MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 207
JULY 1994, PAGES 415-419

CARMICHAEL'S CONJECTURE ON THE EULER FUNCTION IS VALID BELOW $10^{10,000,000}$

AARON SCHLAFLY AND STAN WAGON

ABSTRACT. Carmichael's conjecture states that if $\phi(x) = n$, then $\phi(y) = n$ for some $y \neq x$ (ϕ is Euler's totient function). We show that the conjecture is valid for all x under $10^{10,900,000}$. The main new idea is the application of a prime-certification technique that allows us to very quickly certify the primality of the thousands of large numbers that must divide a counterexample.

Let the *multiplicity* of an integer be the number of times it occurs as a value of $\phi(x)$, where ϕ is the Euler function. Table 1 shows the multiplicities of the first 50 integers (odd numbers greater than 1 have multiplicity 0, since $\phi(x)$ is even if $x > 1$). For example, the multiplicity of 4 is 4 because the numbers 5, 8, 10, and 12 (and only these) have ϕ-value 4.

TABLE 1. These multiplicities show that the number of times a ϕ-value can occur might be 0 (as is the case for all odd numbers greater than 1 and some evens, such as 14) or 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11

ϕ-value:	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50
Multiplicity:	2	3	4	4	5	2	6	0	6	4	5	2	10	0	2	2	7	0	8	0	9	4	3	2	11	0

In 1907 R. D. Carmichael [1] claimed that 1 is not a multiplicity; equivalently: ϕ takes on no value precisely once. The result appears as an exercise in his 1914 book [2], but in 1922 his proof was found to be erroneous [3] and the assertion is now known as Carmichael's conjecture. An algebraic formulation of the conjecture is: No finite cyclic group is characterized by the number of its generators. Carmichael himself proved [3] that any counterexample x must be greater than 10^{37}. This was improved by V. Klee [5] to 10^{400}, and by Masai and Vallette [6] to $10^{10,000}$. In this note we describe a computation using *Mathematica* on a Macintosh that pushes the lower bound on x to beyond $10^{10,900,000}$. Throughout this note, x represents a counterexample to the conjecture. Because $\phi(n) > n \log 2/\log(2n)$ [9, p. 172], a lower bound on n is essentially the same as one on x. We do not know of another unsolved problem in mathematics for which a lower bound on a counterexample is so high.

It is natural to wonder about other patterns in the multiplicities. Erdős [4] has shown that if a multiplicity occurs once it occurs infinitely often, and Sierpiński

Received by the editor May 26, 1993 and, in revised form, August 20, 1993.
1991 *Mathematics Subject Classification.* Primary 11A25, 11Y70; Secondary 11A41.
Key words and phrases. Euler's function, Carmichael's conjecture, prime certification.

TABLE 2. The first occurrences of each ϕ-multiplicity up to 100. For example, there are precisely 90 values of m for which $\phi(m) = 18{,}000$, and 18,000 is minimal with this property. Carmichael conjectured that 1 is never a multiplicity

Multiplicity	First ϕ-value with this multiplicity	Multiplicity	First ϕ-value with this multiplicity	Multiplicity	First ϕ-value with this multiplicity	Multiplicity	First ϕ-value with this multiplicity
0	3	26	2560	51	4992	76	21840
2	1	27	384	52	17640	77	9072
3	2	28	288	53	2016	78	38640
4	4	29	1320	54	1152	79	9360
5	8	30	3696	55	6000	80	81216
6	12	31	240	56	12288	81	4032
7	32	32	768	57	4752	82	5280
8	36	33	9000	58	2688	83	4800
9	40	34	432	59	3024	84	4608
10	24	35	7128	60	13680	85	16896
11	48	36	4200	61	9984	86	3456
12	160	37	480	62	1728	87	3840
13	396	38	576	63	1920	88	10800
14	2268	39	1296	64	2400	89	9504
15	704	40	1200	65	7560	90	18000
16	312	41	15936	66	2304	91	23520
17	72	42	3312	67	22848	92	39936
18	336	43	3072	68	8400	93	5040
19	216	44	3240	69	29160	94	26208
20	936	45	864	70	5376	95	27360
21	144	46	3120	71	3360	96	6480
22	624	47	7344	72	1440	97	9216
23	1056	48	3888	73	13248	98	2880
24	1760	49	720	74	11040	99	26496
25	360	50	1680	75	27720	100	34272

had earlier conjectured that each integer greater than 1 occurs as a multiplicity. Computations along the lines of those that produced Table 1 show that each integer between 2 and 100 does occur; see Table 2.

The idea for generating large lower bounds on x goes back to a theorem of Carmichael [3], later refined by Klee [5, 10]. The result leads to a straightforward algorithm for obtaining prime numbers whose squares divide x.

Theorem (Carmichael and Klee). *Suppose x factors into $d_1 e$, where $d_1 = \prod p_i^{a_i}$ and $e = \prod q_j^{b_j}$ and $\{q_j\}$, $\{p_i\}$ are disjoint, possibly empty, sets of primes. Let $d_2 = \prod q_j^{c_j}$, where $0 \le c_j < b_j$ for each j, and let $P = 1 + d_2\phi(d_1)$. If P is prime, then $P^2 | x$.*

We start by applying the theorem with $d_1 = d_2 = 1$; this tells us that $2^2|x$. Then using $d_1 = 1$ and $d_2 = 2$ yields that $3^2|x$. And letting $d_1 = 1$ and $d_2 = 2 \cdot 3$ gives $7^2|x$, and $d_1 = 1$ and $d_2 = 2 \cdot 3 \cdot 7$ gives $43^2|x$. At this point, following Carmichael [3], we break the proof into two cases according as 3^3 divides x or not. Klee and Masai and Vallette used three and four cases, respectively, but an improvement in the prime-certification method (described later) allows us to return to the original two-case scenario.

In the first case (3^3 does not divide x), we let $L = \{7, 13, 43\}$ and consider all products k of elements in L. For each such k, the theorem says that if either of $6k+1$ or $12k+1$ is prime, then its square divides x; the $6k$ comes from $d_1 = 1$ and $d_2 = 2 \cdot 3 \cdot k$, and the $12k$ from $d_1 = 3^2$ and $d_2 = 2k$. For the primes P that arise in this way we add $2\log_{10} P$ to a counter that keeps track of the lower bound. After checking all products from L we append one of the new primes to L and then repeat, considering all products from L that use the new prime. We continue until we are satisfied with the bound. The number of products increases exponentially, so it takes only a few iterations to reach a very large bound. The second case is similar, with the forms $6k+1$ and $18k+1$.

The main bottleneck is determining (with certainty) the primality of the over eight million large integers (up to 91 digits) that occur as $6k+1$, $12k+1$, or $18k+1$. Masai and Vallette considered only possible primes less than $25 \cdot 10^9$, and so could use, with confidence, an algorithm based on a strong-pseudoprime test with bases 2, 3, 5, and 7, as described in [8]. That algorithm, with small modifications, is now known to be useful up to 10^{13} [9], but this range is too small for our multimillion-digit goal. An elliptic curve certification method will work in principle, but it is too slow for the large number of primes, more than 270,000, that must be certified. In the context of this problem, however, we have the agreeable situation that all the potential primes p that show up are accompanied by the factorization of $p-1$. Since $p-1$ is a product of primes in L, its factorization can be stored alongside p. We may therefore appeal to the following prime certification process (see [9, p. 36]), which is closely related to Pratt's recursive proof that the primes lie in the complexity class NP (see [11, Chapter 8]).

Theorem (Lucas, Lehmer, Brillhart, and Selfridge). *Suppose n is a positive integer, Q is the set of prime factors of $n-1$, and for each $q \in Q$ there is an integer a_q such that $a_q^{n-1} \equiv 1$ and $a_q^{(n-1)/q} \not\equiv 1 \pmod{n}$. Then n is prime. Conversely, if n is prime, it has a primitive root, which serves as a_q for each q.*

Of course, in practice we first used a pseudoprime test to see if a candidate was a probable prime. If so, we applied the certification procedure with $a = 2, 3, 5, 7, 11, 17, 19, 23, 29, 31, 37, 41$ which was always sufficient to prove primality. Another technical detail: we made some preliminary runs in each case to determine a set of 30 small primes whose squares divide x; we then used this set to augment L after each iteration. By keeping the primes in L as small as possible, the total amount of computation is minimized since the size of the candidates is kept small. Tables 3 and 4 (next page) summarize the computations in the first case (3^3 does not divide x) and second case (27 divides x), respectively. Note that each iteration has twice as many candidates for primes and yields very closely twice as many digits. This is because the density of the primes decreases logarithmically but the number of digits increases logarithmically—the two effects exactly balance.

There can be little doubt that Carmichael's conjecture is true. At each iteration we need but a single new prime to keep going: add it to L and then generate a profusion of new possibilities for primes. But instead of one new prime at each iteration we get hundreds and thousands. Even if by some quirk an iteration yielded no new primes, we would have all the leftover primes from previous iterations with which to augment L and try again.

The entire computation required a few hundred hours of Macintosh computing time. One could surely push the bound farther, using faster software and hardware. But what is badly needed is an idea that would allow one to say with certainty that at least one prime shows up at each iteration, for that would prove the conjecture.

TABLE 3. This table shows how the primes arise at each iteration, along with the consequent increase in the lower bound on x, in the case that 3^3 does not divide x

The set L	Number of candidates for primality at each iteration	Number of primes at each iteration	Percentage	lower bound on number of digits in x
{7, 13, 43, 79, 157, 547}	128	31	24.2%	315
{7, 13, 43, 79, 157, 547, 1093}	128	18	20%	596
{7, 13, ..., 1093, 3319}	256	22	8.5%	1280
{7, 13, ..., 3319, 3613}	512	51	10%	2582
{7, 13, ..., 3613, 6163}	1024	83	8.1%	5012
{7, 13, ..., 6163, 6637}	2048	173	8.4%	10627
{7, 13, ..., 6637, 6709}	4096	306	7.5%	21363
{7, 13, ..., 6709, 40507}	8192	504	6.2%	41642
{7, 13, ..., 40507, 42667}	16384	974	5.9%	86078
15 primes: {7, 13, ..., 42667, 45949}	32768	1706	5.2%	170712
16 primes: {7, 13, ..., 45949, 46957}	65536	3204	4.9%	343620
17 primes: {7, 13, ..., 46957, 74419}	131072	5900	4.5%	690567
18 primes: {7, 13, ..., 74419, 81013}	262144	11277	4.3%	1,409,601
19 primes: {7, 13, ..., 81013, 85333}	524288	20543	3.9%	2,820,321
20 primes: {7, 13, ..., 85333, 86269}	1,048,576	41477	4.0%	5,648,822
21 primes: {7, 13, ..., 86269, 91813}	2,097,152	69523	3.3%	11,329,959
Totals	4,194,304	155,792	3.71%	11,329,959

TABLE 4. This table shows how the primes arise at each iteration, along with the consequent increase in the lower bound on x, in the case that 3^3 does divide x. The prime 617,767 was discovered late, and so was not added to L until the 19-prime case

The set L	Number of candidates for primality at each iteration	Number of primes at each iteration	Percentage	lower bound on number of digits in x
{7, 19, 43, 127, 2287, 4903}	128	23	18%	279
{7, 19, ..., 4903, 5419}	128	16	12.5%	623
{7, 19, ..., 5419, 13723}	256	27	10.6%	1283
{7, 19, ..., 13723, 14479}	512	54	10.5%	2774
{7, 19, ..., 14479, 98299}	1024	58	5.7%	4855
{7, 19, ..., 98299, 101347}	2048	140	6.8%	10571
{7, 19, ..., 101347, 304039}	4096	239	5.8%	21425
{7, 19, ..., 304039, 688087}	8192	391	4.8%	41111
{7, 19, ..., 688087, 1676827}	16384	696	4.2%	81214
15 primes: {7, 19, ..., 1676827, 3735583}	32768	1347	4.1%	167731
16 primes: {7, 19, ..., 3735583, 3736087}	65536	2498	3.8%	343919
17 primes: {7, 19, ..., 3736087, 4130323}	131072	4400	3.4%	683457
18 primes: {7, 19, ..., 4130323, 4324363}	262144	8134	3.1%	1,364,713
19 primes: {7, 19, ..., 617767, ..., 4324363}	524288	15138	2.9%	2,464,529
20 primes: {7, 19, ..., 4324363, 4693267}	1,048,576	29124	2.8%	5,248,342
21 primes: {7, 19, ..., 4693267, 4951819}	2,097,152	55536	2.7%	10,920,865
Totals	4,194,304	117,821	2.81%	10,920,865

Notes. Much of this work appeared in the first author's senior honors thesis at Macalester College, 1993. We are grateful to Dan Hornbach who supervised several runs on a Macintosh Quadra.

BIBLIOGRAPHY

1. R. D. Carmichael, *On Euler's ϕ-function*, Bull. Amer. Math. Soc. **13** (1907), 241–243.

2. ———, *The theory of numbers*, Wiley, New York, 1914.

3. ——, *Note on Euler's ϕ-function*, Bull. Amer. Math. Soc. **28** (1922), 109–110.

4. P. Erdős, *Some remarks on Euler's ϕ-function*, Acta Math. **4** (1958), 10–19.

5. V. Klee, *On a conjecture of Carmichael*, Bull. Amer. Math. Soc. **53** (1947), 1183–1186.

6. P. Masai and A. Vallette, *A lower bound for a counterexample to Carmichael's conjecture*, Boll. Un. Mat. Ital. (6) **1** (1982), 313–316.

7. R. Pinch, *The pseudoprimes up to* 10^{13} (to appear).

8. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* 25×10^9, Math. Comp. **35** (1980), 1003–1026.

9. P. Ribenboim, *The book of prime number records*, Springer-Verlag, New York, 1988.

10. S. Wagon, *Carmichael's "empirical theorem"*, Math. Intelligencer **8** (1986), 61–63.

11. ——, *Mathematica in action*, Freeman, New York, 1990.

Department of Mathematics, University of Washington, Seattle, Washington 98195

Department of Mathematics and Computer Science, Macalester College, St. Paul, Minnesota 55105
E-mail address: wagon@macalstr.edu