Anders Thorup

Elementær talteori

Algebra og talteori, F2001

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

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

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 $a_1, a_2, \ldots$, 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 $a_1, \ldots, a_k$ 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 $(3, 5)$, $(5, 7)$, $(11, 13)$, $\ldots$, $(347, 349)$, $\ldots$. 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 $l! + 2, l! + 3, \ldots, l! + l$ 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 uhyrligt 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 $k := [(n+1)/2]$. Specielt er så $k \leqslant (n+1)/2$, og $n/k \leqslant 2$, og $n/2 \leqslant k < n$. 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 $n \geqslant 4$?] ∎

(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 $1p, 2p, \ldots, k'p$. 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 $0<c<1<C$, at ulighederne (1.3.2) gælder for $n \geqslant N_0$. Herefter er, for $n \geqslant N_0$,

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

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 explicit bestemmelse af c, C med $c/C > \frac{1}{2}$ og et tilhørende N_0; herefter bestemmes N_1 og Bertrands 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 utilstrækkelige, idet vi her har $c/C = \frac{1}{9}$.

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

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

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

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

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 $n \leqslant N$. Vi har altså vurderingen,

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

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

$$\log \sum_{n \leqslant N} \frac{1}{n} \leqslant \sum_{p \leqslant N} \Big(\frac{1}{p} + \frac{1}{(p-1)^2} \Big).$$

For $N \to \infty$ 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. ∎

(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 $A(x)/\log x \to 0$ 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). 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,

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

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

$$\pi(x) = \sum_k \frac{\mu(k)}{k} \Pi(\sqrt[k]{x}).$$

(Funktionen $\mu(n)$ har værdien $(-1)^r$ når n er et produkt af r forskellige primtal, og 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. Man kan bevise, at for $n \gg 0$ (mere præcist, for $n \geqslant 17$) gælder uligheden,

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

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. Den største (i 1994) beregnede værdi er i øvrigt

$$\pi(10^{18}) = 24739954287740860.$$

Skønt man således kan sige, at der er numerisk evidens for at differensen $\mathrm{Li}(n) - \pi(n)$ altid er positiv, er dette ikke 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 $\mathrm{Li}(n_0) < \pi(n_0)$. 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 indrog 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 $p_1, \ldots, p_k$. 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,

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

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

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

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 $R(n)$:

$$R(e^z) = \sum_k \frac{\mu(k)}{k}\,\mathrm{Ei}(z/k).$$

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,

$$\sum_k \frac{\mu(k)}{k}(\gamma + \log z), \quad \text{og} \quad -\sum_k \frac{\mu(k)}{k}\log k. \tag{1.16.1}$$

Man kan vise, at der gælder ligningerne,

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

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,

$$\sum_k \sum_m \frac{\mu(k)}{k}\frac{z^m}{k^m m m!}.$$

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.

1. Vis, at Möbius-funktionen $\mu(n)$ kan karakteriseres som den eneste funktion $\mu\colon \mathbb{N}\to\mathbb{C}$ som opfylder, at $\mu(1)=1$ og, for $n>1$, at $\sum_{d|n}\mu(d)=0$.

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

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 $1<x<2$.

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 du må gerne tegne med en blyant, hvis spids er ca 1mm tyk. Men du skal kunne forsvare din tegning. [Vink: $300\approx \log 10^{130}$.]

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

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

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 $F_0=3$, $F_1=2^2+1=5$, $F_2=2^4+1=17$, $F_3=2^8+1=257$, og $F_4=2^{16}+1=65.537$. Man kender ikke andre Fermat-primtal. Euler beviste, at 641 går op i F_5: Det er let at se, at $641 = 5\cdot 2^7+1 = 5^4+2^4$. Modulo 641 gælder derfor, at

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

8. *Mersenne-primtallene* er primtal af formen $p = 2^q-1$. Vis, at hvis $M_q = 2^q-1$ er et primtal, så er q et primtal.

9. Vis, at et *lige* tal n er *perfekt*, dvs lig med summen af sine ægte divisorer (incl. 1), hvis (ifølge Euklid) og kun hvis (ifølge Euler) $n = 2^{q-1}(2^q-1)$, hvor 2^q-1 er et primtal.

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

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

12. Vis ligningen (1.14.5). [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.]

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

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 $a = 1, \ldots, p-1$ 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 et 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,

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

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,

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

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. ∎

(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 Vier-gruppe $\mathrm{C}_2 \times \mathrm{C}_2$, 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,

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

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 $2^{\nu-2}$.

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

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

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 $3p_1 p_2$, hvor $3 < p_1 < p_2$. Betingelsen for primtallet 3 er altid opfyldt, da $p_1 p_2 - 1$ 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,

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

specielt er $p_1 - 1 \mid 6p_2 - 12$. At (i) følger, at $p_1 - 1 \mid 6p_2 - 2$. Altså er $p_1 - 1 \mid 10$, og da $p_1 > 3$ er et primtal, får vi $p_1 = 11$. 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.

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

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

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

4. Bestem alle Carmichael-tal af formen $5p_1p_2$.

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

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 $1 + kp = 2^{10}$.]

7. Lad p være et ulige primtal, og lad z være et helt tal således, at $(z \mod p)$, dvs z's restklasse modulo p, frembringer gruppen $(Z/p)^*$. Betragt de p tal,

$$z_i = z + ip \quad \text{for } 0 \leqslant i < p;$$

de har alle den samme restklasse modulo p, men restklasserne $(z_i \mod p^2)$, af z_i modulo p^2, er forskellige.

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

(ii) Vis, at hvis restklassen $(z \mod p^2)$ frembringer gruppen $(Z/p^2)^*$, så vil restklassen $(z \mod p^\nu)$ frembringe gruppen $(Z/p^\nu)^*$ for alle ν.

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 muliplikative 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 altså $\zeta = \zeta_n{}^a$. De komplekse n'te enhedsrødder udgør altså 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 svarende til at ξ har en given orden d, 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 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,

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

Når karakteristikken er et primtal p, er afbildningen $x \mapsto x^p$ en homomorfi af legemet L ind i sig selv. Med andre ord gælder følgende ligninger for $x, y \in L$:

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

De to sidste 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.

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 polonomium opfattes så i $\mathbb{F}_p[X] \subseteq L[X]$. 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 (3.3.3) får vi, eventuelt ved at reducere koefficienterne, følgende ligning i $L[X]$:

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

Af (*) 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 (*) 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 (*). 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. ∎

(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 $\xi_1, \ldots, \xi_n$ i G. Altså gælder i $L[X]$ ligningen,

$$X^n - 1 = (X - \xi_1) \cdots (X - \xi_n). \qquad (**)$$

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 (**) fås ligningnen,

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

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

Af (**) og (*) sluttes, at hver faktor Φ_d på højresiden af (*) 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 L være et legeme af karakteristik p, og antag, at $p \nmid n$. Betragt cirkelsdelingspolynomiet Φ_n, og i $L[X]$ en irreducibel divisor f, af grad r, i Φ_n. Da er kvotientringen $K := L[X]/(f)$ et legeme som indeholder L, og K er et vektorrum af dimension r over L. Yderligere gælder, at restklassen $\zeta := (X \mod f)$ er et element af orden n i K, og ethvert legeme K_1, som indeholder L og et element af orden n, vil også indeholde K.*

Bevis. Det er velkendt, at kvotienten K omfatter L, og at K herved specielt kan opfattes som vektorrum over L, og at de r første potenser af ζ, altså $1, \zeta, \ldots, \zeta^{r-1}$, udgør en L-basis for K. Da f er irreducibel, er hovedidealet (f) et maksimalideal i $L[X]$, og derfor er kvotienten K et legeme. Yderligere gælder, at restklassen ζ er rod i f. I $L[X]$, og dermed også i $K[X]$, har vi en ligning $\Phi_n = fg$. Følgelig er ζ rod i Φ_n. Af Sætning (3.6) følger derfor, at ζ har orden n.

Antag nu, at K_1 er et legeme, der omfatter L som dellegeme og indeholder et element ξ af orden n. Sætningens sidste påstand er (lidt mere præcist), at der findes en (ring-)homomorfi $K \to K_1$, som på L blot er den identiske afbildning; en sådan homomorfi mellem legemer må som bekendt automatisk være injektiv. Elementet ξ har orden n, så den cykliske undergruppe frembragt af ξ består af n elementer. Af disse har præcis $\varphi(n)$ elementer orden n. Disse $\varphi(n)$ elementer må være rødder i Φ_n. Polynomiet Φ_n har altså i K_1 præcis så mange rødder, som sin grad, og det kan derfor skrives som produkt af førstegradspolynomier $X - \alpha$. På den anden side har vi i $L[X]$, og dermed i $K_1[X]$, en ligning $\Phi_n = fg$. Følgelig kan f skrives som produkt af førstegradspolynomier i $K_1[X]$. Specielt følger det, at polynomiet f har en rod ζ_1 i K_1. Herefter er det velkendt, at homomorfien $L[X] \to K_1$, bestemt ved $h \mapsto h(\zeta_1)$, inducerer en homomorfi $L[X]/(f) \to K_1$, som ønsket. ∎

(3.9) Korollar. *Under forudsætningerne i* (3.8) *gælder i* $L[X]$*, at alle irreducible divisorer i* Φ_n *har den samme grad, og at de forekommer med multiplicitet* 1 *i primopløsningen af* Φ_n*.*

Bevis. Betragt to irreducible divisorer f og f_1 i Φ_n, af grader r og r_1, og de tilhørende kvotienter $K := L[X]/(f)$ og $K_1 := L[X]/(f_1)$. Sætning (3.8) giver en injektiv homomorfi,

$$K \to K_1.$$

Homomorfien er specielt en lineær afbildning mellem vektorrum over L. Da dimensionerne er r og r_1 følger det, at $r \leqslant r_1$. Af symmetrigrunde gælder derfor $r = r_1$.

I K er restklassen ζ rod i f og dermed i Φ_n. Altså har ζ orden n. Blandt potenserne af ζ findes derfor $\varphi(n)$, som har orden n, og de er alle rødder i Φ_n. Polynomiet Φ_n, af grad $\varphi(n)$, har derfor ingen dobbeltrødder. Hvis f indgik med multiplicitet mindst 2 i primopløsningen af Φ_n, ville roden ζ i f være dobbeltrod i Φ_n, i modstrid med det, vi lige har bevist. ∎

(3.10) Sætning. *Lad* L *være et endeligt legeme. Da er karakteristikken af* L *et primtal* p*, og elementantallet* q *i* L *er en potens,* $q = p^r$*, af primtallet* p*. Hvert element i* L *er rod i polynomiet* $X^q - X$*. Den multiplikative gruppe* L^* *er cyklisk af orden* $q - 1$*.*

Bevis. Da L kun har endelig mange elementer, kan den kanoniske homomorfi $\mathbb{Z} \to L$ ikke være injektiv. Karakteristikken for L må derfor være et et primtal p. Vi kan altså opfatte legemet $\mathbb{F}_p$ som dellegeme af L. Specielt kan vi opfatte L som vektorrum over $\mathbb{F}_p$, idet addition af vektorer blot er den givne addition i L og multiplikation af en vektor $x \in L$ med en skalar $\lambda \in \mathbb{F}_p \subseteq L$ blot er produktet λx i L. Da der kun er endelig mange vektorer i dette vektorrum, har vektorrummet en endelig basis. Vælges en sådan basis, og betegner r antallet af basisvektorer (r er altså dimensionen af vektorrummet L), fås som bekendt en bijektiv forbindelse mellem vektorer x i L og koordinatsæt $(\lambda_1, \ldots, \lambda_r)$ i $\mathbb{F}_p^r$. Specielt er $q = p^r$.

Den multiplikative gruppe L^* har orden $q - 1$. For hvert element $\alpha \neq 0$ i L har vi altså $\alpha^{q-1} = 1$, og dermed også $\alpha^q = \alpha$. Den sidste ligning er naturligvis også opfyldt for $\alpha = 0$.

Det er velkendt, at L^* er cyklisk, jfr Bemærkning (3.7). ∎

(3.11) Korollar. *Antag, at* L *er et endeligt legeme med* q *elementer, og at* n *er primisk med* q*. Betragt i* $L[X]$ *en irreducibel divisor* f *i* Φ_n*. Da er graden* r *af* f *lig med ordenen af* q*'s restklasse i* $(\mathbb{Z}/n\mathbb{Z})^*$*.*

Bevis. Som i (3.8) betragtes legemet $K := L[X]/(f)$. Det er et vektorrum over L af dimension r. Det følger specielt, at K indeholder q^r elementer. Den multiplikative gruppe K^* har altså orden $q^r - 1$. Restklassen ζ, af X modulo f, er i K^* et element af orden n. Derfor må n være divisor i gruppens orden, dvs divisor i $q^r - 1$. Modulo n gælder derfor, at $q^r \equiv 1$.

Det skal yderligere vises, at $r \geqslant 1$ er den mindste eksponent med denne egenskab. Antag derfor, for $s \geqslant 1$, at $n \mid q^s - 1$. Da $\zeta^n = 1$, følger det, at $\zeta^{q^s-1} = 1$. Heraf følger videre, at $\zeta^{q^s} = \zeta$, og nu følger, under brug at (3.5.1), at $\alpha^{q^s} = \alpha$ for alle $\alpha \in K$. Polynomiet $X^{q^s} - X$ har altså alle de q^r elementer α i K som rødder. Specielt er $q^r \leqslant q^s$, og derfor er $r \leqslant s$. ∎

(3.12) Korollar. *For hver primtalspotens* $q = p^r$ *findes et legeme* L *med* q *elementer, fx beskrevet 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 ækvivalensklassen $\zeta := (X \bmod f)$ en frembringer for den cykliske gruppe K^*. Yderligere gælder, at alle legemer med q elementer er isomorfe.

Bevis. Med $n := p^r - 1$ er det klart, at restklassen af p modulo n har orden r i $(\mathbb{Z}/n)^*$. Af (3.11), med $L := \mathbb{F}_p$, følger derfor, at f har grad r. Kvotienten $K = \mathbb{F}_p[X]/(f)$ er derfor et legeme med $p^r = q$ elementer. Ækvivalensklassen ζ er ifølge konstruktionen rod i f, og dermed i Φ_{q-1}. Af (3.6) følger, at ζ har orden $q-1$, altså at ζ er en frembringer for den cykliske gruppe K^*.

Lad nu K_1 være et endeligt legeme med q elementer. Den multiplikative gruppe K_1^* er cyklisk af orden $q-1$. Derfor findes i K_1 et element af orden $q-1$. Sætning (3.8), med $L := \mathbb{F}_p$, giver nu en inklusion $K \subset K_1$. Da begge sider har q elementer, må de være ens. ∎

(3.13) Korollar. *Lad p være et primtal. Da gælder om primopløsningen af $X^{p^r} - X$ i $\mathbb{F}_p[X]$, at faktorerne er samtlige (normerede) irreducible polynomier i $\mathbb{F}_p[X]$ af en grad, som går op i r, og hver af faktorerne forekommer præcis én gang.*

Bevis. Hvis en primfaktor g indgik to gange, ville vi have en ligning $X^{p^r} - X = g^2 h$, 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 irreducibelt polynomium i $\mathbb{F}_p[X]$, og lad s betegne graden af f. Det skal vises, at

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

Betragt hertil kvotienten $K := \mathbb{F}_p[X]/(f)$ og ækvivalensklassen $\xi := (X \bmod f)$. Da er K et legeme med p^s elementer og ξ er rod i f. Da $|K| = p^s$ gælder $\xi^{p^s} = \xi$. Følgelig er f divisor i $X^{p^s} - X$.

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

Antag omvendt, at $f \mid X^{p^r} - X$. Det skal vises, at $s \mid r$. Det er klart, hvis $s = 1$, så vi kan antage, at $s > 1$. Specielt er så $f \neq X$, og følgelig er $f \mid X^{p^r-1} - 1$. Heraf følger, at $\xi^{p^r-1} = 1$. Idet n er ordenen af ξ i K^*, følger det, at $n \mid p^r - 1$, altså $p^r \equiv 1 \pmod{n}$. På den anden side har vi i (3.11) bestemt s som ordenen af p i gruppen $(\mathbb{Z}/n)^*$. Af $p^r \equiv 1 \pmod{n}$ følger derfor, at $s \mid r$.

Hermed er det vist, at primfaktorerene i $X^{p^r} - X$ netop er de irreducible polynomier af grad s med $s \mid r$. ∎

(3.14) 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 (3.12) 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 ζ, 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

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

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,

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

heraf følger fx, at $\zeta^5 = \zeta + \zeta^2$, at $\zeta^6 = \zeta^2 + \zeta^3$, at $\zeta^7 = \zeta^3 + \zeta^4 = \zeta^3 + \zeta + 1$, 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 (3.12), 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 $p \gg 0$).

(3.15) 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

$$f = X^2 - 6X - 4 = X^2 + X + 3.$$

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

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

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

hvor μ er Möbius-funktionen.

Bevis. Produktet af samtlige irreducible polynomier af grad $s \mid r$ er ifølge Korollar (3.13) lig med $X^{p^r} - X$. Den første anførte ligning følger nu ved sammenligne graderne, og heraf følger den anden ligning ved Möbius-inversion. ∎

(3.17) Bemærkning. Af (3.11) fremgår, hvordan man undersøger, om cirkeldelingspolynomiet Φ_n er irreducibelt i $\mathbb{F}_p[X]$. Det er et fundamentalt resultat i algebraisk talteori, at Φ_n altid er irreducibelt i $\mathbb{Q}[X]$.

Hertil betragtes, for en given kompleks primitiv n'te enhedsrod ζ, det minimale polynomium F for ζ, dvs det normerede polynomium F i $\mathbb{Q}[X]$ af mindst mulig grad, som har ζ som rod. Ækvivalent: polynomierne i $\mathbb{Q}[X]$ med ζ som rod udgør et ideal, altså et hovedideal, og F er den normerede frembringer for dette ideal. Det fremgår, at F er divisor i ethvert polynomium i $\mathbb{Q}[X]$, der har ζ som rod. Specielt er F et irreducibelt polynomium.

Da ζ er rod i Φ_n, er F divisor i Φ_n. Det er derfor nok at vise, at enhver primitiv n'te enhedsrod er rod i F. De primitive n'te enhedsrødder er tallene ζ^a, hvor a er primisk med n. Eksponenten a kan skrives som produkt af primtal p, der er primiske med n. Det er derfor nok at vise, når p er primisk med n, at ζ^p er rod i F.

Hertil betragtes det minimimale polynomium G for ζ^p. Antag, indirekte, at ζ^p ikke er rod i F. Da er $G \neq F$, og da begge polynomier er irreducible divisorer i Φ_n, har vi en fremstilling i $\mathbb{Q}[X]$,

$$\Phi_n = FGH. \qquad (*)$$

Da polynomierne er normerede, følger det af Gauss's Sætning, at F, G, H har koefficienter i $\mathbb{Z}$. Da ζ^p er rod i G, er ζ rod i $G(X^p)$. Altså er F divisor i $G(X^p)$. Nu reduceres koefficienterne modulo p. Af (*) fås $\bar{\Phi}_n = \bar{F}\bar{G}\bar{H}$. Videre er $\bar{G}(X^p) = (\bar{G}(X))^p$, og $\bar{F}$ er altså divisor i $\bar{G}^p$. En irreducibel divisor f i $\bar{F}$ går derfor også op i $\bar{G}$. Men så er fremstillingen $\bar{\Phi}_n = \bar{F}\bar{G}\bar{H}$ ikke forenelig med at primdivisorerne i $\bar{\Phi}_n$ er forskellige.

(3.18) 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 $p_1, \ldots, p_k$. 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,

$$(h-1)^{\varphi(n)} < \Phi_n(h), \text{ når } h \geqslant 1. \qquad (3.18.1)$$

Tallet $\Phi_n(h)$ er nemlig produktet af faktorerne $h - \zeta$ for primitive n'te enhedsrødder ζ. For hver sådan er også $\bar{\zeta} = \zeta^{-1}$ en primitiv n'te enhedsrod. Idet (3.18.1) er triviel for $n = 2$,

antager vi $n > 2$, og så er $\bar{\zeta} \neq \zeta$. Med $h - \zeta$ forekommer altså også $h - \bar{\zeta}$ 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 $|h - \zeta|$ lig med afstanden fra h til ζ. Da ζ ligger på enhedscirklen, og $\zeta \neq 1$, er $|h - \zeta| > |h - 1|$. Altså gælder (3.18.1).

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 $a = 1$.

(3.19) 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 (3.10) 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,

$$q^r - 1 = q - 1 + \sum{}' |\Lambda^* : C^*(\alpha_j)|, \tag{3.19.1}$$

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 (3.18.1) giver nu en modstrid, med mindre $r = 1$.

(3.20) Opgaver.

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}.]

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 $\Phi_{2u}(X) = \Phi_u(-X)$.

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 (1.17)(1).]

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 (3.15), at i $\mathbb{F}_7[X]$ er $f := X^2 + X - 2$ divisor i Φ_{48}. Bestem kvotienten Φ_{48}/f.

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

7. For hvilke primtal p er Φ_n irreducibel i $\mathbb{F}_p[X]$.

8. Vis, for $n > 2$, at der er uendelig mange primtal p med $p \not\equiv 1 \pmod{n}$.

9. Vis, når $p \nmid n$, at $\Phi_{np}(X) = \Phi_n(X^p)/\Phi_n(X)$.

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

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 $1/n$.

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 $C = \log p$.

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

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 $\overline{a}$ 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) Den generelle Reciprocitetssætning. *Legendre-symbolet har en udvidelse til et symbol $\left(\frac{a}{b}\right)$, defineret når nævneren b er enten ulige og positiv eller en diskriminant, med 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,*

$$\left(\frac{u}{D}\right) = \left(\frac{D}{u}\right). \tag{4.2.1}$$

For et helt tal $b \neq 0$ kaldes en funktion $\chi : \mathbb{Z} \to \mathbb{C}$ en (restklasse-)*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: $\chi(a_1 a_2) = \chi(a_1)\chi(a_2)$. 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.

De tilladte „nævnere" b er enten positive og ulige, eller *diskriminanter*, dvs tal forskellige fra 0 (eventuelt negative), som modulo 4 er kongruente med 0 eller 1. Symbolet kaldes *Jacobi-symbolet*, når nævneren b er ulige og positiv, og *Kronecker-symbolet*, når nævneren er en diskriminant.

(4.3) Bemærkning. Inden vi beviser Reciprocitetssætningen, 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 $\left(\frac{3}{-4}\right)$. Med den sidste værdi lig med $+1$ bestemmes det trivielle symbol, med værdien -1 bestemmes altså udvidelsen af Legendre symbolet.

Det er nok betragte værdierne $\left(\frac{a}{b}\right)$, når a er primisk med b. Da symbolet er en homomomorfi $(\mathbb{Z}/b)^* \to \{\pm 1\}$, gælder altid, at $\left(\frac{aq}{b}\right) = \left(\frac{a}{b}\right)$, når q er et kvadrat (dvs af formen $q = a_1^2$)

primisk med b. Specielt er naturligvis $\left(\frac{1}{b}\right) = 1$. Symbolet $\left(\frac{a}{-4}\right)$ er således fastlagt ved værdien $\left(\frac{3}{-4}\right)$.

For $b = 8$ får vi under brug af egenskaberne:

$$\left(\frac{3}{8}\right) = \left(\frac{8}{3}\right) = \left(\frac{-4}{3}\right) = \left(\frac{3}{-4}\right), \qquad \left(\frac{5}{8}\right) = \left(\frac{8}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{-4}{3}\right) = \left(\frac{3}{-4}\right).$$

Da vi videre har $\left(\frac{7}{8}\right) = \left(\frac{8}{7}\right) = \left(\frac{1}{7}\right) = 1$ og $\left(\frac{1}{8}\right) = 1$, er symbolet $\left(\frac{a}{8}\right)$ bestemt.

For en *ulige* diskriminant D er

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

Ligningen er naturligvis triviel, hvis D er positiv, så vi antager $D < 0$. Tallet D er ulige, så ved at trække et passende multiplum af D fra a kan vi 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 $\left(\frac{2}{b}\right) = \left(\frac{8}{b}\right) = \left(\frac{b}{8}\right)$, som blev bestemt ovenfor. Hvis b er ulige og negativ, er b nødvendigvis en diskriminant, og derfor er $\left(\frac{2}{b}\right) = \left(\frac{2}{|b|}\right)$ ifølge (4.3.1). Symbolet $\left(\frac{2}{b}\right)$ er således bestemt i alle tilfælde.

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

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 $\left(\frac{a}{b}\right)$.

(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.

(4.4) Bemærkning. Symbolet i Reciprocitetssætningen er ikke-trivielt, idet vi for eksempel for Legendre-symbolet har $\left(\frac{2}{3}\right) = -1$. Det generelle symbol svarer altså til at værdien $\left(\frac{3}{-4}\right)$ er -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

$$\left(\frac{-1}{u}\right) = \left(\frac{u}{-4}\right) = \begin{cases} 1 & \text{hvis } u \equiv 1 \pmod 4, \\ -1 & \text{hvis } u \equiv 3 \pmod 4. \end{cases} \tag{4.4.1}$$

Videre er $\left(\frac{2}{u}\right) = \left(\frac{8}{u}\right) = \left(\frac{u}{8}\right)$, og af udregningerne i (4.3) følger, at

$$\left(\frac{2}{u}\right) = \left(\frac{u}{8}\right) = \begin{cases} 1, & \text{hvis } u \equiv \pm 1 \pmod 8, \\ -1, & \text{hvis } u \equiv \pm 3 \pmod 8. \end{cases} \tag{4.4.2}$$

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

$$\left(\frac{v}{u}\right) = \begin{cases} \left(\frac{u}{v}\right), & \text{når } u \text{ eller } v \text{ er } \equiv 1 \pmod 4, \\ -\left(\frac{u}{v}\right), & \text{når } u \text{ og } v \text{ er } \equiv 3 \pmod 4. \end{cases} \tag{4.4.3}$$

I det første tilfælde kan vi nemlig antage, at $u \equiv 1 \pmod 4$, og så følger resultatet direkte af (4.2.1). I det andet tilfælde er $u \equiv 3 \pmod 4$. Følgelig er $-u \equiv 1 \pmod 4$, så $-u$ er en ulige diskriminant. Af (4.3.1) 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 (4.4.1), da $v \equiv 3 \pmod 4$.

(4.5) Eksempel. Af (4.4.2) 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 (4.4.1) fås mere direkte: $\left(\frac{15}{89}\right) = \left(\frac{89}{15}\right) = \left(\frac{-1}{15}\right) = -1$.

(4.6) Bemærkning. Det skal understreges, at de tre formler i (4.4) er udledt som konsekvenser af egenskaberne ved det generelle symbol $\left(\frac{a}{b}\right)$. De tre formler, for ulige primtal $u = p$ og $v = q$, udgør *Gauss's Reciprocitetsformler*. De vedrører alene Legendre-symbolet, og de er essentielle i vores bevis for Den generelle Reciprocitetssætning. I det følgende ser vi nærmere på Legendre-symbolet, vi beviser Gauss's Reciprocitetsformler, og vi viser hvorledes det generelle symbol $\left(\frac{a}{b}\right)$ kan defineres sådan, at Den generelle Reciprocitetssætning er opfyldt.

Vi bemærker først, for et ulige primtal p, 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.

(4.7) Lemma. *For et ulige primtal p er Legendre-symbolet $\left(\frac{a}{p}\right)$ en ikke-triviel kvadratisk karakter modulo p. Yderligere gælder Euler's Kriterium:*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}. \tag{4.7.1}$$

Bevis. Som nævnt i (4.6) udgør de kvadratiske rester en undergruppe Q af index 2 i gruppen $(\mathbb{Z}/p)^*$. Kvotientgruppen af $(\mathbb{Z}/p)^*$ modulo Q har altså orden 2, og kan derfor identificeres med gruppen $\{\pm 1\}$. Under denne identifikation er Legendre-symbolet, som funktion på $(\mathbb{Z}/p)^*$, den kanoniske homomorfi på kvotienten. Altså er Legendre-symbolet en homomorfi, og den er surjektiv, og altså ikke triviel.

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

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

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 (4.7.1). ∎

(4.8) Bemærkning. For et ulige primtal p er Legendre-symbolet $\left(\frac{a}{p}\right)$ altså en ikke-triviel 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 (4.4.1); vi betegner den χ_{-4}. For $n = 8$ er der fire primiske restklasser, ± 1 og ± 3. Gruppen $(\mathbb{Z}/8)^*$ er Klein's Vier-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 (4.4.2); den betegner 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_1a og x_2a. 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,

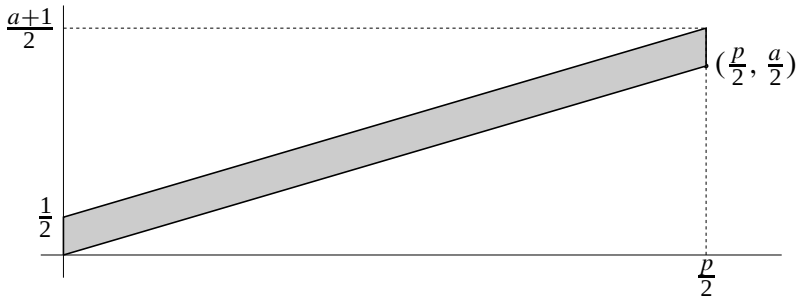
$$1a \cdot 2a \cdots \tfrac{p-1}{2}a \equiv (-1)^n 1 \cdot 2 \cdots \tfrac{p-1}{2},$$

og heraf følger $a^{(p-1)/2} \equiv (-1)^n$. Ligning (4.9.1) følger nu af Euler's Kriterium (4.7.1). ∎

(4.10) Bevis for Gauss's Reciprocitetsformler. En geometrisk fortolkning af tallet n 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:

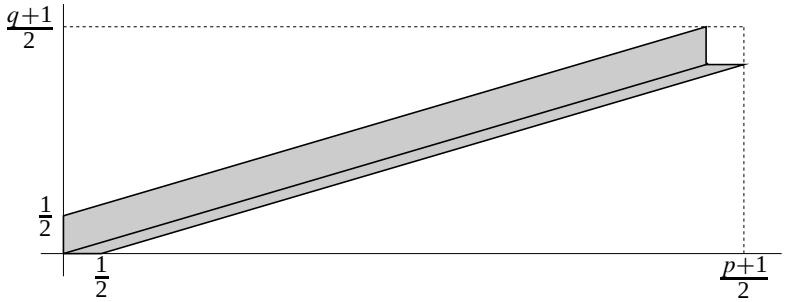


og tallet n er altså antallet af gitterpunkter i det indre af parallellogrammet.

Reciprocitetsformlen (4.4.3), for ulige primtal $p \neq q$, er ækvivalent med ligningen,

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

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 $(p/2, q/2)$).

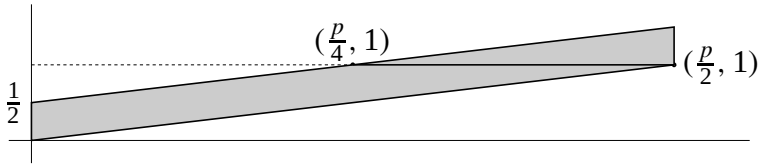


Det (åbne) rektangel består af den markerede figur, to trekanter, og et kvadrat med sidelængde $\frac{1}{2}$. I kvadratet findes ingen gitterpunkter. De to trekanter er kongruente, og indeholder derfor samme antal gitterpunkter. Modulo 2 er antallet, $n + m$, af gitterpunkter i den markerede figur altså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

Reciprocitetsformlen (4.4.2), for et ulige primtal p, er ligningen,

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

hvor χ_8 er karakteren defineret ved højresiden af (4.4.2). 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

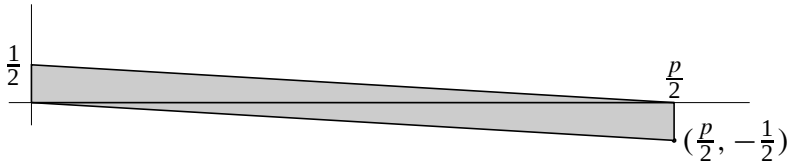
$$\left[\frac{p}{2}\right] - \left[\frac{p}{4}\right] = \begin{cases} 4h - 2h = 2h, & \text{hvis } p = 8h + 1, \\ (4h - 1) - (2h - 1) = 2h, & \text{hvis } p = 8h - 1, \\ (4h + 1) - 2h = 2h + 1, & \text{hvis } p = 8h + 3, \\ (4h - 2) - (2h - 1) = 2h - 1, & \text{hvis } p = 8h - 3. \end{cases}$$

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

Betragt endelig formel (4.4.1),

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

Da p er ulige, er $\chi_{-4}(p) = (-1)^{(p-1)/2}$. Formlen følger derfor umiddelbart af Euler's Kriterium (4.7.1). 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 nu til det generelle symbol $\left(\frac{a}{b}\right)$ nævnt i Sætning (4.2) på følgende måde: 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 $-4, 8, -8$.

For en primdiskriminant p^* defineres *Kronecker-symbolet* ved ligningerne,

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

hvor p er et ulige primtal i den første ligning. Enhver diskriminant D kan entydigt faktoriseres:

$$D = (\text{kvadrat}) \cdot p_1^* \cdots p_t^*, \tag{4.11.1}$$

hvor faktorerne p_i^* er forskellige primdiskriminanter og højst én er lige. Kronecker-symbolet $\left(\frac{a}{D}\right)$, hvor D er en diskriminant, defineres herefter som 0, hvis a ikke er primisk med D, og ellers som produktet af symbolerne $\left(\frac{a}{p_i^*}\right)$. *Jacobi-symbolet* $\left(\frac{a}{u}\right)$, hvor u er positiv og ulige, defineres tilsvarende: værdien er 0, hvis a ikke er primisk med u, og ellers lig med produktet af symbolerne $\left(\frac{a}{q_j}\right)$ for en „primopløsning",

$$u = (\text{kvadrat}) \cdot q_1 \cdots q_r. \tag{4.11.2}$$

Det er klart, at de to definitioner af $\left(\frac{a}{b}\right)$ stemmer overens, når b både er en diskriminant og positiv og ulige.

(4.12) Bevis for Den generelle Reciprocitetssætning. Det skal vises, at det udvidede symbol har egenskaberne (1) og (2) i (4.2). Egenskaben (1) er triviel, idet $\left(\frac{a}{b}\right)$, ud fra primopløsningen af b, er defineret som et produkt af karakterer. Betragt Reciprocitetsformlen (4.2.1). Skriv D som produkt på formen i (4.11.1), og skriv u som produkt af formen i (4.11.2). 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 $u = q$ er et ulige primtal og $D = p^*$ er en primdiskriminant. Det skal altså vises, når q ikke går op i p^*, at

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

Denne ligning følger let af Gauss's Reciprocitetsformler. ∎

(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 (4.4).

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 (4.11.1) 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 (4.3.1) får vi,

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

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 (4.3.1) får vi,

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

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

(4.14) Definition. I det følgende giver vi et alternativt bevis for Gauss's Reciprocitetsformler. Lad χ være en kvadratisk karakter modulo n. Lad der videre være givet et legeme L, og i L^* et element ζ, hvis orden netop er n. Under disse forudsætninger defineres den tilhørende *Gauss-sum* $G := G_{\chi,\zeta}$ som summen,

$$G := \sum_a \chi(a)\zeta^a,$$

hvor index a – her og i det følgende – gennemløber et repræsentantsystem for restklasserne primiske med n. Gauss-summen G er naturligvis element i det givne legeme L.

(4.15) Sætning. *For Gauss-summen $G_{\chi,\zeta}$ gælder ligningen,*

$$G_{\chi,\zeta}^2 = A_\chi,$$

hvor

$$A_\chi := \chi(-1)\sum_b \chi(b)W(b), \quad \textit{og} \quad W(b) := \sum_a \zeta^{a(b-1)};$$

begge summer er over de primiske restklasser modulo n. Leddene $W(b)$ tilhører primlegemet i L, og derfor kan de, og altså også summen A_χ, opfattes som hele tal bestemt modulo karakteristikken af L. Tallet $W(b)$ er bestemt ved udtrykket,

$$W(b) = \frac{\varphi(n)}{\varphi(d)}\,\mu(d),$$

hvor $d = n/(b-1,n)$ er ordenen af ζ^{b-1} (og $\mu(d)$ er Möbius-funktionen).

Bevis. Da funktionen χ er multiplikativ, følger det, at

$$G^2 = \sum_{a,b} \chi(ab)\zeta^{a+b},$$

hvor de to summationsindices a og b gennemløber de primiske restklasser modulo n. Erstattes i dobbeltsummen summationsindices a, b med $-a, ab$ ses, at

$$G^2 = \sum_{a,b} \chi(-a^2b)\zeta^{a(b-1)} = \chi(-1)\sum_b \chi(b)\sum_a \zeta^{a(b-1)} = \chi(-1)\sum_b \chi(b)W(b),$$

hvor $W(b) := \sum_a \zeta^{a(b-1)}$. Hermed er formlen for G^2 bevist.

Lad nu b være fast og primisk med n. Lad d, som i sætningen, betegne ordenen af ζ^{b-1}. Når a gennemløber restklasserne primiske med n, vil ζ^a gennemløbe de $\varphi(n)$ elementer af orden n i L^*, og $\zeta^{a(b-1)}$ vil gennemløbe de $\varphi(d)$ elementer ξ af orden d, idet hvert sådant ξ rammes $\varphi(n)/\varphi(d)$ gange. Følgelig er

$$W(b) = \frac{\varphi(n)}{\varphi(d)} \times \Big(\sum_\xi \xi\Big),$$

hvor ξ gennemløber de $\varphi(d)$ elementer af orden d i L^*. Det er klart, at disse $\varphi(d)$ elementer ξ netop er rødderne i L for cirkeldelingspolynomiet Φ_d; summen $\sum \xi$ er altså lig med -1 gange koefficienten til næsthøjestegradsleddet i Φ_d, og dermed, som det let ses, lig med $\mu(d)$. Heraf følger den i sætningen angivne formel for $W(b)$. ∎

(4.16) Udregning. Lad $n = q$ være et ulige primtal. I (4.15) antages ζ altså at have orden q, så ζ^{b-1} har også orden q med mindre $b-1 = 0$. I undtagelsestilfældet $b = 1$ har $\zeta^0 = 1$ orden 1, og vi finder $W(1) = \varphi(q) = q-1$. Cirkeldelingspolynomiet Φ_q er $\Phi_q = (X^q-1)/(X-1)$, så koefficienten til næsthøjestegradsleddet er 1. For $b \neq 1$ er altså $W(b) = -1$. Derfor er

$$A_\chi = \chi(-1)\Big(\chi(1)(q-1) - \sum_{b\neq 1}\chi(b)\Big) = \chi(-1)\Big(\chi(1)q - \sum_b \chi(b)\Big).$$

Her er naturligvis $\chi(1) = 1$. Hvis χ er triviel, dvs er konstant 1 på alle primiske restklasser, så er den sidste sum lig med antallet af primiske restklasser, altså lig med $q-1$, og følgelig

er $A = 1$. Antag, at χ er ikke-triviel, dvs også antager værdien -1. Da antages værdierne 1 og -1 lige mange gange på de primiske restklasser, og summen $\sum_b \chi(b)$ er derfor lig med 0. Altså gælder:

Hvis χ er en ikke-triviel karakter modulo et ulige primtal q, så er

$$A_\chi = \chi(-1)q. \tag{4.16.1}$$

Som nævnt i (4.8) findes der modulo q præcis to kvadratiske karakterer, nemlig den trivielle karakter og karakteren bestemt ved Legendre symbolet, $\chi_q(a) := \left(\frac{a}{q}\right)$. Karakteren χ_q er altså den eneste, som opfylder forudsætningerne for (4.16.1).

(4.17) Udregning. Antag, at $n = 4$ og at ζ har orden 4. De primiske restklasser b er 1 og $3 \equiv -1$. Øjensynlig er $W(1) = \zeta^0 + \zeta^0 = 2$ og $W(3) = \zeta^2 + \zeta^2 = -2$. For tallet A_χ har vi derfor

$$A_\chi = \chi(-1)\Big(\chi(1)2 - \chi(3)2\Big) = 2\chi(-1)\Big(1 - \chi(-1)\Big).$$

Hvis χ er triviel, får vi $A_\chi = 0$. Og videre:

Hvis χ er en kvadratisk karakter modulo 4*, med $\chi(-1) = -1$, så er*

$$A_\chi = 4\chi(-1) = -4. \tag{4.17.1}$$

Som nævnt i (4.8) er χ_{-4} den eneste karakter, som opfylder forudsætningen for (4.17.1).

(4.18) Udregning. Antag, at $n = 8$ og at ζ har orden 8. De primiske restklasser b er da 1, 3, 5 og 7, og de tilsvarende værdier af d, dvs ordenerne af ζ^0, ζ^2, ζ^4 og ζ^6, er henholdsvis 1, 4, 2 og 4. Cirkeldelingspolynomierne Φ_d for $d = 1, 2, 4$ er øjensynlig $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, og $\Phi_4 = X^2 + 1$, så koefficienterne til næsthøjestegradsleddet er henholdsvis -1, 1 og 0. Følgelig bidrager kun $b = 1$ og $b = 5$ til formlen for A_χ. Det ses, at

$$A_\chi = \chi(-1)\Big(\chi(1)4 - \chi(5)4\Big) = 4\chi(-1)\Big(1 - \chi(5)\Big).$$

Tallet A_χ afhænger således kun af værdierne $\chi(-1)$ og $\chi(5)$. Hvis $\chi(5) = 1$, så er $A_\chi = 0$. Og:

Hvis χ er en kvadratisk karakter modulo 8*, med $\chi(5) = -1$, så er*

$$A_\chi = 8\chi(-1). \tag{4.18.1}$$

Karaktererne modulo 8 blev bestemt i (4.8). Det er netop karaktererne χ_8 og χ_{-8}, som opfylder forudsætningen for (4.18.1).

(4.19) Note. For en given kvadratisk karakter χ modulo n kan vi naturligvis som L vælge legemet $\mathbb{C}$ af komplekse tal og som ζ en primitiv n'te enhedsrod. (Som vi skal se i det følgende, er andre valg af L dog mere interessante for vores anvendelse af Sætning (4.15).) Antag, at $L = \mathbb{C}$. Gauss-summen $G = G_\zeta$ er da et komplekst tal. Dets kvadrat $A = G^2$ er ifølge sætningen et helt tal, uafhængigt af den valgte enhedsrod ζ. Hvis $A \geqslant 0$, er altså

$G_\zeta = \pm\sqrt{A}$ et reelt tal og hvis $A < 0$ er $G_\zeta = \pm i\sqrt{|A|}$ rent imaginært. Fortegnet afhænger af valget af enhedsrod ζ. Vælg specielt enhedsroden $\zeta_n := \exp(2\pi i/n)$.

For $n = 4$ er $\zeta_4 = i$. Gauss-summen G svarende til karakteren χ_{-4} er så

$$G = i - i^3 = 2i,$$

i overensstemmelse med at $G^2 = -4$ ifølge (4.17.1).

For $n = 8$ er $\zeta_8 = (1+i)/\sqrt{2}$. For karakteren χ_8 finder vi for den tilhørende Gauss-sum,

$$G = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 = 2\sqrt{2},$$

og for χ_{-8},

$$G = \zeta_8 + \zeta_8^3 - \zeta_8^5 - \zeta_8^7 = i2\sqrt{2},$$

begge resultater i overensstemmelse med udregningen af G^2 i (4.18.1).

Antag endelig, at $n = q$ er et ulige primtal og at $\chi(a) = \left(\frac{a}{q}\right)$ er Legendre symbolet. Af (4.16.1) følger, at $G^2 = q$ hvis q er kongruent med 1 modulo 4, og at $G^2 = -q$, hvis q er kongruent med 3. Man kan vise, for $\zeta = \zeta_q$, at der faktisk gælder ligningen,

$$G = \begin{cases} \sqrt{q} & \text{når } q \equiv 1 \pmod 4, \\ i\sqrt{q} & \text{når } q \equiv 3 \pmod 4, \end{cases}$$

men det er et dybtliggende resultat.

(4.20) Lemma. *Lad χ være en kvadratisk karakter modulo n, og lad p være et ulige primtal. Antag, at n og tallet $A := A_\chi$, defineret i Sætning* (4.15)*, er primiske med p. Da er*

$$\left(\frac{A}{p}\right) = \chi(p).$$

Bevis. Det er velkendt, at når n er primisk med p findes et legeme (endda et endeligt legeme), som har karakteristik p og indeholder et element ζ af orden n. Vi kan derfor i L betragte Gauss-summen $G = G_{\chi,\zeta}$. Af Sætning (4.15) følger, at $G^2 = A$. Heraf fås, at

$$G^p = (G^2)^{(p-1)/2}G = A^{(p-1)/2}G = \left(\frac{A}{p}\right)G,$$

hvor det sidste lighedstegn følger af Euler's Kriterium (4.7.1). På den anden side gælder, da L har karakteristik p, at afbildningen $L \to L$, bestemt ved $x \mapsto x^p$, bevarer addition og multiplikation. Da G er en heltalslinearkombination af potenser ζ^a med koefficienter ± 1 får vi, at

$$G^p = \sum_a \chi(a)\zeta^{ap} = \chi(p)\sum_a \chi(ap)\zeta^{ap} = \chi(p)\sum_a \chi(a)\zeta^a = \chi(p)G.$$

Sammenligning af de to udtryk for G^p viser, at i legemet L gælder ligningen,

$$\left(\frac{A}{p}\right)G = \chi(p)G.$$

Ifølge forudsætningen er $G^2 = A$ forskellig fra 0 i L, og følgelig er $G \neq 0$. Ved division med G ses derfor, at i L er $\left(\frac{A}{p}\right) = \chi(p)$. Følgelig gælder den påståede ligning modulo karakteristikken p. Da ligningens to sider begge er ± 1, følger det, at ligningen gælder. ∎

(4.21) Bevis for Gauss's Reciprocitetsformler. Formlerne er de tre formler i (4.10). De følger af Lemmaet. Betragt nemlig først for $n = 4$ karakteren $\chi = \chi_{-4}$, og det tilhørende tal $A = A_\chi$. Ifølge Udregning (4.17) er $A = -4$. Specielt er A primisk med p. Af (4.20) fås derfor, at $\left(\frac{-4}{p}\right) = \chi_{-4}(p)$. Da Legendre-symbolet er multiplikativt, får vi $\left(\frac{-1}{p}\right) = \left(\frac{-4}{p}\right) = \chi_{-4}(p)$, som ønsket. Det skal dog straks understreges, at vi allerede har set, at dette resultat følger af Euler's Kriterium (4.7.1), og at dette kriterium indgik i beviset for Lemma (4.20).

Betragt dernæst for $n = 8$ karakteren $\chi = \chi_8$ og det tilhørende tal $A = A_\chi$. Ifølge Udregning (4.18) er $A = 8$, og altså $\left(\frac{8}{p}\right) = \chi_8(p)$. Da Legendre-symbolet er multiplikativt, får vi, som ønsket,

$$\left(\frac{2}{p}\right) = \left(\frac{8}{p}\right) = \chi_8(p).$$

Betragt endelig, for et ulige primtal $q \neq p$, karakteren $\chi(a) = \chi_q(a) = \left(\frac{a}{q}\right)$, og det tilhørende tal $A = A_\chi$. Ifølge Udregning (4.16) er $A = \chi(-1)q = (-1)^{(q-1)/2}q$, idet vi allerede har vist, at $\chi(-1) = \left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$. Idet $q \neq p$, er $A \not\equiv 0 \pmod{p}$. Vi får

$$\left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) = \left(\frac{A}{p}\right) = \chi_q(p) = \left(\frac{p}{q}\right).$$

Da $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, følger den ønskede ligning (4.10.1). ∎

(4.22) 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 $2^q - 1$. ∎

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

(4.23) Opgaver.

1. Bestem for $n = 12$ tallene $W(b)$, som indgår i Sætning (4.15), dvs tallene $W(1)$, $W(5)$, $W(7)$, og $W(11)$. Vis, at der er fire kvadratiske karakterer $\chi : (\mathbb{Z}/12)^* \to \{\pm 1\}$, og angiv for hver af dem tallet A_χ.

2. Lad $\chi : (\mathbb{Z}/12)^* \to \{\pm 1\}$ være den kvadratiske karakter bestemt ved Kronecker-symbolet $\left(\frac{a}{12}\right)$. Bestem værdierne $\chi(1)$, $\chi(5)$, $\chi(7)$, og $\chi(11)$, og værdien A_χ.

3. Legemet $L = \mathbb{F}_{49}$ består af elementer $x + iy$, hvor x, y er restklasser modulo 7, og $i^2 = -1$. Vis, at elementet $\zeta := 2i$ i L har orden 12. Bestem i L den tilhørende Gauss-sum $G_{\chi,\zeta}$, hvor χ er som i opgave (2). Harmonerer det med resultatet fra (2)?

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

5. Der var lidt at vise sidst i beviset for (4.15): Hvis elementet ξ har orden d i en cyklisk gruppe af orden n, så gennemløber ξ^a, for primiske restklasser a modulo n, samtlige elementer af orden d lige mange gange.

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 n. [Vink: Med $ab \equiv 1 \pmod{n}$ er $a(a+1) \equiv a^2(1+b)$.]

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

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).

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 pseudo-primtal*. 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 metode er altså med sikkerhed 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 er 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* $1, \ldots, N$*, 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 $(m, b_1, \ldots, b_k)$ 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 $b = b_1, \ldots, b_k$; $\mathcal{P}$: 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; et primtal m vil ikke passere psp_b, når b er et multiplum af m.] ∎

(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-psp$_b(m)$, udsagnet:

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

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*. 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-psp$_b \implies$ 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-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 Sætning (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:

$$\begin{cases} \text{Enten:} & b^u \equiv 1 \pmod{m} \\ \text{Eller:} & \text{Der findes et } t \text{ så at } 1 \leqslant t \leqslant s \text{ og } (b^u)^{2^{t-1}} \equiv -1 \pmod{m}. \end{cases} \qquad \text{(s-psp}_b\text{)}$$

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

I praksis udføres testen på følgende måde: Først dannes b^u. Hvis $b^u \equiv 1 \pmod m$, så gælder s-psp$_b$. Er dette ikke opfyldt, sættes $x_0 := b^u$ og (induktivt) $x_{j+1} := x_j^2$. Fremkommer herved et j med $0 \leqslant j < s$ således, at $x_j \equiv -1 \pmod m$, 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 $b^u \equiv \pm 1$. Det er således klart, at e-psp$_b$ $\implies$ s-psp$_b$. Antag omvendt, at $b^u \equiv \pm 1$. Det skal så vises, at værdien af ± 1 netop er værdien af $\left(\frac{b}{m}\right)$. Da $m \equiv 3 \pmod 4$, gælder ifølge (4.4.1), at $\left(\frac{\pm 1}{m}\right) = \pm 1$. Altså er $\left(\frac{b^u}{m}\right) = \pm 1 \equiv b^u$. Derfor er

$$\left(\frac{b}{m}\right) = \left(\frac{b \cdot (b^{(u-1)/2})^2}{m}\right) = \left(\frac{b^u}{m}\right) \equiv b^u,$$

som ønsket. □

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

$$m - 1 = u2^s \quad \text{og} \quad p_i - 1 = u_i 2^{s_i} \text{ for } i = 1, \ldots, k,$$

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

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

hvor faktoren $C = C_{k,s_0}$ *er betemt 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,

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

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

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 $i = 1, \ldots, k$. 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 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 er større end et af s_i'erne, 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 naturlige tal t som er mindre end eller lig med s og mindre end eller lig med ethvert af s_i'erne. Med andre ord skal der summeres over $t = 1, \ldots, s_0$. Summen er følgelig

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

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'). Hermed er Lemma'ets første påstand bevist.

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

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

Skrives som ovenfor $b = ac$, er det nok at vise påstanden for $b := a$ og $b := c$. For $b := a$, er antagelsen, at (1) er opfyldt, altså at $b^u = 1$. 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 $b^u = 1$ med ulige u medfører derfor, at højresiden i (4) er lig med 1. Altså gælder (4).

For $b := c$, er antagelsen, at (2) er opfyldt. Hvis $b = 1$, er (4) trivielt opfyldt, så vi antager, at $b^{2^{t-1}} = -1$ for et $t = 1, \ldots, s$. Venstresiden i (4) er da $b^{u2^{s-1}} = (-1)^{2^{s-t}}$, altså lig med -1, hvis $s = t$, og lig med 1, hvis $t < s$.

Højresiden i (4) Jacobi-symbolet. For at bestemme værdien bestemmes først Legendre symbolet $\big(\frac{b}{p_i}\big)$ for $i = 1, \ldots, k$. Som nævnt medfører ligningen $b^{2^{t-1}} = -1$, at b i gruppen G_i, og dermed også modulo p_i, har orden lig med 2^t. Heraf følger let, at der må gælde $t \leqslant s_i$, og videre, at b modulo p_i er et kvadrat, hvis og kun hvis $t < s_i$. Altså er $\big(\frac{b}{p_i}\big) = 1$, hvis $t < s_i$, og $\big(\frac{b}{p_i}\big) = -1$, hvis $t = s_i$. For højresiden af (4) har vi derfor

$$\Big(\frac{b}{m}\Big) = (-1)^l,$$

hvor l er antallet af de p_i (talt med multipliciteten μ_i), for hvilke $t = s_i$. Tallet $(-1)^l$ bestemmes nu ved regninger modulo 2^{t+1}. Modulo 2^{t+1} gælder nemlig for et ulige tal v, at $v2^t \equiv 2^t$. For hvert p_i fås derfor, at $p_i \equiv 1 \pmod{2^{t+1}}$, hvis $t < s_i$, og $p_i \equiv 1 + 2^t \pmod{2^{t+1}}$, hvis $t = s_i$. Heraf ses, at der modulo 2^{t+1} gælder følgende kongruens:

$$m = \prod_i p_i^{\mu_i} \equiv \prod_{s_i = t} (1 + 2^t)^{\mu_i} = (1 + 2^t)^l \equiv 1 + l2^t \pmod{2^{t+1}}.$$

Da $m - 1 = u2^s$, følger det af kongruensen, at l må være ulige, hvis $t = s$, og at l må være lige, hvis $t < s$. Højresiden af (4) har derfor samme værdi som den ovenfor bestemte værdi af venstresiden.

Hermed er ligningen (4), og dermed Lemma'ets sidste påstand, bevist. ∎

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 $u_i \mid u$ og $s_i = s_0$ for $i = 1, \ldots, k$. At det sidst indtræffer betyder, at s_i'erne er ens og at $p_i - 1 \mid m - 1$ for $i = 1, \ldots, k$. 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 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 primtal og d er større end 1 og primisk med p. Vælg et tal g, der modulo p er en frembringer for gruppen af primiske restklasser modulo p, dvs er af orden $p - 1$. Specielt er g's orden lige, så $g^u \not\equiv 1 \pmod{p}$. Ifølge Den kinesiske Restklassesætning findes et tal b, så at $b \equiv g \pmod{p}$ og $b \equiv 1 \pmod{d}$. Modulo p, og derfor også modulo m, er $x := b^u \not\equiv 1$. Da b øjensynlig er primisk med m og af s-psp$_b$ følger, at der findes en potens af x (endda med en exponent, der er en potens af 2), der modulo m er kongruent med -1. Men det er en modstrid, da x er kongruent med 1 modulo divisoren d i m.

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). ∎

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,

$$\zeta_\chi(s) = \sum_{n \geqslant 1} \frac{\chi(n)}{n^s},$$

hvor $\chi : \mathbb{Z} \to \{0, \pm 1\}$ er en kvadratisk karakter, dvs χ fås ved at udvide en homomorfi $\chi : (\mathbb{Z}/m)^* \to \{\pm 1\}$ med værdien 0 på restklasser, der ikke er primiske med m. Den generaliserede Riemann-hypotese er påstanden om at der også for de 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.

1. Bestem for de første primtal $p = 3, 5, 7, \ldots, 31$ 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.

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.

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 angiver ordenen af restklassen af b.] Vis omvendt, hvis m er et primtal, så er det „let“ at finde et sådant b.

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). Den retmæssige modtager af en hemmelig meddelelse skal, hvis han ønsker det, 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 sitation 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 $1, 2, \ldots, n$, 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 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 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 følgende:

(6.8) Sætning. *Antag, at n er kvadratfri, $n = p_1 \cdots p_r$. Lad $l = \lambda(n)$ være det mindste fælles multiplum af tallene $p_i - 1$. For hvert tal $e \geqslant 1$ gælder da, at afbildningen $E\colon \mathbb{Z}/n \to \mathbb{Z}/n$ bestemt ved*

$$E\colon x \mapsto x^e \pmod{n} \tag{6.8.1}$$

er bijektiv, hvis og kun hvis e er primisk med l. Når e er primisk med l, er den inverse afbildning $D = E^{-1}$ bestemt ved

$$D\colon y \mapsto y^d, \quad \text{hvor } d \geqslant 1 \text{ opfylder, at } de \equiv 1 \pmod{l}. \tag{6.8.2}$$

De bijektive afbildninger af formen (6.8.1) *udgør en gruppe $\mathcal{E}$, og afbildningen, der til et tal e primisk med l knytter afbildningen E, er en isomorfi af gruppen $(\mathbb{Z}/l)^*$ på gruppen $\mathcal{E}$.*

Bevis. Antag først, at e er primisk med l. Da har kongruensen i (6.8.2) en løsning $d \geqslant 1$. Det påstås, at E er bijektiv, med D som den inverse. Det er nok at vise, at ED er den identiske afbildning af $\mathbb{Z}/n$, altså at der for alle hele tal x gælder kongruensen,

$$x^{de} \equiv x \pmod{n}.$$

Tallet n er kvadratfrit. Kongruensen modulo n er derfor opfyldt, hvis og kun hvis den er opfyldt modulo p_i for alle i. Modulo p_i er begge sider lig med 0, hvis p_i går op i x. Antag derfor, at $p_i \nmid x$. Da gælder modulo p_i, at $x^{p_i-1} \equiv 1$. Da $p_i - 1$ går op i l, og l går op i $de - 1$, følger det, at $x^{de-1} \equiv 1 \pmod{p_i}$. Altså er $x^{de} = x^{de-1}x \equiv x \pmod{p_i}$, som ønsket.

Antag i stedet, at e ikke er primisk med l. Da har e en ikke-triviel (prim-)divisor, h, 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. Modulo p_j har kongruensen $x^h \equiv 1 \pmod{p_j}$, og dermed også kongruensen $x^e \equiv 1 \pmod{p_j}$, en ikke-triviel løsning x_0. Ifølge Den kinesiske Restklassesætning kan vi modulo n bestemme x således, at $x \equiv x_0 \pmod{p_j}$ og $x \equiv 1 \pmod{p_i}$ for $i \neq j$. Modulo n er x en ikke-triviel løsning i $\mathbb{Z}/n$ til ligningen $x^e = 1$. Afbildningen E i (6.8.1) er derfor ikke injektiv.

Hermed er sætningens første to påstande bevist. Af beskrivelsen af den inverse følger, at de bijektive afbildninger af formen (6.8.1) udgør en gruppe $\mathcal{E}$. Det er klart, at afbildningen, der til et e primisk med l knytter den bijektive afbildning E, er en homomorfi $(\mathbb{Z}/l)^* \to \mathcal{E}$. Øjensynlig er homomorfien surjektiv. For at vise at den er injektiv, antages, at restklassen af e 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 l. Følgelig er $e \equiv 1 \pmod{l}$. Homomorfiens kerne består derfor kun af det neutrale element 1 i $(\mathbb{Z}/l)^*$. Homomorfien $(\mathbb{Z}/l)^* \to \mathcal{E}$ er derfor en isomorfi. □

(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, $n = pq$. Specielt er $l := \lambda(n)$ så 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

$$de \equiv 1 \pmod{l}. \tag{6.9.2}$$

Hertil hører afbildningerne,

$$E\colon x \mapsto x^e \pmod{n}, \quad \text{og} \quad D\colon y \mapsto y^d,$$

der ifølge (6.8) er permuationer af $\mathbb{Z}/n$, og „hinandens inverse“.

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 (eller parret (n, 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.

(6.10) Bemærkning. Beviset for at afbildningen $D\colon y \mapsto y^d$ i (6.8.2) er den inverse til afbildningen $E\colon x \mapsto x^e$ når $de \equiv 1 \pmod{l}$, udnytter kun, at n er kvadratfri og at l er et multiplum af $p_i - 1$ for alle primdivisorer p_i i n. Det bruges ikke, at l er det mindste fælles multiplum, og vi kan fx erstatte l med produktet af tallene $p_i - 1$. (Derimod indgår værdien $l = \lambda(n)$ naturligvis i bestemmelsen af isomorfien $(\mathbb{Z}/l)^* = \mathcal{E}$.)

I forbindelse med RSA-transformationerne i (6.9) følger det, at tallet $l = \lambda(n)$ i (6.9.1) for eksempel kan erstattes af $\varphi(n) = (p - 1)(q - 1)$.

Antag, mere generelt end i (6.9), at $n = pq$ er et produkt af to primiske faktorer p, q, hvor hver faktor er et pseudoprimtal, dvs et primtal eller et Carmichael-tal. Da er hver primdivisor p_i i n divisor i p eller i q, og følgelig er $p_i - 1$ divisor i $p - 1$ eller i $q - 1$. For et sådant tal n gælder altså konklusionen i (6.9), når l defineres ved (6.9.1), eller ved $l := (p-1)(q-1)$. Forudsætningen om at p og q i (6.9) skal være primtal, er altså et krav, der stilles af hensyn til sikkerheden: det skal være „svært" at bestemme d ud fra n og e.

(6.11) 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 (6.5) 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 $\mathbb{Z}/n$). 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 $D_A(s_A)$.

(6.12) 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.]

(6.13). 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 $\varphi(n)$.

(6.14) 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". □

(6.15). 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 således, at der for alle x, der er primiske med n gælder:*

$$x^f \equiv 1 \pmod{n}. \tag{6.15.1}$$

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 (6.15.1). Nu erstattes f med $f/2$, og det undersøges, om (6.15.1) 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 f, for hvilken betingelsen (6.15.1) er opfyldt med eksponenten $2f$, men ikke med eksponenten f.

Betragt nu gruppen $G := (\mathbb{Z}/n)^*$ og den ved $x \mapsto x^f$ 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 $x \mapsto x^f$ til homomorfien,

$$(x_1, x_2) \mapsto (x_1^f, x_2^f).$$

Valget af f 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 $x^f = \pm 1$. Undergruppen H er en ægte undergruppe af G. Ifølge antagelsen findes nemlig et par (x_1, x_2), så at billedet (x_1^f, x_2^f) ikke er $(1, 1)$. Det kan fx antages, at $x_1^f = -1$. 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 $z := x^f$. 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 (6.14). 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 (6.15) viser, at det må udelukkes, at F kan bestemme f, så at (6.15.1) 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 (6.15.1), er bestemt ved

$$(f, p - 1) \cdot (f, q - 1).$$

Antallet er således lille, med mindre f er meget speciel (og det er et „tilfældigt" tal f ikke).

(6.16) 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 (6.15) 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.

(6.17). 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

$$b^{n-1} \equiv 1 \pmod{n}. \tag{6.17.1}$$

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 $j = 1, \ldots, s-1$ 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 (6.14) 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 $(p-1, q-1)$, og produktet er derfor 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.

(6.18) Angreb. *Hvis F ved iteration af krypteringstransformationen $E\colon x \mapsto x^e$ 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 $E^{i-1}E = E^i = 1$ 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 $E\colon x \mapsto x^e$. 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 (6.19) 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.

(6.19) 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,

$$G = G' \times G'' \tag{6.19.1}$$

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 (6.19.1) 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. ∎

(6.20). 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 $E: x \to x^e$, 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

$$\big[1 + (e-1, p-1)\big] \cdot \big[1 + (e-1, q-1)\big].$$

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.

(6.21) Bemærkning. Der findes mange andre foreslåede systemer for udveksling af hemmelige meddelelser mellem en kreds af brugere. Som nævnt indgår i systemerne 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. Videre vælges tilfældigt et tal 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 g^{ν_A}. Det er det diskrete log-problem, at „ingen" udfra g^ν er i stand til at bestemme ν. Nøglen, der skal benyttes ved kommunikation mellem brugerne A og B er herefter tallet $\kappa = g^{\nu_A \nu_B}$. Dette tal kan begge beregne: A kan opnå det ved at opløfte det offentlige g^{ν_B} til sin hemmelige eksponent ν_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 $(g^\alpha, tg^{\nu_B \alpha})$, hvor α er en afsenderen tilfældigt valgt eksponent. Tallet $g^{\nu_B \alpha}$ kan beregnes af afsenderen, som kender α og det offentlige tal g^{ν_B}, og af B, som modtager g^α og kender sin egen eksponent ν_B. Herefter kan B dekryptere: $t = (tg^{\nu_B \alpha}) \cdot (g^{\nu_B \alpha})^{-1}$.

(6.22) 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.

(6.23) 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-komplette" problemer. Et eksempel på et NP-komplet problem er 'knapsack' (rygsæk-problemet): Der er givet et sæt af positive tal v_i (rumfang) for $i = 1, \ldots, k$ og et positivt tal V (rygsækkens rumfang). Bestem, om muligt, en delmængde I af tallene $1, \ldots, k$ således, at $V = \sum_{i \in I} v_i$. En løsning kan angives ved en følge af bits $(t_1, \ldots, t_k)$ 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 $v_i > \sum_{j<i} v_j$. 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 $(v_1, \ldots, v_k)$, 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 $w_i = av_i$. Krypteringstransformationen E_A er herefter afbildningen,

$$t = (t_1, \ldots, t_k) \mapsto W = \sum_{i=1}^{k} t_i w_i.$$

Klarteksten t på venstresiden sendes altså til A som tallet W på højresiden. A kan dekryptere: ved multiplikation modulo m af W med b fremkommer $V = \sum_{i=1}^{k} t_i v_i$; 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 fra $W = \sum_{i=1}^{k} t_i w_i$.

Det skal understreges, at fjendens problem naturligvis *ikke* er det helt generelle knakpsack-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.

(6.24) Opgaver. 1. Antag, for et givet $e > 1$, at $x \mapsto x^e$ er bijektiv modulo n. Vis, at n må være kvadratfri.

2. Vis, modulo 95, at afbildningen $x \mapsto x^7$ er bijektiv, og angiv den inverse.

3. Hvorfor står der, i kommentaren til *simpelhed*, at modtageren skal kunne dekode, „hvis han ønsker det“?

4. Min offentlige RSA-nøgle er $(33, 7)$. Restklasserne $0, \ldots, 32$ modulo 33 fortolkes som de 29 danske bogstaver efterfulgt af de 4 specialtegn: ‘.’, ‘,’, ‘!’, ‘?’. En student sender mig h-teksten ÅPFLØE. Hvad var klarteksten?

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 $q = 2, 3, 4, 5, \ldots$ 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 uafhængigig 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 $s := s_0 + 1, s_0 + 2, \ldots$ 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 $c = 1, 2, 3, \ldots$.

(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 $x_0, x_1, \ldots$. 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 $i > 0$ og hertil et $j < i$, så at der modulo n gælder kongruensen,

$$x_i \equiv x_j. \qquad (*)$$

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 $(x_i - x_j, n)$ 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 $x_0, x_1, \ldots, x_l$ 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 bestemt ved

$$\frac{q(q-1)\cdots(q-l)}{q^{l+1}} = \prod_{\nu=1}^{l}(1 - \frac{\nu}{q}).$$

Som bekendt gælder for $0 < x < 1$, at $\log(1-x) < -x$. Logaritmen af brøkdelen kan derfor vurderes:

$$\sum_{\nu=1}^{l} \log(1 - \frac{\nu}{q}) < \sum_{\nu=1}^{l} (-\frac{\nu}{q}) = \frac{-l(l+1)}{2q} < \frac{-l^2}{2q}\,.$$

Lad nu $\varepsilon > 0$ være givet. Af vurderingerne ovenfor fremgår, at brøkdelen er mindre end ε, når blot $-l^2/2q \leqslant \log \varepsilon$, dvs når $l \geqslant l_\varepsilon(q)$, hvor

$$l_\varepsilon(q) := \sqrt{2q \log(1/\varepsilon)} \tag{1}$$

Heraf fås:

Observation. *Hvis $l \geqslant l_\varepsilon(q)$, så vil en tilfældig følge $x_0, \ldots, x_l$ med sandsynlighed større end $1 - \varepsilon$ indeholde en gentagelse modulo q.*

Denne observation er baggrund for følgende algoritme: Frembring modulo n en følge $x_0, x_1, x_2, \ldots$ af tilfældige tal. Bestem i det i'te skridt den største fælles divisor $(x_i - x_j, n)$ for alle $j = 0, \ldots, i-1$. 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 i, der højst er konstanten $\sqrt{2\log(1/\varepsilon)}$ ganget med

$$\sqrt[4]{n}.$$

Algoritmen er aldeles uanvendelig i praksis: Der er dels et pladsproblem, idet der i det i'te skridt skal bestemmes den største fælles divisor $(x_i - x_j, n)$ for alle $j < i$, hvilket kræver, at alle x_j'erne gemmes under forløbet. Men først og fremmest er problemet, at antallet af beregninger vokser med i: i det i'skridt skal der foretages i beregninger af en største fælles divisor. For antallet af beregninger fås derfor vurderingen $1 + 2 + \cdots + (l_\varepsilon - 1) < l_\varepsilon^2/2$, som kun kan vurderes 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 $x_0, x_1, \ldots$ 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 højst $l_\varepsilon(q)$ skridt indeholder en gentagelse i_0. Der findes altså et $j_0 < i_0$, så at den største fælles divisor $(x_{i_0} - x_{j_0}, n)$ er større end 1. Og med god 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 $x_{i_0} \equiv x_{j_0}$, at $f(x_{i_0}) \equiv f(x_{j_0})$, altså at $x_{i_0+1} \equiv x_{j_0+1}$, og videre (induktivt), at $x_{i_0+k} \equiv x_{j_0+k}$. Efter den første gentagelse i skridt nummer i_0 er der altså en gentagelse i hvert eneste skridt. Heraf ses imidlertid, at der findes en gentagelse $x_i \equiv x_j$, hvor j har formen $j = 2^h - 1$ og $j < i < 2(j+1)$. Vælges nemlig h så at $2^{h-1} \leqslant i_0 < 2^h$, og sættes $j := 2^h - 1$, så er $j = j_0 + (j - j_0)$ og betingelsen er opfyldt for $i := i_0 + (j - j_0)$.

I stedet for i hvert skridt i at undersøge for alle $j < i$, om x_i er en gentagelse af x_j, er det altså nok for hvert i at undersøge, om x_i er en gentagelse af x_{2^h-1}, hvor h er bestemt ved at $2^h \leqslant i < 2^{h+1}$. De i bestemmelser af en største fællses divisor i det i'te skridt kan altså erstattes af en enkelt, og af x_j'erne for $j < i$ 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 i_0 forekommer efter højst l_ε skridt, så vil algoritmen afsløre en gentagelse efter et antal skridt, der højst er $i_0 + (j - j_0) < 2^h + 2^h - 1 < 4 \cdot 2^{h-1} < 4i_0 \leqslant 4l_\varepsilon$.

Pollard's ρ-algoritme. *Input: et ulige, sammensat tal n. Registre:* **x**, **i**, **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* $\mathbf{i} \leftarrow 0$ *og* $\mathbf{x} \leftarrow 2$.
ρ**2** Iteration. *Sæt* $\mathbf{i} \leftarrow \mathbf{i} + 1$. *Hvis* **i** *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 $4l_\varepsilon$, hvor l_ε er bestemt ved (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. 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 $n = p_1p_2$, og som output leverer divisoren q i n, samt skridtantallet. Hvorfor stopper det? Hvad sker, når $p_1 = 23$, $p_2 = 29$? **2.** „Rent Monte Carlo" er det naturligvis, for et givet 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.

8. Lidt om Möbius-funktionen.

(8.1). For to funktioner $\alpha, \beta : \mathbb{N} \to \mathbb{C}$ (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 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 $\mathcal{D}_{\mathbb{Z}}$). Mere generelt, for hver given kommutativ ring R udgør afbildningerne $\alpha : \mathbb{N} \to R$, med tilsvarende kompositioner, en kommutativ ring $\mathcal{D}_R$.

Bemærk, at den konstante funktion $\mathbf{1}$ (bestemt ved $\mathbf{1}(n) = 1$) *ikke* er et-elementet i $\mathcal{D}$. 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 $\alpha : \mathbb{N} \to R$ 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 muliplikativ*.

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 $\alpha : \mathbb{N} \to R$ er invertibel i ringen $\mathcal{D}_R$, hvis og kun hvis $\alpha(1)$ er invertibel i R. De multiplikative funktioner $\alpha : \mathbb{N} \to R$ 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 $\sum_{d|n} \alpha(n/d)\xi(d) = 0$ for $n > 1$. Den første ligning kan opfyldes, hvis og kun hvis $\alpha(1)$ er invertibel i R. Den anden ligning kan omformes:

$$\alpha(1)\xi(n) = -\sum_{d|n,\, d<n} \alpha(n/d)\xi(d). \tag{8.3.1}$$

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

$$(\alpha * \beta)(nm) = \sum_{d|n,\, e|m} \alpha(nm/de)\beta(de)$$
$$= \sum_{d|n} \alpha(n/d)\beta(d) \sum_{e|m} \alpha(m/e)\beta(e) = (\alpha * \beta)(n)(\alpha * \beta)(m).$$

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 **1**, kaldes *Möbius-funktionen*. Den er altså bestemt ved $\mathbf{1} * \mu = 1_{\mathcal{D}}$, altså ved ligningerne:

$$\mu(1) = 1, \quad \text{og} \quad \sum_{d|n} \mu(d) = 0, \text{ når } n > 1.$$

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 delmænger 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 $k = 1, \ldots, n$. Ethvert $k = 1, \ldots, n$ 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 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 $\alpha : \mathbb{N} \to \mathbb{Z}$ har heltalsværdier og $\psi : \mathbb{N} \to G$ 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 $\Psi, \psi : \mathbb{N} \to G$ 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 brøklegmet $\mathbb{Q}(X)$. 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,

$$\sum_{k \leqslant x} (\alpha * \beta)(k) = \sum_{k \leqslant x} \sum_{d|k} \alpha(d)\beta(k/d) = \sum_{d \leqslant x} \alpha(d) \sum_{q \leqslant x/d} \beta(q).$$

Som eksempel betragtes summen $\sum_{k \leqslant N} \varphi(n)$. 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 $\sum_{q \leqslant x} q = \frac{1}{2}[x]\big([x] + 1\big)$, og dermed er

$$2\sum\nolimits_{q \leqslant x} q - x^2 = [x] - \big(x - [x]\big)\big(x + [x]\big) =: S(x). \tag{2}$$

I udtrykket for funktionen $S(x)$ ligger faktoren $x - [x]$ mellem 0 og 1. Heraf ses, at $|S(x)| \leqslant x$. Af (1) og (2) fås følgende ligning:

$$2\sum\nolimits_{k \leqslant N} \varphi(k) - \sum\nolimits_{d \leqslant N} \mu(d)(N/d)^2 = \sum\nolimits_{d \leqslant N} \mu(d) S(N/d). \tag{3}$$

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. Antallet af primiske par (k,l) med $k \geqslant l$ er nemlig $\sum_{k\leqslant N}\varphi(k)$, 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. Videre gælder som bekendt, at $\zeta(2) = \sum d^{-2} = \pi^2/6$; heraf følger, at $6/\pi^2 = 1/\zeta(2) = \sum_d \mu(d)d^{-2}$. Af (3) får vi derfor ligningen,

$$p_N - 6/\pi^2 = \frac{1}{N^2}\Big(-1 + \sum_{d\leqslant N}\mu(d)S(N/d)\Big) - \sum_{d>N}\mu(d)d^{-2}. \tag{4}$$

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 $\sum_{d\leqslant N} N/d \leqslant N(1+\log N)$. Sammenligning med $\int_N^\infty t^{-2}dt = 1/N$ viser, at den anden sum på højresiden af (4) numerisk højst er $1/N$. Ved addition fremkommer den påståede ulighed (8.10.1). ∎

(8.11) Opgaver.

1. Vis følgende uligheder (den første kun for $n > 1$),

$$2 \leqslant \tau(n) < 2\sqrt{n}, \qquad n \leqslant \sigma(n) < 2n\sqrt{n},$$
$$n^2/2 \leqslant \varphi(n)\sigma(n) < n^2, \qquad \sqrt{n}/4 < \varphi(n) \leqslant n.$$

[Vink (til 3. 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 på højresiden er mindre end 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 $\zeta(2)^{-1} = 6/\pi^2$.]

2. Vis, at udtrykket i formlen (8.9.1) for $\alpha_p(n)$ er positivt for alle n, også når $p > 1$ ikke er et primtal.

3. Bestem grænseværdien $\lim a_N/N^2$, hvor a_N er antallet af Farey-brøker af orden N.

9. Funktionalligningen for Riemann's zeta-funktion.

(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 $\Gamma(s) = \frac{1}{s}\Gamma(s+1)$ 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:

$$z^s = e^{s \log z} = e^{s(\log|z| + i \arg z)} = |z|^s e^{i s \arg z}. \tag{9.1.3}$$

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 ikke er negativ reel, vil vi altid 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 to lige gode muligheder:

$$z^s = \begin{cases} t^s e^{i\pi s}, \\ t^s e^{-i\pi s}. \end{cases}$$

Den første mulighed vælges naturligt, når z opfattes som et randpunkt for den øvre halvplan ($\mathcal{I}m\, z > 0$), den anden, når z opfattes som et randpunkt for den nedre halvplan.

Af definitionen får vi umiddelbart for modulus:

$$|z^s| = |z|^{\mathcal{R}e\, s} e^{-\mathcal{I}m\, s \arg z} \leqslant |z|^{\mathcal{R}e\, s} e^{\pi |\mathcal{I}m\, s|}, \tag{9.1.4}$$

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,

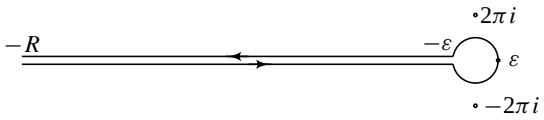
$$I(s) := \frac{1}{2\pi i} \oint_{-\infty}^{-\infty} \frac{z^s}{e^{-z}-1} \frac{dz}{z}. \tag{9.2.1}$$

Polerne for integranden er nulpunkterne for $e^{-z}-1$, altså tallene $2\pi ik$ 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 $\mathcal{R}e\, s > 0$,

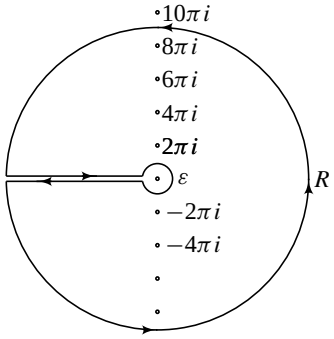
$$\Gamma(s) = n^s \int_0^{\infty} t^s e^{-nt}\frac{dt}{t}.$$

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 cirlen 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 $f(z) = z^s/[(e^{-z} - 1)z]$ i området D_R. Polerne er tallene $a = \pm 2\pi ni$. 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

$$\frac{1}{2\pi i}\int_{|z|=R} f(z)\,dz - \frac{1}{2\pi i}\oint_{-R}^{-R} f(z)\,dz = \sum \mathrm{Res}_{z=a}\, f(z), \tag{2}$$

hvor summen er over alle poler a i området D_R, altså tallene $a = \pm 2\pi in$ for $1 \leqslant n \leqslant N$. Funktionen $1/(e^{-z} - 1)$ har residuet -1 i $z = 0$ og dermed også i $\pm 2\pi in$. Funktionen $f(z)$ har derfor i $a = 2\pi in$ residuet:

$$-(2\pi in)^s/(2\pi in) = -(2\pi n)^{s-1}e^{is\pi/2}/i\,,$$

og i $a = -2\pi in$ er residuet tilsvarende $-(2\pi n)^{s-1}e^{-is\pi/2}/(-i)$. Summen af de to residuer svarende til $a = \pm 2\pi in$ bliver altså $-(2\pi n)^{s-1}2\sin(\pi s/2)$, og højresiden i (2) er summen,

$$-2\sin(\pi s/2)\sum_{1\leqslant n\leqslant N}(2\pi n)^{s-1}. \tag{3}$$

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 $0, -1, -2, \ldots$ og $\Gamma(1-s)$ har (derfor) simple poler i $1, 2, \ldots$. Af ligningen følger derfor, at $\Gamma(s)$ ikke har nulpunkter. Ækvivalent har $\Gamma(s)^{-1}$ simple nulpunkter i $0, -1, -2, \ldots$, 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 $z^{k-1}/(e^{-z}-1) = \sum_n (-1)^{n-1}(B_k/k!)z^{k+n-2}$, 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 $k = 1, 2, \ldots$.

Bemærk, at ligning (9.4.3) ikke giver information om værdierne $\zeta(k)$ for $k = 1, 2, \ldots$, 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), $s = 1, 2, \ldots$, og de er simple nulpunkter. Da $I(s)$ også har nulpunkter for $s = 2, 3, \ldots$, 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 $\operatorname{Res}_{s=1}\zeta(s) = 1$.
4. Bestem værdierne $\zeta(2)$ og $\zeta(4)$.
5. Vis, at $\zeta(s)$ er reel for alle reelle værdier af $s \neq 1$.

I. Index.