STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1951 - 013

Over de deelbaarheid van $a^{n-1}-1$ door n

H.J.A. Duparc

MC
1951

Over deelbaarheid van $a^{n-1}-1$ door n.

H.J.A. Duparc.

Als n ondeelbaar is en als de getallen a en n onderling ondeelbaar zijn is $a^{n-1}-1$ deelbaar door n. Gevraagd wordt of er ook samengestelde getallen n bestaan, waarvoor deze eigenschap geldt. Wij willen hieronder aangeven hoe men bij bepaalde a getallen n met de genoemde eigenschap kan vinden.

Wij beschouwen eerst het geval a=2. Zij $n=p_1p_2\ldots p_r$ een getal met de gewenste eigenschap ($p_1,\ldots,p_r$ priem). Stel $m_\rho = \frac{n}{p_\rho}$ ($\rho=1,\ldots,r$). Dan is, als 2 een primitieve wortel mod p_ρ is, omdat $2^{m_\rho p_\rho - 1}-1$ deelbaar door p_ρ is, het getal $p_\rho-1$ een deler van $m_\rho p_\rho - 1$, dus van $m_\rho - 1$ en omgekeerd, als p_ρ een deler is van $m_\rho-1$ voor $\rho=1,\ldots,r$, dan is $2^{n-1}\equiv 1 \pmod{p_\rho}$. De voorwaarde $p_\rho - 1 \mid m_\rho - 1$ ($\rho=1,\ldots,r$) is dus voldpende, maar niet noodzakelijk om getallen n van de gewenste gedaante te vinden. In het geval r=2 kan men als volgt te werk gaan om getallen $n=p_1p_2$ van het gezochte type te vinden. Men make een tabel van de getallen $2^{p_1-1}-1$ en probere of hun delers p_2, die groter dan p_1 zijn, voldoen aan de eis dat $p_1-1 \mid 2^{p_2-1}-1$. Is 2 een primitieve wortel mod p_1, dan is p_2 een veelvoud van p_1-1, vermeerderd met 1, dus het getal $n=p_1p_2$ voldoet.

p_1	$2^{p_1-1}-1$	keuze van p_2
3	3	--
5	3.5	--
7	3^2.7	--
11	3.11.31	31
13	3^2.5.7.13	--
17	3.5.17.257	257
19	3^3.7.19.73	73
23	3.23.89.683	89 ; 683
29	3.5.29.113.5461	113 ; 5461
31	3.7.11.31.151.331	151 ; 331
37	3^3.5.7.13.19.37.73.109	73 ; 109.

De kleinste oplossing die wij hierbij vinden is n=11.31=341 en men heeft

$\frac{2^{340}-1}{341}$ = 65681 66399 34839 94444 49977 36257 08043 34667 58210 33274 17990 90905 89471 07894 05038 17036 52143 33575 73947 42275.

Wenst men getallen n van b.v. de gedaante $n=p_1p_2p_3$ te vinden, dan kan men op analoge wijze te werk gaan en vindt dan de volgende tabel voor $m_3=p_1p_2$

m_3	$2^{m_3-1}-1$	eventuele keuze van p_3
15	3.43.127	43 ; 127
21	3^2.11.31.44	11 ; 31 ; 41
25	3^2.5.7.13.17.241	3 ; 7 ; 13 ; 17 ; 241
27	3.2731.8191	2731 ; 8191
33	3.5.17.257.65537	5 ; 17 ; 257 ; 65537

Niet iedere waarde van p_3 in de derde kolom is bruikbaar want men dient er eveneens voor te zorgen dat m_1 eh m_2 deelbaar zijn op $2^{n-1}-1$. Het kleinste getal n dat men op deze wijze vindt is n=3.11.17=561.

Bij de opsomming in L.E.Dickson's "History of the theory of numbers" van de door Banachiewits gevonden getallen n met $n \mid 2^n-2$ en $n<2000$ (deze opsomming bevat de getallen 341=11.31 ; 561=3.11.17 ; 1387=19.73 ; 1729=7.13.19; 1905=3.5.127) ontbreekt echter het getal n=3.5.43 dat wij uit onze 2de tabel konden vinden en het getal n=5.13.17 dat wij aldaar eveneens kunnen ontlenen als wij deze tabel voldoende ver voortzetten.

Bij a=3 verloopt het onderzoek analoog. Om een exponent $n=p_1p_2$ te vinden beschouwen wij nu de tabel

p_1	3^{p_1-1}	p_2
2	2	--
5	2^4.5	--
7	2^3.7.13	13
11	2^3.11^2.61	11 ; 61
13	2^4.5.7.13.73	73
17	2^6.5.17.41.193	41 ;193

Hier vindt men voor n o.a. de waarden n=7.13=91 ; $n=11^2=121$, terwijl uit een tabel, analoog aan de tweede bij a=2 opgestelde, voor n o.a. een waarde 5.13.17=1105 volgt.

Bij a=5 luidt onze eerste tabel

p_1	$5^{p_1-1}-1$	p_2
2	2^2	2
3	$2^3.3$	--
7	$2^3.3^2.7.31$	31
11	$2^3.3.11.71.521$	71 ; 521.

Wij vinden hier voor n o.a. de waarden 4 en 781. Een getal van 3 priemfactoren dat voldoet blijkt o.a. n=561 te zijn. Dit getal heeft de eigenschap dat $a^{560}-1$ deelbaar is door 561 voor alle a, die relatief priem zijn met 561.

Wenst men tenslotte getallen n met deze laatste eigenschap te vinden, dan merke men op dat er bij $n=p^s m$ (p priem$\geqq 3$; $s\geqq 1$; $p\nmid m$) een getal a te vinden is, dat relatief priem is met n en dat een primitieve wortel is mod p^s. De exponent $p^{s-1}(p-1)$ is dan deelbaar op n-1, wat slechts mogelijk is voor s=1.

Is $n=2^s pm$ ($s\geqq 1$; p priem$\geqq 3$) dan is, als a een oneven primitieve wortel mod p is, het getal p-1 deelbaar op $2^s pm-1$, ~~dus op $2^s m-1$~~, wat uitgesloten is want p-1 is even en $2^s m-1$ is oneven. Is $n=2^s$, dan is er een a te vinden waarvan de exponent mod 2^s gelijk is aan 2^{s-2}, zodat 2^{s-2} deelbaar moet zijn op 2^s-1, wat uitgesloten is voor $s\geqq 3$. Voor s=2 is n=4 en dan heeft men voor a=3 de relatie $3^3-1\equiv 2 \pmod 4$, zodat geen enkele macht van 2, die niet priem is, voldoet.

Is n=pq (p,q priem), dan is als wij $p<q$ onderstellen, en als a een primitieve wortel mod q is, die onderling ondeelbaar is met pq, het getal q-1 deelbaar op pq-1, dus op p-1, wat wegens $p<q$ uitgesloten is.

Het getal n bevat dus slechts verschillende oneven priemfactoren en hun aantal is $\geqq 3$.

Om zo 'n getal n van de gedaante pqr te vinden, waarbij $3\leqq p<q<r$, (p,q,r priem), stelle men qr-1=x(p-1) ; pr-1=y(q-1) ; pq-1=z(r-1). In het geval p=3 is vanzelf aan de eerste relatie voldaan en men krijgt dan 3r-1=y(q-1) ; 3q-1=z(r-1), dus, na eliminatie van r,

$$q-1=\frac{2z+6}{zy-9}.$$

Wegens $r\geqq q-1$ is $z\leqq 2$; wegens $z\neq 1$ moet dus z=2 zijn. Men vindt dan wegens $2y-9\mid 10$, dat 2y-9=1,2,5 of 10 is, dus slechts y=5 of 7. Als y=7 is q=3, wat niet kan bij p=3. Dus y=5. Dan is q=11 en r=17, zodat men het

getal n=3.11.17=561 vindt. Men ziet gemakkelijk in dat dit het kleinste getal is met de gewenste eigenschap, want er is geen zo 'n getal van 4 factoren te vinden onder 561 en de getallen met 3 factoren bevatten de factor 3 niet, zodat men slechts heeft te onderzoeken n=5.7.11 en 5.7.13, welke echter geen van beide voldoen aan de relatie $r-1 \mid pq-1$.