STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1953 - 004

Voordracht in de serie Actualiteiten

H.J.A. Duparc op 31 jan.1953

On Carmichael numbers, Poulet numbers, Mersenne numbers and Fermat numbers

1953

Rapport ZW 1953-004

Voordracht door H.J.A. Duparc in de serie
Actualiteiten op 31 Januari 1953.

On Carmichael numbers, Poulet numbers, Mersenne numbers and Fermat numbers.

§1. Introduction.

The theorem of Fermat says that $a^{p-1} \equiv 1 \pmod{p}$ for all primes p and for all integers a which are prime to p.

For odd p and a=2 this result was already known to the Chinese, who incorrectly believed that also the converse of this theorem is true, which says that all integers satisfying

$$(1) \qquad 2^{m-1} \equiv 1 \pmod{m}$$

are prime. If this were true it would give us a means for testing a number m on primality. In order still to be able to apply this test for integers which are not too large, Poulet [1]) made a table of composite m which are $< 10^8$ and satisfy (1).

We shall call every composite m which satisfies (1) a Poulet number or pseudo prime. Banachiewicz [2]) gave in 1909 five Poulet numbers < 2000 and later found the two others < 2000.

We shall prove that there exist infinitely many Poulet numbers. Proofs of this result were already given by Sierpiński [3]) and Jarden [4]).

Sierpiński considered numbers $m_0, m_1, \ldots,$ satisfying

$$\text{I} \qquad m_{h+1} = 2^{m_h} - 1 \qquad (h = 0,1,\ldots), \qquad (m_0 \text{ prime})$$

whereas Jarden used the sequence

$$\text{II} \qquad u_h = 2^{2^h} + 1 \qquad (h = 0,1,\ldots).$$

We shall generalise their results and deduce further results on the sequences I and II.

Further we consider composite integers m for which (1) holds for all integers a prime to m. We shall call these integers of which Carmichael [5]) proved some properties Carmichael numbers and derive properties of them.

§2. The sequence I.

Definition. A Mersenne number is a number of the form 2^p-1, where p is prime. Consequently a prime of the form 2^p-1 is a Mersenne number.

Theorem 1. If m satisfies (1), then $M = 2^m-1$ also satisfies (1) [3].

Proof. From $m \mid 2^{m-1}-1$ we infer

$$M = 2^m-1 \mid 2^{2^{m-1}-1}-1 \mid 2^{2^m-2}-1 = 2^{M-1}-1.$$

Corollary . Every Mersenne number is a prime or pseudo prime.

Theorem 2. There exist infinitely many Poulet numbers [3].

Proof. The sequence I with $m_o = 11$ gives in virtue of $m_1 = 2^{11}-1 = 23.89$ for all integer $h \geqslant 1$ composite numbers m_h which by theorem 1 satisfy (1). Hence there exist infinitely many Poulet numbers.

We deduce further properties of the Mersenne numbers and of sequence I.

Obviously either every element of sequence I is prime or there exists a positive integer k such that m_k is prime, m_{k+1} is composite. From theorem 1 we then see that all elements m_h with $h \geqslant k+1$ are pseudo prime.

In order to find a further result on composite numbers of sequence I we use a special case of a result of Bang generalised by C.G. Lekkerkerker [6] which says that for every odd m the number 2^m-1 possesses a prime factor which does not occur in any number 2^d-1 with $0 < d < m$. We use this result to prove the following

Theorem 3. If the number m possesses at least s different odd prime factors, then $M = 2^m-1$ possesses at least $S = 2^s-1$ different prime factors.

Proof. Put $m = p_1 p_2 \cdots p_s n$, where $p_1, \ldots, p_s$ are different primes. Now let $i_1, \ldots, i_t$ be a combination of t of the s integers $1, \ldots, s$ $(1 \leqslant t \leqslant s)$. Put $q_{i_1 \ldots i_t} = 2^{p_{i_1} \ldots p_{i_t}} - 1$. Then any $q = q_{i_1 \ldots i_t}$ possesses at least one prime factor which does not occur in any $q_{i_1 \ldots i_u}$ with $u = 1, \ldots, t$, which differ from q. In fact every common prime factor of $q_{i_1 \ldots i_t}$ and such a $q_{i_1 \ldots i_u}$ is a prime factor of a $q_{i_1 \ldots i_v}$ with $v < t$ and by Bang's result a prime factor of q exists which does not occur in any $q_{i_1 \ldots i_v}$ with $v < t$. Consequently by considering all $\binom{s}{t}$ divisors $q_{i_1 \ldots i_t}$ of M we find $\binom{s}{t}$ different prime divisors of M. Using this result for $t = s, s-1, \ldots, 1$ we obtain certainly $\sum_{j=1}^{s} \binom{s}{j} = 2^s-1$ different prime factors of M.

Corollary 1. By the general result of Bang we can apply the theorem also to expressions of the form $\frac{a^m-b^m}{a-b}$ instead of 2^m-1 for all $m \geqslant m_o$ where m_o only depends on a and b.

Corollary 2. If s(m) denotes the number of different prime factors of m and $T(m) = 2^m-1$, then the result of theorem 3 may be formulated as follows

$$s(T(m)) \geqslant T(s(m)).$$

Corollary 3. Considering the sequence I with $m_0 = 11$, we have $s(m_1) = 2$, hence by theorem 1 there exist Poulet numbers the number of prime factors of which is greater than every given integer.

Theorem 4. If in sequence I the element $m = m_k$ is prime, $M = m_{k+1}$ composite, then every composite divisor of M is a pseudo prime [7].

Proof. For the composite divisor M of M the assertion follows from theorem 1. Now let n be a composite divisor of M. We prove the theorem by induction and may assume the assertion proved for any divisor $>$ n of M. Let N be a composite divisor of M such that $q = \frac{N}{n}$ is prime. Since $q \mid 2^m-1$ and since m is prime we have $m \mid q-1$. Hence $n \mid M = 2^m-1 = 2^{q-1}-1$. Since $N > n$ we have by induction $n \mid N \mid 2^{N-1}-1 = 2^{qn-1}-1$. Hence $n \mid 2^{n-1}-1$.

Remark. It is not true that if m has the property that all its divisors are prime or pseudo prime, also $M = 2^m-1$ has this property. For instance take $m = 2^{11}-1 = 23.89$. By theorem 1 the integer m is a pseudo prime of two factors, hence all divisors of m are prime. The number $M = 2^m-1$ possesses the factors $2^{23}-1$, $2^{89}-1$ and hence also the factor 47 of $2^{23}-1$. The divisor $d = 47(2^{89}-1)$ of M however does not satisfy $2^{d-1} \equiv 1 \pmod d$ for $2^{89}-1 \nmid 2^{47(2^{89}-1)-1}-1$, because $47(2^{89}-1)-1 \equiv 46 \pmod{89}$.

In order to find Poulet numbers of the form $m = pq$, where p and q are different primes, we remark that **from** $p \mid m \mid 2^{m-1}-1$ and $p \mid 2^{p-1}-1$ follows $p \mid 2^{q-1}-1$ and similarly $q \mid 2^{p-1}-1$. Conversely from the last two relations follows for different primes p and q that pq satisfies (1). For instance, take $p = 11$, then $q \mid 2^{10}-1 = 3.11.41$, hence we must try either $q = 3$ or $q = 41$. Now $q = 3$ does not satisfy $11 \mid 2^{q-1}-1$, but $q = 41$ does. So $m = 11.41$ is a pseudo prime.

Similarly Poulet numbers of the form $m = pqr$ (where p, q and r are different primes) can be found from $p \mid 2^{qr-1}-1$, $q \mid 2^{pr-1}-1$, $r \mid 2^{pq-1}-1$ and so on. For instance $p = 3$, $q = 5$ gives $m = 3.5.43 = 645$.

§ 3. The sequence II.

Definition. A Fermat number is a number of the form $2^{2^h}+1$ where h is a non negative integer. Consequently every prime of the form 2^n+1 is a Fermat **number**.

Theorem 5. If $0 \leq k \leq 2^n-n-1$, the number $u = \prod_{h=n}^{n+k}(2^{2^h}+1)$ is a Poulet number.

Remark. For $k = 0$ and $k = 1$ (supposed $n \geq 2$) this property was proved by Jarden [4].

Proof. Put $u_h = 2^{2^h}+1$ $(h = 0,1,\ldots)$. Consider an arbitrary positive integer n and an integer k satisfying $0 \leq k \leq 2^n-n-1$. If $0 \leq i < j$ the integers u_{n+i} and u_{n+j} are relatively prime, for if a prime p divides u_{n+i} we have

$$2^{2^{n+i}} \equiv -1 \pmod p,\quad 2^{2^{n+i+1}} \equiv 1 \pmod p,\quad 2^{2^{n+j}} \equiv 1 \pmod p;$$

hence $p \nmid u_{n+j}$. Consequently to prove the theorem it is sufficient to prove $u_i \mid 2^{u-1}-1$ for $i = 0,1,\ldots,k$. Now for $i = 0,1,\ldots,k$ we get on account of $n+i+1 \leq n+k+1 \leq 2^n$ the relations

$$2^{n+i+1} \mid 2^{2^n} \mid (2^{2^n}+1)(2^{2^{n+1}}+1)\ldots(2^{2^{n+k}}+1)-1 = u-1,$$

hence

$$u_{n+i} = 2^{2^{n+i}}+1 \mid 2^{2^{n+i+1}}-1 \mid 2^{u-1}-1,$$

which proves the theorem.

Corollary. For all $n \geq 0$ the integer k may be taken $= 0$, hence every non prime Fermat number is a Poulet number.

Second proof of theorem 2.

By theorem 5 there exist Poulet numbers with arbitrary many prime factors. This proves theorem 2.

Theorem 6. If the number $M = 2^{2^m}+1$ is composite, every composite factor of M is a Poulet number.

Proof. For the divisor M of M the assertion follows from theorem 5, corollary. Now let n be a composite divisor of M. We prove the theorem by induction and may assume the assertion proved for any divisor $> n$ of M. Let N be a composite divisor of M such that $q = \frac{N}{n}$ is prime. Since $q \mid 2^{2^a}+1$ we have $q \mid 2^{2^{a+1}}-1$ and $q \nmid 2^b-1$ for $0 < b < 2^{a+1}$. Hence $2^{a+1} \mid p-1$, $2^{2^{a+1}}-1 \mid 2^{p-1}-1$ and on account of $n \mid M = 2^{2^a}+1 \mid 2^{2^{a+1}}-1$ we have $n \mid 2^{p-1}-1$. Since $N > n$ we have by induction $n \mid N \mid 2^{N-1}-1 = 2^{qn}-1$. Hence $n \mid 2^{n-1}-1$.

§ 4. Carmichael numbers.

We now consider the above defined Carmichael numbers. By definition they satisfy

(2) $\qquad a^{m-1} \equiv 1 \pmod m$

for each a which is prime to m. Obviously every Carmichael number is a Poulet number. In order to deduce some properties of these numbers we prove the

Lemma. If a, m and n are positive integers with $(a,m) = 1$, then there exists a positive integer b satisfying $b \equiv a \pmod m$ and $(b,mn) = 1$.

Proof. Suppose $n = n_1 n_2$, where n_1 contains only prime factors which divide m and where $(n_2,m) = 1$. Then by the Chinese remainder theorem an integer b exists with

$$b \equiv a \pmod m; \qquad b \equiv 1 \pmod{n_2}.$$

We then have

$$(b,n_2) = 1, \quad (b,m) = (a,m) = 1, \text{ hence } \quad (b,n_1) = 1,$$

whence we find

$$(b,mn) = (b,mn_1n_2) = 1.$$

Corollary. If a primitive root mod m exists, there also exists a primitive root mod m which is prime to mn, where n is an arbitrary integer.

In fact let a be a primitive root mod m, then $(a,m) = 1$. By the lemma there exists an integer b with $b \equiv a \pmod{m}$ (hence also b is a primitive root mod m) and with $(b,mn) = 1$.

Theorem 7. A Carmichael number is [5]):

1°. Odd;

2°. Quadratfrei;

3°. The product of at least three different prime factors.

Proof.

1°. If $m = 2pn$, where p is an odd prime, is a Carmichael number, then by the corollary of our lemma a primitive root b of p exists which is prime to m. From $b^{p-1} \equiv 1 \pmod{p}$ and $b^{2pn-1} \equiv 1 \pmod{p}$ we deduce $p-1 \mid 2pn-1$, which is impossible since $p-1$ is even and $2pn-1$ odd.

In the case no odd prime divides the composite even number m we have $m = 2^h$ $(h \geqslant 2)$. If $h = 2$, thus $m = 4$ we have the relation $3^3 \equiv -1 \not\equiv$ $\not\equiv 1 \pmod{4}$, hence m is no Carmichael number. If $h \geqslant 3$ a number a can be found satisfying $a^{2^{h-2}} \equiv 1 \pmod{2^h}$, $a^k \not\equiv 1 \pmod{2^h}$ if $0 < k < 2^{h-2}$. If a were a Carmichael number we had $a^{2^h-1} \equiv 1 \pmod{2^h}$ hence $2^{h-2} \mid 2^h-1$, which is impossible.

2°. Suppose that $m = p^2n$, where p is an odd prime, is a Carmichael number. By the corollary of the lemma an integer b exists which is a primitive root mod p^2 with $(b,m) = 1$. Then from $b^{p(p-1)} \equiv 1 \pmod{p^2}$ and $b^{p^2n-1} \equiv 1 \pmod{p^2}$ we deduce $p(p-1) \mid p^2n-1$ which is impossible since p does not divide p^2n-1.

3°: Suppose $m = pq$, where p and q are different odd primes. By the corollary of the lemma a primitive root b mod p exists which is prime to m. From $b^{p-1} \equiv 1 \pmod{p}$ and $b^{pq-1} \equiv 1 \pmod{q}$ we deduce $p-1 \mid pq-1$, hence $p-1 \mid q-1$. Similarly $q-1 \mid p-1$, hence $p-1 = q-1$, $p = q$ which contradicts the assertion.

Theorem 8. If $m = p_1 p_2 \cdots p_s$ where $p_1, \ldots, p_s$ are different primes and $s \geqslant 3$, then the number m is a Carmichael number if and only if

$$p_i-1 \mid m_i-1, \text{ where } m_i = \frac{m}{p_i} \qquad (i = 1, \ldots, s).$$

Proof. For $i = 1, \ldots, s$ we know by our lemma the existence of a primitive root a_i mod p_i which is prime to m. Then from $a_i^{p_i-1} \equiv 1 \pmod{p_i}$, $a_i^{m-1} \equiv 1 \pmod{p_i}$ we obtain $p_i-1 \mid m-1$, hence $p_i-1 \mid m_i-1$.

Conversely if $p_i-1 \mid m_i-1$ for $i = 1, \ldots, s$, then we have for $i = 1, \ldots, s$ $p_i-1 \mid m-1$, hence for all a prime to m we have

$$p_i \mid a^{p_i-1}-1 \mid a^{m-1}-1, \text{ thus } m \mid a^{m-1}-1.$$

Remark. Using this property Ore finds Carmichael numbers [8]).

I do not know whether there are infinitely many Carmichael numbers.

Remark. It is obvious that there are only a finite number of Carmichael numbers $m = p_1p_2\cdots p_s$ ($p_1,\ldots,p_s$ prime) of which s-1 of the s prime factors are given. In fact by theorem 9 we have for the remaining prime p_s the relation $p_s-1 \mid p_1p_2\cdots p_{s-1}-1$, so only a finite number of values of p_s are possible.

Beeger [9]) proved that there are only a finite number of Carmichael numbers $m = pqr$ (p,q,r prime), the smallest prime factor of which is given (if one of the other prime factors is given, this property is obvious from the above remark).

I prove the following extension of Beeger's theorem.

Theorem 9. There exist only a finite number of Carmichael numbers $p_1p_2\cdots p_s$ ($p_1,\ldots,p_s$ prime) of which s-2 prime factors are given [10]).

Proof. Without loss of generality we may suppose that the Carmichael number $m = npq$, where n is given and where the primes p and q satisfy the relation $p < q$.

By theorem 8 positive integers x and y must exist with

(3) $$qn-1 = x(p-1); \quad pn-1 = y(q-1).$$

We then have $x > y$, and further $x \neq 1$, $y \neq 1$ (since p and q are prime), Eliminating q from the relations (3) we find

(4) $$p-1 = \frac{(n-1)(n+y)}{xy-n^2}.$$

Since $p \leqslant q-2$ the second relation (3) gives

$$y = \frac{pn-1}{q-1} \leqslant \frac{pn-1}{p+1} = n - \frac{n+1}{p+1},$$

thus

(5) $$y \leqslant n-1.$$

We now distinguish two cases.

1°. $xy-n^2 \geqslant 2$. Then from (4) and (5) it follows

$$p \leqslant 1 + \frac{(n-1)(2n-1)}{2} < 1 + (n-1)(2n+\tfrac{1}{2}-\sqrt{n-\tfrac{3}{4}}).$$

2°. $xy-n^2 = 1$. By (5) and $y \neq 1$ we may put $y = n-d$ with $1 \leqslant d \leqslant n-2$. Then we have $x = \frac{n^2+1}{y} = \frac{n^2+1}{n-d} = n+d+\frac{d^2+1}{n-d}$, hence $x \geqslant n+d+1$. Thus

$$1 = xy-n^2 \geqslant (n+d+1)(n-d)-n^2 = -d^2+n-d,$$

hence

$$d \geqslant -\tfrac{1}{2}+\sqrt{n-\tfrac{3}{4}}.$$

Then (4) gives

(6) $$p \leqslant 1+(n-1)(2n+\tfrac{1}{2}-\sqrt{n-\tfrac{3}{4}}).$$

From the second relation (3) and $y \geqslant 2$ we conclude $q \leqslant 1+\tfrac{1}{2}(pn-1)$, which proves the assertion.

Remark. The relation (6) is rather sharp as is seen by taking $n = 43$, in which case it gives $p \leqslant 3361$ and actually $m = 43\cdot 3361\cdot 3907$ is a Carmichael number.

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) T. Banachiewicz, Spraw Tow Nauk, Warsaw 2(1909), 7-10, found the 5 numbers

$341=11.31$; $561=3.11.17$; $1387=19.73$; $1729=7.13.19$; $1905=3.5.127$,

to which he added afterwards

$645=3.5.43$; $1105=5.13.17$.

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

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

5) R.D. Carmichael, Note on a new number theoretic function, Bull. Amer. Math. Soc. 16(1909), 232-238.

R.D. Carmichael, On composite numbers P which satisfy the Fermat Congruence $a^{P-1} \equiv 1 (\mathrm{mod}\ P)$, Amer. Math. Monthly 19(1912), 22-27.

6) C.G. Lekkerkerker, Prime factors of the elements of certain sequences of integers, Math. Centrum, Rapport ZW 1953-003.

7) H.J.A. Duparc, On Mersenne numbers and Poulet numbers, Math. Centrum, Rapport ZW 1953-001.

8) O. Ore, Number theory and its history, New York 1948, 329-339.

9) N.G.W.H. Beeger, On composite numbers n for which $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$ for every a prime to n, Scripta Math. 16(1950), 133-135.

Instead of (8) he proves the relation $p \leq 1+2(n-1)^2$, which is stronger than our result only for n = 3 and 5.

10) H.J.A. Duparc, On Carmichael numbers, Simon Stevin, 29(1952), 21-24.