STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1956-005

Enige generalisaties van de getallen van Poulet en Carmichael

H.J.A. Duparc

1956

MATHEMATISCH CENTRUM
2e Boerhaavestraat 49
A m s t e r d a m -O.

Rapport ZW 1956-005

Enige generalisaties van de getallen van Poulet en Carmichael

H.J.A. Duparc

Verschillende wiskundigen hebben de gedachte gehad om een eigenschap die voor priemgetallen geldt te gebruiken als methode van onderzoek naar primaliteit van een gegeven natuurlijk getal. Bij eigenschappen die niet karakteristiek zijn voor priemgetallen dient men dan de uitzonderingsgevallen te kennen, dat zijn de samengestelde getallen die de bewuste eigenschap ook bezitten. Wij zullen hier een aantal uitzonderingsgevallen van dergelijke eigenschappen nader beschouwen.

Als p priem is geldt volgens Fermat $p \mid 2^{p-1}-1$. Er blijken echter oneindig veel samengestelde m te zijn met $m \mid 2^{m-1}-1$ (getallen van Poulet, naar Poulet die al dergelijke $m < 10^8$ heeft getabelleerd [1]). Dit is op tweeërlei wijze aan te tonen:

1^o: Is m een Pouletgetal, dan $M=2^m-1$ ook [2] (Sierpiński).

2^o: Als $n < m < 2^n$ dan is $(2^{2^n}+1)(2^{2^m}+1)$ een Pouletgetal [3] (Jarden).

Wij geven hier de generalisatie: Bij gegeven natuurlijke $a \neq 1$ bestaan er oneindig veel samengestelde getallen m met $m \mid a^{m-1}-1$. Ook dit is op diverse wijzen aan te tonen [4] :

1^o: Als m voldoet aan $m \mid a^{m-1}-1$ en $(m,a-1)=1$, dan voldoet $M=\frac{a^m-1}{a-1}$ ook aan deze beide relaties;

2^o: Als $n < m < a^n$ dan voldoet $M = \dfrac{a^{a^{n+1}}-1}{a^{a^n}-1} \; \dfrac{a^{a^{m+1}}-1}{a^{a^m}-1}$ aan $M \mid a^{M-1}-1$;

3^o: Als p ondeelbaar is en $p \nmid a^2-1$, dan voldoet $m = \dfrac{a^{2p}-1}{a^2-1}$ aan $m \mid a^{m-1}-1$.

Het is mij niet bekend of er bij gegeven a en b oneindig veel samengestelde m zijn met $m \mid a^{m-1}-1$ en $m \mid b^{m-1}-1$. Dat er echter dergelijke getallen zijn blijkt als volgt.

Er bestaan samengestelde getallen m die voldoen aan $m \mid a^{m-1}-1$ voor alle a met $(a,m)=1$ (getallen van Carmichael), bv. $m=3.11.17$. Opdat m deze eigenschap bezitte is het nodig en voldoende [5] dat m quadraatvrij is en dat elke priemdeler p van m voldoet aan $p-1 \mid m-1$ (ofwel $p-1 \mid \frac{m}{p}-1$). Bijgevolg moet m ook oneven zijn. Het is mij evenmin bekend of er oneindig veel getallen van Carmichael zijn.

Als verdere generalisatie beschouwen wij de rij (u) gedefinieerd door

$$u_0=0, \; u_1=1, \; u_{n+2}=au_{n+1}+bu_n \qquad (n = 0,1,\dots)$$

met $b \neq 0$ (anders vinden wij het bovenstaande terug)...

rij (v) met $v_n=u_{2n}/u_n$, welke ook te definiëren is door

$$v_0 = 2,\ v_1 = a,\ v_{n+2} = av_{n+1} + bv_n \quad (n=0,1,\ldots),$$

heeft men $p \mid v_p - a$, indien p een priemgetal is. Wij onderzoeken nu weer of er samengestelde getallen m zijn met $m \mid v_m - a$ (bijna-priemgetallen van de tweede orde).

Voor het geval dat a=b=1 (rij van Fibonacci) blijken er oneindig veel zulke getallen m (getallen van Van der Poel) te zijn. Het bewijs [6] gebruikt de eigenschap: Is m samengesteld en voldoet m aan $(m,6)=1$, $m \mid v_m - 1$, dan bezit het getal $M=v_m$ ook deze drie eigenschappen.

Tot dusverre bleek het mij slechts mogelijk deze eigenschap te generaliseren voor het geval dat a willekeurig is, maar $b=\pm 1$.

Men kan zich voorts afvragen of er samengestelde getallen m zijn, die voldoen aan $m \mid v_m - a$ voor alle rijen (u) met $(m,b)=1$ (getallen van Carmichael van de tweede orde). Het laat zich aantonen dat zo'n getal m allereerst een gewoon getal van Carmichael moet zijn. Verder blijkt dat de nodig en voldoende voorwaarde die aan m moet worden opgelegd als volgt luidt.

Zij p een willekeurige priemdeler van m. Is het gehele quotiënt $\frac{m-1}{p-1}$ even dan moet ook $\frac{m-1}{p+1}$ geheel en even zijn; is echter $\frac{m-1}{p-1}$ oneven dan moet ook $\frac{m+1}{p+1}$ oneven zijn. Onder de 10^8 liggen geen dergelijke getallen m, erboven zijn ze (nog?) niet gevonden.

[1] P. Poulet, Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à 100 000 000, Sphinx 8(1938), 42-52.

[2] W. Sierpiński, Remarque sur une hypothèse des chinois concernant les nombres $\frac{2^n-2}{n}$, Coll.Math.I (1947),9.

[3] D. Jarden, Existence of an infinitude of composite n for which $2^{n-1} \equiv 1 \pmod{n}$, Riv.Lemat. 4(1950), 65-67.

[4] H.J.A. Duparc, On almost primes, Rapport ZW 1955-012, Math.Centrum, 1-4.

[5] R.D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, Amer.Math.Monthly 19 (1912), 22-27.

[6] H.J.A. Duparc, On almost primes of the second order, Rapport ZW 1955-013, Math.Centrum, 1-13.