J. Austral. Math. Soc. **21** (Series A) (1976), 508–510.

STRONG CARMICHAEL NUMBERS

Dedicated to George Szekeres on his 65th birthday

D. H. LEHMER

(Received 18 December 1974; revised 3 April 1975)

Communicated by Jennifer Seberry Wallis

A composite number N is called a pseudoprime for the base a in case

$$a^{N-1} \equiv 1 \pmod{N}. \tag{1}$$

An odd pseudoprime N is called strong for the base a in case

$$a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N} \tag{2}$$

where the symbol on the right is that of Jacobi. To explain the terminology, experiments show that (2), which implies (1), holds only rarely among the ordinary pseudoprimes. Hence (2) makes a good hypothesis item in a test for primality. $N = 561$, which is a pseudoprime for every base prime to 561, is a strong pseudoprime for the base 2 but not for the base 5 since

$$5^{280} \equiv 67 \pmod{561}.$$

A pseudoprime, like 561, for which (1) holds for all bases a prime to N is called a universal pseudoprime or Carmichael number. The first 23 such numbers are

$561 = 3\cdot 11\cdot 17$	$15841 = 7\cdot 31\cdot 73$	$101101 = 7\cdot 11\cdot 13\cdot 2101$
$1105 = 5\cdot 13\cdot 17$	$29341 = 13\cdot 37\cdot 61$	$115921 = 13\cdot 37\cdot 241$
$1729 = 7\cdot 13\cdot 19$	$41041 = 7\cdot 11\cdot 13\cdot 41$	$126217 = 7\cdot 13\cdot 19\cdot 73$
$2465 = 5\cdot 17\cdot 29$	$46657 = 13\cdot 37\cdot 97$	$162401 = 17\cdot 41\cdot 233$
$2821 = 7\cdot 13\cdot 31$	$52633 = 7\cdot 73\cdot 103$	$172081 = 7\cdot 13\cdot 31\cdot 61$
$6601 = 7\cdot 23\cdot 41$	$62745 = 3\cdot 5\cdot 47\cdot 89$	$188461 = 7\cdot 13\cdot 19\cdot 109$
$8911 = 7\cdot 19\cdot 67$	$63973 = 7\cdot 13\cdot 19\cdot 37$	$252601 = 41\cdot 61\cdot 101$
$10585 = 5\cdot 29\cdot 73$	$75361 = 11\cdot 13\cdot 17\cdot 31$	

https://doi.org/10.1017/S1446788700019364 Published online by Cambridge University Press

A strong Carmichael number N would be such that (2) holds for all bases a prime to N. In this note we show that such numbers do not exist.

THEOREM. *No Carmichael number is strong.*

PROOF. In 1912 Carmichael (1912) showed that every Carmichael number N is the product of distinct primes. Therefore we can write

$$N = p_1 \cdot p_2 \cdots p_t \qquad (p_1 > 2, t > 1)$$

and we see that

$$a^{N-1} \equiv 1 \pmod{p_i} \qquad (i = 1(1)t)$$

holds for every a prime to N and in particular for $a = g$ any common primitive root of all the p's. Therefore

$$N - 1 \equiv 0 \pmod{p_i - 1}.$$

Now the t primes p_i can be of two types:

Type 1 those p for which $(N-1)/2 \equiv 0 \pmod{p-1}$

Type 2 those p for which $(N-1)/2 \equiv (p-1)/2 \pmod{p-1}$.

Thus we have

$$a^{(N-1)/2} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \text{ is of Type 1} \\ \left(\dfrac{a}{p}\right) \pmod{p} & \text{if } p \text{ is of Type 2.} \end{cases} \tag{3}$$

We now choose a to be a quadratic nonresidue of p_1 and a residue of all the other p' s. First suppose there is a prime of Type 1 which we may take to be p_1. If N were strong (2) and (3) would give us

$$-1 = \left(\frac{a}{N}\right) \equiv a^{(N-1)/2} \equiv 1 \pmod{p_1}.$$

This contradiction shows that all the p's are of Type 2.

Hence (3) gives

$$a^{(N-1)/2} \equiv 1 \pmod{p_2}.$$

But, by (2)

$$a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{p_1 p_2},$$

https://doi.org/10.1017/S1446788700019364 Published online by Cambridge University Press

that is,

$$a^{(N-1)/2} \equiv -1 \pmod{p_2}.$$

This contradiction completes the proof.

Reference

R. D. Carmichael (1912), Amer. Math. Monthly **19**, 22–27.

Department of Mathematics
University of California
Berkeley, California, U.S.A.