

## 1. Primtallene.

**(1.1) Setup.** Et tal  $p$  kaldes som bekendt et *primtal*, hvis  $p \geq 2$  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  $2 \leq a_1 < a_2 < \dots$ . 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.  $\square$

**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  $p_k \leq a_k$ . Øjensynlig er, for  $k \geq 2$ ,

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

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

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  $k \geq 2$ ) altid mindst 2. *Primtalstvillinger* er par  $(p_k, p_{k+1})$ , hvor afstanden er netop 2, fx  $(3, 5)$ ,  $(5, 7)$ ,  $(11, 13)$ ,  $\dots$ ,  $(347, 349)$ ,  $\dots$ . 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  $p \leq x$ . 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:

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

Uligheden  $\log_2 \log_2 n < \pi(n)$  medfører naturligvis Euklid's resultat, da  $\log_2 \log_2 n$  går mod  $\infty$  for  $n \rightarrow \infty$ . 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,*

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

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

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

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,

$$\frac{c}{\log n} \leq \frac{\pi(n)}{n} \leq \frac{C}{\log n}. \quad (1.3.2)$$

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

$$\frac{1}{3} \leq \frac{\pi(n)}{n} \leq \frac{3}{\log n}. \quad (1.3.3)$$

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  $n \geq n_0$ . Primtalssætningen blev først bevist i 1896 af Hadamard [1865–1963] og (uafhængigt) af de la Vallée Poussin [1866–1962].

27. oktober 2008

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

$$\pi(n) - n/\log n = \varepsilon(n)(n/\log n), \quad (1.3.4)$$

og Primtalssætningen er ækvivalent med, at  $\varepsilon(n) \rightarrow 0$  for  $n \rightarrow \infty$ . 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  $\infty$  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  $p \leq n$  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  $n \rightarrow \infty$ , 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  $n \geq 1$  og  $n/2 \leq k \leq n$  er  $\binom{n}{k} \geq k^{\pi(n)-\pi(k)}$ .

*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 større end  $k$ . Da  $k \geq n - k$ , kan ingen af disse primtal gå op i nævneren. Binomialkoefficienten er derfor delelig med produktet af disse primtal. Heraf følger påstanden.  $\square$

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

*Bevis.* Uligheden vises let for  $n \leq 3$ , 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  $n/2 \leq k \leq (n+1)/2$ . Af (1.4) og induktionsantagelsen (og de trivielle vurderinger  $\pi(n) \leq n-2$  og  $\binom{n}{k} \leq 2^n$ ) får vi derfor, at

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

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

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

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

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

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

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

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

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

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

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 fra regnet tallet 2, tallene delelige med 3 fra regnet tallet 3 og tallene delelige med 6, samt tallet 25, hvis  $n \geq 25$ . Idet vi antager, at  $n \geq 25$ , er antallet af ikke-primtal altså mindst:

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

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

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

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

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

Ved indsættelse i (1.5.3) fås, at

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

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

I udregningerne er det antaget, at  $n \geq 25$ , 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*  $n \geq 1$ , mangler vi at vise de 24 uligheder for  $n = 1, \dots, 24$ . For  $n = 1, 2, 3$  er det helt trivielt. I almindelighed, for  $n \geq 2$ , er det ækvivalent at vise, med  $\kappa(n) := (8/3)n(\log 2)/(\log n)$ , at  $\pi(n) \leq \kappa(n)$ . Betragt følgende uligheder:

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

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  $n \geq e$ ) er voksende. Derfor gælder de yderste uligheder i den første linie for  $16 \leq n \leq 30$ , i den 2. linie for  $8 \leq n \leq 15$ , og i den 3. linie for  $4 \leq n \leq 7$ . Specielt gælder de manglende uligheder for  $4 \leq n \leq 24$ .

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

*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  $p^v \mid b$ . Det skal vises, at  $p^v \leq n$ . Det er trivielt for  $v = 0$ , så vi kan antage, at  $v > 0$ . Specielt er så  $n > k \geq 1$ , 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  $p^\nu \leq n'$ , og så er  $p^\nu \leq n' < n'p \leq n$ .

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  $p^{\nu-1} \leq n'$  (hvis  $n'$  er primisk med  $p$  følger det endda, at  $p^{\nu-1} \leq n' - 1$ ). Altså er  $p^\nu \leq n'p \leq n$ , som ønsket.  $\square$

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

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

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

hvormed uligheden er eftervist.  $\square$

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

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

$$\pi(n) \log n \geq \left( \log 2 - \frac{\log(n+1)}{n} \right) n.$$

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

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

**(1.9) Konsekvenser.** Af Primtalssætningen følger fx, at

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

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

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

og dermed at

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

27. oktober 2008

Efter division med  $\log p_n$  fås, at

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

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

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

Hermed er den første relation i (1.9.1) bevist.

Af (1) og (2) følger, at

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

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  $c \leq 1$  og  $C \geq 1$ , at ulighederne (1.3.2) gælder for  $n \geq N_0$ . Herefter er, for  $n \geq N_0$ ,

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

Det er klart, at hvis  $2c > C$ , så er højresiden positiv for  $n \geq N_1$ , med et  $N_1 \geq N_0$ . Påstanden i Bertrand's postulat gælder altså for  $n \geq N_1$ . 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  $n \leq N_1$ .

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  $n \geq 1$  er  $\pi(n) \leq 1,3 \cdot n/\log n$  og for alle  $n \geq 17$  er  $\pi(n) \geq n/\log n$ , og på den baggrund er det let at vise Postulatet. Vi giver senere et elementært bevis for Postulatet.

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

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

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):

27. oktober 2008

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

*Bevis.* I beviset bruger vi følgende vurdering for  $0 < x < 1$ :

$$\log \frac{1}{1-x} = \sum_{n \geq 1} \frac{1}{n} x^n \leq x + \sum_{n \geq 2} x^n = x + \frac{x^2}{1-x} < x + \frac{x^2}{(1-x)^2}.$$

Betragt nu for et naturligt tal  $N$  produktet, over primtal  $p \leq N$ ,

$$\prod_{p \leq N} \frac{1}{1-1/p}.$$

Faktoren svarende til  $p$  er summen  $\sum_i 1/p^i$ ; når disse summer multipliceres fremkommer summen af alle brøker  $1/n$ , hvor  $n$  har en primopløsning med primfaktorer, der alle er højst  $N$ . Heri indgår specielt alle brøker  $1/n$ , hvor  $n \leq N$ . Vi har altså vurderingen,

$$\sum_{n \leq N} \frac{1}{n} \leq \prod_{p \leq N} \frac{1}{1-1/p}.$$

Ved brug af uligheden ovenfor, for  $x := 1/p$ , får vi derfor uligheden,

$$\log \sum_{n \leq N} \frac{1}{n} \leq \sum_{p \leq N} \left( \frac{1}{p} + \frac{1}{(p-1)^2} \right).$$

For  $N \rightarrow \infty$  går venstresiden mod uendelig, fordi den harmoniske række er divergent. På højresiden er rækken  $\sum_p 1/(p-1)^2$  konvergent, fordi rækken  $\sum 1/k^2$  er konvergent. Følgelig må rækken  $\sum 1/p$  være divergent.  $\square$

**(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  $x \rightarrow \infty$  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

27. oktober 2008

$A(x)$  er begrænset. Man kan vise, at hvis grænseværdien  $\lim_{x \rightarrow \infty} A(x)$  eksisterer, så må den være lig med 1. I lyset af dette resultat kunne man håbe, at tilnærmelsen,

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

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 Primtalsætningen heuristisk, for et stort tal  $n$ , at sandsynligheden for at et tal  $p \leq n$  er et primtal er lig med  $1/\log n$ . Mere præcist må det forventes, at et „lille“ interval af længde  $\Delta$  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,

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

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

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

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

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  $\Pi(n) \sim \text{Li}(n)$ , og heraf kan formelt udledes, at

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

Funktionen  $R(n)$  på højresiden af (1.12.3) kaldes *Riemann's række*. I rækkens  $k$ 'te led går faktoren  $\text{Li}(\sqrt[k]{n})$  mod  $-\infty$  for  $k \rightarrow \infty$ , og det er faktisk ækvivalent med Primtalsætningen at vise, at rækken overhovedet er (betinget) konvergent. Riemann selv betragtede kun rækkens afsnitssummer. Hvis vi snyder, og tillægger  $\text{Li}(x)$  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  $n \geq 17$ ) følgende ulighed:

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

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

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

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  $\text{Li}(n) - \pi(n)$  (afrundet opad).

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

$n$	$\pi(n)$	$R(n) - \pi(n)$	$\text{Li}(n) - \pi(n)$
$10^1$	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  $\text{Li}(n) - \pi(n)$  positiv, og altså  $\pi(n) < \text{Li}(n)$ . På baggrund af tabellen kunne man fristes til at tro, at differensen  $\text{Li}(n) - \pi(n)$  vokser ubegrænset for  $n \rightarrow \infty$ . Dette er langt fra tilfældet. Littlewood viste allerede i 1914, at differensen  $\text{Li}(n) - \pi(n)$  skifter fortegn uendelig mange gange. Beviset er ikke konstruktivt, og angiver

ikke en værdi  $n_0$ , for hvilken  $\pi(n_0) > \text{Li}(n_0)$ . 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  $\text{Li}(n)$  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,

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

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

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

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

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

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

hvor  $p_1 < p_2 < p_3 < \dots$  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  $n \geq 1$ , 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  $n \geq 1$ , 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  $\sigma := \operatorname{Re} s > 1$ , får vi vurderingen,

$$\left| \sum'' \frac{1}{n^s} \right| \leq \sum_{n \geq p_{k+1}} \frac{1}{n^\sigma},$$

og her går højresiden mod 0 for  $k \rightarrow \infty$ , da rækken  $\sum n^{-\sigma}$  er konvergent. Hermed er (\*) bevist. Det følger, for  $\operatorname{Re} s > 1$ , 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),

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

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

$$\frac{1}{\zeta(s)} = \sum_{n \geq 1} \frac{\mu(n)}{n^s}. \quad (1.14.3)$$

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,

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

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

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

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

Rækken på højresiden er betinget konvergent for  $\operatorname{Re} s > 0$  (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  $\operatorname{Re} s > 0$ . Bemærk dog, at faktoren  $1 - 2^{1-s}$  på venstresiden er 0, når  $s = 1 + 2\pi ia / \log 2$  med  $a \in \mathbb{Z}$ . For  $a = 0$ , dvs for  $s = 1$ , har højresiden værdien  $\log 2$ , og

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

27. oktober 2008

hvor „ $\cdot \cdot \cdot$ “ 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:

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

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  $\operatorname{Re} s = \frac{1}{2}$ , er  $1 - s$  det konjugerede af  $s$ .

Af særlig interesse er nulpunkterne for  $\zeta(s)$ . For  $\operatorname{Re} s > 1$  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  $s = 3, 5, 7, \dots$ . I området  $\operatorname{Re} s < 0$  har  $\zeta(s)$  derfor kun de *trivielle* nulpunkter  $-2, -4, -6, \dots$ . Riemann viste, at Primtalsætningen er ækvivalent med, at  $\zeta(s)$  ikke har nulpunkter på de to linier  $\operatorname{Re} s = 0$  og  $\operatorname{Re} s = 1$ . Det var faktisk ved hjælp af denne ækvivalens, at Primtalsætningen blev bevist.

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

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

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

$$\pi(n) = R(n) - \sum_{\rho} R(n^{\rho}), \quad (1.14.6)$$

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

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

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

hvor „*store-O-notationen*“ indikerer, at differensen  $\pi(n) - \operatorname{Li}(n)$  numerisk er begrænset af en konstant gange  $\sqrt{n} \log n$ . Det skal understreges, at de asymptotiske relationer i (1.12) er ækvivalente med Primtalsætningen. 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  $\operatorname{Li}(w)$ , også for komplekse tal  $w$  (af formen  $w = n^{\rho}$ ). Når  $x > 1$  og  $\rho \neq 0$  definerer vi  $\operatorname{Li}(x^{\rho}) := \operatorname{Ei}(\rho \log x)$ , hvor  $\operatorname{Ei}(z)$  er *eksponential-integralet*, defineret for komplekse  $z \neq 0$  ved udtrykket,

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

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  $Ei(z)$  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  $e^z/z = 1/z + \sum_{m \geq 1} z^{m-1}/m!$ . Med en konstant  $\gamma$  har vi altså ligningen,

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

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

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

hvoraf

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

At  $\gamma$  faktisk er *Euler's konstant* følger af udregningerne,

$$\begin{aligned} 1 + \frac{1}{2} + \dots + \frac{1}{n} - \log n &= \int_0^1 \frac{1 - u^n}{1 - u} du - \int_1^n \frac{1}{t} dt \\ &= \int_0^n \frac{1 - (1 - t/n)^n}{t} dt - \int_1^n \frac{1}{t} dt = \int_0^1 \frac{1 - (1 - t/n)^n}{t} dt - \int_1^n \frac{(1 - t/n)^n}{t} dt; \end{aligned}$$

Euler's konstant er grænseværdien, for  $n \rightarrow \infty$ , 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  $R(n)$ :

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

Indsæt, i rækken på højresiden, udtrykket (1.15.2) for  $Ei(z/k)$ , 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,

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

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  $s \rightarrow 1$ , at  $1/\zeta(s) \rightarrow 0$  og  $(1/\zeta(s))' \rightarrow 1$ , og dette kan tages som en vag indikation for ligningerne i (1.16.2), men langt fra 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 tredje 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,

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

**(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  $\mu: \mathbb{N} \rightarrow \mathbb{C}$  som opfylder:  $\mu(1) = 1$  og  $\sum_{d|n} \mu(d) = 0$  for  $n > 1$ .
- H1 **2.** Bevis formelen  $\pi(n) = \sum_k (\mu(k)/k) \Pi(\sqrt[k]{n})$ , hvor  $\Pi(n)$  er defineret i (1.12).
- H1 **3.** Vis, at de tre asymptotiske formler,  $\pi(n) \sim \text{Li}(n)$ ,  $\Pi(n) \sim \text{Li}(n)$ ,  $\pi(n) \sim R(n)$ , 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  $0 \leq x \leq N$ , 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

27. oktober 2008

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 med sikkerhed 39 Mersenne-primtal. Det største, svarende til  $p = 13.466.917$ , har 4.053.946 cifre.

U3 **9.** Med  $\sigma(n)$  betegnes summen af divisorerne i  $n$ , altså  $\sigma(n) = \sum_{d|n} d$ . Bestem  $\sigma(p^v)$ , 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  $2^v - 1$  er et primtal, så er tallet  $n = 2^{v-1}(2^v - 1)$  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  $n = p_1^{v_1} \cdots p_r^{v_r}$  som  $\tau(n) = (v_1 + 1) \cdots (v_r + 1)$ ). Find en tilsvarende formel for  $\alpha(2^v u)$ , når  $u$  er ulige. [Vink: Pas på, der er noget lusk omkring  $v = 1$ .]

U1 **14.** Vis, at tallene  $l! + 2, l! + 3, \dots, l! + l$  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,  $n = 2^v p_1 \cdots p_r$ , 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  $m = 1, 2, \dots$ . 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  $m = 1, \dots, 6$ .

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

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  $R_{l+m} = R_l R_m$  ?]

27. oktober 2008

**19.** Stirling's formel udsiger, at  $n! \sim \sqrt{2\pi n} n^{n+\frac{1}{2}} e^{-n}$ . 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  $b_n \leq C2^n/\sqrt{n}$ . Vis, at for hvert positivt tal  $c$  er  $b_n \leq 2^{n-c}$  for  $n \gg 0$ . Vis, at hvis  $b_n \leq 2^{n-c}$  for  $n = n_0$ , så er  $b_n \leq 2^{n-c}$  for alle  $n \geq n_0$ . [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  $n \geq N$ . 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 irrationalt. Hvad gælder, hvis grundtallet 10 erstattes med et mere generelt helt grundtal  $g$ ,  $g \geq 2$ ?

**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-sxsystemet. Ligningens højreside er så tallet 11111 (med fem cifre). 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 cifre (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  $v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots$  (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  $\pi(x) \geq cx/\log x$ .)

Lad os her definere en *primtalstvilling* som et primtal  $q$  for hvilket  $q+2$  eller  $q-2$  ligeledes er et primtal. Som nævnt ved man ikke, om der er uendelig mange primtalstvillinger. Man kan vise, at rækken  $\sum \frac{1}{q}$ , hvor summen er over primtalstvillinger  $q$ , er konvergent, og man kan vise, at der for antallet  $\pi_2(x)$  af primtalstvillinger mindre end eller lig med  $x$  gælder en vurdering af formen  $\pi_2(x) \leq Kx/(\log x)^2$ .

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 konvergens 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  $q \leq x$  i delmængden  $Q$ . Betragt for en given talfølge  $\alpha_n$  summen  $\sum_{a \leq q \leq b} \alpha_q$ , hvor notationen indikerer, at der summeres over  $q \in Q$  med  $a \leq q \leq b$ . Af og til kan man have gavn af

27. oktober 2008

følgende omskrivninger (hvor  $n$  gennemløber naturlige tal):

$$\begin{aligned} \sum_{a \leq q \leq b} \alpha_p &= \sum_{a \leq n \leq b} \alpha_n (\pi_Q(n) - \pi_Q(n-1)) \\ &= \alpha_{b+1} \pi_Q(b) - \alpha_a \pi_Q(a-1) + \sum_{a \leq n \leq b} (\alpha_n - \alpha_{n+1}) \pi_Q(n); \end{aligned}$$

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  $\pi(x) \geq cx / \log x$ . Vis, at konvergens af rækken  $\sum \frac{1}{q}$  over primtalstvillinger  $q$  er en konsekvens af en vurdering af formen  $\pi_2(x) \leq Kx / (\log x)^2$ . [Vink: benyt, og begrund, at  $\sum 1/(n(\log n)^s)$  (over  $n \geq 2$ ) er konvergent, præcis når  $s > 1$ .]

**30.** Check lige, at definitionen i (1.15),  $\text{Li}(x) = \text{Ei}(\log x)$ , harmonerer med, at logaritme-integralet 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  $\text{Ei}(x)$  er reelt, når  $x$  er reel og positiv? Og at  $\text{Ei}(x) = \lim_{\varepsilon \rightarrow 0} (\int_{-\infty}^{-\varepsilon} + \int_{\varepsilon}^x) e^t t^{-1} dt$ .

**34.** Lad  $b_n$  betegne den midterste af binomialkoefficienterne  $\binom{n}{i}$  (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:

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

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

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

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