STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1950-017

Deelbaarheidseigenschappen

Dr. P. Mullender

1950

Rapport Z.W. 1950-017.
8 November 1950.

Voordracht door Dr P. Mullender
over

DEELBAARHEIDSEIGENSCHAPPEN

in de serie "Elementaire onderwerpen van hoger standpunt uit".

Bij het bestuderen van de deelbaarheidseigenschappen van de geheel rationale getallen kunnen we ons af vragen van welke speciale eigenschappen van de geheel rationale getallen bepaalde deelbaarheidseigenschappen een consequentie zijn.

Men kan de eigenschappen van de geheel rationale getallen bijvoorbeeld in twee groepen verdelen:

1e. De eigenschappen, die voortvloeien uit de som- en productierelaties, welke tussen de geheel rationale getallen bestaan.

2e. De eigenschappen, die slechts bewezen kunnen worden als men, behalve van die som- en productierelaties ook gebruik maakt van de orderelaties tussen de geheel rationale getallen.

We kunnen nu vragen welke deelbaarheidseigenschappen tot de eerste groep behoren.

Wij beschouwen daarom een verzameling van elementen waartussen wel som- en productierelaties zijn gedefinieerd maar geen orderelaties en willen proberen hoever we in zo'n verzameling kunnen komen met de deelbaarheidseigenschappen.

Zij R een integriteitsgebied, d.w.z. een verzameling van elementen a,b,c,... met de volgende eigenschappen:

R. 1. Aan ieder geordend elementenpaar a,b zijn twee elementen $c = a + b$ en $d = a.b$ toegevoegd, resp. de som en het product van a en b.

2. $a + b = b + a$, $a.b = b.a$.

3. $a + (b + c) = (a + b) + c = a + b + c$, $a(bc) = (ab)c = abc$.

4. $(a + b)(c + d) = ac + ad + bc + bd$.

5. Er is een nulelement 0 met de eigenschap, dat $a + 0 = a$ voor alle a.

6. Bij ieder element a hoort een element -a, zodanig, dat $a + (-a) = 0$.

7. Er is een eenheidselement e met de eigenschap, dat $a.e = a$ voor alle a.

8. Er zijn geen nuldelers, d.w.z. uit $ab = 0$ volgt $a = 0$ of $b = 0$.

Uit deze eigenschappen volgen een aantal andere

R. 9. Er is maar één nulelement 0.
10. Bij ieder element a hoort maar één tegenegesteld element $-a$.
11. Voor alle a en b heeft $a + x = b$ precies één oplossing $x = b + (-a)$.
12. Voor alle a geldt $a.0 = 0$.
13. Er is maar één eenheidselement e.
14. Voor alle a en b heeft $ax = b$ hoogstens één oplossing in x, indien $a \neq 0$.

We definieren nu: Een element a heet deelbaar op een element b als er een element c bestaat, zodanig, dat $ac = b$. We schrijven $a \mid b$.

De elementen, die deelbaar zijn op e noemen we de eenheden van R en duiden we aan met $e_1, e_2, \ldots$.

De elementen, die men krijgt door een element a met de eenheden te vermenigvuldigen noemen we de geassocieerden van a.

We hebben de volgende eigenschappen:

D. 1. $a \mid b \Rightarrow ac \mid bc$.
2. $ac \mid bc \Rightarrow a \mid b$.
3. $a \mid b,\ b \mid c \Rightarrow a \mid c$.
4. $a \mid b,\ c \mid d \Rightarrow ac \mid bd$.
5. $a \mid b,\ a \mid c \Rightarrow a \mid xb + yc$.
6. $a \mid 0$ voor alle a.
7. $e \mid a,\ e_1 \mid a,\ e_2 \mid a, \ldots$ voor alle a.
8. $a \mid a,\ e_1 a \mid a,\ e_2 a \mid a, \ldots$ voor alle a.

We noemen a en b congruent modulo m als $m \mid a-b$. We schrijven $a \equiv b \bmod m$.

De congruentie is reflexief, symmetrisch en transitief.

De verzameling van alle elementen van R, die congruent zijn met een gegeven element a modulo m noemen we de restklasse van a modulo m.

Door de congruentie modulo m wordt R verdeeld in restklassen modulo m. Ieder element ligt namelijk in zo'n restklasse, terwijl twee restklassen, die een element gemeen hebben, geheel samenvallen:

Kiezen we uit elke restklasse nodulo m één vertegenwoordiger uit, dan krijgen we, wat we noemen, een volledig restsysteem modulo m.

We leggen R nu de beperking op, dat voor ieder element $m \neq 0$ het aantal restklassen modulo m eindig is. We duiden dat aantal aan met N(m). Dan geldt:

Stelling 1. $N(m.n) = N(m).N(n)$.

Bij de behandeling van de congruenties van de geheel rationale getallen komt men tot een drietal beroemde stellingen, namelijk die van Euler, Fermat en Wilson. De vraag is nu: Gelden deze stellingen ook in ons integriteitsgebied R?

Het antwoord is bevestigend, mits wij echter geschikte definities kiezen voor de begrippen relatief priem en priemelement.

Wij noemen a en b relatief priem indien er twee elementen x en y te vinden zijn, zodanig dat $a\,x + b\,y = e$. We schrijven $a \cup b$.

Dan hebben we de eigenschappen:

O. 1. $a \cup bc \Rightarrow a \cup b$ en $a \cup c$.

2. $a \cup b$ en $a \cup c \Rightarrow a \cup bc$.

3. $a \mid bc$ en $a \cup b \Rightarrow a \mid c$.

4. $a \cup m \Rightarrow a + m\,x \cup m$ voor iedere x.

De laatste eigenschap houdt in: Als één element van een restklasse modulo m relatief priem is met m, dan geldt hetzelfde voor alle elementen van die restklasse.

Nemen we alleen die restklassen, waarvoor dit het geval is en kiezen we uit elk van die restklassen een vertegenwoordiger, dan krijgen we, wat we noemen, een gereduceerd restsysteem modulo m.

Het aantal van die restklassen, dat is dus ook het aantal elementen van ieder gereduceerd restsysteem, duiden we aan met $\varphi(m)$.

Dan geldt:

Stelling 2. $\varphi(mn) = \varphi(m).\varphi(n)$ indien $m \cup n$.

Stelling 3. $a^{\varphi(m)} \equiv e \bmod m$ indien $a \cup m$. (Euler).

We noemen een element p een priemelement als $\varphi(p) = N(p) - 1$. Reserveren we de letter p voor priemelementen, dan volgt uit O.3

P. 1. $p \mid ab$ en $p \nmid a \Rightarrow p \mid b$.

Verder krijgen we als bijzonder geval van stelling 3:

P. 2. $a^{N(p)-1} \equiv e \bmod p$ indien $p \nmid a$. (Fermat).

Tenslotte geldt ook

Stelling 4. Als $r_1, \ldots, r_{N(p)-1}$ een gereduceerd restsysteem modulo p vormen, dan is

$$r_1 . r_2 \cdots r_{N(p)-1} \equiv -e \bmod p. \qquad \text{(Wilson).}$$

Van de functies N(m) en $\varphi(m)$ kunnen we nog enige andere eigenschappen aantonen.

We schrijven

$e + e = 2\,e$

$e + e + e = 3\,e$

$e + e + \ldots + e = N\,e$

We kunnen nu twee gevallen onderscheiden:

1^e. $Ne = 0$ voor zekere $N \neq 0$. In dat geval is het kleinste natuurlijk getal N, waarvoor dit geldt een priemgetal P. We noemen P de karakteristiek van R.

2^e. $Ne \neq 0$ voor alle N. In dat geval zeggen we dat de karakteristiek van R nul is.

Nu geldt:

Stelling 5. Als R de karakteristiek P heeft, dan is N(a) voor ieder element a van R een macht van P, en een analoge stelling:

Stelling 6. Als R de karakteristiek nul heeft en $a \mid Pe$, waarbij P een natuurlijk priemgetal voorstelt, dan is N(a) een macht van P.

Als bijzonder geval krijgen we, dat voor een natuurlijk priemgetal P geldt: $N(Pe) = P^K$.

Zou hetzelfde gelden voor ieder natuurlijk getal, dan zou volgen, dat K altijd dezelfde waarde zou moeten hebben. Dat is niet het geval hetgeen blijkt als we voor R nemen de verzameling van alle rationale getallen met een zuivere macht van P in de noemer. Dan is namelijk $N(P) = 1$ terwijl voor ieder ander natuurlijk priemgetal Q blijft gelden $N(Q) = Q$.

Wel kunnen we gemakkelijk aantonen:

Stelling 7: Is M(a) het kleinste natuurlijk getal, waarvoor geldt $a \mid M(a).e$, dan is $M(a) \mid N(a)$ en $N(a) \mid \{M(a)\}^K$ voor zekere K. (Dat M(a) bestaat is evident).