MATHEMATICS OF COMPUTATION
VOLUME 53, NUMBER 187
JULY 1989, PAGES 411-414

A New Method for Producing Large Carmichael Numbers

By H. Dubner

Abstract. A new method for producing large three-component Carmichael numbers is derived. Only two primes must be found simultaneously instead of three as in the "standard" method. For each set of two primes many third primes can be found. Several Carmichael numbers with more than 3000 digits are shown, with the largest having 3710 digits.

1. Introduction. Fermat's "Little Theorem" states:

If a is any integer prime to N, and if N is prime, then

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

Unfortunately, this is not a sufficient condition for a number to be prime since there are composite numbers which satisfy this congruence. Chernick [2] stated the following theorem for these Carmichael numbers:

> *Fermat's theorem holds for composite integers if and only if N may be expressed as a product of distinct odd primes $P_1, P_2, \ldots P_n$, $(n > 2)$, and each $P_i - 1$ divides $N - 1$.*

Chernick derived one-parameter expressions for Carmichael numbers which he called "Universal Forms," the most prominent of these being

$$U_3 = (6M+1)(12M+1)(18M+1). \tag{2}$$

U_3 is a Carmichael number when the quantities in parentheses are simultaneously prime. The largest known Carmichael numbers are of this form. In 1980 Wagstaff [6] published a 321-digit Carmichael number. Woods and Huenemann [7] cleverly added a fourth term to Wagstaff's 321-digit number and constructed a four-component Carmichael number with 432 digits.

In August, 1985 the author reported to Wagstaff a 1057-digit number [3], the result of searching for large Carmichael numbers using a specially designed computer for number theory [4]. Since then the author has found, but not reported, a 1265-digit number, a project that took approximately 400 hours on this special computer.

2. The New Method. The difficulty in finding larger Carmichael numbers using Eq. (2) is caused by the necessity of finding three primes simultaneously. The new method is based on finding two primes simultaneously, and then the third prime.

For $N = PQR$, N is a Carmichael number if P, Q, R are distinct primes and

$$PQR \equiv 1 \pmod{R-1}, \quad PQR \equiv 1 \pmod{Q-1}, \quad PQR \equiv 1 \pmod{P-1}.$$

Received June 17, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A99.

It is easy to see that these conditions are equivalent to

$$PQ \equiv 1 \pmod{R-1}, \quad PR \equiv 1 \pmod{Q-1}, \quad QR \equiv 1 \pmod{P-1}. \tag{3}$$

Next, let $P = 6M + 1$, $Q = 12M + 1$, both prime. Then

$$PQ = (6M+1)(12M+1) = 72M^2 + 18M + 1 = 6M \cdot 3(4M+1) + 1. \tag{4}$$

But

$$\begin{gathered} (R-1)X = PQ - 1, \\ R = \frac{6M \cdot 3(4M+1)}{X} + 1. \end{gathered} \tag{5}$$

Also, $PR - 1$ must be divisible by $Q - 1 = 12M$. Now

$$\begin{aligned} PR - 1 &= (6M+1)\left(\frac{6M \cdot 3(4M+1)}{X} + 1\right) - 1 \\ &= \frac{6M \cdot 3(4M+1)(6M+1)}{X} + 6M = 6M\left(\frac{3(4M+1)(6M+1)}{X} + 1\right), \end{aligned}$$

$$\frac{PR-1}{Q-1} = \frac{1}{2}\left(\frac{3(4M+1)(6M+1)}{X} + 1\right). \tag{6}$$

Since $6M + 1$ is prime, and considering Eqs. (5) and (6), X must be a divisor of $3(4M + 1)$. The 2 in Eq. (6) will automatically divide since the quantity inside the parentheses is always even. The third condition of Eq. (3) is easily seen to be satisfied.

Thus,

$$R = 6Mk + 1, \tag{7}$$

where k is a divisor of $3(4M + 1)$.

The procedure for searching for large Carmichael numbers is as follows:

1. Find M so that $P = 6M + 1$ and $Q = 12M + 1$ are prime simultaneously.
2. Find $R = 6Mk + 1$ prime where k is a divisor of $3(4M + 1)$.

For the method to be productive, the following practical conditions should be met:

1. M should be easily factorable so that P, Q, R can be proven prime using techniques from [1].
2. $4M + 1$ should have many factors so that there are many possibilities for finding R's that are prime.

Finding functions which fulfill these conditions is like solving a puzzle. The following has been used successfully:

$$M = \frac{(TC-1)^A}{4}, \tag{8}$$

where

T is fixed, odd, and has many factors;

A is fixed and odd;

C is odd and varies until P and Q are prime;

$TC - 1$ is less than 24 digits and therefore is easily factored.

Then,

$$4M+1=(TC-1)^A+1. \tag{9}$$

Since b^A+1 is always divisible by $b+1$ for A odd, $4M+1$ will be divisible by TC and therefore has many factors.

Typically, if T is the product of all odd primes through 47, then R has at least 48,000 possibilities of being prime.

3. Results. It is surprising how easy it is to produce many three-component Carmichael numbers that have two fixed components. For example,

$$N=PQR, \qquad M=\frac{5^3\cdot 7\cdot 11\cdot 13-1}{4}=31281,$$

$$P=6M+1=187687, \quad Q=12M+1=375373, \quad R=6Mk+1;$$

each of the following values of k gives a prime value of R which makes N a Carmichael number. The list is complete since there are no other such R's.

k	R	k	R
11	2064547	231	43355467
13	2439919	385	72259111
35	6569011	825	154840951
55	10322731	975	182993851
75	14076451	3575	670977451
77	14451823	11375	2134928251
91	17079427	25025	4696842151
175	32845051	34125	6404784751

In another test, using a 60-digit M, 501 prime values of R were found with k limited to a value of one million. Without a limit on k, the expected number of prime values of R should exceed 10^9. In other tests, 600-digit Carmichael numbers could be produced at the average rate of one per minute.

The largest Carmichael numbers found appear in Table 1.

TABLE 1

Parameters for Carmichael Numbers

$N=PQR,\ P,Q,R$ prime;

$P=6M+1,\ Q=12M+1,\ R=1+(PQ-1)/X;$

$M=(TC-1)^A/4,$

$T=3\cdot 5\cdot 7\cdot 11\cdots 43\cdot 47=30744489\ 1294245705.$

A	C	P	Q	X	R	$N=PQR$
35	135449	792 digits	793 digits	83421	1580 digits	3164 digits
				80073	1580	3164
41	141847	929	929	1172885	1852	3709
				803985	1852	3709
				325941	1852	3709
				217341	1852	3709
				123165	1853	3710

It took about twenty hours to find P and Q for the 3710-digit Carmichael number. The expected time was 110 hours for the computer and program used. A new large prime R could be expected about every five hours.

4. The Future. The number of tests (heuristically) required to find P and Q simultaneously prime is proportional to $(\log P)^2$. The time to test for probable primality is proportional to $(\log P)^3$ using Eq. (1) and standard multiple precision multiplies and divides. Thus, the total time to find P and Q prime is (heuristically)

$$T = K_1(\log P)^5 = K_2 D^5,$$

where D is the number of digits of P. The time to find R can be ignored since it is proportional to only D^4. The process can be speeded up by using faster computers and more efficient multiplying techniques [5].

It appears possible to extend this new method to further decrease the search time. By choosing $Q = 18M + 1$, new equations similar to Eqs. (5) and (6) can be developed but with additional restrictions on M and X. It may be possible to eventually develop an algorithm to first find a $P = 6Mp + 1$, then a $Q = 6Mq + 1$, then $R = 6Mr + 1$ so that PQR is a Carmichael number, but the components have been found sequentially.

Dubner Computer Systems
6 Forest Avenue
Paramus, New Jersey 07675

1. J. BRILLHARD, D. H. LEHMER & J. L. SELFRIDGE, "New primality criteria and factorizations of $2^n \pm 1$," *Math. Comp.*, v. 29, 1975, pp. 620–647.

2. J. CHERNICK, "On Fermat's simple theorem," *Bull. Amer. Math. Soc.*, v. 45, 1939, pp. 269–274.

3. H. DUBNER, Letter to S. S. Wagstaff, Jr., dated August 13, 1985.

4. H. DUBNER & R. DUBNER, "The development of a powerful low-cost computer for number theory applications," *J. Recreational Math.*, v. 18, no. 2, 1985–1986, pp. 81–86.

5. D. E. KNUTH, *The Art of Computer Programming, Vol. 2. Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981, pp. 278–299.

6. S. S. WAGSTAFF, JR., "Large Carmichael numbers," *Math. J. Okayama Univ.*, v. 22, 1980, pp. 33–41.

7. S. WOODS & J. HUENEMANN, "Larger Carmichael numbers," *Comput. Math. Appl.*, v. 8, no. 3, 1982, pp. 215–216.