STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1952- 27r

On Carmichael numbers

H.J.A. Duparc

Reprinted from
Simon Stevin, 29(1951/53), p 21-24

1952

ON CARMICHAEL NUMBERS

by H. J. A. Duparc (Amsterdam)

The theorem of Fermat says that $c^{p-1} \equiv 1 \pmod{p}$ for all c which are relatively prime with the prime p. If however $c^{n-1} \equiv 1 \pmod{n}$ for all c relatively prime to n, the number n is not necessarily prime. Any composite n which has this property is called a Carmichael number. [1])

It is easily shown [2]) that a Carmichael number n possesses the three following properties

1°. n is odd;

2°. n is quadratfrei;

3°. n contains at least three different prime factors.

Be $n = p_1 p_2 \dots p_r$, where the prime numbers $p_1, \dots, p_r$ satisfy $p_1 < p_2 < \dots < p_r$. Let for $\varrho = 1, \dots, r$ the number c_ρ be prime to n and be a primitive root mod p_ρ (the existance of such an integer c_ρ is obvious); then the exponent $p_\rho - 1$ of c_ρ mod p_ρ divides $n - 1$, hence $p_\rho - 1$ divides $\frac{n}{p_\rho} - 1$.

Conversely if $p_\rho - 1$ divides $\frac{n}{p_\rho} - 1$ for all $\varrho = 1, \dots, r$, then $p_\rho - 1$ divides also $n - 1$, hence n is a Carmichael number.

The necessary and sufficient condition for $n = p_1 p_2 \dots p_r$ to be a Carmichael number is therefore

$$(1) \qquad p_\rho - 1 \text{ divides } \frac{n}{p_\rho} - 1 \quad (\varrho = 1, \dots, r)$$

We now proceed to give a generalisation of a theorem of Beeger [3]) which generalisation says:

There exists only a finite number of Carmichael numbers of r prime factors, the smallest $r - 2$ of which are given.

More precisely, if $n = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$, then

---

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

2) For a proof of these properties also given by Carmichael see for instance: O. Ore, Number theory and its history, N.Y. 1948, p. 332—333.

3) N. G. W. H. Beeger. On composite numbers n for which $a^{n-1} \equiv 1$ (mod n) for every a, prime to n, Scripta Mathem. 16 (1950), 133—135. In this article a table of Carmichael numbers with $r = 3$ and $p_1 \leqq 43$ is given.

(2) $$p_{r-1} \leqq 1+2\,(m-1)^2;\; p_r \leqq m\,(m-1)^2 + \tfrac{1}{2}\,(m+1),$$

where $m = p_1 p_2 \dots p_{r-2}$, provided $m > 3$.

The case $r = 3$ yields Beegers theorem.

To prove the theorem, for convenience put $p_{r-1} = p$; $p_r = q$. Then from (1), considered for $\varrho = r-1$ and r, follows the existance of two integers x and y ($x \neq 1$; $y \neq 1$; $y > x$) with

(3) $$mp - 1 = x\,(q-1);\; mq - 1 = y\,(p-1).$$

Eliminating q one obtains

(4) $$p - 1 = \frac{(m-1)\,(m+x)}{xy - m^2}.$$

Since $p \leqq q - 2$ the first relation of (3) gives

$$x \leqq \frac{mp-1}{p+1} = m - \frac{m+1}{p+1},$$

hence $x \leqq m - 1$.

If $x = m - 1$, from (4) follows, in virtue of $m > 1$ hence $xy > m^2$, that $y > \dfrac{m^2}{m-1} = m + 1 + \dfrac{1}{m-1}$ hence $y \geqq m + 2$ so $xy - m^2 \geqq m - 2$ and then again from (4) one obtains for $m > 3$

$$p - 1 \leqq \frac{(m-1)\,(2m-1)}{m-2} < 2(m-1)^2$$

If $x \leqq m - 2$ relation (4) gives since $xy - m^2 \geqq 1$

$$p - 1 \leqq 2\,(m-1)^2.$$

So in either case we have $p \leqq 1 + 2(m-1)^2$.

Since $x \geqq 2$ the first relation of (3) gives $q - 1 \leqq \frac{1}{2}\,(mp-1)$, wherefrom the second inequality of (2) follows.

We can however go somewhat further and prove for $m > 3$

(5) $$p \leqq 1 + (m-1)\,(2m + \tfrac{1}{2} - \sqrt{m - \tfrac{3}{4}}).$$

To prove this result we consider two cases.

1°. $xy - m^2 \geqq 2$. Above we found $x \leqq m - 1$. We then get

$$p \leqq 1 + \frac{(m-1)\,(2m-1)}{2} = 1 + (m-1)\,(m - \tfrac{1}{2})$$
$$< 1 + (m-1)(2m + \tfrac{1}{2} - \sqrt{m - \tfrac{3}{4}}).$$

2°. $xy - m^2 = 1$. Since $2 \leqq x \leqq m - 1$, put $x = m - d$ with $1 \leqq d \leqq m - 2$. Then

$$y = \frac{m^2+1}{m-d} = m + d + \frac{d^2+1}{m-d}, \text{ hence } y \geqq m + d + 1.$$

So

$$1 = xy - m^2 \geqq - d^2 + m - d \text{ or } d \geqq - \tfrac{1}{2} + \sqrt{m - \tfrac{3}{4}}.$$

From (4) we find immediately the required result (5).

The result (5) is not better than Beeger's only if m $\leqq 6$, so only for $m = 5$. That the result is a good estimation is shown by taking $m = 43$ in which case from (5) we get $p \leqq 3361$ and actualy $n = 43.3361.3907$ is a Carmichaelnumber.

Beeger constructed his table by taking $x = 2,3, \ldots, m - 1$ and choosing y in such a way that $xy - m^2$ divides $(m - 1)\,(m + x)$. We might however proceed as follows.

Take $c = xy - m^2 = 1,2, \ldots, 2m - 4$ and obtain values x and y with $xy = m^2 + c$, which from (4) satisfy $(m - 1)\,(m + x) \equiv 0$ (mod c) and similarly $(m - 1)\,(m + y) \equiv 0$ (mod c).

In the remaining cases we have $c \geqq 2m - 3$ so from (4) we then have

$$p \leqq 1 + \frac{(m-1)\,(2m-1)}{2m-3} = m + 1 + \frac{1}{2m-3}, \text{ hence } p \leqq m.$$

If m is prime this contradicts $p \geqq m + 2$ so that in that case the work is done by only considering the above mentioned possibilities for c. If m is composite we must further consider the cases in which the prime p is $\leqq m - 2$.

A few remarks may help to reduce the work.

1°. Since $x \geqq 2$ the integer $m^2 + c$ is not prime.

2°. Since $p - 1$ divides $mq - 1$, the prime p satisfies $p \not\equiv 1$ (mod m_1), where m_1 is any prime factor of m. The same holds for q.

3°. If $m - 1$ and c are relatively prime, we have for $m < c < 2m$ the relation $m + x \equiv 0$ (mod c) so $x = c - m$. But then

$$p = 1 + \frac{(m-1)\,c}{c} = m \text{ which is impossible.}$$

4°. If m_1 denotes any prime factor of m,we have $c \neq m_1 c_1$, where $m_1 \nmid c_1$.

In fact we have $m_1 \nmid m - 1$, hence $m_1 \mid m + x$, so $m_1 \mid x$ and similarly $m_1 \mid y$. Herefrom follows $m_1^2 \mid xy = m^2 - c$, which contradicts $m_1^2 \nmid c$.

Using these remarks the number of values c to be investigated can be reduced considerably. For instance if $m = 15$, we have $1 \leqq c \leqq 26$, but in virtue of 1° the cases $c = 2, 4, 8, 14, 16, 26$ do not occur, in virtue of 3° the cases $c = 17, 19, 23, 25$ may be omitted and in virtue of 4° we do not have to consider $c = 3, 5, 6, 10, 12,$

15, 20, 21, 24. So only the cases $c = 1, 7, 9, 11, 13, 18, 22$ are left. We show shortly how the investigation proceeds for these cases.

$c = 1$; $xy = 226$; $x = 2$; $y = 113$. But then $q = 1 + 14.128 = 1793$ is not prime.

$c = 7$; $xy = 232$; $x = 2$, 4 or 8; $y = 116, 58$ or 29. Only $x = 8$, $y = 29$ gives for both p and q suitable prime values 47 resp. 89, which also satisfy $4 \mid 3pq - 1$.

$c = 9$ $xy = 234$; no x and y exist for which $9 \mid m+x$ and $9 \mid m+y$.

$c = 11$; $xy = 236$; no x exists with $11 \mid m+x$.

$c = 13$; $xy = 238$; no x exists with $13 \mid m+x$.

$c = 18$; $xy = 243$; no x and y exist for which $9 \mid m+x$ and $9 \mid m+y$.

$c = 22$; $xy = 247$; no x exists with $11 \mid m+x$.

Further we must consider the possible values for p, which are < 15, i.e. $p = 7, 11$ or 13. None of these cases can occur in virtue of 2°, so that the only Carmichael number of the form $15pq$ is $n = 3.5.47.89 = 62745$.

For $m = 33$ we find only the possibility $n = 3.11.101.197.$ and for $m = 35$ we only get $n = 5.7.443.3877$ and $n = 5.7.647.7549$. In virtue of 2° no Carmichael numbers exist of the form $n = 21pq$ and $n = 39pq$, so the 4 found numbers are the only ones of the form $n = mpq$ with $m<47$, which have to be added tot Beeger's table.