STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 31

Elementaire getallentheorie.

Cursus den Haag 1954/55.

B.Meulenbeld en S.C.van Veen.

1955

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM-O.
TELEF. 51660-56643

Elementaire getallentheorie

1954/55

door

Prof.Dr B. Meulenbeld en Prof.Dr S.C. van Veen

Aanbevolen literatuur: E Landau, Vorlesungen über Zahlentheorie, deel I.
G.H. Hardy en E.M. Wright, An introduction in the theory of number.

De getallen ....-3, -2, -1, 0, 1, 2... gehele rationale getallen, kortweg gehele getallen; de getallen 0,1,2,3,.... de niet-negatieve gehele, en de getallen 1,2,3,.....de positieve gehele getallen.

Als a geheel is, is ook -a geheel. Met a en b zijn ook a+b, a-b en ab geheel. Uit $a > b$ volgt $a \geqq b+1$.

Definitie: Zij $a \neq 0$, b willekeurig. b heet door a deelbaar, als er een geheel getal q bestaat met $b = qa$.
b heet dan een veelvoud van a, a is een deler van b.
Schrijfwijze: a/b. Is b niet deelbaar door a, dan schrijft men $a \not/ b$.

De volgende stellingen zijn eenvoudig te bewijzen:

1. Uit a b volgt: $a/-b$; $-a/b$; $|a| / |b|$.
2. Uit a/b en b/c volgt a/c. (de deelbaarheid is transitief)
3. Uit ac/bc volgt a/b, en omgekeerd: uit a/b en $c \neq 0$ volgt ac/bc.
4. Uit a/b volgt a/bx voor elke x.
5. Uit a/b, a/c volgt: $a/b+c$ en $a/b-c$.
6. Uit a/b en a/c volgt $a/bx+cy$.
7. Is $a > 0$ en b willekeurig, dan bestaat er precies één paar getallen (q,r) met $b = aq+r$, $0 \leqq r < a$. Kortweg: deeltal = deler x quotiënt + rest. ($0 \leqq$ rest $<$ deler)

Stelling (ontwikkeling in g-tallig stelsel)

Zij $g > 1$. Elk getal $a > 0$ kan men op één en slechts één manier schrijven in de vorm:

$$a = c_0 + c_1 g + c_2 g^2 + \ldots + c_n g^n$$

met

$$n \geqq 0,\ c_n > 0,\ 0 \leqq c_i < g \quad (0 \leqq i \leqq n)$$

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

Bewijs. 1) de mogelijkheid. Wij bewijzen dit met volledige inductie naar a. Voor a = 1 duidelijk. Stel voor a > 1 en 1,2...,a-1 is de stelling bewezen. a ligt dan zeker in één der intervallen:

$$1 \leqq a < g,\ g \leqq a \leqq g^2,\ g^2 \leqq a \leqq g^3, \text{ enz.}$$

Er is dus een $n \geqq 0$ met $g^n \leqq a \leqq g^{n+1}$. Dan is $a = c_n g^n + r$ $(0 \leqq r < g^n)$. Hierin is $c_n > 0$, want $c_n g^n = a - r > g^n - g^n = 0$; en $c_n < g$, want $c_n g^n \leqq a < g^{n+1}$. Is $r = 0$, dan klaar. Is $r > 0$ dan wegens $r < g^n \leqq a$ (inductie) $r = b_0 + b_1 g + \ldots + b_t g^t$ $(t \geqq 0$, $b_t > 0$, $0 < b_i < g$ $(0 \leqq i \leqq t)$. Hierin is $t < n$, daar $g^n > r \geqq b_t g^t \geqq g^t$, dus

$$a = b_0 + b_1 g + \ldots + b_t g^t + 0 \cdot g^{t+1} + \ldots + 0 \cdot g^{n-1} + c_n g^n.$$

2. Eenduidigheid.

Zij $a = c_0 + c_1 g + \ldots + c_n g^n = d_0 + d_1 g + \ldots + d_r g^r$, dan te bewijzen:

$$n = r \text{ en } c_i = d_i \ (0 \leqq i \leqq n).$$

Was dit niet het geval, dan zou

$$0 = e_0 + e_1 g + \ldots + e_s g^s \ (s > 0,\ e_s \neq 0,\ -g < e_i < g,\ 0 \leqq i \leqq s)$$

dus

$$g^s \leqq |e_s g^s| = |e_0 + \ldots + e_{s-1} g^{s-1}| = (g-1)(1+g+\ldots+g^{s-1}) = g^s - 1$$

Tegenspraak.

Kleinst gemene veelvoud. Zij $a > 0$, $b > 0$. Onder al de gemeenschappelijke veelvouden van a en b zij m het kleinste positieve.

Stelling. Zij n een willekeurig veelvoud van a en b. Dan is m/n.

Bewijs. q en r zijn te bepalen zodat $n = qm + r$ $(0 \leqq r < m)$. $r = n - qm$. Nu is a/n en a/m, dus a/r. Evenzo: b/r . r is dus een kleiner gemeenschappelijk veelvoud van a en b dan m, dus $r = 0$.

Stelling. Is $a \neq 0$. b/a dan is $|b| \geqq |a|$.

Bewijs. b/a, dus $a = qb$ met $q \neq 0$, dus $|q| \geqq 1$, en $|a| = |q|\,|b| \geqq |b|$. Hieruit volgt: Elk getal $a \neq 0$ heeft slechts een eindig aantal delers.

Grootst gemene deler. Laten a en b niet beide 0 zijn. Onder de gemeenschappelijke delers van a en b zij d de grootste positieve. Deze bestaat, want minstens een der beide getallen a en b heeft een eindig aantal delers, en 1 is zeker een gemeenschappelijke deler. Schrijfwijze: (a,b).

Stelling. 1) Zij f een gemeenschappelijke deler van a en b , dan is f/d.

2) Als $a > 0$, $b > 0$ en m het K.G.V. van a en b, dan

is md = ab.

Bewijs. I Zij $a>0$ $b>0$. ab is gem. veelvoud, dus m/ab of ab = mg (g = geheel). Zullen bewijzen: g = d.
Uit f/a, f/b volgt $\frac{a}{f}$ geheel, $\frac{b}{f}$ geheel, dus a/ $\frac{ab}{f}$ en b/$\frac{ab}{f}$.
Dus m/ $\frac{ab}{f}$ of $\frac{ab}{g}$ / $\frac{ab}{f}$. Dus $\frac{ab}{f} : \frac{ab}{g} = \frac{g}{f}$ geheel of f/g.
Verder is $\frac{a}{g} = \frac{m}{b}$ = geheel, $\frac{b}{g} = \frac{m}{a}$ = geheel, dus g/a en g/b.
g is dus gemeenschappelijke deler voor a en b; en elke gemeenschappelijke deler f gaat in g op en $|f| \leqq |g|$. Dus g = d.

II. Is $a \neq 0$ $b \neq 0$, maar niet $a>0$, $b>0$, dan bedenke men dat |a| dezelfde deler heeft als a, |b| dezelfde als b, dus is ook d juist de G.G.D. van |a| en |b|.

III. Is een van beide getallen a en b nul, bijv. a = 0, dus $b \neq 0$. Dan is d = |b|, en volgt uit f/0, f/b weer f/d.

Is (a.b) = 1, dan heten a en b onderling ondeelbaar.
Gemakkelijk bewijst men:
Stelling. Uit (a,b)= d volgt $(\frac{a}{d}, \frac{b}{d}) = 1$. en omgekeerd.
Uit $c>0$ c/a, c/b en $(\frac{a}{c}, \frac{b}{c}) = 1$ volgt c = (a,b).
Hiermede bewijst men de voorname stelling:
Stelling. Uit a/bc en (a,b) = 1 volgt a/c.
Bewijs. $a \neq 0$. 1) Is b = 0, dan is a = 1, dus a/c.
2) Is $b \neq 0$ en is m het K.G.V. van |a| en |b|, dan is m.1 = |a| |b| . bc is dus een gemeenschappelijk veelvoud van |a| en van |b|, dus m/bc of |a| |b| / bc of ab/bc of a/c. Hieruit volgt direct:
Stelling. Uit $a/a_1 \ldots a_n$ en $(a,a_i) = 1$ $(1 \leqq i < n)$ volgt a/a_n.
Elk getal $a>1$ heeft minstens 2 positieve delers nl. 1 en a.
Definitie. Elk getal $a>1$ heet priemgetal, als dit slechts twee positieve delers 1 en a heeft. Gebruiken voor priemgetallen steeds p, p', p_1, p_2, enz. Het getal 1 wordt niet als priemgetal gerekend. Een getal > 1 dat niet priemgetal is, heet samengesteld getal.
Stelling. Elk getal $a>1$ is steeds voor te stellen als een product van priemgetallen. $a = \prod_{n=1}^{r} p_n$ $(r = 1)$.
Bewijs. (voor volledige inductie). Voor a = 2 is de stelling duidelijk. Zij $a>2$ en de stelling bewezen voor $2,3,\ldots,a-1$.
Is a priem, dan is de stelling triviaal. Is a samengesteld, dan kunnen wij schrijven: $a = a_1 a_2$, $1 < a_1 < a$, $1 < a_2 < a$.
volgens inductie kunnen a_1 en a_2 in priemfactoren worden ontbonden.
Is n = ab, dan kunnen niet beide factoren a en b groter

zijn dan $\sqrt{n}$. Elk samengesteld getal is dus deelbaar door een priemgetal dat niet groter is dan $\sqrt{n}$.

Stelling. Er zijn oneindig veel priemgetallen.

Bewijs. (van Euclides). Laat $2,3,5,\ldots,p$ de verzameling zijn van priemgetallen tot en met p zijn, dan beschouwen we

$$a = 2.3.5\ldots p+1.$$

a is niet deelbaar door een van de priemgetallen $2.3.5\ldots p$. Dus òf a is zelf priem, of deelbaar door een priemgetal groter dan a.

De volgende stellingen zijn weer eenvoudig te bewijzen.

Stelling. Is $p \nmid a$, dan is $(p,a) = 1$.

Stelling. Is $p/a_1\ldots a_n$, dan is voor minstens voor één i p/a_i.

Stelling. Is $p/p_1\ldots p_n$ dan is voor minstens één i $p=p_i$.

Hoofdstelling. De ontbinding in priemfactoren

$$a = p_1 p_2,\ldots,p_n$$

van elk getal $a > 1$, is op de volgorde van de factoren na eenduidig:

Bewijs. We moeten bewijzen dat uit $a = p_1 p_2,\ldots p_n = p_1' p_2' \ldots p_n'$ $p_1 \leqq p_2 \leqq \ldots \leqq p_n$, $p_1' \leqq p_2' \leqq \ldots \leqq p_n'$ volgt $n = n'$, $p_i = p_i'$ $(1 \leqq i \leqq n)$.

I. Voor $a = 2$ is de bewering juist. $n = n' = 1$, $p_1 = p_1' = 2$.

Zij voor $a > 2$ de bewering voor $1,2,\ldots, a-1$ bewezen. Is a priemgetal, dan is de bewering triviaal.

Is a samengesteld, dan is $n > 1$. $n' > 1$. Uit $p_1'/p_1\ldots p_n$ en $p_1/p_1' \ldots p_n'$ volgt, dat voor minstens één i en voor minstens één j geldt $p_1' = p_i$, $p_1 = p_j'$. Nu is

$p_1 \leqq p_i = p_1' \leqq p_j' = p_1$, dus $p_1 = p_1'$. Daar $1 < p_1 < a, p_1/a$ is dus

$1 < \frac{a}{p_1} = p_2 p_3,\ldots,p_n = p_2' p_3' \ldots p_n' < a$. Dus volgens inductie-onderstelling $n-1 = n'-1$ of $n = n'$, en $p_i = p_i'$ $(2 \leqq i \leqq n)$.

Gevolg. Elk getal $a > 1$ is dus van de vorm

$$a = \prod_{p/a} p^{l}$$

waarin p de verschillende in a bevatte priemgetallen doorloopt.

De eerste priemgetallen zijn:

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

Men kan een tabel van deze priemgetallen construeren, die niet groter zijn dan N, met behulp van de z.g. "zeef van Eratosthenes".

Voor elke n $\leq$ N, en n niet priem, is n deelbaar door een priemgetal dat niet groter is dan $\sqrt{N}$. We schrijven nu alle getallen op 2,3,4,5,6,...,N en strepen achtereenvolgens door:

4,6,8,10,... dus 2^2 en verder elk 2-voud,

9,15,21,... dus 3^2 en verder elk nog niet doorgestreept 3-voud.

enz.

We zetten dit proces voort, totdat het getal waarvan de veelvouden doorgestreept worden groter wordt dan $\sqrt{N}$.

Elementaire Getallentheorie II

door Prof.Dr B.Meulenbeld en Prof.Dr S.C.v.Veen

Stelling. Het aantal delers van $a=p_1^{l_1}\ldots p_n^{l_n}$ bedraagt $(l_1+1)\ldots(l_n+1)$.

Getallentheoretische functies.

Definitie. Elke functie F(a) die voor elke gehele $a>0$ is gedefinieerd, heet getallentheoretische functie.

Voorbeelden: $F(a)=a!$; $F(a)=\cos a$; $F(a)=\frac{1}{a^4+1}$, enz.

De som van de positieve delers van $a>0$ noemen we S(a).

Stelling: Is $a>1$ en $a=\prod_{p/a} p^l$, dan is

$$S(a)=\prod_{p/a}\frac{p^{l+1}-1}{p-1}\ .$$

Bewijs. Telt men de delers op, dan vindt men

$$(1+p_1+..+p_1^{l_1})(1+p_2+..+p_a^{l_2})\ldots(1+p_n+..+p_n^{l_n})=\prod_{p/a}\frac{p^{l+1}-1}{p-1}\ .$$

Definities.

1) Elke positieve deler van a, behalve a, heet echte deler van a. 15 heeft als echte delers 1,3,5.
2) a heet even als $2/a$, oneven als $2\nmid a$. 0 is even. Van twee op elkaar volgende natuurlijke getallen is er een even en een oneven. Elke $p>2$ is oneven.
3) a heet volkomen getal, als a= som van de echte delers van a, dus als $S(a)=2a$.

Voorbeelden: $6=1+2+3$, $28=1+2+4+7+14$, enz.

Stelling: Is $p=2^n-1$ (dus $n>1$), dan is $a=\frac{p+1}{2}\,p=2^{n-1}(2^n-1)$ een volkomen getal, en anders zijn er geen even volkomen getallen

Bewijs a) $S(a)=S\{2^{n-1}(2^n-1)\}=\frac{2^n-1}{2-1}\cdot\frac{p^2-1}{p-1}=(2^n-1)2^n=2a$.
a is dus volkomen.

b) Is a een volkomen even getal, dan is

$a=2^{n-1}u$, $n>1$, $u>0$ en oneven
dus $2^nu=2a=S(a)=\frac{2^n-1}{2-1}S(u)=(2^n-1)S(u)$.

$$S(u)=\frac{2^nu}{2^n-1}=u+\frac{u}{2^n-1}\ .$$

$\frac{u}{2^n-1}=S(u)-u$ is geheel, dus wegens $n>1$ een echte deler van u. De som $S(u)$ is gelijk aan de som van u en een echte deler. Dus u is priem en de echte deler $\frac{u}{2^n-1}=1$ of $u=2^n-1$.

Dus $a=2^{n-1}(2^n-1)$.

Men weet niet of er oneindig veel even volkomen getallen zijn, dus of er oneindig veel getallen n zijn, waarvoor 2^n-1 priem is. Voor n=4 is 2^n-1 niet priem. Voor n= niet-priem is 2^n-1 samengesteld. n=5 geeft volkomen getal 496=16.31. n=7 8128. Voor n=11 is $2^n-1=2047=23.89$, levert dus geen volkomen getal.

Mersenne beweerde in 1644 dat $M_p=2^p-1$ priem is voor p=2,3,5,7,13,17,19,31,67,127,257 en voor de overige tussengelegen waarden van p samengesteld. Dit is echter onjuist, daar in 1886 Pervusin en Seelhoff ontdekten, dat M_{61} priem is, en in 1903 bewees Cole dat $M_{67}=193707721.761838257287$ samengesteld is. Men weet nu dat Mp priem is voor p=2,3,5,7,13,17,19,31,61,89,107,127 en samengesteld voor de andere waarden van $p\leqq 257$, behalve voor p=157,167,193,199,227,229 waarvan men de aard niet kent.

Deze getallen noemt men de <u>getallen van Mersenne</u>. Men weet niet of er zelfs een oneven volkomen getal is.

De getallen van <u>Fermat</u> zijn gedefinieerd door

$$F_n=2^{2^n}+1, \text{ zodat } F_1=5,\ F_2=17,\ F_3=257, \text{ enz.}$$

Deze getallen spelen een rol in de cirkeldelingstheorie. Gauss bewees dat als F_n priem p is, er een regelmatige p-zijdige veelhoek in een cirkel kan geconstrueerd worden met passer en lineaal.

<u>Stelling</u>: Geen twee Fermat-getallen hebben een G.G.D. > 1.

<u>Bewijs</u>. Stel m/F_n, m/F_{n+k} $(k>0)$.

Is $x=2^{2^n}$, dan is $\dfrac{F_{n+k}-2}{F_n}=\dfrac{2^{2^{n+k}}-1}{2^{2^n}+1}=\dfrac{x^{2^k}-1}{x+1}=$ geheel

dus $F_k/F_{n+k}-2$. Uit m/F_{n+k} en $m/F_{n+k}-2$ zou volgen m/2, en daar F_n oneven is, is m=1.

De eerste vier Fermat-getallen zijn priem, en Fermat vermoedde dat ze alle priem waren. Euler vond echter in 1732, dat $F_5=2^{2^5}+1=641.6700417$. Later is bewezen dat F_n samengesteld is voor n=7,8,9,11,12,15,18,23,36,38,73.

<u>Functie van Möbius</u>: De getallentheoretische functie $\mu(a)$ van Möbius wordt gedefinieerd door:

$$\mu(a)=\begin{cases} 1 \text{ voor } a=1 \\ (-1)^n, \text{ in het geval dat a het product is van } n(\geqq 1) \text{ verschillende priemgetallen.} \\ 0, \text{ overigens, d.i. als a minstens een priemgetalkwadraat bevat.} \end{cases}$$

<u>Voorbeelden:</u> $\mu(1)=1$, $\mu(2)=-1$, $\mu(3)=-1$. In 't algemeen $\mu(p)=-1$, $\mu(4)=0$, $\mu(6)=1$, $\mu(8)=0$, $\mu(9)=0$, $\mu(10)=1$, enz.

<u>Stelling</u>. Voor a > 0, b > 0, (a,b)=1 geldt $\mu(ab)=\mu(a)\mu(b)$.

<u>Bewijs</u>. a) Is a of b niet kwadraatvrij, dan is ab dit ook niet. Dus

$$\mu(ab)=0=\mu(a)\mu(b).$$

b) Zijn a en b kwadraatvrij, dan is wegens (a.b)=1 ook ab kwa-

draatvrij. Is a=1 of b=1, dan stelling triviaal. In de andere gevallen is het aantal priemfactoren van ab gelijk aan de som van de aantallen priemfactoren van a en b.

Stelling. $\sum_{d/a} \mu(d) = \begin{cases} 1 \text{ voor } a=1 \\ 0 \text{ voor } a>1 \end{cases}$

Bewijs. a) $\sum_{d/1} \mu(d) = \mu(1) = 1$.

b) Is $a>1$ en $a = p_1^{l_1} \ldots p_n^{l_n}$, dan is

$$\sum_{d/a} \mu(d) = \sum_{d/p_1 \ldots p_n} \mu(d) = 1 + \binom{n}{1}(-1) + \binom{n}{2}(-1)^2 + \binom{n}{3}(-1)^3 + \ldots + \binom{n}{n}(-1)^n = (1-1)^n = 0.$$

Stelling. (Möbius-omkering). Zij F(a) een willekeurige getallentheoretische functie, en zij $G(a) = \sum_{d/a} F(d)$, dan is

$$F(a) = \sum_{d/a} \mu(d) G\left(\frac{a}{d}\right).$$

Bewijs. Voor elke positieve d/a is $G\left(\frac{a}{d}\right) = \sum_{b/\frac{a}{d}} F(b)$

$$\mu(d) G\left(\frac{a}{d}\right) = \sum_{b/\frac{a}{d}} \mu(d) F(b), \text{ dus } \sum_{d/a} \mu(d) G\left(\frac{a}{d}\right) = \sum_{d/a} \sum_{b/\frac{a}{d}} \mu(d) F(b) =$$

$$= \sum_{b/a} \sum_{d/\frac{a}{b}} \mu(d) F(b) = \sum_{b/a} F(b) \sum_{d/\frac{a}{b}} \mu(d) = F(a).$$

Functie van Euler. Onder de getallentheoretische functie $\varphi(a)$ verstaat men het aantal van de getallen n uit de rij 1,2,...,a, waarvoor (n,a)=1.
Voorbeelden. $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$. $\varphi(p)=p-1$.
Stelling. $\sum_{d/a} \varphi(d) = a$.

Bewijs. Verdeel de a getallen 1,2,...,a in klassen naar de waarden van d=(n,a), voor die d > 0 die in a opgaan. Bij elke d/a behoren die n=kd, waarvoor (kd,a)=d of $\left(k, \frac{a}{d}\right)=1$.
Dit zijn wegens $0<kd\leq a$, of $0<k\leq\frac{a}{d}$ juist $\varphi\left(\frac{a}{d}\right)$ getallen.
Dus is $a = \sum_{d/a} \varphi\left(\frac{a}{d}\right) = \sum_{d/a} \varphi(d)$.

Stelling. $\varphi(a) = a \sum_{d/a} \frac{\mu(d)}{d}$.

Bewijs. We passen de Möbius-omkering toe met $F(a)=\varphi(a)$.
$G(a) = \sum_{d/a} \varphi(d) = a$, dus $\varphi(a) = \sum_{d/a} \mu(d) \frac{a}{d} = a \sum_{d/a} \frac{\mu(d)}{d}$.

Stelling. $\varphi(a) = a \prod_{p/a} \left(1-\frac{1}{p}\right)$.

Bewijs. a) voor a=1 is $\varphi(1)=1$ (leeg product).

b) zij a>1, $a = p_1^{l_1} \ldots p_n^{l_n}$. Dan is

$$\varphi(a) = a \sum_{d/p_1 \ldots p_n} \frac{\mu(d)}{d} = a \prod_{i=1}^{n} \left(1-\frac{1}{p_i}\right).$$

Stelling. Voor $a>1$ is $\varphi(a)=\prod_{n=1}^{r} p_n^{l_n-1}(p_n-1)$.

Bewijs: $\varphi(a)=\prod_{i=1}^{n} p_i^{l_i} \prod_{i=1}^{n}(1-\frac{1}{p_i})=\prod_{i=1}^{n} p_i^{l_i}(1-\frac{1}{p_i})=\prod_{i=1}^{n} p_i^{l_i-1}(p_i-1)$.

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

Stelling. Voor $a>0$, $b>0$, $(a,b)=1$ is $\varphi(ab)=\varphi(a)\varphi(b)$.

Bewijs: Is $a=1$ of $b=1$, dan is de stelling triviaal.

Dus $a=\prod_{i=1}^{n} p_i^{l_i}>1$, $b=\prod_{j=1}^{s} q_j^{m_j}>1$, dus

$$\varphi(a)=\prod_{i=1}^{n} p_i^{l_i-1}(p_i-1),\ \varphi(b)=\prod_{j=1}^{s} q_j^{m_j-1}(q_j-1).$$

Daar $(a,b)=1$ is

$$ab=\prod_{i=1}^{n} p_i^{l_i} \prod_{j=1}^{s} q_j^{m_j}.$$

$$\varphi(ab)=\prod_{i=1}^{n} p_i^{l_i-1}(p_i-1) \prod_{j=1}^{s} q_j^{m_j-1}(q_j-1)=\varphi(a)\varphi(b).$$

ELEMENTAIRE GETALLENTHEORIE III

door Prof. Dr B. Meulenbeld en Prof. Dr S.C. van Veen

Leer der congruenties.

Def. $a \equiv b \pmod m (m>0)$, als $m/a-b$

$a \not\equiv b \pmod m$ als $m \nmid a-b$.

Eigenschappen: 1. $a \equiv a \pmod m$ (reflexief)

2. uit $a \equiv b \pmod m$ volgt $b \equiv a \pmod m$ (symmetrisch)

3. uit $a \equiv b \pmod m$, $b \equiv c \pmod m$ volgt $a \equiv c \pmod m$ (transitief)

Deelt men c door m volgens $c=qm+r$ $(0 \leq r < m)$, dan wordt r de rest van c (mod m) genoemd. $a \equiv b \pmod m$ geldt dan en alleen dan als a en b dezelfde rest mod m hebben.

De gehele getallen vallen dus mod m in m restklassen uiteen, zodat elk tweetal getallen uit dezelfde klas congruent mod m zijn, en elk tweetal uit verschillende klassen incongruent zijn.

Stellingen: 1. Uit $a \equiv b$, $c \equiv d$ volgt $a+c \equiv b+d$, $a-c \equiv b-d$.

2. Uit $a_1 \equiv b_1$, $a_2 \equiv b_2, \ldots a_n \equiv b_n$ volgt

$a_1+\ldots+a_n \equiv b_1+\ldots+b_n$.

3. Uit $a \equiv b$ volgt voor elke c $ac \equiv bc$.

4. Uit $a \equiv b$, $c \equiv d$ volgt $ac \equiv bd$.

5 Uit $a_1 \equiv b_1$, $a_2 \equiv b_2, \ldots, a_n \equiv b_n$ volgt

$a_1 a_2 \ldots a_n \equiv b_1 b_2 \ldots b_n$.

6. Uit $a \equiv b$, $n > 0$ volgt $a^n \equiv b^n$.

7. Zij $f(x)=c_0+c_1x+\ldots+c_nx^n$ een veelterm met gehele coëfficiënten. Uit $a \equiv b$ volgt $f(a) \equiv f(b)$.

8. Uit $ac \equiv bc$ $(c,m)=1$ volgt $a \equiv b$.

9. Uit $ac \equiv bc \pmod m$ volgt

$$a \equiv b \pmod{\frac{m}{(c,m)}}. \qquad \text{(I)}$$

Bewijs: $m/(a-b)c$, dus $\frac{m}{(c,m)} / (a-b)\frac{c}{(c,m)}$.

Daar $(\frac{m}{(c,m)}, \frac{c}{(c,m)}) = 1$ is, volgt $\frac{m}{(c,m)}/a-b$.

10. Uit $a \equiv b \pmod m$, $n > 0$ n/m volgt $a \equiv b \pmod n$.

11. Uit $a \equiv b \pmod m$, $c > 0$ volgt $ac \equiv bc \pmod{c\,m}$ en omgekeerd

Def. Onder een volledig restsysteem mod m verstaat men een systeem van m getallen, waarvan er elk $\equiv 0,1,\ldots, m-1 \pmod m$ is. Het is dus een systeem von m representanten van alle restklassen.

Def. Het aantal oplossingen van $f(x)\equiv 0 \pmod m$ is het aantal der oplossingen in een willekeurig volledig restsysteem.

Def. Onder een gereduceerd restsysteem mod m verstaat men een systeem van $\varphi(m)$ getallen, die representanten zijn van die klassen, waarvan de getallen onderling ondeelbaar zijn met m.

Stelling. Is $(k,m)=1$ en $a_1,a_2,..,a_m$ een willekeurig volledig restsysteem, dan is $a_1k,a_2k,..,a_mk$ dit ook.

Bewijs: Deze m getallen zijn onderling incongruent, immers uit $a_rk\equiv a_sk \pmod m$ $1\leq r\leq m$, $1\leq s\leq m$ volgt wegens $(k,m)=1$: $a_r\equiv a_s \pmod m$, dus $r=s$.

Stelling. Is $(k,m)=1$ en $a_1,a_2,..,a_{\varphi(m)}$ een willekeurig gereduceerd restsysteem, dan is a_1k, $a_2k,..,a_{\varphi(m)}k$ dit ook.

Bewijs: Volgens de vorige stelling zijn ze onderling incongruent en onderling ondeelbaar met m wegens $(k,m)=1$.

Stelling. Is $(a,m)=1$ dan heeft de congruentie

$$ax+a_0\equiv 0 \pmod m \qquad (1)$$

precies één oplossing.

Bewijs: De getallen $a.0$, $a.1,\ldots,a.(m-1)$ vormen een volledig restsysteem. Een van deze getallen is dus $\equiv -a_0 \pmod m$.

Deze stelling is een bijzonder geval van de volgende

Stelling. De congruentie $ax+a_0\equiv 0 \pmod m$ is dan en alleen dan oplosbaar als $(a,m)/a_0$.

In dat geval is het aantal oplossingen $=(a,m)$, en aan de congruentie voldoen precies alle x van een bepaalde restklasse mod $\left(\frac{m}{(a,m)}\right)$.

Bewijs: Is (1) oplosbaar, dan is $ax+a_0\equiv 0 \pmod{(a,m)}$; $a_0\equiv 0 \pmod{(a,m)}$. Is $a_0\equiv 0 \pmod{(a,m)}$ dan is de congruentie

$$\left(\frac{a}{(a,m)}\right)x+\frac{a_0}{(a,m)}\equiv 0 \pmod{\frac{m}{(a,m)}} \qquad (2)$$

oplosbaar, dus ook (1). (2) heeft dan precies één oplossing en dus (1) (a,m) oplossingen.

Stelling. Zij $n>1$, de getallen $a_1\ldots a_n$ niet alle 0, $d=(a_1,a_2,..,a_n)$, dan heeft de diophantische vergelijking $a_1x_1+\ldots+a_nx_n=c$ dan en alleen dan een oplossing als d/c.

Bewijs: Zonder de algemeenheid te schaden mag men stellen $a_1>0,\ldots,a_n>0$.

Is de vergelijking oplosbaar, dan is $d/a_1x_1+..+a_nx_n$, dus d/c. Zij nu d/c. Is $n=2$, dan moeten we oplossen $a_1x_1+a_2x_2=c$ of $a_1x_1-c\equiv 0 \pmod{a_2}$. Deze is oplosbaar, daar $(a_1,a_2)/-c$. Zij $n>2$, dan wordt de bewering voor $2,\ldots,n-1$ als bewezen aangenomen. We stellen $(a_1,..,a_{n-1})=a$, dan is $(a,a_n)=d$. We kunnen nu oplossen $ax+a_nx_n=c$. Daar $(a_1,..,a_{n-1})/ax$ zijn volgens inductieonderstelling $x_1,..,x_{n-1}$ te vinden met $a_1x_1+..+a_{n-1}x_n=ax$, en dus $a_1x_1+..+a_{n-1}x_{n-1}+a_nx_n=c$.

Gevolg. Is (a,b)=1 dan is de "onbepaalde"vergelijking: ax+by=1 oplosbaar.

Stelling. Is (a,b)=d, en d/c, dus ax+by=c oplosbaar, dan volgen uit de oplossing (x_0,y_0) alle oplossingen: $x=x_0+t\frac{b}{d}$, $y=y_0-t\frac{a}{d}$ (t willekeurig).

Bewijs: 1) Het zijn oplossingen:

$$a(x_0+t\tfrac{b}{d})+b(y_0-t\tfrac{a}{d}) = ax_0+by_0=c.$$

2) Er zijn geen andere oplossingen. Zonder beperking der algemeenheid mag men stellen $b\neq 0$. Uit $ax+by=c=ax_0+by_0$ volgt $ax-c\equiv 0 \pmod{|b|}$, $ax_0-c\equiv 0 \pmod{|b|}$, dus $x\equiv x_0 \pmod{\frac{|b|}{d}}$ of $x=x_0+t\frac{b}{d}$. Verder is $by=c-ax=c-a(x_0+t\frac{b}{d})= (c-ax_0)-b\frac{at}{d} = by_0-b\frac{at}{d} = b(y_0-t\frac{a}{d})$ of $y=y_0-t\frac{a}{d}$.

Gevolg. Is (a,b)=1 en is (x_0,y_0) een oplossing van ax+by=1, dan zijn alle oplossingen: $x=x_0+tb$, $y=y_0-ta$ (t willekeurig).

Stelling. De congruenties $x\equiv a_1 \pmod{m_1}$, $x\equiv a_2 \pmod{m_2}$ hebben dan en alleen dan een oplossing als $(m_1,m_2)/a_1-a_2$. Is dit zo, dan zijn de oplossingen de getallen van een bepaalde restklasse mod m (m=KGV van m_1 en m_2).

Bewijs: 1) Stelt men $(m_1,m_2)=d$, dan is $x\equiv a_1 \pmod d$, $x\equiv a_2 \pmod d$, dus $a_1\equiv a_2 \pmod d$, dus d/a_1-a_2.

2) Is d/a_1-a_2, dan moet men uit de oplossingen $x=a_1+ym_1$ (y willekeurig) er een kiezen die aan $x\equiv a_2 \pmod{m_2}$ voldoet. Dus $a_1+ym_1\equiv a_2 \pmod{m_2}$, of $ym_1+(a_1-a_2)\equiv 0 \pmod{m_2}$. Deze heeft een oplossing, die de vorm heeft $y\equiv y_0 \pmod{\frac{m_2}{d}}$. Dus $x=a_1+(y_0+t\frac{m_2}{d})m_1=a_1+m_1y_0+t\frac{m_1m_2}{d}=a_1+m_1y_0+tm$ (t willekeurig). Dit is een bepaalde restklasse mod m.

Stelling. Zij $n>1$. Elk tweetal van de getallen $m_1,..,m_2$ zijn onderling ondeelbaar. Dan zijn de congruenties $x\equiv a_i \pmod{m_i}(i=1,..,n)$ oplosbaar, en de gemeenschappelijke oplossingen bestaan uit alle getallen van een bepaalde restklasse mod $m_1m_2..m_n$.

Bewijs: Voor m=2 is dit wegens $m=m_1m_2$ in de vorige stelling bewezen. Zij $m>2$ en de beweringen voor n-1 bewezen. De eerste n-1 congruenties hebben dus bij passende a een oplossing: $x\equiv a \pmod{m_1...m_{n-1}}$. Uit de vorige stelling volgt dan verder deze, daar $(m_1...m_{n-1},m)=1$.

Stelling. Zij $n>1$ en elk tweetal van de getallen $m_1,..,m_n$ onderling ondeelbaar. Dan is het aantal oplossingen van $f(x)\equiv 0 \pmod{m_1...m_n}$ gelijk aan het product van de aantallen oplossingen van $f(x)\equiv 0 \pmod{m_1},\ldots, f(x)\equiv 0 \pmod{m_n}$.

Bewijs: Het is duidelijk, dat $f(x)\equiv 0 \pmod{m_1..m_n}$ vervuld is dan en alleen dan als $f(x)\equiv 0 \pmod{m_1},\ldots, f(x)\equiv 0 \pmod{m_n}$.
Heeft een van deze laatste geen oplossing, dan ook de eerste niet. Zijn deze laatste alle oplosbaar, dan komt er volgens de vorige stelling met iedere restklasse mod m_1, mod m_2,..mod m_n, die aan de laatste

congruenties voldoen, een restklasse mod $m_1 \ldots m_n$ overeen die aan de eerste congruentie voldoet.

Stelling. Is $f(x)=c_0+c_1x+..+c_nx^n$, $p \nmid c_n$, dan heeft de congruentie $f(x) \equiv 0 \pmod p$ hoogstens n oplossingen.

Bewijs: 1) Voor $n=0$ is dit duidelijk, daar voor iederex $c_0 \not\equiv 0 \pmod p$

2) Zij $n>0$ en de bewering van n-1 bewezen. Zou $f(x) \equiv 0 \pmod p$ n+1 wortels $x_0, x_1, .., x_n$ hebben, dan zou gelden:

$$f(x)-f(x_0)=(x-x_0)\, g(x), \text{ met } g(x)=b_0+b_1x+\ldots+b_{n-1}x^{n-1}$$

$$b_{n-1}=c_n, p \nmid b_{n-1}, \text{ en } (x_i-x_0)g(x_i) \equiv f(x_i)-f(x_0) \equiv 0 \pmod p$$

voor $i=1,2,..n$. Dus $g(x_i) \equiv 0 \pmod p$ voor $i=1,2,..n$, hetgeen strijdt met de inductie-onderstelling.

Kleine stelling van Fermat. Is $(a,m)=1$, dan is

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Bewijs: Zij $a_1, .., a_{\varphi(m)}$ een gereduceerd restsysteem mod m; dan is $aa_1, \ldots, aa_{\varphi(m)}$ er ook een. Afgezien van de volgorde zijn dus de a_i aan de aa_i congruent ($i=1,.., \varphi(m)$). Dus geldt ook:

$$a_1a_2..a_{\varphi(m)} \equiv aa_1 \cdot aa_2 \cdot \ldots aa_{\varphi(m)} \equiv a^{\varphi(m)} a_1a_2..a_{\varphi(m)} \pmod m$$

dus, daar $m \nmid a_i$: $a^{\varphi(m)} \equiv 1 \pmod m$.

Gevolg. Voor $p \nmid a$ is $a^{p-1} \equiv 1 \pmod p$ en voor elke a $a^p \equiv a \pmod p$.

Stelling van Wilson. $(p-1)! \equiv -1 \pmod p$

Bewijs: Beschouw $f(x)=x^{p-1}-1-\prod_{i=1}^{p-1} (x-i)$.

Dit is een veelterm van de $(p-2)^e$ graad, die p-1 wortels $1,2,..p-1$ zou hebben. Dit kan alleen als alle coëfficienten van f(x) deelbaar zijn door p. De constante term is $-1-(-1)^{p-1}(p-1)!$.

Dus $-1-(-1)^{p-1}(p-1)! \equiv 0(p)$, of $(p-1)! \equiv -1 \pmod p$.

ELEMENTAIRE GETALLENTHEORIE IV

door Prof. Dr B. Meulenbeld en Prof. Dr S.C. van Veen

Omgekeerde van de stelling van Wilson.

Als gegeven is $(a-1)! \equiv -1 \pmod a$, dan is a priem.

Bewijs: Was a samengesteld: $a=bc$ met $2 \leq b \leq a-1$, $2 \leq c \leq a-1$, dan was het linkerlid $\equiv 0 \pmod b$ en het rechterlid niet. Tegenspraak.

Theorie der kwadraatresten.

Definitie. Als de congruentie $x^2 \equiv n \pmod m$ oplosbaar is, heet n kwadraatrest mod m; niet oplosbaar, dan een niet-rest mod m.
n heet dus kwadraatrest mod m, als n representant is van een klasse, waarin kwadraten voorkomen. Zo is 7 kwadraatrest mod 9. Immers $5^2 \equiv 7 \pmod 9$. We onderzoeken eerst het geval dat m een priemgetal p is. Voor p=2 is elk getal kwadraatrest. Daarom nemen wij aan $p > 2$. Is p/n, dan is n kwadraatrest mod p, immers $0^2 \equiv n \pmod p$. We onderstellen dus $p > 2$, $p \nmid n$. Voor deze gevallen is het symbool van Legendre $(\frac{n}{p})$ ingevoerd.

Definitie. Voor $p > 2$, $p \nmid n$ is

$$(\frac{n}{p}) = \begin{cases} 1, & \text{als n kwadraatrest (mod p) is,} \\ -1, & \text{als n niet-rest (mod p) is.} \end{cases}$$

Stelling. Uit $n \equiv n' \pmod p$ volgt $(\frac{n}{p})=(\frac{n'}{p})$.

Bewijs. Als $p \nmid n$, is ook $p \nmid n'$. Het symbool $(\frac{n'}{p})$ heeft dus zin. Uit $x^2 \equiv n \pmod p$ volgt $x^2 \equiv n' \pmod p$ en omgekeerd.

Voorbeeld: $(\frac{352}{37}) = (\frac{19}{37})$.

Stelling. Zij $p > 2$. In elk gereduceerd restsysteem mod p zijn er precies $\frac{p-1}{2}$ kwadraatresten (mod p), dus ook precies $\frac{p-1}{2}$ niet-resten (mod p). De eerste $\frac{p-1}{2}$ getallen worden door de restklassen voorgesteld, waartoe $1^2, 2^2, \ldots (\frac{p-1}{2})^2$ behoren.

Bewijs. De kwadraatresten zijn die en alleen die getallen, die liggen in de restklassen, voorgesteld door $1^2, 2^2, \ldots, (p-1)^2$.
Als x voldoet aan $x^2 \equiv n \pmod p$, voldoet ook p-x hieraan. Immers $(p-x)^2 \equiv (-x)^2 \equiv x^2 \equiv n \pmod p$. Voor kwadraatresten komen dus alleen in aanmerking de restklassen $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. Elk tweetal van deze getallen is echter incongruent mod p. Ze stellen dus alle kwadraatresten voor.

Stelling (Criterium van Euler). Voor $p > 2$, $p \nmid n$ is $n^{\frac{p-1}{2}} \equiv (\frac{n}{p}) \pmod p$.

Bewijs. Volgens de kleine stelling van Fermat heeft de congruentie $n^{p-1} \equiv 1 \pmod p$ de oplossingen:

$n=1,2,..,p-1$. Voor deze congruentie kunnen we ook schrijven $(n^{\frac{p-1}{2}}-1)(n^{\frac{p-1}{2}}+1)\equiv 0 \pmod p$. Een en slechts één van de factoren links is deelbaar door p (beide kan niet, want dan zou p/2). n voldoet dus òf aan $n^{\frac{p-1}{2}}-1\equiv 0$ òf aan $n^{\frac{p-1}{2}}+1\equiv 0 \pmod p$. Is nu n kwadraatrest mod p, dus $(\frac{n}{p})=1$, dan is er dus een a met $a^2\equiv n \pmod p$. In dit geval voldoet dus n aan $n^{\frac{p-1}{2}}-1\equiv a^{p-1}-1\equiv 0 \pmod p$, dus aan $n^{\frac{p-1}{2}}\equiv 1 \pmod p$ of aan $n^{\frac{p-1}{2}}\equiv(\frac{n}{p}) \pmod p$. Alle $\frac{p-1}{2}$ kwadraatresten voldoen hieraan, en daar deze congruentie hoogstens $\frac{p-1}{2}$ wortels heeft, zijn dit dus alle oplossingen. De niet-resten voldoen dus aan $n^{\frac{p-1}{2}}+1\equiv 0 \pmod p$, of $n^{\frac{p-1}{2}}\equiv -1 \pmod p$ of $n^{\frac{p-1}{2}}\equiv(\frac{n}{p}) \pmod p$.

Toepassing. Stel p/a^2+b^2 $(a,b)=1$, dan is zeker $p\nmid b$. Dus is er een getal c te vinden met $bc\equiv 1 \pmod p$. Uit $p/a^2c^2+b^2c^2$ volgt $p/(ac)^2+1$, m.a.w. $(ac)^2\equiv -1 \pmod p$. Dus -1 is kwadraatrest mod p of $(\frac{-1}{p})=1$. (Omgekeerd: Heeft men een p met $(\frac{-1}{p})=1$, dan is p een priemfactor van een som van twee kwadraten: immers $x^2+1\equiv 0(p)$, dus p/x^2+1). Van welke priemgetallen is $(\frac{-1}{p})=1$? Volgens crit. van Euler is $(\frac{-1}{p})=(-1)^{\frac{p-1}{2}} \pmod p$ dus $(\frac{-1}{p})=1$ als p=4 voud +1 of p=2. Bewezen is dus: Alle oneven priemdelers van de som van twee kwadraten a^2+b^2 met $(a,b)=1$ zijn van de gedaante 4 voud + 1.

Stelling. Voor $p>2$, $p\nmid n$, $p\nmid n'$ is $(\frac{nn'}{p})=(\frac{n}{p})(\frac{n'}{p})$.

Dus: de congruenties $x^2\equiv nn' \pmod p$ zijn dan en alleen dan oplosbaar als de congruenties $x^2\equiv n \pmod p$ en $x^2\equiv n' \pmod p$ beide oplosbaar of beide niet oplosbaar zijn.

Bewijs. $(\frac{nn'}{p})\equiv(nn')^{\frac{p-1}{2}}\equiv n^{\frac{p-1}{2}}n'^{\frac{p-1}{2}}\equiv(\frac{n}{p})(\frac{n'}{p}) \pmod p$.

Beide leden zijn ± 1. Wegens $p>2$ is dus $(\frac{nn'}{p})=(\frac{n}{p})(\frac{n'}{p})$.

Uitbreiden tot

Stelling. Voor $p>2$, $r\geq 2$, $p\nmid n_1,..,\ p\nmid n_r$ is

$$(\frac{n_1\ldots n_r}{p})=(\frac{n_1}{p})\ldots(\frac{n_r}{p}).$$

Is $n=\prod_{i=1}^{r} n_i^{\lambda_i}$ dan is dus $(\frac{n}{p})=\prod_{i=1}^{r}(\frac{n_i}{p})^{\lambda_i}$.

Stelling. (Criterium van Gauss) Zij $p>2$, $p\nmid n$. Men beschouwt de $\frac{p-1}{2}$ getallen $n,2n,..,\frac{p-1}{2}n$, en bepaalt hiervan de resten mod p. Dit zijn $\frac{p-1}{2}$ verschillende getallen >0 en $<p$. Is nu m het aantal van deze

resten die $>\frac{p}{2}$ zijn, dan is $(\frac{n}{p}) = (-1)^m$.

Voorbeeld. p=7, u=10. Getallen 10,20,30, resten 3,6 en 2. Dus m=1, dus $(\frac{10}{7})=(\frac{3}{7})=-1$. De congruentie $x^2\equiv 3 \pmod 7$ is onoplosbaar.

Bewijs. Laten de resten mod p van $n,2n,\ldots,\frac{p-1}{2}n$ zijn $r_1,r_2,..,r_{\frac{p-1}{2}}$, dan zijn deze alle ≥ 1 en $\leq p-1$. Het is duidelijk, dat $r_i \not\equiv r_j \pmod p$.

Nu is $r_1 r_2..r_{\frac{p-1}{2}} \equiv n.2n..\frac{p-1}{2}n \equiv (\frac{p-1}{2})!\, n^{\frac{p-1}{2}} \pmod p$. We beschouwen nu de rij $r_1',r_2'...r_{\frac{p-1}{2}}'$, waarbij $r_i'=r_i$ als $r_i<\frac{p}{2}$

$r_i'=p-r_i$ als $r_i>\frac{p}{2}$.

Alle r_i zijn dan $<\frac{p}{2}$. Steeds is $r_i' \not\equiv r_j' \pmod p$. De rij $r_1'..r'_{\frac{p-1}{2}}$ bestaat dus uit $\frac{p-1}{2}$ verschillende getallen die ≥ 1 en $\leq \frac{p-1}{2}$ zijn, is dus gelijk aan de rij $1,2,..,\frac{p-1}{2}$, dus $r_1',r_2'..r'_{\frac{p-1}{2}}=(\frac{p-1}{2})!$ Vergelijken met de rij $r_1,r_2..r_{\frac{p-1}{2}}$ zijn er m getallen vervangen door $p-r_i$; deze zijn $\equiv -r_i \pmod p$. Dus is: $(-1)^m(\frac{p-1}{2})! \equiv (\frac{p-1}{2})!\, n^{\frac{p-1}{2}} \pmod p$, dus is $n^{\frac{p-1}{2}} \equiv (-1)^m \pmod p$, dus volgens crit.van Euler: $(\frac{n}{p})=(-1)^m$.

Toepassing. Stel p/a^2-2b^2, $(a,b)=1$, p oneven. Weer is $p\nmid b$, kunnen dus c bepalen met $bc\equiv 1 \pmod p$. Uit $p/a^2c^2-2b^2c^2$ volgt $p/(ac)^2-2$. M.a.w. $(ac)^2\equiv 2 \pmod p$. Dus 2 is kwadraatrest mod p, of $(\frac{2}{p})=1$. Deze voorwaarde is ook voldoende. Voor welke priemgetallen is $(\frac{2}{p})=1$? We passen het criterium van Gauss toe. We schrijven op de rij: 2,4,6,..,p-1. Dit zijn tevens de resten mod p.

Stel nu p= 8 voud +1 = 8v+1, dan is m=2v, dus $(\frac{2}{p})=1$.

is p= 8v+3, dan is m=2v+1, dus $(\frac{2}{p})=-1$.

p= 8v+5, dan is m=2v+1, dus $(\frac{2}{p})=-1$.

p= 8v+7, dan is m=2v+2, dus $(\frac{2}{p})=1$.

Kunnen dit samenvatten tot $(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}$

We hebben dus bewezen: Alle oneven priemfactoren van a^2-2b^2 $(a,b)=1$ zijn van de gedaante $8v\pm1$.

Onderzoeken we nu p/a^2+2b^2. Nu wordt de voorwaarde $(\frac{-2}{p})=1$.

$(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$. Hieruit leidt men af: $(\frac{-2}{p})=1$ als p=8v+1 of 8v+3

$=-1$ als p=8v+5 of 8v+7.

Dus: Alle oneven priemfactoren van a^2+2b^2 $(a,b)=1$ zijn van de gedaante 8v+1 of 8v+3.

Elementaire getallentheorie V

door

Prof.Dr B.Meulenbeld en Prof.Dr S.C.van Veen.

16 Maart 1955.

De wederkerigheidswet der kwadraatresten.

Wij veronderstellen voorlopig, dat p en q oneven priemgetallen zijn. Wanneer men getallenvoorbeelden narekent, blijkt het gemakkelijk, dat in de meeste gevallen $(\frac{p}{q}) = (\frac{q}{p})$, dus p tegelijkertijd rest (niet rest)van q met q rest (niet rest) van p.

b.v.: $\begin{cases} 8^2 \equiv 13 \pmod{17} \text{ dus } (\frac{13}{17}) = +1. \\ 2^2 \equiv 17 \pmod{13} \text{ dus } (\frac{17}{13}) = +1. \end{cases}$

$\begin{cases} x^2 \equiv 7 \pmod 5 \text{ géén oplossing, dus } (\frac{7}{5}) = -1. \\ x^2 \equiv 5 \pmod 7 \text{ géén oplossing, dus } (\frac{5}{7}) = -1. \end{cases}$

Er zijn echter duidelijke uitzonderingen (globaal in 25% der gevallen).

b.v.: $2^2 \equiv 11 \pmod 7$ dus $(\frac{11}{7}) = +1.$

$x^2 \equiv 7 \pmod{11}$ geen oplossing, dus $(\frac{7}{11}) = -1.$

Gauss heeft (oorspronkelijk langs experimentele weg) ontdekt:

$(\frac{p}{q}) = (\frac{q}{p})$ wanneer ten minste 1 der priemgetallen p en q van de gedaante $4k+1$ is.

$(\frac{p}{q}) = -(\frac{q}{p})$ wanneer beide priemgetallen p en q van de gedaante $4k-1$ zijn.

Dit is de wederkerigheidswet der kwadraatresten.

In het bijzonder met het symbool van Legendre verkrijgt de wederkerigheidswet de volgende elegante gedaante:

$$(\frac{p}{q}).(\frac{q}{p}) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

Wij gaan nu over tot het bewijs van de:

Wederkerigheidswet: Gegeven $p>2$, $q>2$, p en q priemgetallen, $p \neq q$.

Te bewijzen:

$$(\frac{q}{p}).(\frac{p}{q}) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

Bewijs:

Volgens het criterium van Gauss is

$$(\frac{q}{p}) = (-1)^m \qquad (1)$$

waarin m het aantal resten (mod p) uit de rij:

$$q,\ 2q,\ 3q,\ \ldots\ ,\ \frac{p-1}{2}.q$$

die $> \frac{p}{2}$ zijn, of, nog eenvoudiger:
het aantal absoluut kleinste negatieve resten uit deze rij.
Al deze absoluut kleinste resten zijn dus van de gedaante

$$-\frac{p}{2} < qx - py < 0 \qquad (2)$$

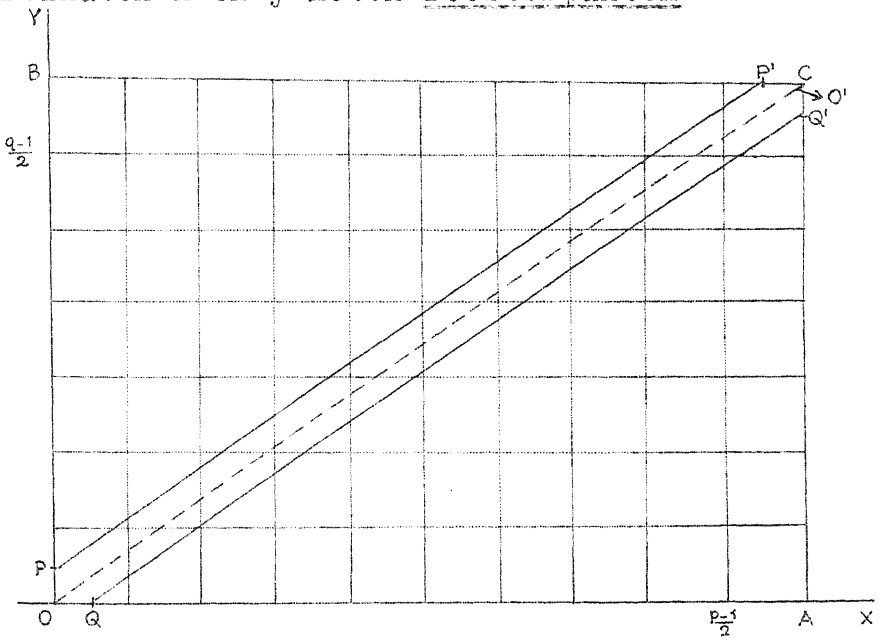
waarin x een geheel getal is uit de rij 1, 2, 3, ..., $\frac{p-1}{2}$, en y is het daarbij behorende gehele getal $\left[\frac{qx}{p}\right]+ 1$. Het getal m uit (1) is dus het aantal oplossingen (x,y) in gehele getallen dat aan (2) voldoet.
Op dezelfde wijze vindt men:

$$\left(\frac{p}{q}\right) = (-1)^n \qquad (3)$$

waarin n het aantal oplossingen (x,y) in gehele getallen voorstelt, dat aan

$$-\frac{q}{2} < py - qx < 0 \qquad (4)$$

voldoet.
Wij stellen nu x en y voor als rechthoekige coördinaten (zie figuur).
De punten met gehele coördinaten x en y heten roosterpunten.



$OA = \frac{p+1}{2}$, $OB = \frac{q+1}{2}$.

Wij tekenen nu de drie lijnen: $PP' \equiv qx-py = -\frac{p}{2}$ (5)

$QQ' \equiv qx-py = +\frac{q}{2}$ (6)

$OO' \equiv qx-py = 0$ (7).

PP' gaat door $P(0,\frac{1}{2})$ en $P'\ (\frac{p}{2}\ ,\ \frac{q+1}{2})$

QQ' gaat door $Q(\frac{1}{2},0)$ en $Q'\ (\frac{p+1}{2}\ ,\ \frac{q}{2})$.

De 3 rechten PP', QQ' en OO' lopen evenwijdig.
Zij gaan door geen enkel roosterpunt binnen OACB of op de grens van

CACB. Immers substitutie van gehele waarden van x en y in (5) en (6) voert tot een tegenstrijdigheid, terwijl in (7): $\frac{y}{x} = \frac{q}{p}$, dus de kleinste gehele van nul verschillende waarden y en x, die hieraan voldoen, zijn q en p (buiten de rechthoek).

Het totaal aantal roosterpunten binnen OACB = $\frac{p-1}{2} \cdot \frac{q-1}{2}$ (8).

Uit de volkomen gelijke ligging van de congruente $\triangle\triangle$ BPP' en AQ'Q ten opzichte van het rooster volgt, dat het aantal roosterpunten d binnen $\triangle$ AQQ' = aantal roosterpunten d binnen $\triangle$ BP'P.

Het aantal roosterpunten binnen OQQ'CP' bedraagt dus:

$$\frac{p-1}{2} \cdot \frac{q-1}{2} - 2d \quad (9).$$

Uit (5) en (7) volgt, dat de coördinaten van de roosterpunten binnen OPP'CO' voldoen aan

$$-\frac{p}{2} < qx-py < 0.$$

Dus in verband met (2) is het aantal roosterpunten binnen OPP'CO' gelijk aan m.

Op dezelfde wijze volgt uit (6), (7) en (4), dat het aantal roosterpunten binnen OQQ'O' gelijk is aan n.

Dus het aantal roosterpunten binnen OQQ'CP' is anderzijds gelijk aan m+n (10).

Uit (9) en (10) volgt:

$$m+n = \frac{p-1}{2} \cdot \frac{q-1}{2} - 2d$$

dus

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{m+n} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2} - 2d} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

w.t.b.w.

Historische opmerkingen: De wederkerigheidswet is feitelijk het eerst (zonder bewijs) uitgesproken door Euler. De eerste niet geslaagde bewijspoging is van Legendre (1785). In Maart 1795 werd de stelling weer gevonden door de nog niet 18 jarige Gauss, die op dat ogenblik niet bekend was met het werk van zijn voorganger. Na een worsteling van meer dan een jaar gelukte het Gauss op 8 April 1796 het eerst deze stelling te bewijzen. Dit bewijs was zeer gecompliceerd. In zijn latere leven is hij er nog geregeld op teruggekomen, en hij heeft nog 7 andere bewijzen gegeven. De eenvoudigste hiervan berusten, evenals het voorafgaande, op het "lemma van Gauss" (= criterium van Gauss) dat door hem in 1808 werd gepubliceerd.

Toepassingen van de reciprociteitswet.

Stel: p is een priemgetal van Fermat: $2^{2^k} + 1$

$$(\tfrac{3}{p})(\tfrac{p}{3}) = 1 \qquad \text{voor } k > 0.$$

dus:

$$(\tfrac{3}{p}) = (\tfrac{p}{3}) \qquad p \equiv 2 \pmod 3$$

dus $$(\tfrac{3}{p}) = (\tfrac{2}{3}) = (-1)^{\frac{3^2-1}{8}} = -1.$$

Dus 3 is een niet-rest van een priemgetal van Fermat.
Volgens het criterium van Euler is dus

$$3^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

$$3^{2^{2^{k-1}}} \equiv -1 \pmod{2^{2^k}+1} \text{ mits } 2^{2^k}+1 \text{ priem is.}$$

Dan is $p-1 = 2^{2^k}$ de <u>laagste</u> exponent l, die $3^l \equiv +1 \pmod p$ maakt.
<u>3 is een primitieve wortel van de congruentie van Fermat voor ieder priemgetal van Fermat.</u>
Dit feit is van betekenis voor de theorie van de veelhoeksconstructies. Op een analoge manier kan men zonder grote moeite aantonen, dat 10 een primitieve wortel is van deze priemgetallen.
Wanneer men dus $\frac{1}{p}$ tot een repeterende breuk wil herleiden, dan gaat het er om, de <u>kleinste</u> exponent l te zoeken, zodat

$$10^l - 1 \equiv 0 \pmod p.$$

zodat

$$\frac{1}{p} = \frac{a}{10^l - 1} .$$

De <u>periode</u> heeft dan l cijfers.
B.v. voor p = 257 heeft de periode van $\frac{1}{257}$ 256 cijfers.

<u>Uitbreiding tot deelbare getallen.</u>
Definitie: Wanneer m een <u>oneven</u> getal > 0 voorstelt, dat ontbonden wordt in zijn priemfactoren

$$m = \prod_{r=1}^{\nu} p_r$$

(meervoudige factoren meervoudig opgeschreven)
en wanneer n een ander getal is, al of niet oneven, al of niet positief, dat <u>onderling ondeelbaar</u> is met m ((n,m)= 1) dan is bij definitie

$$(\tfrac{n}{m}) = \prod_{r=1}^{\nu} (\tfrac{n}{p_r}) .$$

Dit is het <u>symbool van Jacobi</u>.

De factoren onder het productteken zijn gewone symbolen van Legendre.
Het symbool van Jacobi is dus steeds ± 1.
Het symbool van Jacobi betekent niet, dat uit $(\frac{n}{m}) = \pm 1$ volgt, dat $n = \begin{matrix}\text{rest}\\ \text{niet-rest}\end{matrix}$ van m.
$(\frac{n}{m})$ kan + 1 zijn als n niet-rest is van een even aantal priemfactoren uit de ontbinding van m.

Stelling 1: $m > 0$ oneven, $n \equiv n' \pmod{m}$, $(n,m) = 1$.
Dan is $(\frac{n}{m}) = (\frac{n'}{m})$.

Bewijs. Dit volgt uit:

$$(\frac{n}{p_r}) = (\frac{n'}{p_r}) \quad \text{wegens } n \equiv n' \pmod{p_r}.$$

Stelling 2:
$m > 0$ oneven, $m' > 0$ oneven; $(n,m) = 1$, $(n',m) = 1$.
Dan is

$$(\frac{n}{m})(\frac{n}{m'}) = (\frac{n}{mm'}).$$

Bewijs. Stel $m = \prod_{r=1}^{\nu} p_r$, $m' = \prod_{r=1}^{\nu'} p'_r$.

$$(\frac{n}{m})(\frac{n}{m'}) = \prod_{r=1}^{\nu}(\frac{n}{p_r}) \cdot \prod_{r=1}^{\nu'}(\frac{n}{p'_r}) = \prod_{p}(\frac{n}{p}) = (\frac{n}{mm'}).$$

Het laatste product wordt uitgestrekt over alle priemfactoren van mm' (ieder gerekend naar haar meervoudigheid).

Stelling 3: $m > 0$ oneven. $(n,m) = 1$, $(n',m) = 1$.
Dan is:

$$(\frac{nn'}{m}) = (\frac{n}{m})(\frac{n'}{m}).$$

Bewijs. $(nn',m) = 1$; $(\frac{nn'}{p_r}) = (\frac{n}{p_r})(\frac{n'}{p_r})$ (zie IV).
Vermenigvuldiging.

Stelling 4: $m > 0$ oneven.
Dan is:

$$(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$$

(Eerste aanvullingsstelling voor de wederkerigheidswet van Jacobi).

Bewijs. Als u en u' oneven zijn, dan is

$$(u-1)(u'-1) \equiv 0 \pmod 4.$$

dus $uu'-1 \equiv (u-1)+(u'-1) \pmod 4$.
dus voor oneven $u_1, u_2, \ldots, u_\nu$

$$\prod_{r=1}^{\nu} u_r - 1 \equiv \sum_{r=1}^{\nu} (u_r - 1) \pmod 4.$$

of:

$$\frac{\prod_{r=1}^{\nu} u_r - 1}{2} \equiv \sum_{r=1}^{\nu} \frac{u_r - 1}{2} \pmod 2.$$

$$(-1)^{\frac{\sum_{r=1}^{\nu} u_r - 1}{2}} = \prod_{r=1}^{\nu} (-1)^{\frac{u_r - 1}{2}}$$

$$m = \prod_{r=1}^{\nu} p_r \ ;$$

dus wegens:

$$\left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_r - 1}{2}} \quad \text{(Legendre!)}$$

is

$$\left(\frac{-1}{m}\right) = \prod_{r=1}^{\nu} \left(\frac{-1}{p_r}\right) = \prod_{r=1}^{\nu} (-1)^{\frac{p_r - 1}{2}} = (-1)^{\frac{\prod_{r=1}^{\nu} p_r - 1}{2}} = (-1)^{\frac{m-1}{2}}.$$

Stelling 5: $m > 0$ oneven.

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

(2e aanvullingsstelling voor de wederkerigheidswet van Jacobi).

Bewijs: u en u' oneven $\rightarrow (u^2-1)(u'^2-1) \equiv 0 \pmod{16}$.

$$u^2u'^2 - 1 \equiv (u^2-1)+(u'^2-1) \pmod{16}.$$

$u_1, u_2, \ldots, u_\nu$ oneven $\quad \prod_{r=1}^{\nu} u_r^2 - 1 \equiv \sum_{r=1}^{\nu} (u_r^2 - 1) \pmod{16}$.

$$\frac{\prod_{r=1}^{\nu} u_r^2 - 1}{8} \equiv \sum_{r=1}^{\nu} \frac{u_r^2 - 1}{8} \pmod 2.$$

$$(-1)^{\frac{(\prod_{r=1}^{\nu} u_r)^2 - 1}{8}} = \prod_{r=1}^{\nu} (-1)^{\frac{u_r^2 - 1}{8}}$$

$$m = \prod_{r=1}^{\nu} p_r \ ; \quad \left(\frac{2}{p_r}\right) = (-1)^{\frac{p_r^2 - 1}{8}}$$

dus $\left(\frac{2}{m}\right) = \prod_{r=1}^{\nu} \left(\frac{2}{p_r}\right) = \prod_{r=1}^{\nu} (-1)^{\frac{p_r^2 - 1}{8}} = (-1)^{\frac{(\sum_{r=1}^{\nu} p_r)^2 - 1}{8}} = (-1)^{\frac{m^2-1}{8}}$.

ELEMENTAIRE GETALLENTHEORIE VI

door Prof.Dr B. Meulenbeld en Prof.Dr S.C.van Veen.

30 Maart 1955.

De wederkerigheidswet van Jacobi.

Jacobi heeft met behulp van zijn symbool $(\frac{n}{m})$ (m oneven > 0) de volgende uitbreiding van de wederkerigheidswet der kwadraatresten opgesteld.

Stelling 6: Als n en m positieve oneven getallen zijn, die onderling ondeelbaar zijn, dan is

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

Bewijs: Zonder beperking is:

$$n = \prod p > 1$$
$$m = \prod q > 1$$

$$(\frac{n}{m}) = (\frac{\prod p}{\prod q}) = \prod_p (\frac{p}{\prod q}) = \prod_p \prod_q (\frac{p}{q}) \qquad \text{(St.2 en St.3)}.$$

Dus: $$(\frac{n}{m})\cdot(\frac{m}{n}) = \prod_{p,q} (\frac{p}{q})(\frac{q}{p}) = \prod_{p,q} (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = (-1)^{\sum_{p,q} \frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$= (-1)^{\sum_p \frac{p-1}{2}\cdot\sum_q \frac{q-1}{2}} = (-1)^{\frac{\prod p-1}{2}\cdot\frac{\prod q-1}{2}} = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}} \quad \text{w.t.b.w.}$$

Toepassingen:

a): $$(\frac{383}{443}) \text{ (443 is priem)} = (\frac{443}{383})(-1)^{\frac{383-1}{2}\cdot\frac{443-1}{2}} = -(\frac{443}{383})$$

$$= -(\frac{60}{383}) = -(\frac{2^2}{383})(\frac{15}{383}) = -(\frac{15}{383})\times(-1)\times(-1)^{\frac{15-1}{2}\cdot\frac{383-1}{2}} = +$$

$$+(\frac{383}{15}) = (\frac{8}{15})$$

$$= (\frac{2^2}{15})(\frac{2}{15}) = (\frac{2}{15}) = (-1)^{\frac{15^2-1}{8}} = +1.$$

b): $$(\frac{35}{87}) = (\frac{87}{35})(-1)^{\frac{35-1}{2}\cdot\frac{87-1}{2}} = -(\frac{87}{35}) = -(\frac{17}{35}) = -(\frac{35}{17})(-1)^{\frac{35-1}{2}\cdot\frac{17-1}{2}} =$$

$$= -(\frac{35}{17}) = -(\frac{1}{17}) = -1.$$

Deze berekeningen worden vaak vereenvoudigd door:

Stelling 7: n en m oneven en onderling ondeelbaar (niet noodzakelijk > 0).

Dan is

$$\left(\frac{n}{|m|}\right)\left(\frac{m}{|n|}\right) = -(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}} \quad \text{als } n<0 \text{ en } m<0 \text{ is}$$

$$= (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}} \quad \text{in alle andere gevallen.}$$

Bewijs: a) $n>0$, $m>0$. (stelling 6)

b) $n<0$, $m<0$.

$$\left(\frac{n}{|m|}\right)\left(\frac{m}{|n|}\right) = \left(\frac{-|n|}{|m|}\right)\left(\frac{-|m|}{|n|}\right) = \left(\frac{-1}{|m|}\right)\left(\frac{|n|}{|m|}\right)\left(\frac{|m|}{|n|}\right)\cdot\left(\frac{-1}{|n|}\right) =$$

$$= (-1)^{\frac{|m|-1}{2}+\frac{|n|-1}{2}\cdot\frac{|m|-1}{2}+\frac{|n|-1}{2}} = -(-1)^{\frac{|m|-1}{2}+\frac{|n|-1}{2}\cdot\frac{|m|-1}{2}+\frac{|n|-1}{2}+1}$$

$$= -(-1)^{\left(\frac{|n|-1}{2}+1\right)\left(\frac{|m|-1}{2}+1\right)} = -(-1)^{\frac{|n|+1}{2}\cdot\frac{|m|+1}{2}} = -(-1)^{\frac{-n+1}{2}\cdot\frac{-m+1}{2}}$$

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

c) Eén van de getallen n, $n>0$, het andere <0; zonder beperking $n>0$, $m<0$.

$$\left(\frac{n}{|m|}\right)\cdot\left(\frac{m}{|n|}\right) = \left(\frac{n}{|m|}\right)\left(\frac{-|m|}{n}\right) = \left(\frac{n}{|m|}\right)\left(\frac{|m|}{n}\right)\cdot\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{|m|-1}{2}+\frac{n-1}{2}}$$

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

Voorbeeld: $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ voor $p>3$, wegens $p>0$ $\quad -3 \equiv 1 \pmod 4$

Het symbool van Jacobi $\left(\frac{n}{m}\right)$ is alleen gedefinieerd voor m oneven. Volledigheidshalve delen wij mede, dat het in sommige onderzoekingen der getallentheorie gewenst is, over een dergelijk symbool te beschikken voor even waarden van m.

Dit wordt geleverd door het symbool van Kronecker, althans van die waarden van n, waarvoor het symbool nodig is. Daar echter de toepassingen van het Kronecker-symbool op een veel verder terrein liggen, wat wij voorlopig niet zullen betreden, zullen wij dit symbool verder buiten beschouwing laten.

Wij zullen dit hoofdstuk besluiten met enkele eenvoudige stellingen, die criteria leveren voor priemgetallen van speciale gedaante.

Stelling 8: Als $p > 2$, $h < p$, $n = hp+1$ of hp^2+1
en $2^h \not\equiv 1$, $2^{n-1} \equiv 1 \pmod n$
dan is n priem.

Bewijs: Stel d is de laagste macht, waarvoor

$$2^d \equiv 1 \pmod n .$$

$n = hp^b + 1$ met $b = 1$ of 2.

$d \not| h$ wegens $2^h \not\equiv 1 \pmod n$.

$d/(n-1)$ wegens $2^{n-1} \equiv 1 \pmod n \rightarrow d/hp^b$

dus p/d, (want als $p \not| d$ was, zou d/h moeten zijn).

Volgens het theorema van Euler is

$$2^{\varphi(n)} \equiv 1 \pmod n$$

dus $d/\varphi(n) . \rightarrow p/\varphi(n)$.

Kanonieke ontbinding:

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

$$\varphi(n) = p_1^{a_1-1} \cdots p_k^{a_k-1} (p_1-1)\ldots(p_k-1).$$

$p \not| n$, dus $p/$ op p_1-1 of p_2-1 ... of p_k-1 .

Dus n heeft een priemfactor $P \equiv 1 \pmod p$.

Stel $n = Pm$. $n \equiv 1 \equiv P \pmod p \rightarrow m \equiv 1 \pmod p$.

Als $m > 1$ is, dan is dus

$$n = (up+1)(vp+1) \qquad 1 \leq u \leq v$$

$$1 + hp^b = (up+1)(vp+1) \rightarrow hp^{b-1} = uvp+u+v.$$

Voor $b = 1$ is $h = uvp+u+v$ dus $p \leq uvp < h < p$ (tegenspraak).

Voor $b = 2$ is: $hp = uvp+u+v$ $\quad p/(u+v)$, $u+v \geq p$

$2v \geq u+v \geq p$ $\quad v > \frac{1}{2}p$

$uv < h < p$; $\quad uv \leq p-2$, $u \leq \frac{p-2}{v} < \frac{2(p-2)}{p} < 2$

dus $u = 1$, $v \geq p-1$, $uv \geq p-1$ (tegenspraak)

Dus de ontbinding $n = (up+1)(vp+1)$ is onmogelijk, en $m = 1$, $n = P$.

Stelling 9: $m \geq 2$, $h < 2^m$, $n = h.2^m+1$ is een niet-kwadraatrest van p (p oneven). $\frac{n-1}{2}$

Dan is $p \equiv -1 \pmod n$

een noodzakelijke en voldoende voorwaarde voor n priem.

Bewijs: a) Stel n priem. $n \equiv 1 \pmod 4 \rightarrow (\frac{p}{n})=(\frac{n}{p}) = -1$

dus $p^{\frac{n-1}{2}} \equiv -1 \pmod n$. Voorwaarde noodzakelijk.

b) Stel $p^{\frac{n-1}{2}} \equiv -1 \pmod n$.

Stel P is een priemfactor van n.

d is de kleinste exponent, waarvoor $p^d \equiv 1 \pmod P$

$p^{n-1} \equiv 1$, $p^{P-1} \equiv 1 \pmod P$.

dus $d \nmid \frac{1}{2}(n-1); d/(n-1)$, $d/(P-1)$.

of $d \nmid 2^{m-1}h$, $d/2^m h$, $d/(P-1)$.

dus $2^m/d \rightarrow 2^m/(P-1)$ of $P = 2^m x+1$.

Daar $n \equiv 1 \equiv P \pmod{2^m}$ is $\frac{n}{P} \equiv 1 \pmod{2^m}$.

$n = (2^m x+1)(2^m y+1) \quad x \geq 1, \ y \geq 0$.

$2^m xy < 2^m xy + x + y = h < 2^m$, dus $y = 0$, $n = P$.

Voorwaarde voldoende.

Toepassingen: $h = 1$, $m = 2^k$.

$n = 2^{2^k} + 1 = F_k$

$1^2 \equiv 2^2 \equiv 1 \pmod 3$. $F_k \equiv 2 \pmod 3$, dus F_k is niet rest van 3. Dus noodzakelijk en voldoende voor F_k priem is

$F_k/3^{\frac{1}{2}(F_k-1)} + 1$.

Er is een eenvoudig criterium van Euler voor de ontbindbaarheid van de getallen van Mersenne $M_p = 2^p-1$.

Stelling 10: $k \geq 1$, $p = 4k + 3$ priem.

Noodzakelijke en voldoende voorwaarde opdat $2p+1$ priem is is:

$2^p \equiv 1 \pmod{2p+1}$.

Als dus $2p+1$ priem is, dan is $2p+1/M_p$, dus M_p is deelbaar.

Bewijs: a) Stel $2p+1 = P$ = priem. $P \equiv 7 \pmod 8 \rightarrow 2$ is rest van $P \rightarrow 2^p = 2^{\frac{P-1}{2}} \equiv 1 \pmod P$

P/M_p. Voorwaarde noodzakelijk.

$k \geq 1$, $p \geq 3$, $M_p = 2^p-1 > 2p+1 = P$,

dus M_p deelbaar.

b) Stel $2^p \equiv 1 \pmod{2p+1}$.

In stelling 8 $h = 2$, $n = 2p+1$. Dan is $h < p$

$$2^h = 4 \not\equiv 1 \pmod{n}.$$

$$2^{n-1} = 2^{2p} \equiv 1 \pmod{n}.$$

Dus n is priem. Voorwaarde voldoende.

Toepassingen: $23/M_{11}$, $47/M_{23}$, $167/M_{83}$, $263/M_{131}$
$359/M_{179}$, $383/M_{191}$, $479/M_{239}$, $503/M_{251}$.

ELEMENTAIRE GETALLENTHEORIE VII

door Prof.Dr B. Meulenbeld en Prof.Dr S.C.van Veen.

27 April 1955.

De theorie der partities.

Wij willen de laatste lezingen van deze cursus wijden aan een geheel ander gedeelte der elementaire getallentheorie. De voorgaande beschouwingen behoorden tot het gebied der multiplicatieve getallentheorie, waarbij de gehele getallen werden beschouwd als multiplicatief samengesteld uit hun priemfactoren.
In het volgende wordt een speciaal probleem der additieve getallentheorie behandeld. Hierbij worden de gehele getallen additief samengesteld gedacht uit nader te bepalen gehele elementen.
Wij beschouwen het stelsel der natuurlijke getallen 1,2,3,.....
Onder een partitie van een gegeven positief getal n verstaan wij de verdeling van n in de som van een zeker aantal gehele positieve getallen (al of niet gelijk. B.v. de partities van 5 zijn:
5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1.
Het aantal partities van 5 is dus 7.
Wij schrijven dan: p(5)=7.
Een belangrijk probleem uit deze onderzoekingen is:
Gevraagd te bepalen het aantal partities p(n) voor een gegeven waarde van n.
Hoewel dit probleem juist in de laatste tijd volledig is opgelost,zal de behandeling van deze oplossing ons te ver voeren.
Wij willen hier volstaan met enige elementaire beschouwingen, die ons althans enig inzicht kunnen verschaffen in het mysterieuze gedrag van de functie p(n).

Grafische voorstelling der partities.

Wij beschouwen 1 partitie van het getal 18, b.v.

$$18 = 7+4+3+3+1 \qquad (2)$$

Wij kunnen deze partitie voorstellen als volgt:

x x x x x x x
x x x x
x x x
x x x
x

waarin de horizontale rijen de getallen der partitie (2) voorstellen. Lezen wij dit schema verticaal, dan krijgen wij ook een partitie

$$18 = 5+4+4+2+1+1+1 \qquad (3)$$

Zulke partities als (2) en (3) noemen wij: toegevoegd of geconjugeerd. Een grafiek met m horizontale rijen geeft horizontaal gelezen een partitie in m delen; verticaal gelezen krijgen wij dan een partitie waarvan het grootste deel = m.

Stelling 10: Het aantal partities van n in m delen is gelijk aan het aantal partities van n in delen, waarvan het grootste is m.

Stelling 11: Het aantal partities van n in ten hoogste m delen is gelijk aan het aantal partities van n in delen $\leq$ m.

De voortbrengende functie van p(n).

Wanneer wij een functie F(x) hebben, die in een machtreeks kan worden ontwikkeld

$$F(x) = \sum f(n)x^n$$

waarbij de coëfficiënt van x^n gelijk is aan een zekere functie f(n) van de exponent n, dan noemen wij F(x) de voortbrengende functie van f(n). Euler heeft reeds $\pm$ 1740 op zeer eenvoudige wijze de voortbrengende functie van de partitie-functie p(n) gevonden in de uitkomst:

$$F(x) = \frac{1}{(1-x)(1-x^2)(1-x^3).....} = 1 + \sum_{n=1}^{\infty} p(n)x^n \qquad (4)$$

Wij zien de juistheid van deze uitkomst onmiddellijk uit de machtreeksontwikkeling der factoren:

$$(1-x)^{-1} = 1+x+x^2+x^3+.... = 1+x^1+x^{1+1}+x^{1+1+1}+....$$
$$(1-x^2)^{-1} = 1+x^2+x^4+x^6+... = 1+x^2+x^{2+2}+x^{2+2+2}+....$$
$$(1-x^3)^{-1} = 1+x^3+x^6+x^9+... = 1+x^3+x^{3+3}+x^{3+3+3}+....$$
$$.....$$

Wanneer wij deze reeksen vermenigvuldigen, dan levert iedere term met x^n juist 1 partitie van n, wanneer wij iedere exponent van de eerste rij in elementen 1, iedere exponent van de tweede rij in elementen 2, iedere exponent van de derde rij in elementen 3 enz. splitsen.

B.v. de partitie van 10:

$$10 = 3+2+2+2+1,$$

ontstaat bij vermenigvuldiging van x^3 uit de derde rij met x^{2+2+2} uit de tweede rij en met x^1 uit de eerste rij.

Men ziet gemakkelijk, dat iedere partitie van n op zulk een manier ontstaat, en wel precies op 1 wijze, waarmede de juistheid van (4) onmiddellijk is vastgesteld.

Speciaal met behulp van (4) heeft Euler reeds p(n) bepaald voor $n \leqq 24$. In het verloop van de functie p(n) zit op het eerste oog weinig regelmaat.
p(1)=1, p(2)=2, p(3)=3, p(4)=5, p(5)=7, p(6)=11, p(7)=15, p(8)=22,
p(n) loopt snel op:
p(16)=231, p(24)=1575, p(200)=3972999029388.

Toepassing van de theorie der voortbrengende functies op een ander eenvoudig probleem.

Ten einde dit gebruik van voortbrengende functies door een eenvoudig voorbeeld te illustreren, passen wij deze methode toe op het volgende probleem:
Gevraagd het aantal oplossingen in gehele getallen $\geqq 0$ van de diophantische vergelijking:

$$x + 2y + 3z = n \quad \text{(bij gegeven n)} \tag{5}$$

Noemen wij dit aantal f(n), dan ziet men onmiddellijk, dat de voortbrengende functie van f(n) is:

$$F(q) = \frac{1}{(1-q)(1-q^2)(1-q^3)} = \sum_{n=0}^{\infty} f(n)\, q^n \tag{6}$$

(immers iedere oplossing x_1, y_1, z_1 van (5) ontstaat op 1 enkele wijze uit de vermenigvuldiging van

$$(1-q)^{-1} = 1+q+q^2+\ldots+q^{1.x_1}+\ldots.$$
$$(1-q^2)^{-1} = 1+q^2+q^4+\ldots+q^{2.y_1}+\ldots.$$
$$(1-q^3)^{-1} = 1+q^3+q^6+\ldots+q^{3z_1}+\ldots.$$

Nu is het bij (6) heel eenvoudig F(q) in partiële breuken te splitsen:

$$F(q) = \frac{1}{(1-q)^3(1+q)(1-qe^{\frac{2\pi i}{3}})(1-qe^{\frac{4\pi i}{3}})}$$

$$= \frac{1}{6(1-q)^3} + \frac{1}{4(1-q)^2} + \frac{17}{72(1-q)} + \frac{1}{8(1+q)} + \frac{1}{9(1-qe^{\frac{2\pi i}{3}})} + \frac{1}{9(1-qe^{\frac{4\pi i}{3}})}.$$

Nu kan men zeer eenvoudig ieder der partiële breuken in een machtreeks naar machten van q ontwikkelen, aangenomen dat $|q| < 1$ is.
Men vindt dan:

$$\frac{1}{6(1-q)^3} = \sum_{n=0}^{\infty} \frac{(n+1)(n+2)}{12}\, q^n,$$

$$\frac{1}{4(1-q)^2} = \sum_{n=0}^{\infty} \frac{n+1}{4}\, q^n,$$

$$\frac{17}{72(1-q)} = \sum_{n=0}^{\infty} \frac{17}{72} q^n$$

$$\frac{1}{8(1+q)} = \sum_{n=0}^{\infty} \frac{(-1)^n}{8} q^n$$

$$\frac{1}{9(1-q.e^{\frac{2\pi i}{3}})} = \sum_{n=0}^{\infty} \frac{e^{\frac{2n\pi i}{3}}}{9} q^n$$

$$\frac{1}{9(1-qe^{\frac{4\pi i}{3}})} = \sum_{n=0}^{\infty} \frac{e^{\frac{4n\pi i}{3}}}{9} q^n$$

tenslotte is de coëfficiënt van q^n in $F(q)$ $\frac{n\pi i}{3}$ $\frac{n\pi i}{3}$

$$\frac{(n+1)(n+2)}{12} + \frac{n+1}{4} + \frac{17}{72} + \frac{(-1)^n}{8} + \frac{e^{n\pi i}(e^{\frac{n\pi i}{3}} + e^{\frac{n\pi i}{3}})}{9}$$

$$= \frac{(n+3)^2}{12} - \frac{7}{72} + \frac{(-1)^n}{8} + \frac{2}{9}(-1)^n \cos\frac{n\pi}{3}$$

Dus: $f(n) = \frac{(n+3)^2}{12} - \frac{7}{72} + \frac{(-1)^n}{8} + \frac{2}{9}(-1)^n \cos\frac{n\pi}{3}$. (7)

In deze uitkomst zit echter nog de volgende aardigheid verborgen:

$$\left| -\frac{7}{72} - \frac{(-1)^n}{8} + \frac{2}{9}(-1)^n \cos\frac{n\pi}{3} \right| \leq \frac{7}{72} + \frac{1}{8} + \frac{2}{9} = \frac{32}{72} < \frac{1}{2}.$$

Aangezien f'n) volgens zijn ontstaanswijze een <u>geheel</u> getal is en

$$\left| f(n) - \frac{(n+3)^2}{12} \right| < \frac{1}{2} \text{ is}$$

blijkt f(n) eenvoudig het gehele getal te zijn, dat zo dicht mogelijk bij $\frac{(n-3)^2}{12}$ is gelegen.

b.v. voor n is 17 is $\frac{(n+3)^2}{12} = \frac{400}{12} = 33\frac{1}{3}$, dus <u>f(17) = 33</u>.

Dergelijke problemen spelen een rol bij geldwisselproblemen, b.v. op hoeveel manieren kan een gulden worden gewisseld in centen, stuivers, dubbeltjes en kwartjes?
Het antwoord is:

$$x+5y+10z+25u=100$$

Voortbrengende functie

$$F(q) = \frac{}{(1-q)(1-q^5)(1-q^{10})(1-q^{25})} = \sum_{n=0}^{\infty} f(n)\, q^n.$$