-1} \equiv 1$. Antallet af løsninger til den sidste kongruens modulo p er $(e-1, p-1)$. Kongruensen $x^e \equiv x$ har derfor $1+(e-1, p-1)$ løsninger modulo p. Af Den kinesiske Restklassesætning følger derfor, at antallet af løsninger til kongruensen $x^e \equiv x$ modulo n er produktet

$$\bigl[1 + (e-1, p-1)\bigr]\cdot\bigl[1 + (e-1, q-1)\bigr].$$

Dette produkt er altså antallet af tal (modulo n), der ikke ændres ved krypteringen. Skaberen af nøglen bør naturligvis sikre sig, at dette antal ikke er stort.

(6.20) Bemærkning. Der findes mange andre foreslåede systemer for udveksling af hemmelige meddelelser mellem en kreds af brugere. Som nævnt indgår i systemerne en mængde af transformationer $E\kappa$ (og deres inverse $D\kappa$), som afhænger af en nøgle κ. Mængden af nøgler κ skal naturligvis være (overordentlig) stor.

I Diffie og Hellman's foreslåede system foregår udveksling af meddelelser mellem A og B ved at de sammen bestemmer den nøgle $\kappa = \kappa(A, B)$, der skal benyttes. Efter at nøglen κ er bestemt, således at kun A og B kender den, krypterer A med E_κ og B dekrypterer med D_κ; efter nøglebestemmelsen anvendes altså en klassisk kryptering. Nølgebestemmelsen kan fx foregå som følger: Antag, at de mulige nøgler svarer til tal $\kappa < p$, hvor p er et meget stort primtal. Regn modulo p, og vælg en tilfældig restklasse g. Ideelt er g en frembringer for den cykliske gruppe $(\mathbb{Z}/p)^*$; det er i hvert fald et krav, at g har stor orden i denne gruppe. Tallene p og g er offentlige. Videre vælger hver bruger A et tilfældigt tal ν_A, og offentliggør tallet $h_A := g^{\nu_A}$. Det er det diskrete log-problem, at „ingen" udfra potensen g^ν er i stand til at bestemme eksponenten ν. Nøglen, der skal benyttes ved kommunikation mellem to brugere A og B er herefter tallet $\kappa = g^{\nu_A\nu_B}$. Dette tal kan de begge beregne: Da $\kappa = (g^{\nu_A})^{\nu_B} = h_A^{\nu_B}$, kan B beregne tallet ud fra det oftentlige tal h_A og sin egen hemmelige eksponent ν_B, og A kan tilsvarende beregne tallet som $\kappa = (h_B)^{\nu_A}$.

Den offentlige del af Diffie–Hellman's nøgleudvekslingssystem indgår også i det såkaldte *ElGamal-system.* Klarteksten t sendes hemmeligt til B som h-teksten (k, τ), hvor $k = g^\alpha$ og $\tau = th_B^\alpha$, og α er en af afsenderen tilfældigt valgt eksponent. Den første del af h-teksten er „nøglen" k, som kun modtageren B kan lukke teksten op med: Hun kender sin egen eksponent ν_B, og fra den modtagne nøgle k kan hun (uden at kende α) beregne $k^{\nu_B} = g^{\alpha\nu_B} = h_B^\alpha$ og derefter dekryptere: $\tau k^{-\nu_B} = th_B^\alpha h_B^{-\alpha} = t$.

(6.21) Bemærkning. I *Massey–Omura systemet* vælger hver bruger hemmeligt sin egen nøgle. Ækvivalent har hver bruger A altså et par af transformationer (E_A, D_A), som begge holdes hemmelige. Det forudsættes, at brugerne i systemet har den samme mængde $\mathcal{K} = \mathcal{H}$, og at alle transformationerne i systemet kommuterer.

Når A skal meddele klarteksten t til B, sender han $E_A(t)$. Denne h-tekst er volopyk for B, som returnerer h-teksten $E_B(E_A(t))$ til A. Herpå anvender A dekrypteringsafbildningen D_A. Resultatet er h-teksten $D_A E_B E_A(t) = E_B(t)$ (som er volapyk for A). Denne h-tekst sender A til B, som nu kan dekryptere: $D_B E_B(t) = t$.

Bemærk, at denne kommunikation må sikres med signatur. Hvis fjenden F opsnapper den første meddelelse $E_A(t)$, kan han give sig ud for B og returnere $E_F E_A(t)$ til A; herpå returnerer A troskyldigt h-teksten $D_A E_F E_A(t) = E_F(t)$, som opsnappes af F, der nu kan dekryptere med D_F.

(6.22) Bemærkning. Påstanden om, at krypteringsafbildningerne i RSA-systemet er envejsafbildninger, bygger på, at man formoder, at faktorisering er et „svært“ problem. Vurderinger af sådanne formodninger hører hjemme i kompleksitetsteori. Her kender man en række problemer, som regnes for notorisk svære, de såkaldte „NP-hårde“ problemer. Løsningen af bare ét NP-hårdt problem vil samtidig give en løsning på en lang række andre problemer i praktisk anvendelse af computere på komplekse data. Et eksempel på et NP-hårdt problem er ‘knapsack’ (rygsæk-problemet): Der er givet et sæt af positive tal v_i (rumfang) for $i = 1, \dots, k$ og et positivt tal V (rygsækkens rumfang). Bestem, om muligt, en delmængde I af tallene $1, \dots, k$ således, at $V = \sum_{i \in I} v_i$. En løsning kan angives ved en følge af bits $(t_1, \dots, t_k)$ (dvs $t_i = 0$ eller $t_i = 1$) med $V = \sum_{i=1}^{k} t_i v_i$. At bestemme løsningen ved at prøve med samtlige bit-følger er naturligvis umuligt, hvis k er stor.

Imidlertid er knapsack-problemet trivielt, hvis følgen (v_i) vokser med i så hurtigt, at der for hvert i gælder, at $v_i > \sum_{j<i} v_j$. Hvis problemet her har en løsning, bestemmes den af en simpel algoritme: bestem det største i for hvilket $V \geqslant v_i$ (hvis et sådant findes), og pak dette v_i ned i rygsækken; gentag, hvis $V > v_i$, processen med $V := V - v_i$.

Denne observation indgår i *Merkle–Hellman systemet* (1978): I systemet har alle brugere den samme mængde $\mathcal{K}$ af klartekster, der er k-bit tal. Elementantallet i $\mathcal{K}$ er altså 2^k, hvor 2^k er stor (fx $k = 600$). Hver bruger A vælger en følge af hele tal $(v_1, \dots, v_k)$, der vokser så hurtigt som beskrevet ovenfor, og et tal $m > \sum_{i=1}^{k} v_i$, og et par af tal a, b med $ab \equiv 1 \pmod{m}$. A holder følgen (v_i) og tallene m, a, b hemmelige, men offentliggør følgen (w_i) bestemt ved $w_i = av_i$. Ud fra den offentlige følge (w_i) krypteres til A med følgende afbildning:

$$t = (t_1, \dots, t_k) \mapsto W = \sum_{i=1}^{k} t_i w_i .$$

Brugeren A modtager tallet W og kan dekryptere: ved multiplikation modulo m af W med b fremkommer tallet $V = \sum_{i=1}^{k} t_i v_i$; det er det trivielle knapsack-problem, hvorfra A kan genfinde klarteksten t. Fjenden F, der ikke kender b, skal derimod løse det mere generelle knapsack-problem: at bestemme t ud fra $W = \sum_{i=1}^{k} t_i w_i$.

Det skal understreges, at fjendens problem naturligvis *ikke* er det helt generelle knapsack-problem (tallene w_i fremkom jo på speciel måde af tallene v_i). Det blev bevist af Shamir i 1982, at fjenden faktisk har en algoritme, der kan bryde koden.

(6.23) Diskret logaritme. Problemet vedrørende diskret logaritme kan betragtes i en vilkårlig kommutativ (lad og sige additivt skrevet) gruppe E. Betragt ligningen,

$$Q = xP, \tag{*}$$

hvor $P, Q \in E$ og $x \in \mathbb{Z}$. Ligningen udtrykker, at Q er den x'te (additive) potens af P. Det antages, at P og Q er givne, og at ordenen n af P er kendt; tallet x er så entydigt bestemt modulo n. Problemet (*DL-problemet*) består i at bestemme „eksponenten" x, eller lidt mere præcist, at angive en metode til (hurtigt) at bestemme x. Sværhedsgraden afhænger naturligvis af hvordan elementerne i gruppen G er repræsenteret. Fx er problemet helt trivielt, hvis gruppen er den additive gruppe $\mathbb{Z}/n$ (hvis elementer repræsenteres ved restklasser modulo n): Er $P = [a]$ og $Q = [b]$, så siger ligningen (*) blot at $b \equiv xa \pmod{n}$, og denne kongruens løses let ved hjælp af Euklid's algoritme.

Polig–Hellman's metode. Polig og Hellmann observerede, at hvis en metode til at løse DL-problemet for en given gruppe E er kendt for elementer P af primtalsorden, så kan den anvendes til at angive en metode for elementer P af vilkårlig orden n. Det antages her, at primfaktorerne i n er kendte.

Dette indses således: Vi antager, at (*) er opfyldt, og skal bestemme x. Betragt en primdivisor p i n. Lad os sige, at p går præcis ν gange op i n. Ifølge Den kinesiske Restklassesætning er det nok for hver sådan primdivisor p at bestemme et helt tal m således, at

$$x \equiv m \pmod{p^\nu}.$$

Vi viser, induktivt for $i = 0, 1, \dots, \nu$, at vi kan bestemme et helt tal m_i, som løser kongruensen $x \equiv m_i \pmod{p^i}$.

For $i = 0$ kan vi bruge et vilkårligt tal som m_0, fx $m_0 = 0$. Antag nu, for $i < \nu$, at m_i er bestemt med $x \equiv m_i \pmod{p^i}$, altså at $x = m_i + yp^i$. Da $i < \nu$, er p^{i+1} divisor i n, så vi har $n = n'p^{i+1}$. Sættes $P' := n'p^iP$, følger det, at P' har orden p. Sæt nu videre $Q' := n'(Q - m_i)P$. Da er

$$Q' = n'(xP - m_iP) = n'yp^iP = yP'.$$

Da P' har orden p, kan vi ud fra denne ligning ifølge antagelsen bestemme y modulo p, lad os sige $y = k + zp$. Indsættelse giver nu $x = m_i + (k + zp)p^i = m_i + kp^i + zp^{i+1}$, og så er

$$x \equiv m_i + kp^i \pmod{p^{i+1}}.$$

Vi kan altså bruge $m_i + kp^i$ som m_{i+1}.

(6.24) Opgaver.

U7 **1.** Antag, for et givet $e > 1$, at $x \mapsto x^e$ er bijektiv modulo n. Vis, at n må være kvadratfri.

U7 **2.** Vis, modulo 95, at afbildningen $x \mapsto x^7$ er bijektiv, og angiv den inverse.

U7 **3.** Hvorfor står der, i kommentaren til *simpelhed*, at modtageren skal kunne dekode, „hvis det ønskes"?

H4 **4.** Min offentlige RSA-nøgle er (33, 7). Restklasserne $0, \dots, 32$ modulo 33 fortolkes som de 29 danske bogstaver efterfulgt af de 4 specialtegn: '.', ',', '!', '?'. En student sender mig h-teksten 'ÅPFLØE'. Hvad var klarteksten?

5. Vis, at restklassen $g := [2]_{19}$ er en frembringer for $(\mathbb{Z}/19)^*$. Bestem x således, at $[3]_{19} = g^x$.

U9 **6.** Antag, at $n = pq$ er produkt af to primiske pseudoprimtal p, q. Lad l betegne det mindste fælles multiplum af $p - 1$ og $q - 1$. Vis, at $x \mapsto x^e$ er en bijektiv afbildning $\mathbb{Z}/n \to \mathbb{Z}/n$, hvis $(e, l) = 1$. Vis, at „kun hvis" ikke gælder generelt. [Vink: Prøv med det mindste Carmichael-tal som p og et passende primtal som q.]

H4 **7.** Lad $\mathcal{E}_n$ betegne gruppen af de permutationer af $\mathbb{Z}/n$, der er af formen $x \mapsto x^e$. Antag, at $n = 17 \cdot 19$. Bestem gruppen $\mathcal{E}_n$. Vis, at den maksimale orden af en permutation i $\mathcal{E}_n$ er 12. Hvilken orden har permutationen $x \mapsto x^5$.

U8 **8.** Af hvilke grunde er RSA baseret på $n = 31 \cdot 61$ en dårlig ide? Og hvad med $n = 257 \cdot 163$?

U8 **9.** Herunder er en tabel over logaritmen med grundtal 2 for $\mathbb{Z}/19$. Hvad betyder det?

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Brug tabellen til at markere, i øverste række, frembringerne for $(\mathbb{Z}/19)^*$, og de kvadratiske rester i $(\mathbb{Z}/19)^*$. Brug tabellen til at bestemme de inverse til restklasserne af 4 og af 6. Løs kongruensen $6(4x + 3)^5 \equiv 8 \pmod{19}$.

10. Er det diskrete logaritme-problem (se (6.23)) trivielt, hvis gruppen E er gruppen C_n af n'te enhedsrødder i $\mathbb{C}$?

11. Antag, at n er kvadratfri. Lad $\mathcal{E}$ være gruppen af permutationer af $\mathbb{Z}/n$ af formen $E_e : x \mapsto x^e$. Antag, at l er et multiplum af $\lambda(n)$. Vis, at homomorfien $(\mathbb{Z}/l)^* \to \mathcal{E}$, bestemt ved $e \mapsto E_e$, er surjektiv. Vis, at den kun er injektiv hvis $l = \lambda(n)$. [Vink: brug, når $d \mid l$, at $(\mathbb{Z}/l)^* \to (\mathbb{Z}/d)^*$ altid er surjektiv. Tilfældet, hvor $(\mathbb{Z}/l)^* \xrightarrow{\sim} (\mathbb{Z}/d)^*$ og $d < l$, kan jo forekomme, så du må også indse, at det ikke forekommer i anvendelsen på opgaven.]

7. Lidt om faktorisering af store tal.

(7.1). Som tidligere nævnt består det mest oplagt angreb på en RSA-nøgle med den offentlige del (n, e) i at prøve et faktorisere n. Sikkerheden i RSA-systemet bygger på en tro på, at det er vanskeligt at faktorisere et tal n, der er et produkt af to store primfaktorer. Bemærk, at en primtalstestning af n formodentlig hurtigt vil åbenbare, at n er sammensat, men testen fortæller intet om divisorerne.

I det følgende vil vi om tallet n blot forudsætte, at n er ulige og sammensat.

(7.2) Den kanoniske metode. Den oplagte algoritme, der faktoriserer n, er den kanoniske: Prøv med tallene $q = 2, 3, 4, 5, \dots$ om q er divisor i n. Algoritmen stopper med en divisor q, der er den mindste ikke-trivielle divisor i n. Med store-O-notationen fra Kapitel 1 har hver division et tidsforbrug på $O(\log^2 n)$. I denne vurdering af tidsforbruget er den indgående konstant uafhængig af n, men den afhænger naturligvis af den computer, der udfører regningerne. Den mindste ikke-trivielle divisor q kan højst være $\sqrt{n}$, så algoritmen stopper efter højst $\sqrt{n}$ skridt. Det totale tidsforbrug kan derfor vurderes til $O(\sqrt{n}\log^2 n)$. (Vi behøver naturligvis kun at prøve med ulige tal q, og kan altså i stedet vurdere antallet af skridt med $\frac{1}{2}\sqrt{n}$, men den konstante faktor $\frac{1}{2}$ er uinteressant i store-O-notationen.) Med $N := \log n$ betegner vi *størrelsen* af tallet n; det er essentielt antallet af cifre i n. Som funktion af tallet n og af størrelsen af n kan tidsforbruget altså vurderes som

$$O(\sqrt{n}\log^2 n) = O(e^{N/2}N^2);$$

det vokser altså eksponentielt med størrelsen N.

I forbindelse med brydning af en RSA-nøgle, er faktoriseringen fuldført: divisoren q er et primtal og den anden primdivisor i n er $p = n/q$. I almindelighed leverer algoritmen primopløsningen af n efter højst N gentagelser.

(7.3) Fermat's metode. I en faktorisering $n = pq$ (med $q < p$) er p og q begge ulige. Specielt har vi $p = s + t$ og $q = s - t$ med hele tal s og t, nemlig med $s = (p + q)/2$ og $t = (p - q)/2$. At faktorisere $n = pq$ svarer altså til at skrive n som differensen $n = s^2 - t^2$ mellem to kvadrater, eller – ækvivalent – at bestemme $s \geqslant \sqrt{n}$ således, at $k = s^2 - n$ er et kvadrat. Det er ideen i Fermat's simple algoritme: Start med $s := s_0 :=$ det mindste hele tal større end $\sqrt{n}$. Undersøg om $k := s^2 - n$ er et kvadrat, og fortsæt med $s := s_0 + 1, s_0 + 2, \dots$ indtil svaret er ja. Lidt mere algoritmisk: Sæt $k := k + 2s + 1, s := s + 1$, indtil k er et kvadrat. Når algoritmen stopper, er $k = t^2$, og $n = s^2 - t^2$. Tidsforbruget til at bestemme $\sqrt{k}$ kan vurderes til $O(\log^3 k)$. Antallet af skridt er $s - s_0 + 1$. Her er $s = (p+q)/2$ og $s_0 \geqslant \sqrt{n} > q$. Altså er $s - s_0 + 1 \leqslant s - q = (p - q)/2$. Antallet af skridt kan altså vurderes opad ved den halve differens $(p - q)/2$, og algoritmen er kun effektiv, når differensen $p - q$ er „lille". I almindelighed kan denne differens kun vurderes ved $O(n)$, og algoritmens tidsforbrug altså ved $O(n \log^3 n)$, altså klart dårligere end den kanoniske algoritme.

I forbindelse med RSA-systemet er p og q primtal med samme antal cifre. Altså er p og q, og dermed $p - q$, med tilnærmelse $\sqrt{n}$. Skridtantallet kan altså vurderes ved $O(\sqrt{n})$, og køretiden ved $O(\sqrt{n}\log^3 n)$; her er metoden altså sammenlignelig med den kanoniske metode.

En forfining af metoden er baseret på følgende observation: hvis differensen $ap - bq$ er lille (og lige) for passende små tal a, b, så vil den simple algoritme ovenfor, anvendt på tallet abn, stoppe med en fremstilling $abn = s^2 - t^2$, og heraf fås faktoriseringen $abn = (ap)(bq)$, som også bestemmer p, q. Den forfinede algoritme forsøger at anvende den simple algoritme på cn med små værdier af $c = 1, 2, 3, \dots$.

(7.4) Eksempel. For $n = 583 = 11{\cdot}53$ er $s = 32$ og $t = 21$. Den simple algoritme giver $s_0 = 25$; den kræver altså $s - s_0 + 1 = 8$ skridt (og kendskab til kvadrattallene mindre end $(n/2)^2$).

Anvend i stedet den simple algoritme på $5n = 2.915$. Her er $5n = 55{\cdot}53$, altså $s = 54$ og $t = 1$. Algoritmen stopper altså efter første skridt, med fremstillingen $5n = 54^2 - 1$.

(7.5) Probabilistiske metoder. Specielt i forbindelse med brydning af en RSA-nøgle spiller *probabilistiske algoritmer* eller *Monte Carlo metoder* en vigtig rolle. For at hævde, at en RSA-nøgle (n, e) ikke kan brydes, er det jo nødvendigt at sikre, at fjenden ikke blot med den mindste positive sandsynlighed kan faktorisere n. Det er altså en forudsætning for RSA, at også probabilistiske metoder vil have en køretid, der vokser eksponentielt med N.

I det følgende skitserer vi en enkelt algoritme, der med positiv sandsynlighed faktoriserer n hurtigere end den kanoniske metode.

Det er øjensynlig nok at angive en algoritme, der bestemmer en ikke-triviel divisor i n (ikke nødvendigvis den mindste). Betragt modulo n en følge af tal $x_0, x_1, \dots$. Hvis følgen er lang nok (fx har mere end n elementer), så optræder der med sikkerhed en gentagelse i følgen, dvs der findes et index $l > 0$ og hertil et $j < l$, så at der modulo n gælder kongruensen,

$$x_l \equiv x_j. \tag{*}$$

Den samme følge kan betragtes modulo en ægte divisor q i n. Hvis kongruensen (*) gælder modulo n, så gælder den også modulo q. På den anden side må det forventes, at hvis den betragtede følge er blot „tilfældig“ og q „meget mindre“ end n, så vil den første gentagelse i følgen modulo q med stor sandsynlighed indtræffe inden den første gentagelse modulo n. For den første gentagelse modulo q er kongruensen (*) altså opfyldt modulo q, men ikke modulo n. Den største fælles divisor $(x_l - x_j, n)$ er derfor en ægte divisor i n, og større end 1, idet den er et multiplum af q. Hermed er bestemt en ikke-triviel divisor i n.

Antag nu, at vi frembringer en følge $x_0, x_1, \dots, x_l$ af tilfældige tal modulo n. Lad os først skønne over hvor mange elementer, der skal medtages i følgen før vi kan forvente, at der indtræffer en gentagelse modulo q, hvor q er en (ukendt) divisor i n. Modulo q er der q^{l+1} følger med $l + 1$ elementer. Af disse er $q(q-1)\cdots(q-l)$ uden gentagelser. Af alle følger modulo q vil følgerne uden gentagelser derfor udgøre brøkdelen c bestemt ved

$$c := \frac{q(q-1)\cdots(q-l)}{q^{l+1}} = \prod_{\nu=1}^{l}(1 - \frac{\nu}{q}).$$

For $l \geqslant q$ er $c = 0$. Antag $l < q$. Som bekendt gælder for $0 < x < 1$, at $\log(1-x) < -x$. Logaritmen af brøkdelen c kan derfor vurderes:

$$\log c = \sum_{\nu=1}^{l} \log(1 - \frac{\nu}{q}) < \sum_{\nu=1}^{l} (-\frac{\nu}{q}) = \frac{-l(l+1)}{2q} < \frac{-l^2}{2q}.$$

Lad nu $\varepsilon > 0$ være givet. Af vurderingerne ovenfor fremgår, at $c < \varepsilon$. altså $\log c < \log \varepsilon$, når blot $-l^2/2q \leqslant \log \varepsilon$, dvs når $l \geqslant l_\varepsilon(q)$, hvor

$$l_\varepsilon(q) := \sqrt{2q \log(1/\varepsilon)}. \tag{7.5.1}$$

Heraf fås:

Observation. *Hvis $l \geqslant l_\varepsilon(q)$, så vil en tilfældig følge $x_0, \dots, x_l$ med sandsynlighed større end $1 - \varepsilon$ indeholde en gentagelse modulo q.*

Denne observation er baggrund for følgende algoritme: Frembring modulo n en følge $x_0, x_1, x_2, \dots$ af tilfældige tal. Bestem i det l'te skridt den største fælles divisor $(x_l - x_j, n)$ for alle $j = 0, \dots, l-1$. Når der herved fremkommer en fælles divisor q, der er større end 1, stoppes algoritmen. Som tidligere nævnt vil denne største fælles divisor, når algoritmen stopper, med stor sandsynlighed være en ægte divisor i n. Udregningerne ovenfor viser, at for et givet ε kan algoritmen med sandsynlighed større end $1 - \varepsilon$ forventes at stoppe efter et antal skridt, der er mindre eller lig med $l_\varepsilon(q)$ (hvor q er en ukendt divisor i n). Vi kan vurdere q opad ved $\sqrt{n}$, og altså $l_\varepsilon(q)$ ved $\sqrt{2\log(1/\varepsilon)}\sqrt[4]{n}$. Med sandsynlighed $1 - \varepsilon$ kan algoritmen altså forventes at stoppe efter et skridtantal l, der højst er konstanten $\sqrt{2\log(1/\varepsilon)}$ ganget med

$$\sqrt[4]{n}.$$

I praksis kan algoritmen ikke anvendes. Der er dels et pladsproblem, idet der i det l'te skridt skal bestemmes den største fælles divisor $(x_l - x_j, n)$ for alle $j < l$, hvilket kræver, at alle x_j'erne gemmes under forløbet. Men først og fremmest er problemet, at antallet af beregninger vokser med l: i det l'skridt skal der foretages l beregninger af en største fælles divisor. For antallet af beregninger af største fælles divisor efter l skridt fås derfor vurderingen $1 + 2 + \cdots + (l-1) = l(l-1)/2$, som kan vurderes opad ved $l_\varepsilon^2/2$, og altså ved en konstant gange $(\sqrt[4]{n})^2 = \sqrt{n}$. Idet hver beregning af største fælles divisor har et tidsforbrug på $O(\log^3 n)$, får vi et skøn over algoritmens tidsforbrug på

$$O(\sqrt{n}\log^3 n) = O(e^{N/2}N^3).$$

Algoritmen kan altså kun vurderes som dårligere end den kanoniske algoritme.

(7.6). Overvejelserne ovenfor er imidlertid grundlag for en forbedret algoritme, den såkaldte *Monte Carlo metode* eller *Pollard's ρ-metode*. Det antages her, at følgen $x_0, x_1, \dots$ frembringes af et fast polynomium f med hele koefficienter (polynomiet $f = X^2 + 1$ er i denne sammenhæng det foretrukne) således: x_0 sættes til et tilfældigt tal (i denne sammenhæng ser det ud til, at $x_0 := 2$ faktisk er tilstrækkeligt tilfældigt), og modulo n defineres induktivt $x_{i+1} := f(x_i)$. Det antages nu, at følgen modulo den ukendte divisor q er „tilstrækkelig" tilfældig. Overvejelserne ovenfor viser derfor, at følgen modulo q med sandsynlighed $1-\varepsilon$ efter et antal skridt $l_0 \leqslant l_\varepsilon(q)$ indeholder en gentagelse modulo q. Der findes altså et $j_0 < l_0$ således, at den største fælles divisor $(x_{l_0} - x_{j_0}, n)$ er større end 1. Og med stor sandsynlighed er denne største fælles divisor en ikke-triviel divisor i n.

Nu er følgen naturligvis slet ikke tilfældig modulo q. Da f er et polynomium, følger nemlig af $x_{l_0} \equiv x_{j_0}$, at $f(x_{l_0}) \equiv f(x_{j_0})$, altså at $x_{l_0+1} \equiv x_{j_0+1}$, og videre (induktivt), at $x_{l_0+k} \equiv x_{j_0+k}$ for $k \geqslant 0$. Efter den første gentagelse (modulo q) i skridt nummer l_0 er der altså en gentagelse i hvert eneste skridt.

Heraf ses imidlertid, at der modulo q findes en gentagelse $x_l \equiv x_j$, hvor j har formen $j = 2^h - 1$. Mere præcist kan vi, ud fra den første gentagelse $x_{l_0} \equiv x_{j_0}$, vælge $h \geqslant 0$, så $2^{h-1} < l_0 \leqslant 2^h$. Da $j_0 < l_0$, er $j_0 \leqslant 2^h - 1$, altså $j_0 + k = 2^h - 1$ med passende $k \geqslant 0$; med $l = l_0 + k$ og $j = 2^h - 1$ følger så, at $x_l \equiv x_j$. Med dette valg er $k = 2^h - 1 - j_0 \leqslant 2^h - 1$, så $l = l_0 + k \leqslant 2^h + 2^h - 1 = 2^{h+1} - 1$. Gentagelsen kommer altså med et index j af formen $2^h - 1$, og med et $l \leqslant 2^{h+1} - 1$.

I stedet for i hvert skridt l at undersøge for alle $j < l$ om x_l er en gentagelse af x_j, er det altså nok at undersøge for hvert l om x_l er en gentagelse af x_{2^h-1}, hvor h er bestemt ved $2^h - 1 < l \leqslant 2^{h+1} - 1$. De l bestemmelser af en største fælles divisor i det l'te skridt kan altså erstattes af en enkelt, og af x_j'erne for $j < l$ behøver vi kun at gemme x_{2^h-1}. Prisen er naturligvis, at vi så ikke finder den første gentagelse. Prisen er imidlertid moderat. Det fremgår nemlig af udregningerne ovenfor, at hvis den første gentagelse l_0 forekommer efter højst l_ε skridt, så vil algoritmen, med k defineret ovenfor, afsløre en gentagelse efter et skridtantal l, hvor $l = l_0 + k \leqslant l_0 + 2^h - 1 = l_0 + 2{\cdot}2^{h-1} < 3l_0$, altså $l \leqslant 3l_\varepsilon(q)$.

Pollard's ρ-algoritme. *Input: et ulige, sammensat tal n. Registre:* **x**, **l**, **y**, **q**. *Output: når algoritmen stopper, vil* **q** *indeholde en divisor $q > 1$ i tallet n. Med stor sandsynlighed er q en ægte divisor i n.* [Bruger funktioner sfd og $\mathrm{f}(x) = x^2 + 1$.]

ρ**1** Initialisering*: Sæt* $\mathbf{l} \leftarrow 0$ *og* $\mathbf{x} \leftarrow 2$.
ρ**2** Iteration*: Sæt* $\mathbf{l} \leftarrow \mathbf{l} + 1$. *Hvis* **l** *har formen* 2^h*, sættes* $\mathbf{y} \leftarrow \mathbf{x}$.
ρ**3** Anvend f*: Sæt* $\mathbf{x} \leftarrow \mathrm{f}(\mathbf{x}) \pmod{n}$.
ρ**4** Beregning af største fælles divisor*: Sæt* $\mathbf{q} \leftarrow \mathrm{sfd}(\mathbf{x} - \mathbf{y}, n)$.
ρ**5** Stoptest*: Hvis* $\mathbf{q} > 1$*, så STOP, ellers GOTO* ρ**2**.

Antages, at den frembragte følge x_i er tilstrækkelig tilfældig, så følger det af overvejelserne ovenfor, at algoritmen virker, og at antallet l af skridt med sandsynlighed $1-\varepsilon$ højst er $3l_\varepsilon(q)$, hvor $l_\varepsilon(q)$ er bestemt ved (7.5.1). Vi kan vurdere $q \leqslant \sqrt{n}$, og kan altså vurdere køretiden som
$$O(\sqrt[4]{n}\log^3 n) = O(e^{N/4}N^3).$$

(7.7) Bemærkning. En følge x_i bestemt *rekursivt* ved en ligning $x_{i+1} = f(x_i)$, hvor $f\colon \mathbb{Z}/n \to \mathbb{Z}/n$ er en afbildning, er naturligvis *ikke* tilfældig: Følgens bane har et udseende, der kan sammenlignes med det græske bogstav ρ. Pointen ved at vælge f som et polynomium er, at følgen modulo den ukendte divisor q så igen er rekursiv.

(7.8) Opgaver.

U9 **1.** Implementer Pollard's algoritme i et program (Pascal eller C eller ...), der som input skal have to (prim)tal p_1, p_2, som beregner $n = p_1 p_2$, og som output leverer divisoren q i n, samt skridtantallet. Hvorfor stopper det? Hvad sker, når $p_1 = 23$, $p_2 = 29$?

U9 **2.** „Rent Monte Carlo" er det naturligvis, for et givet (sammensat, ulige) n, at undersøge, gentagne gange, om et tilfældigt valgt $q < n$ er divisor i n. Giv en vurdering af det skridt-antal, der er nødvendigt for at denne algoritme med sandsynlighed mindst $\frac{1}{2}$ finder en ikke-triviel divisor i n. [Vink: $l \geqslant (\frac{1}{2} \log 2)n$.]

3. Lad n (ulige, sammensat) være givet. I stedet for at undersøge, gentagne gange, om det tilfældigt valgte q er divisor i n, kan man spørge, om q har en ikke-triviel divisor fælles med n. Giver det en forbedring af det forventede skridt-antal?

8. Lidt om Möbius-funktionen.

(8.1). For to funktioner $\alpha, \beta\colon \mathbb{N} \to \mathbb{C}$ (altså komplekse talfølger) defineres *foldningen* $\alpha * \beta$ som funktionen,

$$(\alpha * \beta)(n) = \sum_{d|n} \alpha(n/d)\beta(d), \tag{8.1.1}$$

hvor summen er over alle (positive) divisorer i n. Lidt mere symmetrisk kan foldningen af α og β bestemmes ved $(\alpha * \beta)(n) = \sum_{de=n} \alpha(d)\beta(e)$, hvor der summeres over alle fremstillinger $n = de$ af n som et produkt af to (positive) faktorer. Det er let at se, at mængden af alle funktioner $\mathbb{N} \to \mathbb{C}$ med sædvanlig sum af funktioner som addition og med foldning som multiplikation er en kommutativ ring. Vi betegner den $\mathcal{D}_{\mathbb{C}}$. Nul-elementet er den konstante funktion 0, og et-elementet er funktion $1_{\mathcal{D}}$ defineret ved

$$1_{\mathcal{D}}(n) = \begin{cases} 1 & \text{når } n = 1, \\ 0 & \text{ellers.} \end{cases}$$

Det er umiddelbart klart, at ved udelukkende at betragte reelle (eller rationale eller heltallige) funktioner fremkommer tilsvarende en ring $\mathcal{D}_{\mathbb{R}}$ (eller $\mathcal{D}_{\mathbb{Q}}$ eller $\mathcal{D}_{\mathbb{Z}}$).

Det kan af og til være bekvemt at betragte følger i en vilkårlig kommutativ ring R, altså funktioner $\mathbb{N} \to R$. Disse funktioner udgør, med sædvanlig sum af funktioner som addition og med foldningen (8.1.1) som multiplikation, en kommutativ ring. Vi betegner den $\mathcal{D}_R$. I det følgende betragtes denne generelle situation.

Bemærk, at den konstante funktion $\mathbf{1}$ (bestemt ved $\mathbf{1}(n) = 1$) *ikke* er et-elementet i ringen $\mathcal{D}$. Foldning med $\mathbf{1}$ knytter til hver funktion α funktionen,

$$(\mathbf{1} * \alpha)(n) = \sum_{d|n} \alpha(d).$$

Fx kan funktionen $\tau(n)$, defineret som antallet af divisorer i n, beskrives ved $\tau(n) = \sum_{d|n} 1$. Vi har altså

$$\tau = \mathbf{1} * \mathbf{1}.$$

Tilsvarende kan funktionen $\sigma(n)$, bestemt som summen af divisorerne i n, beskrives ved $\sigma(n) = \sum_{d|n} d$; vi har altså

$$\sigma = \mathbf{1} * \iota,$$

hvor $\iota(n) = n$ er den kanoniske afbildning.

(8.2) Multiplikative funktioner. En funktion $\alpha\colon \mathbb{N} \to R$ kaldes *multiplikativ*, hvis

$$\alpha(1) = 1 \quad \text{og} \quad \alpha(mn) = \alpha(m)\alpha(n), \text{ hvis } (m, n) = 1.$$

Den sidste ligning forudsættes altså kun, når n og m er primiske. Hvis den gælder for alle n, m siges α også at være *stærkt multiplikativ*.

Fx er funktionerne $1_{\mathcal{D}}$, ι og $\mathbf{1}$ stærkt multiplikative. Funktionen $\tau(n)$ er ikke stærkt multiplikativ; fx er $\tau(2\cdot 2) = \tau(4) = 3$ forskellig fra $\tau(2)\tau(2) = 2\cdot 2 = 4$. Men den er multiplikativ: fx er det umiddelbart at indse, at når n er primopløst, $n = p_1^{\nu_1}\cdots p_r^{\nu_r}$, så er $\tau(n) = (\nu_1+1)\cdots(\nu_r+1)$, og heraf følger multiplikativiteten. Alternativt: Divisorerne i et produkt nm, hvor n og m er primiske, er netop produkterne de, hvor $d \mid n$ og $e \mid m$; antallet af divisorer i nm er derfor $\tau(n)\tau(m)$.

(8.3) Sætning. *En funktion $\alpha\colon \mathbb{N} \to R$ er invertibel i ringen $\mathcal{D}_R$, hvis og kun hvis $\alpha(1)$ er invertibel i R. De multiplikative funktioner $\alpha\colon \mathbb{N} \to R$ udgør en undergruppe i gruppen $\mathcal{D}_R^*$ af invertible elementer i $\mathcal{D}_R$.*

Bevis. En funktion α er invertibel, hvis og kun hvis der findes en funktion ξ så $\alpha * \xi = 1_{\mathcal{D}}$, dvs $\alpha(1)\xi(1) = 1$ og $\sum_{d\mid n}\alpha(n/d)\xi(d) = 0$ for $n > 1$. Den første ligning kan opfyldes, hvis og kun hvis $\alpha(1)$ er invertibel i R. Den anden ligning kan omformes:

$$\alpha(1)\xi(n) = -\sum_{d\mid n,\, d<n}\alpha(n/d)\xi(d). \tag{8.3.1}$$

Ligningen fastlægger øjensynlig, når $\alpha(1)$ er invertibel, værdierne $\xi(n)$ rekursivt. Heraf følger den første påstand.

Antag nu, at n og m er primiske. Divisorerne i nm kan da entydigt skrives de, hvor $d \mid n$ og $e \mid m$. Når α og β er multiplikative, får vi derfor, at

$$\begin{aligned}(\alpha*\beta)(nm) &= \sum_{d\mid n,\, e\mid m}\alpha(nm/de)\beta(de)\\ &= \sum_{d\mid n}\alpha(n/d)\beta(d)\sum_{e\mid m}\alpha(m/e)\beta(e) = (\alpha*\beta)(n)(\alpha*\beta)(m).\end{aligned}$$

Heraf følger, at delmængden af multiplikative funktioner er stabil under foldning. At den også er stabil under dannelse af invers følger tilsvarende af den rekursive bestemmelse (8.3.1) af den inverse. Trivielt indeholder delmængden et-elementet $1_{\mathcal{D}}$. Altså er delmængden en undergruppe af $\mathcal{D}_R^*$. ▯

(8.4) Möbius-funktionen. Den inverse, med hensyn til folding, af den konstante funktion $\mathbf{1}$, kaldes *Möbius-funktionen*. Den er altså bestemt ved $\mathbf{1} * \mu = 1_{\mathcal{D}}$, altså ved ligningerne:

$$\mu(1) = 1, \quad \text{og} \quad \sum_{d\mid n}\mu(d) = 0, \ \text{når } n > 1.$$

Eksplicit er $\mu(n)$ bestemt ved udtrykket:

$$\mu(n) = \begin{cases} 1 & \text{når } n = 1,\\ (-1)^r & \text{når } n = p_1\cdots p_r \text{ er kvadratfri},\\ 0 & \text{ellers.}\end{cases}$$

For at eftervise dette, lader vi μ være funktionen bestemt ved udtrykket. Vi skal så vise, for $n > 1$, at summen $\sum_{d|n} \mu(d)$ er lig med 0. Betragt primopløsningen $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$. Det er kun de kvadratfri divisorer d, der bidrager til summen, og de kvadratfri divisorer svarer til delmængder af de r primdivisorer i n. Der er $\binom{r}{s}$ kvadratfri divisorer d med s faktorer, og her er $\mu(d) = (-1)^s$. Altså får vi (som ønsket):

$$\sum_{d|n} \mu(d) = \sum_{s=0}^{r} \binom{r}{s} (-1)^s = (1-1)^r = 0.$$

Möbius's Inversionsformel. *For funktioner $\psi(n)$ og $\Psi(n)$ er følgende betingelser ensbetydende:*

(1) $\Psi(n) = \sum_{d|n} \psi(d)$ *for alle* n.
(2) $\psi(n) = \sum_{d|n} \mu(n/d)\Psi(d)$ *for alle* n.

Bevis. (1) siger nemlig, at $\Psi = \mathbf{1} * \psi$ og (2), at $\psi = \mu * \Psi$. □

(8.5) Eksempel. For $\tau(n)$ har vi $\tau(n) = \sum_{d|n} 1$, og dermed, for alle n,

$$1 = \sum_{d|n} \tau(n/d)\mu(d). \tag{8.5.1}$$

Euler's φ-funktion er bestemt ved $\varphi(n) = \sum_{(n,k)=1} 1$, hvor summen er over $k = 1, \dots, n$. Ethvert $k = 1, \dots, n$ har formen $k = ld$, hvor $d = (k, n)$ og l er primisk med n/d. Vi har altså

$$n = \sum_{k=1}^{n} 1 = \sum_{d|n} \sum_{(k,n)=d} 1 = \sum_{d|n} \varphi(n/d).$$

Ækvivalent er $\iota = \mathbf{1} * \varphi$ og dermed $\varphi = \iota * \mu$. Det følger, at φ er multiplikativ, og at

$$\varphi(n) = \sum_{d|n} (n/d)\mu(d). \tag{8.5.2}$$

Specielt får vi for en primtalspotens p^ν, at

$$\varphi(p^\nu) = p^\nu - p^{\nu-1}.$$

(8.6) Eksempel. Betragt funktionen $\Lambda(n)$ bestemt ved

$$\Lambda(n) = \begin{cases} \log p & \text{når } n \text{ er en primtalspotens } p^\nu \ (\nu > 0), \\ 0 & \text{ellers.} \end{cases}$$

Her finder vi

$$\sum_{d|n} \Lambda(n) = \log n, \tag{8.6.1}$$

thi når n er primopløst, $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, er det kun divisorer af formen $d = p_i^{\lambda}$, der bidrager til summen på venstresiden, og de bidrager med

$$\sum_i \nu_i \log p_i = \log(p_1^{\nu_1} \cdots p_r^{\nu_r}) = \log n.$$

Af (8.6.1) og Inversionsformlen følger, at

$$\sum_{d|n} \log(n/d)\mu(d) = \Lambda(n). \tag{8.6.2}$$

Ækvivalent kan ligningen skrives:

$$\sum_{d|n} \mu(d) \log d = -\Lambda(n), \tag{8.6.3}$$

idet $\log(n/d) = \log n - \log d$ og $(\log n) \sum_{d|n} \mu(d) = 0$ for alle n (for $n > 1$ ifølge (8.4) og for $n = 1$, fordi $\log 1 = 0$).

(8.7) Dirichlet-rækker. Til hver funktion (talfølge) $\alpha : \mathbb{N} \to \mathbb{C}$ knyttes den uendelige række af komplekse funktioner, *Dirichlet-rækken* for α,

$$L_\alpha(s) := \sum_{n=1}^{\infty} \frac{\alpha(n)}{n^s}.$$

Multiplikation af det d'te led i rækken L_α med det e'te led i rækken L_β (for endnu en følge β) giver $(\alpha(d)/d^s)(\beta(e)/e^s) = \alpha(d)\beta(e)/(de)^s$. Summen af disse produkter, for $de = n$, er øjensynlig det n'te led i rækken for $\alpha * \beta$. Specielt følger det, at hvis rækkerne $L_\alpha(s)$ og $L_\beta(s)$ er absolut konvergente for en given værdi af $s \in \mathbb{C}$, så er rækken $L_{\alpha*\beta}(s)$ absolut konvergent, og

$$L_{\alpha*\beta}(s) = L_\alpha(s)\, L_\beta(s).$$

Trivielt svarer sum af følger til ledvis addition af de tilhørende rækker. Sum og foldning af følger svarer altså naturligt til sum og produkt af de tilhørende rækker (og trivielt svarer nul-elementet 0 og et-elementet $1_{\mathcal{D}}$ i $\mathcal{D}_{\mathbb{C}}$ til rækkerne 0 og 1). Ringen $\mathcal{D}_{\mathbb{C}}$ kaldes derfor også ringen af *formelle Dirichlet-rækker*.

Dirichlet-rækken $L_{\mathbf{1}}(s)$, svarende til den konstante følge $\mathbf{1}$, er øjensynlig Riemann's ζ-funktion,

$$\zeta(s) = L_{\mathbf{1}}(s) = \sum\nolimits_n n^{-s}.$$

Det følger af integralkriteriet, at rækken for $\zeta(s)$ er absolut konvergent i halvplanen $\mathcal{R}e\, s > 1$. Af samme grund er rækken $L_\mu(s)$ absolut konvergent i samme område. Ligningen $\mathbf{1} * \mu = 1_{\mathcal{D}}$ i $\mathcal{D}_{\mathbb{C}}$ giver altså, for $\mathcal{R}e\, s > 1$, at $\zeta(s)L_\mu(s) = 1$. Med andre ord er $\zeta(s) \neq 0$ og

$$\frac{1}{\zeta(s)} = \sum\nolimits_n \mu(n) n^{-s}. \tag{8.7.1}$$

Tilsvarende følger af $\mathbf{1} * \mathbf{1} = \tau$, at

$$\zeta(s)^2 = \sum \tau(n) n^{-s}, \tag{8.7.2}$$

og af $\mathbf{1} * \iota = \sigma$ og $\iota * \mu = \varphi$ følger, for $\mathcal{R}e\, s > 2$,

$$\zeta(s)\zeta(s-1) = \sum \sigma(n) n^{-s}, \quad \zeta(s-1)/\zeta(s) = \sum \varphi(n) n^{-s}. \tag{8.7.3}$$

Differentiation af Dirichlet-rækken $L_\alpha(s)$ giver Dirichlet-rækken $L_\alpha(s)' = L_{\alpha'}(s)$, hvor følgen α' er bestemt ved $\alpha'(n) = -(\log n)\alpha(n)$. Specielt, med $\alpha := \mathbf{1}$, følger det af (8.6.2), at

$$\zeta'(s)/\zeta(s) = -\sum \Lambda(n) n^{-s}.$$

(8.8) Eksempel. Ligningen (8.1.1), der bestemmer foldningen $\alpha * \psi$, giver mening, når $\alpha\colon \mathbb{N} \to \mathbb{Z}$ har heltalsværdier og $\psi\colon \mathbb{N} \to G$ har værdier i en kommutativ (additivt skrevet) gruppe G. Som før gælder „associativiteten“ $(\alpha * \beta) * \psi = \alpha * (\beta * \psi)$, og $1_\mathcal{D} * \psi = \psi$. Specielt følger Möbius's Inversionsformel for afbildninger $\Psi, \psi\colon \mathbb{N} \to G$ med værdier i gruppen G. Hvis gruppen G er multiplikativt skrevet, skal Inversionsformlen naturligvis tilsvarende skrives multiplikativt.

Heltalspolynomierne udgør et integritetsområde $\mathbb{Z}[X]$, og det ligger i brøklegemet $\mathbb{Q}(X)$. Specielt ligger heltalspolynomier forskellige fra 0 i den multiplikative gruppe $\mathbb{Q}(X)^*$. Afbildningen $n \mapsto X^n - 1$ har altså værdier i denne gruppe. Som bekendt gælder ligningen,

$$X^n - 1 = \prod_{d|n} \Phi_d,$$

hvor Φ_d er det d'te cirkeldelingspolynomium. Ved Möbius-inversion fås derfor ligningen,

$$\Phi_n = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}. \tag{8.8.1}$$

Fx, for $n = 48$ er de kvadratfri divisorer 1, 2, 3, 6, og vi får:

$$\Phi_{48} = \frac{(X^{48} - 1)(X^8 - 1)}{(X^{24} - 1)(X^{16} - 1} = \frac{X^{24} + 1}{X^8 + 1} = X^{16} - X^8 + 1.$$

(8.9) Eksempel. Lad p være et primtal, og betragt polynomiet $X^{p^n} - X$ i $\mathbb{F}_p[X]$. Som bekendt gælder, at i primopløsningen af dette polynomium indgår præcis de irreducible (normerede) polynomier af grad, der er divisor i n, og hvert sådant forekommer med multiplicitet 1. Idet $\alpha_p(n)$ er antallet af normerede, irreducible polynomier af grad n i $\mathbb{F}_p[X]$ fås, ved sammenligning af graderne,

$$p^n = \sum_{d|n} d\alpha_p(d).$$

Ved Möbius-inversion følger det, at $n\alpha_p(n) = \sum_{d|n} p^{n/d}\mu(d)$, altså,

$$\alpha_p(n) = \frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}. \tag{8.9.1}$$

(8.10) Summer. Ved vurderinger af en sum $\sum_{k\leqslant x}\alpha(k)$ kan man af og til med fordel inddrage foldning, idet der øjensynlig gælder ligningen,

$$\sum_{k\leqslant x}(\alpha*\beta)(k) = \sum_{k\leqslant x}\sum_{d|k}\alpha(d)\beta(k/d) = \sum_{d\leqslant x}\alpha(d)\sum_{q\leqslant x/d}\beta(q).$$

I summerne her og i det følgende er det underforstået, at summationsindex er et naturligt tal; grænserne for summationen kan være bestemt ved reelle (oftest positive reelle) tal.

Som eksempel betragtes summen $\sum_{k\leqslant N}\varphi(k)$. Vi har $\varphi = \mu * \iota$ ifølge (8.5.2). Altså er

$$\sum_{k\leqslant N}\varphi(k) = \sum_{d\leqslant N}\mu(d)\sum_{q\leqslant N/d} q. \tag{1}$$

Den indre sum kan umiddelbart summeres: Vi har $2\sum_{q\leqslant x} q = \lfloor x\rfloor + \lfloor x\rfloor^2$. Derfor er

$$2\sum_{q\leqslant x} q = S(x) + x^2, \quad \text{hvor } S(x) := \lfloor x\rfloor - \big(x - \lfloor x\rfloor\big)\big(x + \lfloor x\rfloor\big). \tag{2}$$

I udtrykket for funktionen $S(x)$ ligger faktoren $x - \lfloor x\rfloor$ mellem 0 og 1. Heraf ses, at $|S(x)| \leqslant x$. Af (1) og (2) fås følgende ligning:

$$2\sum_{k\leqslant N}\varphi(k) = \sum_{d\leqslant N}\mu(d)S(N/d) + \sum_{d\leqslant N}\mu(d)(N/d)^2. \tag{3}$$

Sætning. *Lad p_N betegne sandsynligheden for at et tilfældigt udtrukket par (k,l) af tal mellem 1 og N er primisk. Da gælder for alle N vurderingen,*

$$\Big|p_N - \frac{6}{\pi^2}\Big| < \frac{2+\log N}{N}. \tag{8.10.1}$$

Bevis. Betragt primiske par (k,l) udtaget fra intervallet. Med $k \geqslant l$ er antallet $\sum_{k\leqslant N}\varphi(k)$, og antallet af alle primiske par er derfor $2\sum_{k\leqslant N}\varphi(k) - 1$; sandsynligheden p_N fås heraf ved at dividere med antallet N^2 af alle par. Altså er $N^2 p_N = 2\sum_{k\leqslant N}\varphi(k) - 1$. Videre gælder som bekendt, at $\zeta(2) = \sum d^{-2} = \pi^2/6$; heraf følger, at $N^2\cdot 6/\pi^2 = N^2/\zeta(2) = \sum_d \mu(d)(N/d)^2$. Af (3) får vi derfor ligningen,

$$N^2\big(p_N - 6/\pi^2\big) = \Big(-1 + \sum_{d\leqslant N}\mu(d)S(N/d)\Big) - \sum_{d>N}\mu(d)(N/d)^2. \tag{4}$$

Som nævnt er $|S(x)| \leqslant x$. Det d'te led i den første sum på højresiden er altså numerisk højst N/d. Da $S(N) = N$, bevares denne vurdering, hvis vi lader -1 indgå i det første led. Numerisk er parentesen på højresiden af (4) altså højst $\sum_{d\leqslant N} N/d \leqslant N(1+\log N)$, hvor uligheden fås ved vurdere $\sum_{1<d\leqslant N} 1/d$ opad med $\int_1^N (1/t)\,dt = \log N$. Tilsvarende er det andet led i (4) numerisk højst lig med N, idet uligheden fås ved at vurdere $\sum_{d>N} 1/d^2$ opad ved $\int_N^\infty (1/t^2)\,dt = 1/N$. Ved addition og divsion med N^2 fremkommer den påståede ulighed (8.10.1). ∎

(8.11) Opgaver.

H4 **1.** Vis følgende uligheder (den første kun for $n > 1$):

$$2 \leqslant \tau(n) < 2\sqrt{n}, \qquad n \leqslant \sigma(n) < 2n\sqrt{n},$$
$$\sqrt{n/2} \leqslant \varphi(n) \leqslant n, \qquad n^2/2 < \varphi(n)\sigma(n) \leqslant n^2.$$

[Vink til 3. ulighed: $\varphi(n)/\sqrt{n}$ er multiplikativ. Vurder for en primtalspotens: $\varphi(p^\nu)/p^{\nu/2} = (p-1)p^{\nu/2-1} \geqslant 1$, når $\nu \geqslant 2$ eller $p \geqslant 3$. (Det kan forbedres til $\varphi(n) \geqslant \sqrt{n}$, når $n \neq 2, 6$.)

Vink til 4. ulighed: $\varphi(n)\sigma(n)$ er multiplikativ, og for en primtalspotens p^ν finder vi umiddelbart, at $\varphi(p^\nu)\sigma(p^\nu) = (p^\nu - p^{\nu-1})(p^{\nu+1}-1)/(p-1) = p^{2\nu}(1-1/p^{\nu+1})$. For $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ fås altså

$$\varphi(n)\sigma(n) = n^2(1-1/p_1^{\nu_1+1})\cdots(1-1/p_r^{\nu_r+1}).$$

Produktet af parenteserne på højresiden er højst 1, og større end eller lig med

$$(1-1/p_1^2)\cdots(1-1/p_r^2) > \prod_{q=2}^{\infty}(1-1/q^2) = \frac{1}{2}\,.$$

(Den sidste ligning er jo triviel, ikke?) Du kan også vurdere ned ved $\zeta(2)^{-1} = 6/\pi^2$.]

H4 **2.** Vis, at udtrykket i formlen (8.9.1) for $\alpha_p(n)$ er positivt for alle n, også når $p \geqslant 2$ ikke er et primtal.

U9 **3.** Bestem grænseværdien $\lim a_N/N^2$, hvor a_N er antallet af Farey-brøker af orden N. (Farey-brøkerne af orden N er brøkerne i intervallet mellem 0 og 1 med nævner højst N, altså mængden af brøker af formen a/s, hvor $0 \leqslant a < s \leqslant N$.)

U9 **4.** Vis, at $\sum_{d|n} \mu(d)^2/\varphi(d) = n/\varphi(n)$. [Vink: brug, at begge sider er multiplikative.]

5. Vis *Brauer–Rademacher's identitet:*

$$\varphi(r)\sum_{d|r,\,(d,n)=1}\frac{d}{\varphi(d)}\mu\Big(\frac{r}{d}\Big) = \mu(r)\sum_{d|(n,r)} d\mu\Big(\frac{r}{d}\Big).$$

6. *Antag, at $\alpha\colon \mathbb{N} \to \mathbb{R}$ er multiplikativ og monoton. Vis, at så er α en potensfunktion, $\alpha(n) = n^c$.

7. Betragt antallet af løsninger til den diofantiske ligning $x^2 + y^2 = k$ (dvs løsninger med $x, y \in \mathbb{Z}$). Det er velkendt, at antallet kan bestemmes ud fra primopløsningen af k. Mere præcist: Antag, at $k = 2^l q_1^{n_1}\cdots q_r^{n_r} p_1^{m_1}\cdots p_s^{m_s}$, hvor $q_i \equiv 3 \pmod 4$ og $p_j \equiv 1 \pmod 4$. Da er antallet af løsninger lig med $4V(k)$, hvor $V(k) = (m_1+1)\cdots(m_s+1)$ hvis alle eksponenterne $n_1, \dots, n_r$ er lige, og $V(k) = 0$ ellers. Vis, at $V(k) = \sum_{d|k}\chi(d)$, hvor $\chi(d) = 0$ hvis d er lige, og $\chi(d) = (-1)^{(d-1)/2}$ hvis d er ulige. [Vink: χ er multiplikativ.]

8. Vis, at $\sum_{k \leqslant n} V(k) = \sum_{d \leqslant n} \chi(d) \lfloor n/d \rfloor$. Vis, at $4 \sum_{k \leqslant n} V(k) + 1$ er lig med antallet af gitterpunkter i cirkelskiven bestemt ved $x^2 + y^2 \leqslant n$. Udled, at $\sum_{d \leqslant n} \chi(d) \lfloor n/d \rfloor \sim \frac{\pi}{4} n$. Vis herved formlen $1 - \frac{1}{3} + \frac{1}{5} - \cdots = \frac{\pi}{4}$.

9. Vis uligheden $\varphi(n)/n \geqslant 1/\log_2 n$ for alle $n > 6$. [Vink: Fra primopløsningen $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ fås $\varphi(n)/n = (1 - 1/p_1) \cdots (1 - 1/p_r)$. Vurder følgen $p_1, \dots, p_r$ nedad ved $2, 3, \dots, r+1$. Det følger, at $\varphi(n)/n \geqslant \prod_{i=2}^{r+1} (1 - 1/i)$. Produktet kan udregnes: det har værdien $1/(r+1)$. Altså er $\varphi(n)/n \geqslant 1/(r+1)$. Vurder nu $r+1$ opad: Da $p_i^{\nu_i} \geqslant 2$, er $1 \leqslant \log_2 p_i^{\nu_i}$. Derfor er $r \leqslant \log_2 n$, og hvis $p_i^{\nu_i} \geqslant 4$ for bare et i, fås vurderingen $r + 1 \leqslant \log_2 n$. Den ekstra forudsætning er opfyldt, når n ikke er et af tallene $1, 2, 3, 6$.] Er uligheden $\varphi(n)/n \geqslant 1/\log_2 n$ opfyldt for $n = 3$?

10. *Vis, at udtrykket i formlen (8.9.1) for $\alpha_p(n)$ er et helt tal for alle n, når p er et vilkårligt naturligt tal. [Vink: Erstat p med a i summen på højresiden. Det skal så vises, at der modulo n gælder følgende kongruens:

$$\sum_{d|n} \mu(d) a^{n/d} \equiv 0.$$

Brug hertil den kinesiske restklassesætning, og regn modulo en given primtalspotens q^ν i primopløsningen af n. Lad D være mængden af kvadratfri divisorer d i n, der er primiske med q. De resterende kvadratfri divisorer har så formen $d' = qd$ med $d \in D$. Reducer til at vise, at $a^{n/d} - a^{n/d'} \equiv 0$ for $d \in D$. Vis og brug hertil, at $b^{q^\nu} - b^{q^{\nu-1}} \equiv 0$ for alle b.]

11. *Vis, at udtrykket i formlen (8.9.1) for $\alpha_p(n)$ er positivt for alle n, når $p > 1$ er et reelt tal.

9. Funktionalligningen for zeta-funktionen.

(9.1) Setup. *Riemann's ζ-funktion* er funktionen $\zeta(s)$, defineret for $\mathcal{R}e\, s > 1$ som summen,

$$\zeta(s) = \sum \frac{1}{n^s}, \tag{9.1.1}$$

hvor summen er over $n = 1, 2, \ldots$, og $n^s = e^{s \log n}$. Rækken har i området $\mathcal{R}e\, s \geqslant \sigma$, hvor $\sigma > 1$, den konvergente majorantrække $\sum n^{-\sigma}$. Funktionen $\zeta(s)$ er altså en holomorf funktion i halvplanen $\mathcal{R}e\, s > 1$.

I det følgende indgår også *gamma-funktionen* $\Gamma(s)$, defineret for $\mathcal{R}e\, s > 0$ ved integralet,

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t}\, dt. \tag{9.1.2}$$

Ved partiel integration er det let at vise funktionalligningen,

$$\Gamma(s+1) = s\Gamma(s). \tag{9.1.3}$$

Trivielt er $\Gamma(1) = 1$, og af funktionalligningen fås $\Gamma(k) = (k-1)!$ for $k = 1, 2, \ldots$. Ved gentagen anvendelse af ligningen (9.1.3), på formen $\Gamma(s) = \frac{1}{s}\Gamma(s+1)$, udvides gamma-funktionen umiddelbart til en meromorf funktion defineret i hele den komplekse plan. Den udvidede funktion har poler af orden 1 i tallene $0, -1, -2, \ldots$, og er holomorf i alle andre punkter.

Endvidere indgår *potensfunktionen* z^s, defineret for $z \neq 0$ og alle komplekse tal s via den komplekse logaritme:

$$z^s = e^{s \log z} = e^{s(\log|z| + i \arg z)} = |z|^s e^{is \arg z}. \tag{9.1.4}$$

Som funktion af $z \neq 0$ er z^s en *flertydig funktion*: argumentet $\arg z$ har flere mulige værdier (der afviger med et heltalsmultiplum af 2π), og tilsvarende har z^s flere *determinationer*. Når z ligger i et område, der ikke indeholder negative reelle tal, er det naturligt at lade z^s betegne *hoveddeterminationen*, defineret ved at argumentet er valgt med $-\pi < \arg z < \pi$. Når z er negativ reel, $z = -t$ hvor $t > 0$, er der i hvert fald to lige gode muligheder:

$$(-t)^s = \begin{cases} t^s e^{i\pi s}, \\ t^s e^{-i\pi s}. \end{cases}$$

Den første mulighed vælges naturligt, når $-t$ opfattes som et randpunkt for den øvre halvplan ($\mathcal{I}m\, z > 0$), den anden, når $-t$ opfattes som et randpunkt for den nedre halvplan.

Af definitionen får vi umiddelbart for modulus:

$$|z^s| = |z|^{\mathcal{R}e\, s} e^{-\mathcal{I}m\, s \arg z} \leqslant |z|^{\mathcal{R}e\, s} e^{\pi |\mathcal{I}m\, s|},$$

hvor ulighedstegnet gælder under forudsætning af at determinationen er hoveddeterminationen.

Når eksponenten s er et helt tal, forsvinder flertydigheden: z^s er den sædvanlige potens af z i gruppen $\mathbb{C}^*$. Vi definerer ikke z^s for $z = 0$.

(9.2) Riemann's kurveintegral. Udgangspunktet for Riemann's elementære overvejelser er funktionen $I(s)$, for komplekse værdier af s, bestemt ved udtrykket,

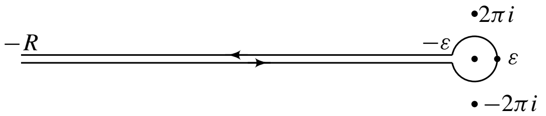
$$I(s) := \frac{1}{2\pi i} \oint_{-\infty}^{-\infty} \frac{z^s}{e^{-z}-1} \frac{dz}{z}. \tag{9.2.1}$$

Polerne for integranden er nulpunkterne for $e^{-z}-1$, altså tallene $2\pi k i$ for $k \in \mathbb{Z}$. I kurveintegralet $\oint_{-\infty}^{-\infty}$, og mere generelt, i $\oint_{-R}^{-R}$, hvor R er positiv reel eller ∞, integreres der langs en kurve, der løber langs den negative halvakse fra $-R$ til $-\varepsilon$, dernæst en gang rundt langs cirklen med radius ε i den sædvanlige omløbsretning, og endelig tilbage langs den negative halvakse fra $-\varepsilon$ til $-R$, altså

$$\oint_{-R}^{-R} = \int_{-R}^{-\varepsilon} + \int_{|z|=\varepsilon} + \int_{-\varepsilon}^{-R}. \tag{9.2.2}$$

Radius ε er valgt så lille, at cirklen kun indeholder polen $z=0$ for integranden.

Bemærk, at (en del af) integrationsvejen forløber langs den negative halvakse, altså netop gennem de punkter, hvor z^s har 2 determinationer. Det skal altså yderligere præciseres, at ved gennemløbet fra $-R$ til $-\varepsilon$ opfattes de gennemløbne punkter som randpunkter for den nedre halvplan, ved tilbageløbet fra $-\varepsilon$ til $-R$ opfattes punkterne som randpunkter for den øvre halvplan:



I det første kurveintegral på højresiden af (9.2.2), hvor $z=-t$, er altså $z^s = t^s e^{-i\pi s}$, og i det tredie kurveintegral er $z^s = t^s e^{i\pi s}$, altså

$$\int_{-\infty}^{-\varepsilon} \frac{z^s}{e^{-z}-1} \frac{dz}{z} = \int_{\infty}^{\varepsilon} \frac{t^s e^{-i\pi s}}{e^t-1} \frac{dt}{t}, \qquad \int_{-\varepsilon}^{-\infty} \frac{z^s}{e^{-z}-1} \frac{dz}{z} = \int_{\varepsilon}^{\infty} \frac{t^s e^{i\pi s}}{e^t-1} \frac{dt}{t}.$$

Slå de to bidrag sammen, og brug at $\sin w = (e^{iw}-e^{-iw})/2i$. Herved får vi ligningen,

$$I(s) = \frac{\sin \pi s}{\pi} \int_{\varepsilon}^{\infty} \frac{t^s}{e^t-1} \frac{dt}{t} + \frac{1}{2\pi i} \int_{|z|=\varepsilon} \frac{z^s}{e^{-z}-1} \frac{dz}{z}. \tag{9.2.3}$$

(9.3) Sætning. *Der gælder følgende to ligninger:*

$$\text{(i)} \quad I(s) = \frac{\sin \pi s}{\pi} \Gamma(s)\zeta(s), \qquad \text{(ii)} \quad I(s) = 2(2\pi)^{s-1} \sin \frac{\pi s}{2}\, \zeta(1-s),$$

den første for $\mathcal{R}e\, s > 1$, *den anden for* $\mathcal{R}e\, s < 0$.

Bevis. Med substitutionen nt for t i (9.1.2) fås, når $\mathcal{R}e\, s > 0$,

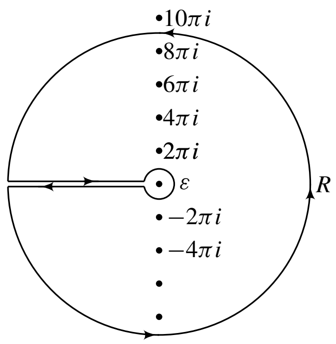
$$\Gamma(s) = n^s \int_0^\infty t^s e^{-nt}\, \frac{dt}{t}\,.$$

Divider med n^s og dan summen for $n = 1, 2, \ldots$. Da $\sum_{n \geqslant 1} e^{-nt} = 1/(e^t - 1)$ følger det let, når $\mathcal{R}e\, s > 1$, at

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{t^s}{e^t - 1}\, \frac{dt}{t}\,. \tag{1}$$

Betragt på den anden side ligningen (9.2.3). Når $\mathcal{R}e\, s > 1$ kan det uendelige integral integreres helt ind i 0, og kurveintegralet langs cirklen konvergerer mod 0 for $\varepsilon \to 0$; sammenligning med (1) giver derfor den ønskede ligning (i).

For at vise den anden ligning betragtes området D_R, der fremkommer ved at fjerne, fra cirkelskiven med centrum 0 og radius R, en lille cirkelskive med radius ε og den negative reelle halvakse. Randen af D_R er dels cirklen med radius R, dels en kurve, der løber først fra $-R$ til $-\varepsilon$, dernæst rundt i negativ omløbsretning langs cirklen med radius ε, og endelig tilbage fra $-\varepsilon$ til $-R$.



Bemærk, at den sidste del af randen gennemløbes modsat den retning, der tilsvarende definerede kurveintegralet $\oint_{-R}^{-R}$. Vi har altså $\int_{\partial D_R} = \int_{|z|=R} - \oint_{-R}^{-R}$.

Vi anvender Cauchy's Integralsætning på funktionen $f(z) = z^{s-1}/(e^{-z} - 1)$ i området D_R. Polerne er tallene $a = 2\pi k i$ for $k \in \mathbb{Z}$. Radius vælges, så cirklen med radius R ikke går gennem nogen pol; mere præcist vælges $R = (2N + 1)\pi$, hvor N er et naturligt tal. Af Integralsætningen følger, at

$$\frac{1}{2\pi i} \int_{|z|=R} f(z)\, dz - \frac{1}{2\pi i} \oint_{-R}^{-R} f(z)\, dz = \sum_{a \in D_R} \operatorname{Res}_{z=a} f(z), \tag{2}$$

hvor summen er over alle poler a i området D_R, altså tallene $a = \pm 2\pi n i$ for $1 \leqslant n \leqslant N$. Funktionen $1/(e^{-z} - 1)$ har for $z = 0$ – og derfor også for $z = \pm 2\pi n i$ – en simpel pol med residuet -1. Multiplikation med z^{s-1} giver $f(z)$. I polerne $a = \pm 2\pi n i$ er $|a| = 2\pi n$ og $\arg a = \pm\pi/2$, så residuerne er

$$-a^{s-1} = -(2\pi n)^{s-1} e^{\pm(s-1)i\pi/2}.$$

Her er $e^{(s-1)i\pi/2} = e^{is\pi/2}/i$ og $e^{-(s-1)i\pi/2} = e^{-is\pi/2}/(-i)$, med summen $2\sin s\pi/2$. Højresiden i (2) er derfor summen,

$$-2\sin(s\pi/2)\sum_{1\leqslant n\leqslant N}(2\pi n)^{s-1}. \tag{3}$$

På venstresiden af (2) konvergerer det andet integral, for $R \to \infty$, mod $\oint_{-\infty}^{-\infty} f(z)dz$. På cirklen, i det første integral, er $z = Re^{iv}$ for $-\pi \leqslant v \leqslant \pi$. Altså er $dz/z = idv$. Videre er $|z^s| \leqslant R^{\mathcal{R}e\, s}e^{\pi|\mathcal{I}m\, s|}$. Endelig, da R har formen $(2N+1)\pi$, skærer cirklen med radius R den imaginære akse midt mellem to nulpunkter for nævneren $e^{-z}-1$, og det følger, at nævneren er begrænset væk fra 0. Vi får heraf en vurdering opad for integralet rundt langs cirklen af formen en konstant gange $R^{\mathcal{R}e\, s}$. Antag, at $\mathcal{R}e\, s < 0$. Det følger, at det første integral i (2) konvergerer mod 0 for $R \to \infty$, altså for $N \to \infty$. Af (2) og (3) fås derfor ligningen,

$$-I(s) = -2(2\pi)^{s-1}\sin(\pi s/2)\sum_{n=1}^{\infty} n^{s-1},$$

og dermed den ønskede ligning (9.3)(ii). □

(9.4) Funktionalligningen. Funktionen $I(s)$ er holomorf i hele den komplekse plan. Som nævnt er gamma-funktionen meromorf i hele den komplekse plan. En vilkårlig af de to ligninger (9.3)(i) eller (ii) fastlægger derfor funktionen $\zeta(s)$ som en meromorf funktion i hele den komplekse plan, og begge ligninger gælder for *alle* s. At de to højre-sider er ens for alle s er funktionalligningen for $\zeta(s)$. Da $\sin\pi s = 2\sin(\pi s/2)\cos(\pi s/2)$, kan funktionalligningen skrives:

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\cos(\pi s/2)\Gamma(s)\zeta(s). \tag{9.4.1}$$

Ligningen, anvendt med $s := 1-s$, udtrykker $\zeta(s)$ ved $\zeta(1-s)$. Indsættes dette udtryk på højresiden af (9.4.1), fås følgende velkendte(?) ligning for gamma-funktionen,

$$\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s). \tag{9.4.2}$$

Højresiden har ingen nulpunkter, og simple poler i de hele tal. På venstresiden har $\Gamma(s)$ simple poler i $0, -1, -2, \dots$ og $\Gamma(1-s)$ har (derfor) simple poler i $1, 2, \dots$. Af ligningen følger derfor, at $\Gamma(s)$ ikke har nulpunkter. Ækvivalent har $\Gamma(s)^{-1}$ simple nulpunkter i $0, -1, -2, \dots$, og ingen poler. Af (9.4.2) følger, at (9.3)(i) alternativt kan skrives,

$$I(s) = \frac{1}{\Gamma(1-s)}\zeta(s). \tag{9.4.3}$$

(9.5) Specielle værdier. Værdien $I(s)$ kan umiddelbart bestemmes, når argumentet s er et helt tal. Antag nemlig, at $s = k \in \mathbb{Z}$. Da er z^s holomorf i hele den komplekse plan. Følgelig er de to uendelige integraler i (9.2.2) modsatte, og det midterste integral er integralet rundt langs en (lille) cirkel af en meromorf funktion. Altså er

$$I(k) = \mathrm{Res}_{z=0}\, z^{k-1}/(e^{-z}-1).$$

Værdien kan udtrykkes ved *Bernoulli-tallene* B_k, der bestemmes ved rækkeudviklingen,

$$\frac{z}{e^z-1}=\sum\frac{B_n}{n!}z^n\,,$$

hvor $B_n=0$ for $n<0$. Det følger, at $z^{k-1}/(e^{-z}-1)=\sum_n(-1)^{n-1}(B_n/n!)z^{k+n-2}$, og specielt er

$$I(k)=(-1)^k\frac{B_{1-k}}{(1-k)!}\,,$$

hvor højresiden naturligvis er 0, når $k>1$. Når k er ulige, $k=1-2n$, er $\sin(\pi k/2)=(-1)^n$, så (9.3)(ii) giver ligningen,

$$\zeta(2n)=(-1)^{n+1}(2\pi)^{2n}\frac{B_{2n}}{2(2n)!}\,. \tag{9.5.1}$$

Specielt er $\zeta(0)=-\frac{1}{2}$, og $\zeta(-2n)=0$ for $n\geqslant 1$. For $n\geqslant 1$ er (9.5.1) klassiske værdier af rækken (9.1.1).

Alternativt kan vi direkte bruge (9.4.3):

$$(-1)^k\frac{B_{k+1}}{(k+1)!}=\frac{1}{\Gamma(k+1)}\zeta(-k). \tag{9.5.2}$$

For $k\geqslant 0$ er $\Gamma(k+1)=k!$, og det følger, at

$$\zeta(-k)=(-1)^k\frac{B_{k+1}}{k+1}\,. \tag{9.5.3}$$

De ulige Bernoulli-tal er $B_1=-\frac{1}{2}$ og $B_{2k+1}=0$ for $k>0$. Af (9.5.3) følger altså igen, at $\zeta(0)=-\frac{1}{2}$, og $\zeta(-2k)=0$ for $k=1,2,\dots$.

Bemærk, at ligning (9.4.3) ikke giver information om værdierne $\zeta(k)$ for $k=1,2,\dots,$ idet vi her har $1/\Gamma(1-k)=0$.

(9.6) Bemærkning. Funktionen $I(s)$ på venstresiden af ligning (9.4.3) er holomorf i hele den komplekse plan; faktoren $\Gamma(1-s)^{-1}$ på højresiden er ligeledes holomorf. Af ligningen følger derfor, at $\zeta(s)$ er holomorf på nær eventuelt i nulpunkterne for $\Gamma(1-s)^{-1}$. Disse nulpunkter er, ifølge (9.1), $s=1,2,\dots,$ og de er simple nulpunkter. Da $I(s)$ også har nulpunkter for $s=2,3,\dots,$ er $\zeta(s)$ altså også holomorf i disse punkter. Tilbager bliver punktet $s=1$. Her har $\Gamma(1-s)^{-1}$ et simpelt nulpunkt, og $I(1)=1$; punktet $s=1$ er altså en simpel pol for $\zeta(s)$.

(9.7) Opgaver.

1. Vis, at $I(s)$ er holomorf i hele den komplekse plan, og uafhængig af valget af ε.

2. Vis, at $\Gamma(\frac{1}{2})=\sqrt{\pi}$.

3. Vis, at $\mathrm{Res}_{s=1}\,\zeta(s)=1$.

4. Bestem værdierne $\zeta(2)$ og $\zeta(4)$.

5. Vis, at $\zeta(s)$ er reel for alle reelle værdier af $s\neq 1$.

6. For gamma-funktionen gælder $\Gamma(s)=\Gamma(s/2)\Gamma((s+1)/2))2^{s-1}/\sqrt{\pi}$ ("Fordoblingsformlen"). Brug fordoblingsformlen til at vise, at funktionalligningen for zeta-funktionen kan udtrykkes sådan: Med $Z(s):=\pi^{-s/2}\Gamma(s/2)\zeta(s)$ gælder: $Z(1-s)=Z(s)$.

10. Nogle diofantiske ligninger.

(10.1). I dette kapitel betragtes nogle diofantiske ligninger, specielt nogle af de ligninger, der kan behandles via kvadratiske talringe. Ligningerne har fået deres tilnavn efter matematikeren Diofant, der levede i Alexandria ca 200–284. Han interesserede sig for rationale løsninger til visse lineære ligninger. I forbindelse med de diofantiske ligninger omtalt her vil vi imidlertid underforstå, at det er ligninger, hvortil man søger *heltalsløsninger*, – i hvert fald hvis intet andet er nævnt. At *løse den diofantiske ligning* går principielt ud på følgende: (1) afgør, om ligningen har (heltals)løsninger); (2) (hvis den har løsninger) afgør, hvor mange løsninger den har; (3) hvis den kun har endelig mange løsninger, så bestem dem alle sammen; (4) hvis den har uendelig mange løsninger, så beskriv dem (sig noget begavet om dem!).

De mest berømte diofantiske ligninger indgår i følgende resultat:

Fermat's store Sætning. *For hver eksponent $n > 2$ har den diofantiske ligning,*

$$x^n + y^n = z^n, \quad \text{med } x, y, z > 0, \tag{10.1.1}$$

ingen løsninger.

Det generelle resultat, for alle $n > 2$, blev bevist af Andrew Wiles i 1995.

Enhvert naturligt tal $n > 2$ er deleligt enten med 4 eller med et ulige primtal p. Det følger let, at for at indse det generelle resultat er det nok at vise, at ligningen ikke har løsninger, når $n = 4$ og når $n = p$ er et ulige primtal. Vi viser umuligheden for $n = 4$, essentielt med Fermat's bevis, og for $n = 3$.

Yderligere behandler vi nogle diofantiske ligninger af formen $y^2 = x^3 + k$, og vi slutter kapitlet af med nogle ligninger af formen $x^2 - bxy + cy^2 = \pm p$.

For $n = 2$ har den diofantiske ligning (10.1.1) som bekendt mange løsninger. Det første resultat herunder kan opfattes som en parmeterfremstilling af løsningerne.

(10.2) Pytagoræiske tripler. *Løsningerne til den diofantiske ligning,*

$$x^2 + y^2 = z^2, \quad \text{med} \quad (x, y) = 1, \quad x, y, z > 0, \quad y \text{ er lige},$$

er netop talsættene (x, y, z) med følgende fremstillinger:

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2, \quad \text{hvor} \quad 0 < b < a,\ (a, b) = 1 \text{ og } ab \text{ er lige.}$$

Parret (a, b) er entydigt bestemt ved (x, y, z).

Bevis. Antag, at (x, y, z) opfylder betingelserne. Af ligningen følger, at en fælles divisor i x, z også er divisor i y. Derfor er $(x, z) = 1$ og $(y, z) = 1$. Da y er lige og $(x, y) = 1$, er x og z ulige. Skriv nu ligningen på formen,

$$y^2 = (z - x)(z + x). \tag{10.2.1}$$

Et tal $d > 1$, der er divisor i begge faktorer $z - x$ og $z + x$ på højresiden, er også divisor i summen $2z$ og i differensen $2x$; da $(x, z) = 1$, er $d = 2$. Omvendt er 2 divisor i begge faktorer, da x og z begge er ulige. Divideres begge faktorer med 2, bliver de primiske, og deres produkt bliver $(y/2)^2$, altså et kvadrat. Af Aritmetikkens Fundamentalsætning følger så, at hver af de dividerede faktorer må være et kvadrat, og vi får fremstillinger:

$$z - x = 2b^2, \quad z + x = 2a^2, \quad y^2 = 4a^2b^2, \quad \text{hvor } (a, b) = 1, \text{ og } 0 < b < a,$$

hvoraf

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Og et af tallene a og b er lige, da x er ulige. Omvendt er det klart, at betingelserne på a, b medfører betingelserne på x, y, z, og at (a, b) er entydigt bestemt. □

Vi vil referere til resultatet som „Pytagoras". Bemærk, at det er enten a eller b, der er lige, og at fremstillingen af x ikke er symmetrisk i a, b. Hvis man fx ønsker, at a skal være lige, kan man i stedet kræve $\pm x = a^2 - b^2$, og så kun $a, b > 0$.

(10.3) Sætning. (Fermat) *Den diofantiske ligning,*

$$x^2 + y^4 = z^4, \qquad x, y, z > 0, \tag{0}$$

har ingen løsninger. Specielt gælder, at ligningen $x^4 + y^4 = z^4$, altså Fermat's ligning (10.1.1) *med $n = 4$, ikke har positive heltalsløsninger.*

Bevis. Den anden påstand er en konsekvens af den første, thi hvis (x, y, z) løser den anden ligning, vil (x^2, y, z) løse den første.

Den første påstand vises ved 'descente infinie', der essentielt er fuldstændig induktion: Vi antager, at ligningen (0) har en løsning (x, y, z). Vi viser, at vi hetil kan bestemme en ny løsning (x', y', z') med kravet $z' < z$. Denne bestemmelse ville så kunne gentages, men det er naturligvis umuligt vedvarende at opfylde kravet, når tallene z skal være positive.

Bestemmelsen af den nye løsning sker i en række skridt:

1. Vi kan antage, at $(y, z) = 1$. Sæt hertil $d := (y, z)$. Det følger så af ligningen, at $d^4 \mid x^2$, og dermed at $d^2 \mid x$. Derfor er $(x', y', z') := (x/d^2, y/d, z/d)$ også en løsning, og hvis $d > 1$ er $z' < z$.

2. Da $(y, z) = 1$ følger det umiddelbart af ligningen, at $(x, y) = 1$ og $(x, z) = 1$. Tallene x, y, z er altså parvis primiske.

3. Potenserne y^4 og z^4 er specielt kvadrater, så vi kan anvende „Pytagoras". Specielt er enten x eller y lige.

Antag først, at x er lige. Da findes primiske $a, b > 0$ med

$$x = 2ab, \quad y^2 = a^2 - b^2, \quad z^2 = a^2 + b^2.$$

Multiplicer de to sidste ligninger med hinanden. Det giver $(yz)^2 = a^4 - b^4$, altså

$$(yz)^2 + b^4 = a^4.$$

Denne ligning har den ønskede form, med $z' = a$, og og da $a^2 < z^2$ er $z' < z$, som ønsket.

4. Antag dernæst, at y (og dermed y^2) er lige. Så findes primiske $a, b > 0$, med a lige, således, at

$$\pm x = a^2 - b^2, \quad y^2 = 2ab, \quad z^2 = a^2 + b^2.$$

Af den anden ligning ses, at $2ab$ er et kvadrat, og af aritmetikkens fundamentalsætning følger så, idet $(a, b) = 1$ og a er lige, at b er et kvadrat og at a er 2 gange et kvadrat. I stedet for at indføre nye symboler, erstatter vi b med b^2 og a med $2a^2$, og får så (bl.a.) ligningen,

$$z^2 = 4a^4 + b^4. \tag{10.3.1}$$

Igen er $4a^4$ og b^4 specielt kvadrater, så vi kan anvende Pytagoras. Der findes altså $c > d > 0$, $(b, c) = 1$, så

$$b^2 = c^2 - d^2, \quad 2a^2 = 2cd, \quad z = c^2 + d^2.$$

Af den anden ligning følger, at både c og d er kvadrater. Erstatter vi c med c^2 og d med d^2, bliver den første ligning til $b^2 = c^4 - d^4$ og den sidste til $z = c^4 + d^4$, altså

$$b^2 + d^4 = c^4, \tag{0'}$$

og $z = c^4 + d^4$. Ligningen $(0')$ har den ønskede form, med $z' := c$, og da $c \leqslant c^4 < z$, er det ønskede opnået. ∎

(10.4) Sætning. *Følgende tre diofantiske ligninger har ingen løsninger med $x, y, z > 0$:*

$$(1) \quad x^4 + y^4 = z^2, \qquad (2) \quad x^4 + 4y^4 = z^2, \qquad (3) \quad x^2 + 4y^4 = z^4.$$

Bevis. Betragt ligningen (1) og ræsonner som i beviset for Sætning (10.3). I „descente infinie"-delen antages (1) med $(x, y) = 1$. Pytagoras giver, idet vi kan antage, at y er lige:

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2,$$

hvor $(a, b) = 1$ og en af a, b er lige. Det må være b, der er lige, thi ellers gælder modulo 4, at $b^2 \equiv 1$ og $a^2 \equiv 0$, hvoraf modstriden $x^2 = a^2 - b^2 \equiv -1$. Af den midterste ligning følger så, at $b = 2c^2$ og $a = d^2$, og indsættelse i den første ligning giver $x^2 = d^4 - 4c^4$, altså

$$x^2 + 4c^4 = d^4. \tag{2'}$$

Igen anvendes Pytagoras: $x = e^2 - f^2$, $2c^2 = 2ef$, $d^2 = e^2 + f^2$. Af den midterste ligning følger, at både e og f er kvadrater, og så kan vi i den sidste ligning erstatte e og f med e^2 og f^2. Ligningen bliver så til

$$e^4 + f^4 = d^2, \tag{1'}$$

som har den ønskede form, med $z' := d \leqslant d^2 = a \leqslant a^2 < z$, som ønsket.

Betragt nu ligningen (2). Den har sammen form som $(2')$ herover, og vi har lige vist, hvordan en sådan ligning ville give en ligning af formen (1), og altså en modstrid. Tilsvarende er ligningen (3) af formen i (10.3.1), og i beviset for Sætning (10.3) så vi, hvordan en sådan ligning giver en ligning af formen (10.3)(0), og altså en modstrid. ∎

(10.5) Påstand. *Den diofantiske ligning,*

$$x^2 + y^4 = 2z^4, \quad \textit{med} \quad x, y, z > 0, \tag{10.5.1}$$

har ingen løsninger.

Bevis. Beviset for påstanden er ved 'descente infinie', essentielt som det foregående bevis.
Antag, at (x, y, z) er en løsning. Vi bestemmer en ny løsning (u, v, w) med $w < z$.

1. Det kan antages, at $(y, z) = 1$. Heraf følger videre, at også $(x, z) = 1$.
2. Tallene x, y, z er alle ulige. Det indses ved at reducere ligningen modulo 4.
3. Omskriv ligningen til følgende:

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

Da $(y, z) = 1$, er de to kvadrater på højresiden primiske. Et af dem må være lige; idet vi et øjeblik tillader x at være negativ, kan vi eventuelt erstatte x med $-x$ og antage, at $(y^2 - x)/2$ er lige. Nu kan (10.2) anvendes. Det følger, at der findes fremstillinger $(y^2+x)/2 = a^2-b^2$, $(y^2 - x)/2 = 2ab$, $z^2 = a^2 + b^2$, med $(a, b) = 1$ og ab lige. Ved subtraktion og addition fås ligningerne:

$$x = a^2 - b^2 - 2ab, \quad y^2 = a^2 - b^2 + 2ab, \quad z^2 = a^2 + b^2.$$

4. Tallet b må være lige. Vi har nemlig $y^2 + 2b^2 = (a + b)^2$, som kan betragtes modulo 4. Tallet y er ulige og hvis også b var ulige, ville $y^2 + 2b^2$ være kongruent med 3, i modstrid med at kvadratet $(a + b)^2$ må være kongruent med 0 eller 1.
5. I ligningen $z^2 = a^2 + b^2$ fra (3) er b lige og $(a, b) = 1$. Altså findes fremstillinger,

$$a = c^2 - d^2, \quad b = 2cd, \quad z = c^2 + d^2, \quad \text{med } (c, d) = 1 \text{ og } cd \text{ lige.} \tag{10.5.2}$$

6. Ligningen $y^2 = a^2 - b^2 + 2ab$ fra (3) kan skrives

$$2b^2 = (a + b - y)(a + b + y). \tag{*}$$

Her er $(a, b) = 1$, og da b er lige, er $a + b$ ulige. Yderligere er $a + b$ og y primiske, thi et primtal p, der er divisor i $a + b$ og i y, må være ulige, og divisor i $2b^2$ og dermed i b; men p kan ikke både gå op i $a + b$ og i b, da $(a, b) = 1$.

De to faktorer på højresiden af (*) har altså 2 som største fælles divisor. Da venstresiden er delelig med 8, må en af de to faktorer være delelig 4 og den anden med 2 og ikke med 4. Idet vi et øjeblik tillader y at være negativ, og eventuelt erstatter y med $-y$, kan vi antage, at det er den anden faktor, der er delelig med 4. Nu følger det af (*), og Aritmetikkens

Fundamentalsætning, at vi har fremstillinger $a+b-y=2f^2$, $a+b+y=4g^2$, $b=2fg$, hvor $(f,g)=1$ og f er ulige. Addition og subtraktion giver ligningerne,

$$a+b=2g^2+f^2, \quad y=2g^2-f^2, \quad b=2fg, \quad \text{med } f \text{ ulige og } (f,g)=1. \tag{10.5.3}$$

7. Af de to udtryk for b, i (10.5.2) og (10.5.3), følger specielt, at $fg=cd$. Da $(f,g)=1$ og $(c,d)=1$, følger det af Aritmetikkens Fundamentalsætning, at der findes tal v,w,s,t således, at

$$f=vt, \quad g=ws, \quad c=wt, \quad d=vs, \quad \text{med } (v,w)=1 \text{ og } (s,t)=1.$$

8. Af (10.5.2) og (10.5.3) fås to udtryk for $a+b$, og det giver ligningen $c^2-d^2+2cd=2g^2+f^2$, altså $2g^2+d^2-2cd+f^2-c^2=0$. Indsættelse heri af ligningerne fra (7) giver ligningen:

$$(2w^2+v^2)s^2-2vwst+(v^2-w^2)t^2=0. \tag{10.5.4}$$

Det er en andengradsligning i s,t, homogen af grad 2, med diskriminanten,

$$4v^2w^2-4(2w^2+v^2)(v^2-w^2)=4(2w^4-v^4).$$

Da andengradsligningen har heltalsløsninger, må diskriminanten være et kvadrat. Derfor findes et helt tal u med $2w^4-v^4=u^2$, altså

$$u^2+v^4=2w^4.$$

Efter et eventuelt fortegnsskift, kan det antages at $u,v,w>0$. Altså er (u,v,w) en løsning (10.5.1). Af $tw=c<c^2<c^2+d^2=z$ følger $w<z$. Den nye løsning (u,v,w) har altså mindre trediekoordinat, som ønsket. $\square$

(10.6) Ak og ve. Opdagede du, at der er noget helt galt med Påstand (10.5)? Det er jo aldeles trivielt, at $(x,y,z)=(1,1,1)$ løser ligningen! Hvor i „beviset" går det galt? Vis, at man ved hjælp af „beviset" kan bestemme uendelig mange løsninger til ligningen, ja faktisk alle løsningerne.

Svar. Det er lidt problematisk, at „beviset" går ud fra at de indgående størrelser er positive. Det kan repareres, hvis nogle størrelser undervejs bliver negative, men den egentlige fejl sker fra skridt (3), hvor det antages, at begge kvadrater er forskellige fra 0. Det kan ikke udelukkes, at $y^2-x=0$, altså at $b=0$. Det sker præcis, når $y^2=x$. Da $(x,y)=1$, er det altså, når $x=y=1$. Det er derfor præcis i løsningen $(x,y,z)=(1,1,1)$, at argumentet bryder sammen.

Men det betyder på den anden side, at man ud fra enhver anden løsning efter endelig mange skridt kommer til løsningen $(1,1,1)$. Og faktisk kan proceduren gøres konstruktiv: Ud fra en løsning (u,v,w), med positive og parvis primiske u,v,w, kan man essentielt rekonstruere (x,y,z) således:

Den homogene andengradsligning (10.5.4), for givne (u, v, w), havde diskriminanten $4u^2 = (2u)^2$. De 4 løsninger (s, t) med $(s, t) = 1$ svarer til de to uforkortelige brøker s/t, bestemt ved den sædvanlig løsningsformel,

$$s/t = \frac{vw \pm u}{v^2 + 2w^2}$$

(nemlig med (s, t) også $(-s, -t)$). På højresiden er tælleren lige og nævneren ulige; da $(s, t) = 1$, følger det, at s er lige og t er ulige. Herefter bestemmes f, g, c, d som i (7), og videre, fra (10.5.2) og (10.5.3),

$$a = w^2t^2 - v^2s^2, \quad b = 2vwst, \quad a + b = 2w^2s^2 + v^2t^2,$$
$$z = w^2t^2 + v^2s^2, \quad y = 2w^2s^2 - t^2v^2.$$

Endelig var x bestemt i (3) som $x = a^2 - b^2 - 2ab = 2a^2 - (a+b)^2$; med de fundne udtryk for a og $a + b$ kan det skrives $x = 2(w^2t^2 - v^2s^2)^2 - (2w^2s^2 + v^2t^2)^2$. Under brug af at $2w^4 - v^4 = u^2$ er det let at reducere udtrykket:

$$x = u^2(t^4 - 2s^4) - 8v^2v^2s^2t^2$$

Ud fra løsningen $(u, v, w) = (1, 1, 1)$ fås $s/t = 2/3$ (idet den anden løsning $s/t = 0$ ikke kan bruges), og altså $(s, t) = (2, 3)$. Det giver løsningen $(239, 1, 13)$. Ud fra denne løsning som (u, v, w) fås $s/t = -2/3$ eller $s/t = 84/113$. De to værdier af (s, t) giver, henholdsvis, de nye løsninger:

$$(x, y, z) = (2750251, 1343, 1525), \quad \text{og} \quad (x, y, z) = (??, 2372159, 2165017).$$

Du må selv bestemme det manglende tal x i det sidste koordinatsæt.

(10.7) Sætning. *Den diofantiske ligning,*

$$x^3 + y^3 = z^3, \qquad \textit{med} \quad x, y, z \neq 0, \tag{10.7.1}$$

har ingen løsninger.

I beviset skal vi bruge, at med en 3'die enhedsrod $\rho = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$, hvor så $\rho^2 + \rho + 1 = 0$, kan vi faktorisere ligningens venstreside: for vilkårlige komplekse tal x, y gælder ligningen,

$$x^3 + y^3 = (x + y)(x + \rho y)(x + \rho^2 y). \tag{10.7.2}$$

Ligningen er nemlig trivielt opfyldt for $y = 0$; for $y \neq 0$ fås (10.7.2) ud fra ligningen $X^3 - 1 = (X - 1)(X - \rho)(X - \rho^2)$ ved at indsætte $X = -x/y$ og multiplicere med $-y^3$.

Desuden skal vi i beviset udføre regninger i den kvadratiske talring $R := \mathbb{Z}[\rho]$. Vi beviser Sætning (10.7) ved at vise, at (10.7.1) ikke har løsninger med $x, y, z \in \mathbb{Z}[\rho]$.

Lad os minde om, at $R = \mathbb{Z}[\rho]$ er delringen af $\mathbb{C}$ bestående af alle komplekse tal af formen $a + b\rho$, hvor $a, b \in \mathbb{Z}$. Det er velkendt, at R er et hovedidealområde (et PID); specielt er R en faktoriel ring (et UFD). Den 6'te enhedesrod $\zeta := 1 + \rho$ tilhører R, og enhederne i R er de 6 potenser ζ^i for $i = 0, \dots, 5$:

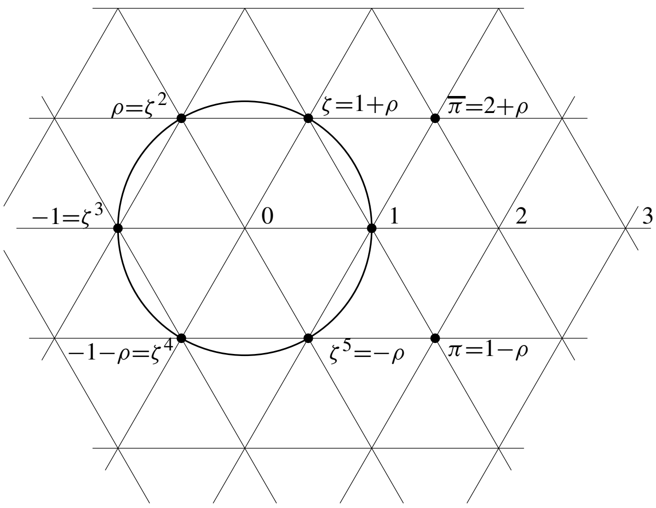
$$R^* : \quad \zeta^0 = 1, \quad \zeta = 1 + \rho, \quad \zeta^2 = \rho, \quad \zeta^3 = -1, \quad \zeta^4 = -\rho - 1, \quad \zeta^5 = -\rho\,.$$

Afbildningen $\mathrm{N}\colon R \to \mathbb{R}$ defineres ved $\mathrm{N}(\alpha) = |\alpha|^2$ (kvadratet på modulus af α). (Den kaldes med en klassisk sprogbrug for *normen*, selv om den jo ikke er en norm i vektorrumsforstand.) Afbildningen er øjensynlig multiplikativ, med positive værdier når $\alpha \neq 0$. Videre har den som bekendt heltalsværdier for $\alpha \in R$; specielt er $|\alpha| \geqslant 1$ for alle $\alpha \neq 0$ i R. Det følger, og vi bruger det gentagne gange herunder, at hvis δ er divisor i α (i ringen R), og $\alpha \neq 0$, så er $|\delta| \leqslant |\alpha|$. (Hvis lighed gælder i denne ulighed, er δ endda en triviel divisor i α, dvs $\alpha = \varepsilon\delta$, hvor ε er en af de 6 enheder.)

I det følgende betragtes tallet $\pi := 1 - \rho = \frac{3}{2} - \frac{i}{2}\sqrt{3} \in R$.

Normen af π er $\mathrm{N}(\pi) = \pi\overline{\pi} = 3$, og normen er altså specielt et (sædvanligt) primtal. Heraf følger som bekendt, at π er et primelement i R. Øjensynlig er $\overline{\pi} = 2 + \rho$. Udregningen $\overline{\pi} = 2 + \rho = (1 + \rho)(1 - \rho) = \zeta\pi$ viser, at det konjugerede tal $\overline{\pi}$ er associeret med π; tallet 3 har i R primopløsningen,

$$3 = \pi\overline{\pi} = \zeta\pi^2.$$



Vi vil flere gange bruge følgende resultat:

Lemma. *Hvis* $\alpha \in R$ *og* $\pi \nmid \alpha$, *så er* $\alpha^3 \equiv \pm 1 \pmod{\pi^4}$.

Bevis. Hertil bemærkes først, at hovedidealet $R3$ i R består af alle tal af formen $3a + 3b\rho$, hvor $a, b \in \mathbb{Z}$. Modulo $R3$ er hvert tal $\alpha \in R$ derfor kongruent med et tal af formen $a + b\rho$, hvor $0 \leqslant a, b < 3$. Der er 3 muligheder for a og 3 muligheder for b, og altså 9 sideklasser modulo $R3$. Af ligningen $3 = \pi\overline{\pi}$ fremgår specielt, at $R\pi \subset R3$. Derfor er antallet af sideklasser modulo $R\pi$ en ægte divisor i 9. Nu følger det nemt, at antallet må være 3. Ringen $R/R\pi$ har derfor 3 elementer, og så må den være isomorf med legemet $\mathbb{Z}/\mathbb{Z}3$. Specielt er hvert tal i R modulo $R\pi$ kongruent med et af de 3 tal 0 og ± 1. Desuden følger det, lige som i Fermat's lille Sætning, at for hvert $\beta \in R$ er $\beta^3 \equiv \beta \pmod{R\pi}$.

Antag nu, at $\pi \nmid \alpha$. Så er $\alpha \equiv \pm 1 \pmod{\pi}$, så vi kan skrive $\alpha = \pm 1 + \beta\pi$ med $\beta \in R$. Binomialformlen og ligningen $3 = \zeta\pi^2$ giver, at

$$\alpha^3 = \pm 1 + 3\beta\pi \pm 3\beta^2\pi^2 + \beta^3\pi^3 = \pm 1 + \pi^3\big(\zeta\beta \pm \zeta\beta^2\pi + \beta^3\big).$$

I parentesen på højresiden er π divisor i $\pm\zeta\beta^2\pi$; yderligere er π divisor i $\zeta\beta - (\zeta\beta)^3 = \zeta\beta + \beta^3$. Derfor er parentesen delelig med π. Med faktoren π^3 foran parentesen følger det, at $\alpha \equiv \pm 1 \pmod{\pi^4}$, som påstået. $\square$

Antag nu, at (10.7.1) har en løsning med $x, y, z \in R$. Vi vil føre dette til en modstrid. For det første følger det klart af ligningen, at hvis to af tallene x, y, z i R har en fælles primfaktor, så vil dette primelement også være divisor i det tredie af tallene. Vi kan derfor, efter at have divideret x, y, z med eventuelle fælles primfaktorer antage, at x, y, z er parvis primiske.

Vi noterer dernæst, at et af tallene x, y, z må være deleligt med π. I modsat fald følger det nemlig af Lemmaet, at modulo π^4 er hver af potenserne x^3, y^3, og z^3 kongruent med ± 1; af ligningen følger derfor, modulo π^4, at med passende fortegnsvalg er $\pm 1 \pm 1 \mp 1 \equiv 0$. Værdien af $\pm 1 \pm 1 \mp 1$ er ± 1 eller ± 3; specielt er værdien ikke 0. Derfor er

$$\left|\pi^4\right|^2 \leqslant \left|\pm 1 \pm 1 \pm 1\right|^2,$$

men det er en modstrid, thi venstresiden er $3^4 = 81$, og højresiden er højst $(1+1+1)^2 = 9$.

I løsningen er altså tallene x, y, z parvis primiske og ét af dem er deleligt med π. Vi kan antage, at $\pi \mid z$, thi hvis fx $\pi \mid x$, så er antagelserne opfyldt for $(z, -y, x)$, som øjensynlig også løser ligningen.

Vi kan altså om løsningen $(x, y, z) \in R^3$ antage, at (10.7.1) gælder, og desuden, at tallene er parvis primiske, altså at $(x, y) = 1$, og at $\pi \mid z$. Modstriden er nu en konsekvens af det følgende resultat.

(10.8) Lemma. *For hver enhed ε i $R = \mathbb{Z}[\rho]$ har ligningen, for elementer $x, y, z \in R$,*

$$x^3 + y^3 = \varepsilon z^3, \quad \text{med } xyz \neq 0, \quad (x, y) = 1, \ \text{og } \pi \mid z, \tag{10.8.1}$$

ingen løsninger.

Bevis. I beviset betegner vi, for hvert tal $\alpha \neq 0$ i R, med $v(\alpha)$ det antal gange π forekommer i primopløsningen af α. Beviset er ved „descente infinie" efter $n := v(z)$: Vi antager, at der et givet en (tænkt) løsning (x, y, z) til (10.8.1) (med et givet ε), og konstruerer en ny løsning (x', y', z') til en ligning af formen (10.8.1) (evt. med et andet ε) og med $v(z') < v(z)$.

Vi bemærker først, at der må gælde $\pi^2 \mid z$, altså at $n \geqslant 2$. Venstresiden i (10.8.1) er nemlig kongruent modulo π^4 med $\pm 1 \pm 1$ og højresiden er kongruent med 0 modulo π^3. Altså er

$\pm 1 \pm 1$ delelig med π^3. Det følger, som ovenfor, at $\pm 1 \pm 1 = 0$. Derfor er venstrsiden delelig med π^4. Altså er z^3 delelig med π^4, og så må z være delelig med π^2.

Nu anvender vi faktoriseringen (10.7.2), her med $x, y, z \in R$, og får ligningen,

$$(x+y)(x+\rho y)(x+\rho^2 y) = x^3 + y^3 = \varepsilon z^3. \tag{10.8.2}$$

Primopløsning af venstresiden fås ved at primopløse de tre parenteser, og primoplsøsning af højresiden fås ved at primopløse z. I primopløsningen må altså alle primfaktorer forekommer med eksponent delelig med 3, og alle primfaktorerne er primfatorer i z. For at bestemme eventuelle primfaktorer, der er fælles for to af parenteserne, betragtes differenserne:

$$(x+y) - (x+\rho y) = (1-\rho)y = \pi y,$$
$$(x+y) - (x+\rho^2 y) = (1+\rho)(1-\rho)y = \zeta\pi y,$$
$$(x+\rho y) - (x+\rho^2 y) = \rho(1-\rho)y = \rho\pi y.$$

Her er ρ og ζ enheder og $\pi \nmid y$. Primfaktorerne i parenteserne er divisorer i z, og specielt ikke divisorer i y. Heraf ses, at det eneste primelement, der kan gå op i to af parenteserne, er π. Desuden ses, at primelementet π, som jo går op i z og derfor går op i parenteserne, må gå op i alle tre, præcis 1 gang i to af parenteserne og derfor $3n-2$ gange i den tredie.

Der er symmetri mellem de tre parenteser, idet vi i ligningen kan erstatte y med ρy eller med $\rho^2 y$. Derfor kan vi antage, at det er den 3'die parentes $x + \rho^2 y$, der er delelig med π^{3n-2}. Ved at sammenligne primopløsningerne på de to sider af (10.8.2) ses nu, at bortset fra multiplikation med faktoren π og en eventuel enhed er hver af de tre parenteser en tredie potens, af parvis primiske tal i R. Med enheder $\varepsilon_j \in R^*$ og elementer $x', y', z' \neq 0$ i R har vi altså ligninger af følgende form:

$$x+y = \varepsilon_1\pi x'^3, \quad x+\rho y = \varepsilon_2\pi y'^3, \quad x+\rho^2 y = \varepsilon_3\pi z'^3, \tag{10.8.3}$$

hvor $(x', y') = 1$. Desuden er $\pi \mid z'$, idet $v(\pi z'^3) = 3n-2$ giver $v(z') = n-1$, og vi har vist, at $n \geqslant 2$.

Multiplicer den første ligning i (10.8.3) med 1, den anden ligning med ρ, og den tredie med ρ^2, og læg sammen. På venstresiden bliver resultatet 0, fordi $1+\rho+\rho^2 = 0$. På højresiden er hvert led deleligt med π; dividerer højresiden med π. Resultatet bliver en ligning, med nye enheder ε_j,

$$0 = \varepsilon_1 x'^3 + \varepsilon_2 y'^3 + \varepsilon_3 z'^3.$$

Efter eventuel division med ε_1 kan det antages, at $\varepsilon_1 = 1$. Flyt så leddet med z'^3 over på den anden side af lighedstegnet. Resultatet bliver en ligning af formen,

$$x'^3 + \varepsilon_2 y'^3 = \varepsilon' z'^3. \tag{10.8.4}$$

Her er π divisor i z', men ikke i x' og y'. Som ovenfor følger det, at $\pm 1 \pm \varepsilon_2 = 0$, altså at $\varepsilon_2 = \pm 1$. Erstattes om nødvendigt y' med $-y'$, kan vi i (10.8.4) antage, at $\varepsilon_2 = 1$. Ligningen har så form som den i (10.8.1). Vi har set, at $(x', y') = 1$, og at $\pi \mid z'$. Altså opfylder (x', y', z') betingelserne i (10.8.1), med enheden ε' i stedet for ε. Yderligere så vi undervejs, at $v(z') = v(z) - 1$.

Hermed er den lovede nye løsning konstrueret. $\square$

(10.9) Sætning. *Følgende diofantiske ligning har ingen løsnininger:*

$$y^2 = x^3 + 7. \tag{10.9.1}$$

Bevis. Ligningen kan også skrive sådan:

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4). \tag{10.9.2}$$

Påstanden vises ved en kongruensbetragtning: Antag, at (x, y) løser (10.9.1), og betragt ligningen modulo 4. Ventresiden er kongruent med 0 eller 1 modul 4. Hvis x er lige, så er højresiden kongruent med 3, og hvis $x \equiv 3 \pmod 4$, så er $x^3 \equiv x \equiv 3$, og højresiden er kongruent med $3 + 7 \equiv 2$, igen i modstrid med ligningen. Altså er $x \equiv 1 \pmod 4$.

Da $x \equiv 1 \pmod 4$, er faktoren $x + 2$ på højresiden af (10.9.2) kongruent med 3 modulo 4. Derfor har $x + 2$ en primfaktor p med $p \equiv 3 \pmod 4$. Da p er divisor i venstresiden, er $y^2 \equiv -1 \pmod p$. Derfor er $\left(\frac{-1}{p}\right) = 1$, og så følger det af Reciprocitetssætningen, at $p \equiv 1 \pmod 4$, i modstrid med at p var valgt med $p \equiv 3 \pmod 4$. □

(10.10) Sætning. *Af de to diofantiske ligninger* (*med* $y \geqslant 0$),

$$\text{(a)}\quad y^2 = x^3 - 2, \qquad \text{(b)}\quad y^2 = x^3 - 4, \tag{10.10.1}$$

har (a) *kun løsningen* $(x, y) = (3, 5)$ *og* (b) *kun de to løsninger* $(x, y) = (2, 2)$ *og* $(5, 11)$.

Bevis. (a) Vi bemærker først, at i en heltalsløsning (x, y) til (10.10.1)(a) må x være ulige, thi hvis x er lige, vil også y være lige; modulo 4 er så venstresiden kongruent med 0 og højresiden kongruent med 2.

I resten af beviset for (a) udnytter vi den kvadratiske talring $R := \mathbb{Z}[i\sqrt{2}]$, bestående af tal af formen $a + bi\sqrt{2}$ med $a, b \in \mathbb{Z}$. Det er velkendt, at R er et PID. Enhederne ± 1 er de eneste enheder i R. Normen er bestemt ved $\mathrm{N}(a + bi\sqrt{2}) = a^2 + 2b^2$. Ligningen kan skrives $y^2 + 2 = x^3$, altså $\mathrm{N}(y + i\sqrt{2}) = x^3$. I R kan vi faktorisere:

$$(y + i\sqrt{2})(y - i\sqrt{2}) = y^2 + 2 = x^3, \tag{10.10.2}$$

og vi sammenligner primopløsningerne af ligningens to sider. De to parenteser på venstresiden er primiske. Antag nemlig, at δ er divisor i begge tallene $y \pm i\sqrt{2}$. Da er δ divisor i differensen $2i\sqrt{2}$, og heraf følger, at normen af δ er divisor i normen af $2i\sqrt{2}$, altså at $\mathrm{N}(\delta)$ er divisor i 8. På den anden side var δ divisor i $y + i\sqrt{2}$, og heraf følger, at normen af δ er divisor i normen af $y + i\sqrt{2}$. Den sidste norm er, ifølge ligningen (10.10.2), lig med x^3. Altså er $\mathrm{N}(\delta)$ divisor både i 8 og i det ulige tal x^3. Følgelig er $\mathrm{N}(\delta) = 1$. Altså er $\delta = \pm 1$ en enhed i R. Derfor er de to parenteser primiske.

I ligningen (10.10.2) er højresiden en 3'die potens. Af entydigheden af primopløsningerne følger derfor, at hver af de to parenteser er en 3'die potens i R. Specielt er $y + i\sqrt{2}$ en tredie potens. Med tal $u, v \in \mathbb{Z}$ har vi altså en ligning,

$$y + i\sqrt{2} = (u + vi\sqrt{2})^3.$$

Brug binomialformlen på ligningens højreside, og sammenlign koefficienterne til 1 og til $i\sqrt{2}$ på ligningens to sider. Det giver to ligninger,

$$y = u^3 - 6uv^2 = u(u^2 - 6v^2), \quad \text{og} \quad 1 = -2v^3 + 3u^2v = v(3u^2 - 2v^2).$$

Af ligningen $1 = v(3u^2 - 2v^2)$ i $\mathbb{Z}$ følger, at begge faktorer må være ± 1. Først fås altså $v = \pm 1$, og dernæst $3u^2 - 2 = \pm 1$. Her er $3u^2 - 2 = -1$ udelukket, og følgelig er $v = +1$ og $3u^2 - 2 = 1$, dvs $u = \pm 1$. Nu fås $y = \pm(1 - 6)$, altså $y = \pm 5$. Da $y \geqslant 0$, følger det, at $y = 5$, og så er $x^3 = 5^2 + 2$, dvs $x = 3$, som påstået.

Beviset for (b) er tilsvarende, men udnytter Gauss's talring $\mathbb{Z}[i]$. Også $\mathbb{Z}[i]$ er som bekendt i PID, med enhederne $\{\pm 1, \pm i\}$. I $\mathbb{Z}[i]$ er tallet 2 specielt: Det har primopløsningen $2 = (1+i)(1-i) = (-i)(1+i)^2$, og det er enheden $-i$, gange kvadratet på primelementet $1+i$. Ligningen kan skrives,

$$(y + 2i)(y - 2i) = y^2 + 4 = x^3. \tag{10.10.3}$$

De to faktorer på venstresiden er konjugerede. En fælles divisor for de to faktorer må også være divisor i differensen, dvs i $2^2 i$; en fælles divisor må altså være en potens af $1 + i$ (med eksponent højst 4). Det følger nu, at det eneste primelement (bortset fra associering), der kan være divisor i begge faktorer, er $1 + i$, og $1 + i$ forekommer med samme eksponent i primopløsningen af de to faktorer.

Da højresiden er et tredie potens følger det, at bortset fra en enhed er begge faktorer på venstresiden trediepotenser. Da gruppen af enheder har orden 4, primisk med 3, er hver enhed en tredie potens (det checkes naturligvis også let direkte for hver af de 4 enheder). Derfor er hver faktor på venstresiden en trediepotens. Der findes altså en ligning, med $u, v \in \mathbb{Z}$,

$$y + 2i = (u + iv)^3.$$

Sammenligning af koefficienterne til 1 og til i giver:

$$y = u^3 - 3uv^2 = u(u^2 - 3v^2), \qquad 2 = 3u^2v - v^3 = (3u^2 - v^2)v.$$

Entydighed af (sædvanlig) primopløsning giver, i den sidste ligning, at begge faktorer på højresiden er ± 1 eller ± 2.

Hvis $v = \pm 1$, må den anden faktor være ± 2, dvs $3u^2 - 1 = \pm 2$; heraf fås $u^2 = 1$ (idet $3u^2 = -1$ kan forkastes). Og så er $y = \pm(1 - 3)$, dvs $y = 2$ og $(x, y) = (2, 2)$.

Hvis $v = \pm 2$, må den anden faktor være ± 1, dvs $3u^2 - 4 = \pm 1$; heraf fås $u^2 = 1$ (idet $3u^2 = 5$ kan forkastes). Og så er $y = \pm(1 - 12)$, dvs $y = 11$ og $(x, y) = (5, 11)$. □

(10.11). Betragt en kvadratisk talring $\mathbb{Z}[\xi]$, hvor det irrationale tal ξ er rod i andengradspolynomiet $X^2 + bX + c$ med hele koefficienter b, c; antagelsen om at ξ er irrational, er ækvivalent med at diskriminanten $D := b^2 - 4c$ ikke er et kvadrat. Lad videre p være et (sædvanligt) primtal.

Som bekendt gælder da, at p er reducibel i $\mathbb{Z}[\xi]$, hvis og kun følgende diofantiske ligning har løsninger:

$$x^2 - bxy + cy^2 = \pm p\,, \tag{10.11.1}$$

og p er ikke et primelement, hvis og kun hvis følgende kongruens har løsninger:

$$z^2 - bz + c \equiv 0 \pmod{p}. \tag{10.11.2}$$

Den velkendte konsekvens er, at hvis ligningen har løsninger, så har kongruensen løsninger, og hvis ringen er UFD, så gælder „hvis og kun hvis".

Det er let at undersøge kongruensen: Hvis $p = 2$ har kongruensen løsninger, hvis og kun hvis b eller c er lige. Antag, at p er ulige. Så er 2 invertibel i $\mathbb{F}_p$; modulo p kan vi derfor omskrive kongruensen til følgende ligning i $\mathbb{F}_p$:

$$\left(z - \frac{b}{2}\right)^2 - \left(\frac{b}{2}\right)^2 + c = 0, \quad \text{eller} \quad (2z - b)^2 = D.$$

I $\mathbb{F}_p$ har den sidste ligning øjensynlig én løsning, hvis $p \mid D$. Hvis $p \nmid D$, har den sidste ligning, og altså kongruensen (10.11.2), løsninger, hvis og kun hvis $\left(\frac{D}{p}\right) = 1$.

Sætning. *Antag, at den kvadratisk talring $\mathbb{Z}[\xi]$ er et UFD. Da har den diofantiske ligning* (10.11.1) *med et ulige primtal p løsninger, hvis og kun hvis $p \mid D$ eller $\left(\frac{D}{p}\right)$=1. Den sidste betingelse er opfyldt, hvis og kun hvis $\left(\frac{p}{D}\right) = 1$, og specielt gælder, at eventuel løsbarhed af ligningen kun afhænger af restklassen af p modulo D.*

Bevis. Den første del af påstanden er vist ovenfor, den sidste del følger umiddelbart af Reciprocitetssætningen. □

(10.12) Bemærkning. Løsninger (x, y) til ligningen $x^2 - bxy + cy^2 = \pm p$ svarer til fremstillinger $p = \pm\pi\pi'$, hvor $\pi = x + y\xi$. Da p er et primtal, må en sådan fremstilling nødvendigvis være en primopløsning i $\mathbb{Z}[\xi]$ af tallet p. Ligningen har altså i almindelighed flere løsninger, svarende til at man i primopløsningen kan ombytte π og π' og multiplicere π med en enhed (og π' med den konjugerede enhed) i $\mathbb{Z}[\xi]$. Enhederne i $\mathbb{Z}[\xi]$ bestemmes som bekendt ved at løse den diofantiske ligning,

$$u^2 - buv + cv^2 = \pm 1; \tag{10.12.1}$$

heltalsløsninger (u, v) svarer til enheder $\varepsilon = u + v\xi \in \mathbb{Z}[\xi]$.

Ligningen (10.11.1) er i en vis forstand to ligninger, nemlig én ligning, hvor højresiden er $+p$ og én, hvor højresiden er $-p$; at (10.11.1) gælder, betyder at en af disse to ligninger er opfyldt. Tilsvarende svarer (10.12.1) til to ligninger.

I det *imaginære tilfælde*, dvs hvis $D < 0$, er $x^2 - bxy + cy^2 = \mathrm{N}(x + y\xi)$ altid positiv. I dette tilfælde svarer (10.11.1) altså til ligningen med højresiden $+p$, og (10.12.1) er kun interessant med højresiden $+1$. Yderligere er der kun 9 værdier af diskriminanten D for hvilke talringen $\mathbb{Z}[\xi]$ er et UFD, nemlig følgende:

$$-3,\ -4,\ -7,\ -8,\ -11,\ -19,\ -43,\ -67,\ -163,$$

og det er altså kun for disse 9 værdier af D, at sætningen kan anvendes. For $D = -3$ består enhederne af de 6. enhedesrødder, for $D = -4$ er det de 4. enhedsrødder, og for $D < -4$ er der kun de trivielle enhedsrødder ± 1.

Fx følger det, svarende til $D = -8$, at de ulige primtal af formen $p = x^2 + 2y^2$ netop er de primtal p, for hvilke $\left(\frac{p}{-8}\right) = 1$, dvs at p er kongruent med 1 eller 3 modulo 8.

Og svarende til $D = -19$ følger det: primtallene af formen $p = x^2 - xy + 5y^2$ er netop primtallene p for hvilke $\left(\frac{p}{19}\right) = 1$ (samt $19 = 1^2 - 1 \cdot 2 + 5 \cdot 2^2$).

I det *reelle tilfælde*, altså hvis $D > 0$, er det mere kompliceret: Af de to ligninger i (10.11.1) kan den ene, eller den anden, eller begge, være opfyldt. Ligningen (10.12.1), til bestemmelse af enhederne i $\mathbb{Z}[\xi]$, kaldes *Pell's ligning*. Med højresiden $+1$ er det den *egentlige Pell'ske ligning*; med højresiden -1 kaldes ligningen også den *ikke-Pell'ske ligning*. Man kan vise, at den egentlige Pell'ske ligning altid har uendelig mange løsninger og at den ikke-Pell'ske ligning hare enten ingen eller uendelig mange løsninger.

Hvis den ikke-Pell'ske ligning, dvs (10.12.1) med højresiden -1, har løsninger, så gælder, at hvis en af ligningerne i (10.12.1) har løsninger, så har de begge løsninger. Hvis derimod den ikke-Pell'ske ligning ikke har løsninger, så er det højst en af ligningerne i (10.11.1), der kan løses.

Man ved ikke, om der er uendelig mange positive værdier af D for hvilke ringen $\mathbb{Z}[\xi]$ er UFD. Det er ikke svært at vise, at hvis $\mathbb{Z}[\xi]$ er et UFD, så må D være kvadratfri som diskriminant. De første kvadratfri diskriminanter er følgende:

$$5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 40, 41, 44, 53, 56, 57, 60, 61, \dots$$

og af dem er det kun talringene svarende til $D = 40$ og $D = 60$, der ikke er UFD.

Fx ses, svarende til $D = 8$, at den ikke-Pell'ske ligning $x^2 - 2y^2 = -1$ har løsninger, fx $(x, y) = (1, 1)$. Heraf følger, at de ulige primtal p, der kan skrives på formen $p = x^2 - 2y^2$ netop er de primtal p, for hvilke $\left(\frac{p}{8}\right) = 1$, dvs at $p \equiv \pm 1 \pmod 8$, og det er de samme primtal, der kan skrives på formen $p = -x^2 + 2y^2$.

Og svarende til $D = 12$ fås: Den ikke-Pell'ske ligning $x^2 - 3y^2 = -1$ har ingen løsninger. En af ligningeren $x^2 - 3y^2 = \pm p$ (og ikke begge) har løsninger, hvis og kun hvis $\left(\frac{p}{12}\right) = 1$ (eller $p = 2, 3$).

(10.13) Opgaver.

1. Bestem den manglende koordinat x i løsningen angivet i (10.5).

2. Marker på figuren i (10.6) punkterne svarende til primelementer associerede med π.

3. Vis for en enhed ε i $\mathbb{Z}[\rho]$, at ligningen $x^3 + y^3 = \varepsilon\zeta^3$ med $x, y, z \neq 0$ ikke har løsninger i $\mathbb{Z}[\rho]$.

4. Vis, for et primtal p, at $\left(\frac{p}{12}\right) = 1$, hvis og kun hvis $p \equiv \pm 1 \pmod{12}$. Bestem de første 8 primtal p, der kan skrives på formen $p = \pm(x^2 - 3y^2)$. Ser du mønsteret på fortegnet? Kan du bevise, at det forholder sig sådan?

5. Antag, at p er et primtal med $p \equiv 5 \pmod 8$. Vis, at den kvadratiske talring $\mathbb{Z}[\sqrt{2p}]$ ikke er et UFD. [Vink: kongruensen $x^2 - 2p \equiv 0 \pmod p$ har løsninger (nemlig $x = 0$), men (regn modulo 8) ligningen $x^2 - 2py^2 = \pm p$ har ingen løsninger.]

6. Antag, at p og q er ulige primtal med $q \equiv 1 \pmod 4$ og $\left(\frac{p}{q}\right) = -1$. Vis, at den kvadratiske talring $\mathbb{Z}[\sqrt{pq}]$ ikke er et UFD. [Vink: Se på ligningen $x^2 - pqy^2 = \pm p$ og på kongruensen $x^2 - pqy^2 \equiv \pm p$ modulo p og modulo q.]

7. *Bestem alle positive rationale løsninger (x, y) til ligningen $x^y = y^x$.

11. L-rækker.

(11.1). I det følgende betragtes et fast naturligt tal $N \geqslant 1$, og komplekse funktioner (talfølger) $\psi\colon \mathbb{N} \to \mathbb{C}$, der er periodiske med perioden N, dvs $\psi(n+N) = \psi(n)$ for alle n. Det er ofte bekvemt at bruge periodiciteten til at udvide definitionsmængden fra $\mathbb{N}$ til $\mathbb{Z}$. Alternativt kan ψ opfattes som en funktion $\psi\colon \mathbb{Z}/N \to \mathbb{C}$. Bemærk specielt, at $\psi(0) = \psi(N) = \psi(-N)$. I det følgende skrives ψ_- og $\hat{\psi}$ for funktionerne bestemt ved

$$\psi_-(n) = \psi(-n), \qquad \hat{\psi}(n) = \sum_{a=1}^{N} \psi(a) e^{2\pi i na/N} = \sum_{a=1}^{N} \psi(a)\zeta^{na},$$

hvor $\zeta = e^{2\pi i/N}$ er den kanoniske primitive N'te enhedsrod. Øjensynlig er $(\psi_-)\hat{} = \hat{\psi}_-$, og $\hat{\psi}(0) = \sum_{a=1}^{N} \psi(a)$.

Den transformerede funktion $\mathcal{F}\psi = \hat{\psi}$ kan opfattes som den *diskrete Fourier-transformation* af ψ. (Andre valg af $\mathcal{F}\psi$ kunne være $\hat{\psi}_-$ eller $\hat{\psi}/\sqrt{N}$, eller . . . .) Det er ikke svært at vise „*Omvendingsformlen*,

$$\psi\hat{}\hat{} = N\psi_- . \tag{11.1.1}$$

(11.2) L-rækker. Funktionen $\psi(n)$ er specielt begrænset, så den tilhørende *L-række*,

$$L_\psi(s) := \sum\nolimits_{n\geqslant 1} \frac{\psi(n)}{n^s}, \qquad \Re s > 1, \tag{11.2.1}$$

fremstiller, ligesom Riemann's ζ-funktion, en holomorf funktion i halvplanen, hvor $\Re s > 1$. Vi vil også betragte følgende sum:

$$L_\psi^{\pm}(s) := L_\psi(s) + e^{i\pi s} L_{\psi_-}(s). \tag{11.2.2}$$

Med valget $(-n)^s := e^{-i\pi s} n^s$ for $n > 0$ er leddet $e^{i\pi s} L_{\psi_-}(s)$ på højresiden, for $\Re s > 1$, lig med summen $\sum_{n\geqslant 1} \psi(-n)/(-n)^s$, og altså

$$L_\psi^{\pm}(s) := \sum_{m\neq 0} \frac{\psi(m)}{m^s}, \qquad \Re s > 1, \tag{11.2.3}$$

hvor summen er over alle *hele* tal $m \neq 0$. Afhængigheden af valget forsvinder naturligvis, når $s \in \mathbb{Z}$; her er $L_\psi^{\pm}(s) = L_\psi(s) + (-1)^s L_{\psi_-}(s)$.

I studiet af L-rækkerne indgår desuden følgende funktion $I_\psi(s)$, hvor $s \in \mathbb{C}$ er vilkårlig:

$$I_\psi(s) := \frac{-1}{2\pi i} \oint_{-\infty}^{-\infty} \sum_{a=1}^{N} \psi(a) \frac{e^{az}}{e^{Nz} - 1} z^s \frac{dz}{z}. \tag{11.2.4}$$

Polerne for integranden er nulpunkterne for nævneren, altså tallene $c = 2\pi i k/N$ for $k \in \mathbb{Z}$. Integrationsvejen er den, der er beskrevet i (9.2), rundt om den negative reelle halvakse.

Radius $\varepsilon > 0$ er valgt så lille, at kun polen $z = 0$ falder inde i cirklen med radius ε. Under gennemløbet af halvaksen fra $-\infty$ til $-\varepsilon$ opfattes $z = -t$ som randpunkt for den nedre halvplan, $z^s = t^s e^{-i\pi s}$, og på gennemløbet fra $-\varepsilon$ til $-\infty$ opfattes $z = -t$ som randpunkt for den øvre halvplan. $z^s = e^{i\pi s} t^s$. Specielt er z^s numerisk begrænset af en konstant gange $t^{\Re s}$. I hvert led er $a \geqslant 1$, så $|e^{az}/(e^{Nz} - 1)| = e^{-at}/(1 - e^{-Nt}) \leqslant Ce^{-t}$. Heraf ses, ganske som for Riemann's ζ-funktion, at $I_\psi(s)$ definerer en holomorf funktion i hele den komplekse plan.

Vi sætter $f_\psi(z) := \sum_a \psi(a)e^{az}$, hvor summen her og i det følgende er over $a = 1, \dots, N$. Integranden i $I(s)$ er $f_\psi(s)z^{s-1}/(e^{Nz} - 1)$. Som i (9.2.3) kan vi omforme, for alle $s \in \mathbb{C}$:

$$I_\psi(s) = \frac{\sin \pi s}{\pi} \int_\varepsilon^\infty \frac{f_\psi(-t)}{1 - e^{-Nt}}\, t^s \frac{dt}{t} + \frac{-1}{2\pi i} \int_{|z|=\varepsilon} \frac{f_\psi(z)}{e^{Nz} - 1}\, z^s \frac{dz}{z}\,, \tag{11.2.5}$$

hvor kurveintegralet er langs cirklen med centrum 0 og (lille) radius ε.

(11.3) Sætning. *I halvplanen $\Re s > 1$ gælder følgende ligninger:*

$$I_\psi(s) = \frac{\sin \pi s}{\pi} \Gamma(s) L_\psi(s), \quad L_\psi(s) = \Gamma(1 - s) I_\psi(s). \tag{11.3.1}$$

Ligningen bestemmer udvidelsen af $L_\psi(s)$ til en meromorf funktion i hele $\mathbb{C}$, holomorf på nær eventuelt (afhængigt af ψ) en pol for $s = 1$.

Bevis. Beviset for den første ligning, for $\Re s > 1$, er helt parallelt med beviset for den første ligning i Sætning (9.3): Af ligningen for Γ-funktionen,

$$\Gamma(s) = \int_0^\infty t^s e^{-t} \frac{dt}{t}, \qquad \Re s > 0,$$

fås for $n \geqslant 1$ ved substitution af t med nt, og multiplikation med $\psi(n)n^{-s}$, at

$$\frac{\psi(n)}{n^s} \Gamma(s) = \int_0^\infty \psi(n) t^s e^{-nt} \frac{dt}{t}\,, \qquad \Re s > 0. \tag{11.3.2}$$

For $\Re s > 1$ kan leddende summeres. Venstresiden bliver $L_\psi(s)\Gamma(s)$ og højresiden bliver (majoriseret konvergens) til integralet af summen. Rækken $\sum_{n \geqslant 1} \psi(n)e^{-nt}$ er essentielt en sum af N kvotientrækker:

$$\sum_{n \geqslant 1} \psi(n) e^{-nt} = \sum_{a=1}^N \sum_{k \geqslant 0} \psi(a) e^{-at} e^{-Nkt} = \sum_{a=1}^N \psi(a) \frac{e^{-at}}{1 - e^{-Nt}} = \frac{f_\psi(-t)}{1 - e^{-Nt}}\,.$$

Summation af leddene i (11.3.2) giver derfor ligningen,

$$L_\psi(s)\Gamma(s) = \int_0^\infty \frac{f_\psi(-t)}{1 - e^{-Nt}}\, t^s \frac{dt}{t}\,, \qquad \Re s > 1. \tag{11.3.3}$$

Sammenlign med (11.2.5) for $\varepsilon \to 0$: Når $\Re s > 1$, følger det, at det andet integral, kurveintegralet langs cirklen, går mod 0. Det første integral konvergerer mod integralet i (11.3.3). Heraf følger den første ligning i (11.3.1).

Den anden ligning i (11.3.1) er blot en omskrivning af den første, idet $\Gamma(s)\Gamma(1-s) = \pi/\sin \pi s$, jfr (9.4.2). Ligningen bestemmer udvidelsen af $L_\psi(s)$ til hele $\mathbb{C}$. Da $I_\psi(s)$ er holomorf, er polerne for $L_\psi(s)$ blandt polerne for $\Gamma(1-s)$, dvs blandt tallene $s = 1, 2, 3, \dots$, men da $L_\psi(s)$ er holomorf for $\Re s > 1$, står kun $s = 1$ tilbage som eventuel pol.

Gamma-funktionen $\Gamma(s)$ har i $s = 0$ en simpel pol med residuum 1, så $\Gamma(1-s)$ har i $s = 1$ en simpel pol med residuum -1. Funktionen $I_\psi(s)$ er specielt holomorf for $s = 1$. Altså er $s = 1$ en simpel pol for $L_\psi(s)$ med residuet $-I_\psi(1)$. Specielt er $L_\psi(s)$ holomorf for alle s, hvis $I_\psi(1) = 0$. □

(11.4) Funktionalligningen. *For alle komplekse tal s gælder de to ligninger:*

$$L_\psi(1-s) = \Gamma(s) I_\psi(1-s), \qquad L_\psi^{\pm}(s) = \Big(\frac{2\pi i}{N}\Big)^s I_{\hat{\psi}_-}(1-s). \tag{11.4.1}$$

Specielt gælder funktionalligningen,

$$L_\psi(1-s) = \frac{1}{N}\Gamma(s)\Big(\frac{2\pi i}{N}\Big)^{-s} L_{\hat{\psi}}^{\pm}(s). \tag{11.4.2}$$

Bevis. Integranden i kurveintegralet i $I_\psi(s)$ er funktionen $z^{s-1} f_\psi(z)/(e^{Nz}-1)$, med $f_\psi(z) = \sum_{a=1}^N \psi(a) e^{az}$. Nævneren $e^{Nz}-1$ er periodisk med perioden $2\pi i/N$. og $z = 0$ er et simpelt nulpunkt: $e^{Nz} - 1 = Nz + \cdots$. Derfor har $(e^{Nz}-1)^{-1}$ for $z = 0$, og derfor også for de øvrige poler $z = c = 2\pi i k/N$ med $k \in \mathbb{Z}$, en simpel pol med residuet $1/N$. Som i beviset for (9.3) følger det så af Residuesætningen, for $\Re s < 0$, at

$$I_\psi(s) = \sum_{c \neq 0} \operatorname{Res}_{z=c} \frac{z^{s-1} f_\psi(z)}{e^{Nz}-1} = \frac{1}{N} \sum_{c\neq 0} c^{s-1} f_\psi(c), \tag{11.4.3}$$

hvor summen er over alle poler $c \neq 0$, dvs $c = \pm 2\pi n/N$ for $n \in \mathbb{N}$.

For $b = 2\pi i n/N$ er er øjensynlig $f_\psi(b) = \hat{\psi}(n)$ og $f_\psi(-b) = \hat{\psi}(-n) = \hat{\psi}_-(n)$. Videre er $\arg(-i) = \arg(i) - \pi$, og altså $(-i)^s = e^{-i\pi s} i^s$. Derfor er $b^s = (2\pi i/N)^s n^s$ og $(-b)^s = e^{-i\pi s}(2\pi i/N)^s n^s$. Polerne $\pm b$ bidrager altså til summen i (11.4.3) med følgende:

$$b^{s-1} f_\psi(b) + (-b)^{s-1} f_\psi(-b) = (2\pi i/N)^{s-1}\Big(\frac{\hat{\psi}(n)}{n^{1-s}} + e^{i\pi(1-s)} \frac{\hat{\psi}_-(n)}{n^{1-s}}\Big).$$

Indsættelse i udtrykket (11.4.3) giver derfor følgende ligning, først for $\Re s < 0$, og dernæst for alle s, da begge sider er meromorfe i hele $\mathbb{C}$:

$$I_\psi(s) = \frac{1}{N}(2\pi i/N)^{s-1} L_{\hat{\psi}}^{\pm}(1-s). \tag{11.4.4}$$

Den første ligning i (11.4.1) fås umiddelbart af (11.3.1) ved at erstatte s med $1-s$. Tilsvarende kan vi erstatte s med $1-s$ i (11.4.4). Af de to ligninger fremgår funktionalligningen (11.4.2) umiddelbart.

Som nævnt gælder omvendingsformlen $\psi\hat{}\hat{} = N\psi_-$. Den anden ligning i (11.4.1) fremkommer derfor af (11.4.4), når ψ erstattes med $\hat{\psi}_-$ og s erstattes med $1-s$. □

(11.5) Lige og ulige. Ligningerne forenkles, hvis ψ er *lige*, dvs $\psi_- = \psi$, eller *ulige*, dvs $\psi_- = -\psi$. Vi har $1+e^{i\pi s} = e^{i\pi s/2}(e^{i\pi s/2}+e^{-i\pi s/2}) = 2i^s\cos(\pi s/2)$; hvis ψ er lige får vi altså $L^{\pm}_{\psi}(s) = (1+e^{i\pi s})L_\psi(s) = 2i^s\cos(\pi s/2)L_\psi(s)$. Når ψ er ulige får vi en tilsvarende ligning ved at udnytte, at $1-e^{i\pi s} = -2i\, i^s\sin(\pi s/2)$. Ialt fås, når ψ er hhv lige og ulige, at

$$L^{\pm}_{\psi}(s) = 2i^s\cos(\pi s/2)L_\psi(s), \quad \text{hhv} \quad L^{\pm}_{\psi}(s) = -2i\, i^s\sin(\pi s/2)L_\psi(s). \tag{11.5.1}$$

Når ψ er lige giver indsættelse i den anden ligning i (11.4.1) og i ligningen (11.4.2), at

$$\cos\frac{\pi s}{2}L_\psi(s) = \frac{1}{2}\Big(\frac{2\pi}{N}\Big)^s I_{\hat\psi}(1-s), \tag{11.5.2$^+$}$$

$$L_\psi(1-s) = \frac{2}{N}\Gamma(s)\Big(\frac{2\pi}{N}\Big)^{-s}\cos\frac{\pi s}{2}L_{\hat\psi}(s), \tag{11.5.3$^+$}$$

$$\Big(\frac{N}{\pi}\Big)^{\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)L_\psi(s) = \frac{1}{\sqrt{N}}\Big(\frac{N}{\pi}\Big)^{\frac{1-s}{2}}\Gamma\Big(\frac{1-s}{2}\Big)L_{\hat\psi}(1-s). \tag{11.5.4$^+$}$$

Ligning (11.5.4$^+$) fås af (11.5.3$^+$) ved at erstatte s med $1-s$ og udnytte egenskaber ved Γ-funktionen. Tilsvarende fås, når ψ er ulige:

$$\sin\frac{\pi s}{2}L_\psi(s) = \frac{1}{2i}\Big(\frac{2\pi}{N}\Big)^s I_{\hat\psi}(1-s), \tag{11.5.2$^-$}$$

$$L_\psi(1-s) = \frac{2}{iN}\Gamma(s)\Big(\frac{2\pi}{N}\Big)^{-s}\sin\frac{\pi s}{2}L_{\hat\psi}(s), \tag{11.5.3$^-$}$$

$$\Big(\frac{N}{\pi}\Big)^{\frac{s}{2}}\Gamma\Big(\frac{s+1}{2}\Big)L_\psi(s) = \frac{1}{i\sqrt{N}}\Big(\frac{N}{\pi}\Big)^{\frac{1-s}{2}}\Gamma\Big(\frac{1-s+1}{2}\Big)L_{\hat\psi}(1-s). \tag{11.5.4$^-$}$$

(11.7) Generaliserede Bernoulli-tal. Antag, at s er et helt tal. Så er z^s holomorf for $z \neq 0$, og integranden i $I_\psi(s)$ er en meromorf funktion, holomorf på nær eventuelt i nulpunkterne for $e^{Nz}-1$. Specielt vil de to kurveintegraler langs den negative reelle akse ophæve hinanden, og $-I(s)$ er $1/2\pi i$ multipliceret med kurveintegralet langs den lille cirkel omkring 0. Produktet er som bekendt residuet for $z=0$ af integranden, altså

$$-I_\psi(s) = \operatorname{Res}_{z=0}\frac{f_\psi(z)}{e^{Nz}-1}z^{s-1}. \tag{11.7.1}$$

Følgelig gælder, at $-I_\psi(s)$ er koefficienten til z^{-s} i Laurent-rækken omkring $z=0$ for funktionen

$$\beta_\psi(z) := \frac{f_\psi(z)}{e^{Nz}-1} = \sum_a \psi(a)\frac{e^{az}}{e^{Nz}-1}.$$

Nævneren $e^{Nz}-1$ har et simpelt nulpunkt for $z=0$, så $\beta_\psi(z)$ har højst en simpel pol for $z=0$. Produktet $z\beta_\psi(z)$ har altså ingen pol, dvs rækken er en potensrække. Koefficienterne er essentielt de *generaliserede Bernoulli-tal* $B_k(\psi)$, der defineres ved rækkeudviklingen,

$$\beta_\psi(z) = \sum_{a=1}^{N}\psi(a)\frac{e^{az}}{e^{Nz}-1} = \frac{1}{z}\sum_{k\geqslant 0}B_k(\psi)\frac{z^k}{k!}. \tag{11.7.2}$$

Bemærk, at $B_k(\psi)/k!$ for $k \geqslant 0$ er koefficienten til z^{k-1} i rækken for $\beta_\psi(z)$, og at denne koefficient er 0 for $k < 0$. Af (11.7.1) fås derfor ligningen for alle hele tal k:

$$I_\psi(1-k) = \begin{cases} -B_k(\psi)/k! & \text{når } k \geqslant 0, \\ 0 & \text{ellers.} \end{cases} \tag{11.7.3}$$

I anvendelserne skal vi også bruge Bernoulli-tallene $B_k(\hat{\psi})$ og $B_k(\hat{\psi}_-)$ for de transformerede funktioner. Rækken $\beta_{\hat{\psi}}(z)$ bestemmes ved en simpel summation:

$$f_{\hat{\psi}}(z) = \sum_a \hat{\psi}(a)e^{az} = \sum_a \sum_b \psi(b)\zeta^{ab}e^{az} = \sum_b \psi(b)\zeta^b e^z \frac{e^{Nz}-1}{\zeta^b e^z - 1},$$

hvor vi har udnyttet, at $\zeta^N = 1$. Da $\beta_\psi(z) = f_\psi(z)/(e^{Nz}-1)$, får vi

$$\beta_{\hat{\psi}}(z) = \sum_b \psi(b)\frac{\zeta^b e^z}{\zeta^b e^z - 1}. \tag{11.7.4}$$

Da $\cot w = -i + 2ie^{2iw}/(e^{2iw}-1)$, er $\cot\bigl(\frac{z}{2} + \frac{\pi b}{N}\bigr) = -i + 2i\zeta^b e^{iz}/(\zeta^b e^{iz} - 1)$, altså

$$\sum_b \psi(b)\cot\bigl(\tfrac{z}{2} + \tfrac{\pi b}{N}\bigr) = -i\sum_b \psi(b) + 2i\beta_{\hat{\psi}}(iz). \tag{11.7.5}$$

Vi indfører nu de *transformerede Bernoulli-tal* $A_k(\psi)$ ved rækkeudviklingen af frembringerfunktionen $\alpha_\psi(z)$:

$$\alpha_\psi(z) := \sum_b \frac{\psi(b)}{N}\cot\frac{z - b\pi}{N} = \frac{1}{z}\sum_{k\geqslant 0} A_k(\psi)\frac{z^k}{k!}. \tag{11.7.6}$$

I punktet $z = 0$ er det kun leddet $\frac{1}{N}\cot\frac{z}{N}$, for $b = N$, der bidrager med en pol. Polen er simpel, med residuum 1, så $A_0(\psi) = \psi(0)$.

(11.8) Formler. *For frembringerfunktionerne $\alpha_\psi(z)$ og $\beta_\psi(z)$ gælder ligningerne:*

$$\alpha_{\psi_-}(z) = -\alpha_\psi(-z), \quad \beta_{\psi_-}(z) = -\beta_\psi(-z) + \psi(0), \tag{11.8.1}$$

og for koefficienterne:

$$A_k(\psi_-) = (-1)^k A_k(\psi), \qquad B_k(\psi_-) = (-1)^k B_k(\psi) \text{ for } k \neq 1, \tag{11.8.2}$$

og $B_1(\psi_-) = -B_1(\psi) + \psi(0)$.

Videre er

$$\alpha_\psi(z) = \tfrac{-i}{N}\hat{\psi}(0) + \tfrac{2i}{N}\beta_{\hat{\psi}_-}\Bigl(\tfrac{2iz}{N}\Bigr), \qquad \tfrac{1}{2i}\alpha_{\hat{\psi}}\Bigl(\tfrac{Nz}{2i}\Bigr) + \tfrac{1}{2}\psi(0) = \beta_\psi(z). \tag{11.8.3}$$

Specielt gælder for koefficienterne,

$$A_k(\psi) = \bigl(\tfrac{2i}{N}\bigr)^k B_k(\hat{\psi}_-) \text{ for } k \neq 1, \quad \text{og } A_1(\psi) = \tfrac{-i}{N}\hat{\psi}(0) + \tfrac{2i}{N}B_1(\hat{\psi}_-). \tag{11.8.4}$$

Bevis. De første to ligninger mellem frembringerfunktionerne følger let af definitionerne. Den tredie ligning mellem frembringerfunktioner fås efter division med N af (11.7.5) med $z := 2z/N$ og $\psi := \psi_-$. Den sidste ligning følger nu ved at erstatte ψ med $\hat{\psi}$ og udnytte omvendingsformlen (11.1.1). $\square$

(11.9) Hovedresultat (specielle værdier). *For hele tal k gælder ligningerne:*

$$L_\psi(1-k) = -\frac{B_k(\psi)}{k} \text{ for } k \geqslant 1, \qquad L_\psi^\pm(k) = -\Big(\frac{2\pi i}{N}\Big)^k \frac{B_k(\hat\psi_-)}{k!} \text{ for } k \geqslant 0, \quad (11.9.1)$$

og $L_\psi^\pm(k) = 0$ for $k < 0$. Alternativt, for $k \geqslant 0$,

$$L_\psi^\pm(k) = -\pi^k \frac{A_k(\psi)}{k!} \quad \text{for } k \neq 1, \qquad L_\psi^\pm(1) = -\pi A_1(\psi) - \tfrac{i\pi}{N}\hat\psi(0).$$

Bevis. Den første ligning i (11.4.1), $L_\psi(1-s) = \Gamma(s)I_\psi(1-s)$ giver ingen information når $s = k \leqslant 0$, idet $\Gamma(s)$ har poler for disse værdier af s. For $k \geqslant 1$ er $\Gamma(k) = (k-1)!$ og værdien af $I_\psi(1-k)$ fremgår af (11.7.3). Heraf fremgår den første ligning i (11.9.1).

Den anden ligning i (11.4.1) giver tilsvarende den anden ligning i (11.9.1). De alternative udtryk følger af formel (11.8.4). □

(11.10) Bestemmelse af Bernoulli-tal. Ligningen $\beta_\psi(z)(e^{Nz}-1) = f_\psi(z)$ bestemmer Bernoulli-tallene rekursivt: Højresiden er $f_\psi(x) = \sum \psi(a)e^{az} = \sum_{n\geqslant 0} S_n(\psi)z^n/n!$, hvor (for fast N) $S_n(\psi) = \sum \psi(a)a^n$, for $n = 0, 1, \dots$. Venstresiden er produktet af $z\beta_\psi(z)$ og $(e^{Nz}-1)/z = N\sum_{l\geqslant 0} N^l/(l+1)z^l/l!$. Altså fås ligningerne,

$$S_n(\psi) = N\sum_{l=0}^{n}\binom{n}{l}B_{n-l}(\psi)N^l/(l+1) = \frac{N}{n+1}\sum_{k=0}^{n}\binom{n+1}{k}B_k(\psi)N^{n-k}.$$

Fx er $S_0(\psi) = NB_0(\psi)$ og $S_1 = \frac12 B_0(\psi)N^2 + B_1(\psi)N$, dvs

$$B_0(\psi) = \frac1N\sum\psi(a), \quad B_1(\psi) = \frac1N\sum\psi(a)a - \frac12\sum\psi(a).$$

De oprindelige *Bernoulli-tal* B_k, *Euler-tallene* E_k og Euler's *zigzag-tal* (*up/down-tal*) A_k er bestemt ved frembringerfunktionerne,

$$\beta(z) = \frac{1}{e^z-1} = \frac1z\sum_{k\geqslant 0}\frac{B_k}{k!}z^k, \qquad \epsilon(z) = \frac{2e^z}{e^{2z}+1} = \sum_{k\geqslant 0}\frac{E_k}{k!}z^k.$$
$$\alpha(z) = \frac{1+\sin z}{\cos z} = \sum_{k\geqslant 0}\frac{A_k}{k!}z^k.$$

Øjensynlig er $\beta(z)+\frac12 = \frac12(e^z+1)/(e^z-1)$ en ulige funktion af z, så $z\beta(z)+\frac z2$ er en lige funktion. Heraf ses, at $B_1 = -\frac12$ og at de øvrige „ulige“ Bernoullli-tal B_{2k+1} alle er 0. Yderligere ses, at $\beta(iz)+\frac12 = \frac{1}{2i}\cot\frac z2$, hvoraf $(2iz)\beta(2iz)+(2iz)/2 = z\cot z$. Indsættelse af $2iz$ i $z\beta(z)+\frac z2$ giver altså $z\cot z$, hvoraf rækkeudviklingen,

$$z\cot z = \sum_{k\geqslant 0 \text{ lige}}(-1)^{k/2}2^kB_k\frac{z^k}{k!}. \qquad (11.10.1)$$

Tilsvarende ses, at $\epsilon(z)$ er en lige funktion, så de ulige Euler-tal E_{2k+1} er alle 0. Yderligere er $\epsilon(iz) = 1/\cos z$, så vi får rækkeudviklingen,

$$\frac{1}{\cos z} = \sum_{k \geqslant 0 \text{ lige}} (-1)^{k/2} E_k \frac{z^k}{k!}. \tag{11.10.2}$$

Som bekendt (se nedenfor) er $\tan z = \cot z - 2\cot 2z$. Af (11.10.1) får vi derfor rækkeudviklingen,

$$z \tan z = \sum_{k \geqslant 2 \text{ lige}} (-1)^{k/2-1} 2^k (2^k - 1) B_k \frac{z^k}{k!}, \tag{11.10.3}$$

Bernoulli- og Euler-tal kan udtrykkes ved zigzag-tallene: Af $\alpha(z) = 1/\cos z + \tan z$, hvor de to led er hhv lige og ulige funktioner, følger, at de lige koefficienter A_{2l} er bestemt ved fremstillingen (11.10.2) af $1/\cos z$, dvs ved Euler-tallene, og de ulige koefficienter A_{2l+1} er bestemt ved fremstillingen (11.10.3) af $\tan z$, dvs ved Bernoulli-tallene. Mere præcist fås ligningerne:

$$\frac{1}{\cos z} = \sum_{k \geqslant 0 \text{ lige}} A_k \frac{z^k}{k!}, \qquad \tan z = \sum_{k \geqslant 1 \text{ ulige}} A_k \frac{z^k}{k!},$$

$$A_k = (-1)^{k/2} E_k, \quad k \text{ lige}, \qquad A_k = (-1)^{(k-1)/2} 2^{k+1} (2^{k+1} - 1) \frac{B_{k+1}}{k+1}, \quad k \text{ ulige},$$

$$E_k = (-1)^{k/2} A_k, \quad k \text{ lige}, \qquad B_k = \frac{(-1)^{k/2-1} k}{2^k (2^k - 1)} A_{k-1}, \quad k \geqslant 2 \text{ lige}.$$

(11.11). Til $\psi \equiv 1$ ($N = 1$), svarer frembringerfunktionerne $\beta_1 = e^z/(e^z - 1)$ og $\alpha_1 = \cot z$. Bemærk, at β_1 ikke har samme konstantled som β: Vi har $\beta_1(z) = 1 + \beta(z)$. Heraf ses, at $B_k(1) = B_k$ for $k \neq 1$ og $B_1(1) = 1 + B_1 = \frac{1}{2}$.

Videre er $z\alpha_1(z) = z \cot z$ en lige funktion. Med ulige index har vi altså $A_{2l+1}(1) = 0$, og $A_{2l}(1)$ bestemmes af (11.10.1): Vi har $A_k(1) = (-1)^{k/2} 2^k B_k$ når $k \geqslant 0$ er lige.

I en del af de følgende bestemmelser er det bekvemt at udnytte, at frembringerfunktionerne er logarimisk afledede af pæne funktioner. Lad $\nabla f(z)$ betegne den *logaritmisk afledede* af $f(z)$, altså

$$\nabla f(z) = \tfrac{d}{dz} \log f(z) = f'(z)/f(z).$$

Fx er

$$\cot z = \nabla \sin z, \quad -\tan z = \nabla \cos z, \quad -\alpha(z) = \nabla(1 - \sin z);$$

den sidste formel følger af at $\alpha(z) = (1 + \sin z)/\cos z = \cos z/(1 - \sin z)$. Af ligningen $\sin 2z = 2 \sin z \cos z$ fås ved logaritmisk afledning, at $2\cot 2z = \cot z - \tan z$, og dermed er $\tan z = \cot z - 2\cot 2z$, som blev udnyttet ovenfor.

(11.12) Eksempel. Lad $\psi_{a/N}$ være den karakteristiske funktion for $a \pmod N$; værdien $\psi_{a/N}(n)$ er altså 1 hvis $n \equiv a \pmod N$, og 0 ellers. Fx finder vi, for $N = 2$, at $\alpha_{1/2} = \frac{1}{2}\cot(z/2 - \pi/2) = -\frac{1}{2}\tan z/2$. Af ligningerne i (11.10) følger så, at

$$z\alpha_{1/2}(z) = -\sum_{k\geqslant 2 \text{ lige}} \frac{kA_{k-1}}{2^k}\frac{z^k}{k!}, \quad \text{dvs } A_k(\psi_{1/2}) = \frac{-kA_{k-1}}{2^k}, \ k \geqslant 2 \text{ lige}, \tag{11.12.1}$$

og $A_k(\psi_{1/2}) = 0$ ellers. For $\psi_{2/2}$ får vi tilsvarende $\alpha_{2/2} = \frac{1}{2}\cot z/2$, altså ifølge (11.10),

$$z\alpha_{2/2}(z) = 1 + \sum_{k\geqslant 2 \text{ lige}} \frac{-kA_{k-1}}{2^k(2^k-1)}\frac{z^k}{k!}, \ \text{dvs } A_k(\psi_{2/2}) = \frac{-kA_{k-1}}{2^k(2^k-1)}, \ k \geqslant 2 \text{ lige}, \tag{11.12.2}$$

samt $A_0(\psi_{2/2}) = 1$ og $A_k(\psi_{2/2}) = 0$ alle andre $k \in \mathbb{Z}$.

For $N = 4$ finder vi $\alpha_{1/4}(z) = \frac{1}{4}\cot(z-\pi)/4$. Af ligningen $\cos 2v = 2\sin^2 v - 1$ fås $2\sin^2(z-\pi)/4 = 1 - \sin z/2$, som giver $2\frac{1}{4}\cot(z-\pi)/4 = -\frac{1}{2}\alpha(z/2)$, hvoraf

$$\alpha_{1/4}(z) = -\tfrac{1}{4}\alpha(z/2), \ \text{altså } A_k(\psi_{1/4}) = -\frac{kA_{k-1}}{2^{k+1}} \quad \text{for alle } k \geqslant 1,$$

og $A_k(\psi_{1/4}) = 0$ for $k \leqslant 0$.

Bemærk, at $\hat{\psi}_{1/4} = \psi_{3/4}$. Værdierne $A_k(\psi_{3/4})$ fås derfor af værdierne ovenfor ved hjælp af (11.8.3). Videre er $\alpha_{2/4}(z) = \frac{1}{4}\cot(z-2\pi)/4 = -\frac{1}{4}\tan z/4$, som bestemmes af (11.10.3), og $\alpha_{0/4} = \frac{1}{4}\cot z/4$ som bestemmes (11.10.4). Funktionerne $z\alpha_{2/4}(z)$ og $z\alpha_{0/4}(z)$ er øjensynlig lige, så $A_k(\psi_{2/4}) = A_k(\psi_{0/4}) = 0$, når k er ulige. Videre er $A_0(\psi_{0/4}) = 1$, og $A_0(\psi_{2/4}) = 0$. I alt fås følgende værdier:

$$\begin{aligned} &A_k(\psi_{2/4}) = -\frac{kA_{k-1}}{4^k}, \quad A_k(\psi_{0/4}) = \frac{-kA_{k-1}}{4^k(2^k-1)}, \ \text{for } k \text{ lige} \\ &A_k(\psi_{1/4}) = -\frac{kA_{k-1}}{2^{k+1}}, \quad A_k(\psi_{3/4}) = (-1)^{k-1}\frac{kA_{k-1}}{2^{k+1}}, \ \text{for alle } k. \end{aligned} \tag{11.12.3}$$

For at bestemme Bernoulli-tallene $B_k(\psi_{1/4})$ udnyttes omformningen,

$$\frac{4e^z}{e^{4z}-1} + \frac{2e^z}{e^{2z}+1} = \frac{2e^z}{e^{2z}-1} = \frac{2}{e^z-1} - \frac{2}{e^{2z}-1},$$

altså $4\beta_{1/4}(z) + \epsilon(z) = 2\beta(z) - 2\beta(2z)$. Da $\beta(z) - \beta(2z)$ er ulige, får vi, for $k \geqslant 0$,

$$B_k(\psi_{1/4}) = \begin{cases} \frac{1}{2}(1-2^{k-1})B_k & k \text{ lige}, \\ -\frac{1}{4}kE_{k-1}, & k \text{ ulige}. \end{cases} \tag{11.12.4}$$

Specielt er $B_0(\psi_{1/4}) = \frac{1}{4}$, og udtrykt ved up/down-tallene A_k fås, fra (11.10.3) og (11.10.2)

$$B_k(\psi_{1/4}) = \begin{cases} \frac{(-1)^{k/2}(1-2^{k-1})}{2^{k+1}(1-2^k)} kA_{k-1} & k \geqslant 2 \text{ lige,} \\ -\frac{1}{4}(-1)^{(k-1)/2} kA_{k-1}, & k \geqslant 1 \text{ ulige.} \end{cases} \tag{11.12.5}$$

Vi kan også bestemme $\beta_{1/4}(z)$ ud fra (11.8.). Øjensynlig er $\hat{\psi}_{1/4}(n) = i^n$, altså $\hat{\psi}_{1/4} = i\psi_{1/4} - \psi_{2/4} - i\psi_{3/4} + \psi_{0/4}$, hvoraf

$$B_k(\psi_{1/4}) = \frac{1}{4}\Big(\frac{-i4}{2}\Big)^k \Big(iA_k(\psi_{1/4}) - A_k(\psi_{2/4}) - iA_k(\psi_{3/4}) + A_k(\psi_{4/4})\Big),$$

som (forhåbentlig?) stemmer med (11.12.5) og (11.12.3).

(11.13) Eksempel. Med $N = 1$ og $\psi = \psi_{1/1}$ er $L_{1/1}(s) = \zeta(s)$ og $L^{\pm}_{1/1}(s) = (1+e^{i\pi s})\zeta(s)$. Når $k \geqslant 0$ er lige er $B_k\psi_{1/1}) = B_k$, for $k = 1$ er $B_1(\psi_{1/1}) = -B_1 = \frac{1}{2}$, og for andre k er $B_k(\psi_{1/1}) = 0$. Den første ligning i (11.9.1) giver så $\zeta(0) = -\frac{1}{2}$ og for $k \geqslant 2$ de velkendte formler,

$$\zeta(1-k) = \begin{cases} -B_k/k & k \geqslant 2 \text{ lige,} \\ 0 & k \geqslant 3 \text{ ulige.} \end{cases} \tag{11.13.1}$$

Nulpunkterne $\zeta(m) = 0$ for m lige og negativ er de *trivielle nulpunkter* for $\zeta(s)$. Betragt den anden ligning i (11.9.1) for $L^{\pm}_{1/1}(k) = (1 + e^{i\pi k})\zeta(k)$. For ulige k er faktoren $1 + e^{i\pi k}$ lig med nul. For $k = 1$ har vi $L^{\pm}_{1/1}(1) = -i\pi$ hvilket modsvarer, at i $s = 1$ har $\zeta(s)$ en pol og $1 + e^{i\pi s}$ et nulpunkt: $\zeta(1 + s) = s^{-1} + \cdots$ og $1 + e^{i\pi(s+1)} = 1 - e^{i\pi s} = -i\pi s + \cdots$. For de øvrige ulige værdier af k fås $L^{\pm}_{1/1}(k) = 0$, som ikke giver information om $\zeta(k)$. Antag k er lige, og altså $1 + e^{i\pi k} = 2$. For $k < 0$ genfinder vi de trivelle nulpunkter for $\zeta(s)$, og for $k \geqslant 0$ får vi de klassiske værdier $\zeta(k) = -\frac{1}{2}(-1)^{k/2}(2\pi)^k B_k/k!$ (k lige). Specielt genfindes værdien $\zeta(0) = -\frac{1}{2}$. For positive k kan værdien skrives:

$$\zeta(k) = \frac{(-1)^{k/2-1}(2\pi)^k B_k}{2k!} = \frac{\pi^k A_{k-1}}{2(2^k-1)(k-1)!}, \quad k \geqslant 2 \text{ lige.} \tag{11.13.2}$$

(11.14) Eksempel. Med $N = 4$ og lad $\psi = \psi_{1/4}$ fås, når $\Re s > 1$,

$$L_{1/4}(s) = \sum_{n\geqslant 1, n\equiv 1 \pmod 4} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{5^s} + \frac{1}{9^s} + \cdots$$

og med konventionen $(-n)^s = e^{-i\pi s}n^s$ er

$$L^{\pm}_{1/4}(s) = \sum_{m\equiv 1 \pmod 4} \frac{1}{m^s} = \frac{1}{1^s} + \frac{1}{(-3)^s} + \frac{1}{5^s} + \frac{1}{(-7)^s} + \cdots$$

hvor summationen i den sidste sum er over *hele* tal m.

Af (11.9) og udregningerne i (11.12) fås, når $k \geqslant 1$ er hel, at $L_{1/4}(1-k) = -B_k(\psi_{1/4})/k$; specielt er $L_{1/4}(0) = -\frac{1}{4}$. Videre har vi $L^{\pm}_{1/4}(k) = 0$ for $k < 0$, og for $k \geqslant 2$,

$$L^{\pm}_{1/4}(k) = \frac{1}{1^k} + \frac{(-1)^k}{3^k} + \frac{1}{5^k} + \frac{(-1)^k}{7^k} + \frac{1}{9^k} + \cdots = \frac{\pi^k A_{k-1}}{2^{k+1}(k-1)!},$$

der normalt skrives som to ligninger,

$$\frac{1}{1^k} + \frac{1}{3^k} + \frac{1}{5^k} + \frac{1}{7^k} + \cdots = \frac{\pi^k A_{k-1}}{2^{k+1}(k-1)!}, \text{ hvis } k \geqslant 2 \text{ er lige,} \tag{11.14.1}$$

$$\frac{1}{1^k} - \frac{1}{3^k} + \frac{1}{5^k} - \frac{1}{7^k} + \cdots = \frac{\pi^k A_{k-1}}{2^{k+1}(k-1)!}, \text{ hvis } k > 2 \text{ er ulige.} \tag{11.14.2}$$

Af den første ligning, for $k \geqslant 2$ lige, genfindes resultatet om $\zeta(k)$ fra (11.13): For $\Re s > 1$ er

$$\zeta(s) = \sum_{n \geqslant 1 \text{ lige}} \frac{1}{n^s} + \sum_{n \geqslant 1 \text{ ulige}} \frac{1}{n^s} = 2^{-s}\zeta(s) + \sum_{n \geqslant 1 \text{ ulige}} \frac{1}{n^s},$$

og dermed $(1-2^{-s})\zeta(s) = \sum_{n \text{ ulige}} n^{-s} = L_{1/2}(s)$ for alle s. Når $s = k \geqslant 2$ er hel og lige, er $L_{1/2}(k) = L^{\pm}_{1/4}(k)$, og altså $\zeta(k) = (1-2^{-k})^{-1} L^{\pm}_{1/4}(k)$. Altså er (11.13.2) også en konsekvens af (11.14.1).

(11.15) Dirichlet-karakterer. Betragt en *kompleks Dirichlet-karakter modulo* N, altså en gruppehomomorfi $\chi\colon (\mathbb{Z}/N)^* \to \mathbb{C}^*$. Når N er fast, kan vi opfatte χ som en periodisk afbildning $\chi\colon \mathbb{Z}/N \to \mathbb{C}$, idet værdien $\chi(a)$ sættes til 0, når a ikke er primisk med N.

Øjensynlig gælder $\chi_-(n) = \chi(-n) = \chi(-1)\chi(n)$, og $\chi(-1) = \pm 1$. Heraf ses, at enten er χ *lige*, nemlig når $\chi(-1) = 1$, eller også er χ *ulige*, nemlig når $\chi(-1) = -1$.

For en Dirichlet-karakter χ, som funktion med periode N, fås for den transformerede:

$$\hat{\chi}(n) = \sum \chi(a)\zeta^{an} = \tau(\chi, \zeta^n),$$

hvor $\tau(\chi, \zeta^n)$ er Gauss-summen svarende til den N'te enhedsrod ζ^n. Betragt specielt Gauss-summen $\tau(\chi) = \tau(\chi, \zeta)$ svarende til $\zeta = e^{2\pi i/N}$. Hvis n er primisk med N, så er

$$\chi(n)\hat{\chi}(n) = \sum_a \chi(an)\zeta^{an} = \tau(\chi),$$

hvoraf ved multiplikation med $\overline{\chi}(n)$,

$$\hat{\chi}(n) = \tau(\chi)\overline{\chi}(n), \text{ når } (n, N) = 1; \tag{11.15.1}$$

værdien $\overline{\chi}(n) = \chi^*(n) = \chi(n)^{-1}$ er værdien af den *konjugerede karakter*.

Antag, at χ er en primitiv karakter. Så følger det, som tidligere nævnt, at når n ikke er primisk med N. så er Gauss-summen $\hat{\chi}(n) = \tau(\chi, \zeta^n)$ lig med 0, altså $\hat{\chi}(n) = 0$. Også højresiden i (11.15.1) er 0, idet værdien $\overline{\chi}(n)$ jo er 0, når n ikke er primisk med N. Med andre ord:

Sætning. *Hvis χ er en primitiv karakter modulo N, så er $\hat{\chi}(n) = \tau(\chi)\overline{\chi}(n)$ for alle n.*

For L-rækken hørende til en primitiv Dirichlet-karakter får funktionalligningerne derfor følgende form: Når χ er henholdvis lige, dvs $\chi(-1) = 1$, og ulige, dvs $\chi(-1) = -1$, gælder

$$\Big(\frac{N}{\pi}\Big)^{\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)L_\chi(s) = \frac{\tau(\chi)}{\sqrt{N}}\Big(\frac{N}{\pi}\Big)^{\frac{1-s}{2}}\Gamma\Big(\frac{1-s}{2}\Big)L_{\overline{\chi}}(1-s). \tag{11.15.2$^+$}$$

$$\Big(\frac{N}{\pi}\Big)^{\frac{s}{2}}\Gamma\Big(\frac{s+1}{2}\Big)L_\chi(s) = \frac{\tau(\chi)}{i\sqrt{N}}\Big(\frac{N}{\pi}\Big)^{\frac{1-s}{2}}\Gamma\Big(\frac{1-s+1}{2}\Big)L_{\overline{\chi}}(1-s). \tag{11.15.2$^-$}$$

(11.16) Opgaver.

1. For fast N (og $\zeta = e^{2\pi i/N}$) betegnes med $\psi_{a/N}$ den karakteristiske funktion for a, dvs værdien $\psi_{a/N}(n)$ er 1, når $n \equiv a \pmod N$, og 0 ellers. Videre sættes $\varepsilon_a(n) = \zeta^{an}$. Vis, at $\widehat{\psi_{a/N}} = \varepsilon_a$ og $\widehat{\varepsilon_a} = N\psi_{-a/N} = N(\psi_{a/N})_-$. Slut heraf omvendingsformlen: $\hat{\hat{\psi}} = N\psi_-$.

2. En funktion $\psi\colon \mathbb{Z} \to \mathbb{C}$ med periode N har naturligvis også periode dN for $d \geqslant 1$. Vis, at $\beta_\psi(z)$ er uafhængig af valget af periode, dvs ikke afhænger af d.

3. Benyt formlen $X^d - 1 = \prod_{a=0}^{d-1}(X - e^{2\pi ai/d})$ til at vise multiplikationsformlen for sinus, altså $\sin dz = (-2)^{d-1}\prod_{a=0}^{d-1}\sin(z - \frac{a\pi}{d})$. Udled heraf formlen for $\cot dz$, og slut, at $\alpha_\psi(z)$ er uafhængig af valget af periode N for ψ.

4. Vis, hvordan fordoblingsformlen $\Gamma(s/2)\Gamma((s+1)/2) = 2^{1-s}\sqrt{\pi}\Gamma(s)$ og spejlingsformlen $\Gamma(s)\Gamma(1-s) = \pi/\sin\pi s$ giver omforningen af funktionalligningen, når ψ er lige eller ulige.

5. Vis, at zigzag-tallene A_k er positive hele tal. [Vink: Brug, at $\alpha = \sigma + \tau$, hvor $\sigma(z) = 1/\cos z$ og $\tau(z) = \tan z$ opfylder $\sigma' = \sigma\tau$ og $\tau' = \sigma^2$, til at vurdere $\alpha^{(k)}(0)$.]

6. Vis, at $\alpha(z) = \alpha'(z)\cos z$, og brug potensrækkeudviklinger for $\alpha(z)$ og $\cos z$ til at udlede rekursionsformlen (hvor $A_0 = 1$):

$$A_{k+1} = A_k + \binom{k}{2}A_{k-1} - \binom{k}{4}A_{k-3} + \binom{k}{6}A_{k-5} \pm \cdots .$$

Check følgende tabel:

k	0	1	2	3	4	5	6	7	8	9	10	11
A_k	1	1	1	2	5	2^4	61	$2^4 \cdot 17$	1385	$2^8 \cdot 31$	50521	$2^9 \cdot 691$

A. Appendix: Løse ender.

(A.1). I dette appendix giver vi et bevis for Bertrand's Postulat, nævnt i Kapitel 1. Som nævnt følger Postulatet af en tilstrækkelig nøjagtig vurdering af primtalsfunktionen $\pi(x)$. I forbindelse med primtallenes fordeling er der en række andre funktioner, der spiller en vigtig rolle, bl.a. følgende:

$$\vartheta(x) = \sum_{p \leqslant x} \log p \qquad \text{og} \qquad \psi(x) = \sum_{p^m \leqslant x} \log p.$$

Den første sum er over alle primtal $p \leqslant x$, den anden over alle primtalspotenser $p^m \leqslant x$. I den første sum er antallet af led lig med $\pi(x)$, og hvert led er højst lig med $\log x$. Altså er $\vartheta(x) \leqslant \pi(x) \log x$. Vurderinger af $\pi(x)$ medfører altså vurderinger af $\vartheta(x)$, og omvendt. Det er ikke så dybtliggende at vise, at

$$\pi(x) \log x \sim \vartheta(x) \sim \psi(x).$$

Primtalssætningen er altså ækvivalent med enhver af relationerne $\vartheta(x) \sim x$ og $\psi(x) \sim x$. Af vurderingen i Kapitel 1 følger, at $\vartheta(n) \leqslant 3n$ for alle $n \geqslant 1$. Den efterfølgende vurdering er lidt bedre; vi vil bruge den i beviset for Bertrand's Postulat.

(A.2) Sætning. *For alle $n \geqslant 1$ er $\vartheta(n) \leqslant (2 \log 2)n$.*

Bevis. Beviset, ganske parallelt til beviset for (1.5), forløber ved fuldstændig induktion efter n. Uligheden er trivielt opfyldt for $n = 1$.

Lad der nu være givet en værdi $n > 1$, og antag, at uligheden gælder for alle mindre værdier. Sæt $k := \lfloor (n+1)/2 \rfloor$. Specielt er så $n/2 \leqslant k \leqslant (n+1)/2$. Betragt binomialkoefficienten,

$$b := \binom{n}{n-k} = \frac{n(n-1)\cdots(k+1)}{(n-k)(n-k-1)\cdot\cdots\cdot 2\cdot 1}.$$

Da $k + 1 > n - k$, er faktorerne i tælleren er større end faktorerne i nævneren. Specielt kan primtallene blandt faktorerne i tælleren ikke forkortes med faktorer fra nævneren. Derfor er b delelig med produktet af disse primtal, og følgelig er $\log b$ mindst lig med logaritmen til produktet, dvs mindst lig med $\sum \log p$, hvor summen er over primtallene p med $k < p \leqslant n$. Den sidste sum er øjensynlig lig med $\vartheta(n) - \vartheta(k)$. Altså er

$$\vartheta(n) - \vartheta(k) \leqslant \log b.$$

Videre er b, som en binomialkoefficienterne $\binom{n}{l}$ for $n \geqslant 1$, højst lig med 2^{n-1}. Under brug af induktionsforudsætningen får vi derfor, at

$$\begin{aligned}\vartheta(n) = \vartheta(n) - \vartheta(k) + \vartheta(k) &\leqslant \log 2^{n-1} + (2\log 2)k \\ &\leqslant (n-1)\log 2 + (2\log 2)(n+1)/2 = (2\log 2)n,\end{aligned}$$

som ønsket. $\square$

(A.3) Bertand's Postulat. *For ethvert $n \geqslant 1$ findes et primtal p med $n < p \leqslant 2n$.*

Bevis. Uligheden $p \leqslant 2n$ må naturligvis være skarp, med mindre $n = 1$ og $p = 2$.

Af postulatet fremgår specielt, at hvis p_k er det k'te primtal, så er $p_{k+1} < 2p_k$. Den sidste påstand er faktisk ækvivalent med Bertrand's postulat. Mere generelt er det let at se, at hvis $q_1, q_2, q_3, \dots$ er en voksende følge af primtal, der opfylder ulighederne $q_{k+1} < 2q_k$ for $k = 1, \dots, l-1$, så gælder Bertrand's Postulat for alle n med $q_1/2 \leqslant n < q_l$. Øjensynlig er uligheden $q_{k+1} < 2q_k$ opfyldt for det k'te primtal i følgen,

$$3, 5, 7, 13, 23, 43, 83, 163, 317, 631.$$

Derfor gælder Bertrand's postulat for alle $n < 631$.

Nu vises påstanden med et indirekte bevis. Antag, at der for et naturligt tal n ikke findes primtal p med $n < p \leqslant 2n$. Specielt er så $n \geqslant 631$. Betragt binomialkoefficienten,

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

Lad p være en primdivisor i b, og lad p^{ν_p} være den potens, der indgår i primopløsningen af b. Af antagelsen følger, at ingen af faktorerne i tælleren er primtal. Derfor er $p \leqslant n$. Yderligere er $p \leqslant \frac{2}{3}n$. Et primtal q med $\frac{2}{3}n < q \leqslant n$ forekommer nemlig én gang blandt faktorerne i nævneren, og i tælleren går q kun op i faktoren $2q$. De to forekomster af q forkortes mod hinanden; derfor er b ikke delelig med q.

Altså er $p \leqslant \frac{2}{3}n$ for enhver primfaktor p i b. Af (A.2) følger derfor:

$$\sum_{p \mid b} \log p \leqslant \sum_{p \leqslant \frac{2}{3}n} \log p = \vartheta(\tfrac{2}{3}n) \leqslant (\tfrac{4}{3}\log 2)n. \tag{A.3.1}$$

Da $p^{\nu_p} \mid b$, følger det af (1.6), at $p^{\nu_p} \leqslant 2n$. Hvis $\nu_p \geqslant 2$, så er $p^2 \leqslant 2n$, og derfor er $p \leqslant \sqrt{2n}$; specielt er der højst $\sqrt{2n}$ primdivisorer p i b med $\nu_p \geqslant 2$, og for hver af dem er $\nu_p \log p \leqslant \log(2n)$. Derfor får vi vurderingen,

$$\sum_{p \mid b,\ \nu_p \geqslant 2} \nu_p \log p < \sqrt{2n}\log(2n).$$

Af denne vurdering og (A.3.1) fås:

$$\log b = \sum_{p \mid b,\ \nu_p = 1} \log p + \sum_{p \mid b,\ \nu_p \geqslant 2} \nu_p \log p < (\tfrac{4}{3}\log 2)n + \sqrt{2n}\log(2n). \tag{A.3.2}$$

På den anden side giver binomialformlen:

$$2^{2n} = 2 + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{2n-1},$$

hvor de to yderste binomialkoefficienter er slået sammen til $1 + 1 = 2$. Der er $2n$ led på højesiden, og b er det største. Derfor er $2^{2n} \leqslant (2n)b$, og altså

$$(2 \log 2)n \leqslant \log(2n) + \log b. \tag{A.3.3}$$

Af (A.3.2) og (A.3.3) følger:

$$(2 \log 2)n - \log(2n) \leqslant \log b < (\tfrac{4}{3} \log 2)n + \sqrt{2n} \log(2n). \tag{A.3.4}$$

Den opnåede ulighed kan omskrives til $(\frac{2}{3} \log 2)n \leqslant (1 + \sqrt{2n}) \log(2n)$, eller

$$\tfrac{1}{3} \log 2 \leqslant \frac{1 + \sqrt{2n}}{\sqrt{2n}} \, \frac{\log(2n)}{\sqrt{2n}} . \tag{A.3.5}$$

De to brøker på højresiden er aftagende som funktioner af n (den sidste for $2n \geqslant e^2$). Værdien på højresiden, for $n \geqslant 631$, er derfor mindre end værdien for $n = 512 = 2^9$. Altså er

$$\tfrac{1}{3} \log 2 < \frac{1 + 2^5}{2^5} \, \frac{10 \log 2}{2^5} = \tfrac{330}{1024} \log 2.$$

Men den ulighed er øjensynlig gal. Hermed er den søgte modstrid opnået, hvormed Bertrand's Postulat er bevist. $\square$

(A.4) Sætning. *For alle naturlige tal* $n \geqslant 7$ *er* $(\log 2)n \leqslant \psi(n)$. *Ækvivalent, hvis* $\mathrm{LCM}(n)$ *betegner det mindste fælles multiplum af alle tallene* $1, 2, \dots, n$, *så er*

$$2^n \leqslant \mathrm{LCM}(n) \quad \textit{for}\ n \geqslant 7. \tag{A.4.1}$$

Bevis. (Efter [Nair].) Det mindste fælles multiplum $\mathrm{LCM}(n)$ er øjensynlig lig med produktet af primtalspotenserne $p^k \leqslant n$ med, for hvert primtal p, den størst mulige eksponent k. Alternativt er $\mathrm{LCM}(n)$ lig med produktet af primfaktorer p, hvor hver faktor p medtages én gang for hver potens p^m med $p^m \leqslant n$. Med den alternative beskrivelse er det klart, at $\log \mathrm{LCM}(n) = \psi(n)$. Derfor er de to anførte uligheder ækvivalente.

Beviset for den sidste ulighed tager udgangspunkt i følgende formel, for $1 \leqslant k \leqslant n$:

$$\sum_{r=0}^{n-k} (-1)^r \binom{n-k}{r} \frac{1}{r+k} = \frac{1}{k\binom{n}{k}} .$$

For at vise formlen bemærkes, at begge formlens sider er lig med det bestemte integral $I := \int_0^1 x^{k-1}(1-x)^{n-k} dx$: At integralet er lig med venstresiden fås ved at anvende binomialformlen på faktoren $(1-x)^{n-k}$ og så integrere de fremkomne potenser x^i. At integralet er lig med højresiden ses ved gentagne partielle integrationer: integrer potensen x^i og differentier potensen $(1-x)^j$.

For at vise den anførte ulighed bemærkes, at alle nævnerne $r+k$ på venstresiden er mindre end eller lig med n. Derfor er alle nævnerne $r+k$ divisorer i $\mathrm{LCM}(n)$. Multipliceres med $\mathrm{LCM}(n)$, fås altså et helt tal ud fra venstresiden, og derfor også ud fra højresiden. Det sidste betyder, at nævneren på højresiden er divisor i $\mathrm{LCM}(n)$, altså

$$k\binom{n}{k} \,\Big|\, \mathrm{LCM}(n). \tag{A.4.2}$$

Relationen (A.4.2) medfører følgende to relationer, for $k \geqslant 1$:

$$k\binom{2k}{k} \,\Big|\, \mathrm{LCM}(2k+1) \quad \text{og} \quad (2k+1)\binom{2k}{k} \,\Big|\, \mathrm{LCM}(2k+1). \tag{A.4.3}$$

Den første relation i (A.4.3) fås nemlig ved at anvende (A.4.2) med $n := 2k$ og udnytte, at $\mathrm{LCM}(2k)\big|\mathrm{LCM}(2k+1)$. Den anden relation i (A.4.3) fås ved at anvende (A.4.2) med $n := 2k+1$ og $k := k+1$; udnyt, at $(k+1)\binom{2k+1}{k+1} = (2k+1)\binom{2k}{k}$.

I de to relationer i (A.4.3) er de to faktorer k og $2k+1$ primiske. De to relationer medfører derfor følgende:

$$k(2k+1)\binom{2k}{k} \,\Big|\, \mathrm{LCM}(2k+1). \tag{A.4.4}$$

Øjensynlig er $2^{2k} = \sum_i \binom{2k}{i}$. I summen er der $2k+1$ binomialkoefficienter $\binom{2k}{i}$ for $i = 0, \dots, 2k$, og af dem er $\binom{2k}{k}$ den største. Derfor er $2^{2k} \leqslant (2k+1)\binom{2k}{k}$. Relationen i (A.4.4) medfører derfor uligheden,

$$k2^{2k} \leqslant \mathrm{LCM}(2k+1). \tag{A.4.5}$$

Heraf ses, for $k \geqslant 2$, at $2^{2k+1} \leqslant \mathrm{LCM}(2k+1)$; uligheden (A.4.1) gælder derfor, når n er ulige og $n \geqslant 5$. Videre er $\mathrm{LCM}(2k+1) \leqslant \mathrm{LCM}(2k+2)$, så af (A.4.5) følger, for $k \geqslant 4$, at $2^{2k+2} \leqslant \mathrm{LCM}(2k+2)$; uligheden (A.4.1) gælder derfor, når n er lige og $n \geqslant 10$. I området $n \geqslant 7$ mangler altså kun uligheden for $n = 8$. Her finder vi:

$$2^8 = 2^3 \cdot 2 \cdot 2^2 \cdot 2^2 \leqslant 2^3 \cdot 3 \cdot 5 \cdot 7 = \mathrm{LCM}(8),$$

hvormed også den manglende ulighed er eftervist. □

(A.5) Opgaver.

1. Vis, at $\psi(x) = \sum_{p \leqslant x} \lfloor \log x / \log p \rfloor \log p$, og at $\psi(x) \leqslant \pi(x) \log x$.

2. Gælder uligheden $2^n \leqslant \mathrm{LCM}(n)$ for $n = 6$? Vis, at uligheden $\pi(n) \geqslant (\log 2)n/\log n$ gælder for naturlige tal $n \geqslant 4$.

3. Brug Lemma (1.6) til at vise, at enhver binomialkoefficient $\binom{n}{k}$ er divisor i $\mathrm{LCM}(n)$, og giv herved et simpelt bevis for (den svagere ulighed) $2^n \leqslant (n+1)\,\mathrm{LCM}(n)$.

4. Vis følgende skærpede form af Bertrand's postulat: For alle $n \geqslant 4$ findes et primtal p med $n < p < 2n - 2$. [Vink: Kig på beviset i (A.3). For at vise den skærpede form for „små“ værdier af n kræves en følge q_i af primtal med $q_{i+1} < 2q_i - 2$. En sådan følge er

$$5, 7, 11, 19, 31, 59, 113, 223, 443, 883.$$

Det fremgår, at den skærpede form gælder for $n < 882$. I et modeksempel må der altså gælde $n \geqslant 882$, og specielt, at $n \geqslant 2^9$.

Kig nu på de følgende argumenter i beviset for (A.3). De fleste er uændrede, men i tælleren på b kan det forekomme, at $n + 1$ er et primtal. Det medfører, at man til højresiden i (A.3.1) må lægge leddet $\log(n + 1)$. Det samme led skal herefter lægges til på højresiden i (A.3.2) og (A.3.4), og til højresiden i (A.3.5) må man lægge brøken $(\log(n + 1))/(2n)$. Også den sidste brøk er aftagende som funktion af n. Vurder den opad ved værdien i 2^9, som kan vurderes videre: $(\log(2^9 + 1))/2^{10} < (\log 2^{10})/2^{10} = (10/1024) \log 2$. Med dette ekstra bidrag fås den afsluttende ulighed $\frac{1}{3} \log 2 < \frac{340}{1024} \log 2$; og det er stadig er en modstrid.]

I. Index.