Math. J. Okayama Univ. 22 (1980), 33—41

LARGE CARMICHAEL NUMBERS

SAMUEL S. WAGSTAFF, JR.

1. Introduction. A *Carmichael number* is an odd composite number n for which $a^{n-1}\equiv 1 (\mathrm{mod}\ n)$ for each integer a relatively prime to n. Many mathematicians believe that there are infinitely many Carmichael numbers, but this conjecture has never been proved. Erdös [4] conjectured that the number $C(x)$ of Carmichael numbers up to x satisfies $C(x)>x^{1-\varepsilon}$ for each positive ε and all sufficiently large x.

Yorinaga [10] has exhibited many quite large Carmichael numbers, thereby supporting the conjecture. He used four different techniques to produce these numbers. In the present work, we use his second method, that of universal forms due to Chernick [3], to find some much larger Carmichael numbers. Our largest one has 321 decimal digits.

In Section 4, we discuss the search for composite n for which $\phi(n)$ divides $n-1$, where ϕ is Euler's function.

2. The universal forms of Chernick. For integers $k\geq 3$ and $m\geq 1$ define

$$U_k(m)=(6m+1)(12m+1)\prod_{i=1}^{k-2}(9\cdot 2^i m+1).$$

Chernick [3] proved that $U_3(m)$ is a Carmichael number whenever all three of the factors $6m+1$, $12m+1$, $18m+1$ are prime. Furthermore, he showed that if $k\geq 4$ and 2^{k-4} divides m, then $U_k(m)$ is a Carmichael number whenever each of its k factors is prime.

Chernick's sufficient conditions for $U_k(m)$ to be a Carmichael number are not necessary conditions. For example,

$$172081=U_3(5)=31\cdot 61\cdot 91$$

is a Carmichael number even though 91 is composite.

Let $a_1, \cdots, a_k$ be positive integers and let $b_1, \cdots, b_k$ be non-zero integers. Let $P(x)$ denote the number of $m\leq x$ for which $a_i m+b_i$ is prime for each $i=1, \cdots, k$. The strong form of the Prime k-tuples Conjecture says that if no prime divides

$$\prod_{i=1}^{k}(a_i m+b_i) \tag{1}$$

for every m, then there is a positive constant c such that $P(x)\sim cx/\log^k x$

as $x \longrightarrow \infty$. Like the conjectures about the growth rate of $C(x)$, the Prime k-tuples Conjecture is supported by numerical data and a heuristic argument, but it has never been proved (except for $k=1$). The heuristic value of the constant c may be extracted from [1].

Chernick [3] called a form (1) *universal* if its value is a Carmichael number for every m for which each of the k factors is prime. He gave many examples of universal forms—not just $U_k(m)$.

The strong form of the Prime k-tuples Conjecture and Chernick's result about $U_k(m)$ together imply that for each $k \geq 3$ there is a positive constant c_k such that for all sufficiently large x, there are at least $c_k x^{1/k}/\log^k x$ Carmichael numbers $\leq x$ with exactly k prime factors (and, in fact, of the form $U_k(m)$). Examination of tables of Carmichael numbers (such as [10]) indicates that most of them do not have the form $U_k(m)$. Thus, it is very likely true that for $k \geq 3$ there are many more than $O(x^{1/k}/\log^k x)$ Carmichael numbers $\leq x$ having exactly k prime factors.

3. Numerical results. We used a sieve to compute some numbers m for which $6m+1$, $12m+1$, and $18m+1$ are all primes. We found such m of 15 to 16 digits very readily. It took a little effort to discover five more of them with 41 and 42 digits. All of these numbers are listed in Table 1. They yield Carmichael numbers $U_3(m)$ of about 50 and 126 digits, respectively. Then we found the Carmichael number

	5	10097651	43959249	35442924	80932774	56279161
66422617	58239613	10579841	88849784	22849780	91128590	52248262
18356898	74002783	53571488	38474305	31105418	73196218	42459950
73938057	88336374	85286596	13137137	81439007	23170631	02191638
94923024	77317009	21197794	18509950	24840245	83806981	21688191
77310433	20215974	89437261	95369370	82075885	79386408	51976601

of 321 decimal digits, which is $U_3(m)$ for the 106 digit

$m=73$	28517132	62373770	42833051	15698260	79825001	98696237
26846779	39558839	14228225	25876339	63462201	59279282	85851850,

and which seems to be largest known Carmichael number at the present time. The previous record was the 77 digit Carmichael number of Hill [11].

When we searched for m such that $6m+1$, $12m+1$, $18m+1$, and $36m+1$ are all prime, we considered only those m which were divisible by 256. We made this restriction to insure that if $72m+1$, $144m+1$, etc., happened to be prime as well, then the appropriate $U_k(m)$ would be a Carmichael number. Table 2 lists some m for which $U_4(m)$ is Carmichael, but for which $72m+1$ is composite. In Table 3, we give the m's which we found for which $U_5(m)$ is Carmichael. We discovered only one value of m, namely

$$m=1810081824371200,$$

which makes $U_6(m)$ a Carmichael number. The Carmichael number is

17013 42440919 43763695 53227755 50557528 57171386 19698240
48592960 03337783 47855414 62105336 02967795 96185601

of 101 decimal digits. It is undoubtedly the largest known Carmichael number with more than three prime divisors.

In order to demonstrate that the large numbers described in this section really are Carmichael numbers, one must prove that various numbers of the form $rm+1$ are prime. In the case of the 321 digit Carmichael number, we used the following theorem to prove primality of the three factors.

Theorem 1 (Brillhart and Selfridge [2]). *Let* $N-1=\prod p_i^{\alpha_i}$. *If for each* p_i *there exists an* a_i *such that* $a_i^{N-1}\equiv 1(\text{mod } N)$, *but* $a_i^{(N-1)/p_i}\not\equiv 1(\text{mod } N)$, *then* N *is prime.*

We arranged the sieve so that only those m with a small largest prime factor would be examined. The factorization of our 106 digit m is

$$m=2\cdot 3^3\cdot 5^2\cdot 7\cdot 577\cdot 1009^{33}.$$

Hence, it is easy to use Theorem 1 to prove that $6m+1$, $12m+1$, and $18m+1$ are primes.

The other numbers $rm+1$ were proved prime by an algorithm of Selfridge and Wunderlich [8] which was implemented by them at Northern Illinois University. Their program uses factors of $N+1$ as well as those of $N-1$ in proving N is prime, and does not require a complete factorization of either number to complete the proof. We helped the program by insuring that m (and hence $N-1$) would factor completely with little effort. In this manner, more than 1000 prime proofs of numbers of about 17 digits were performed in a few minutes.

4. Does $\phi(n)$ ever divide $n-1$ properly? Lehmer [6] asked whether there are any composite numbers n for which $\phi(n)$ divides $n-1$. The question remains unsettled. Kishore [5] announced a proof that any such n must have at least 13 distinct prime factors. It is clear that any composite n with $\phi(n)\mid n-1$ must be a Carmichael number. Yorinaga [10] found 8 Carmichael numbers with 13 or more prime factors. These appear to be the only known Carmichael numbers with so many prime divisors. We determined by calculation that $\phi(n) \mid n-1$ for none of these numbers.

We considered the possibility of searching for m for which $n=U_k(m)$ is a Carmichael number and $k\geq 13$. One might expect such n to be good candidates for $\phi(n)\mid n-1$. One difficulty with this approach is that, assuming the strong form of the Prime k-tuples Conjecture, such numbers ought to be quite rare. Indeed, there should be only $O(x/\log^k x)$ values of $m\leq x$ for which $U_k(m)$ is Carmichael, and we have $k\geq 13$ here. Such values of m should be a bit harder to find than arithmetic progressions of 13 primes (because the sieve for $U_k(m)$ is more complicated), and only recently [9] have seventeen primes in arithmetic progression been discovered. A more fundamental difficulty with this method of seeking composite n with $\phi(n) \mid n-1$ is expressed in the following theorem.

Theorem 2 (Pomerance). *If each of the $k\geq 3$ factors of $n=U_k(m)$ is prime (so that n is a Carmichael number), then $\phi(n)$ does not divide $n-1$.*

Proof. We have

$$\frac{n-1}{\phi(n)}<\frac{n}{\phi(n)}=\left(1+\frac{1}{6m}\right)\left(1+\frac{1}{12m}\right)\prod_{i=1}^{k-2}\left(1+\frac{1}{9\cdot 2^i m}\right),$$

so that

$$\log\left(\frac{n-1}{\phi(n)}\right)<\frac{1}{6m}+\frac{1}{12m}+\sum_{i=1}^{\infty}\frac{1}{9\cdot 2^i m}=\frac{13}{36m}\leq\frac{13}{36}<\log 2.$$

Hence, $n-1<2\phi(n)$, and $n-1$ cannot be a multiple of $\phi(n)$.

Chernick [3] explained how one may construct universal forms (1) with $k=3$ and 4 by solving congruences. He also described a method [3, Theorem 3] of producing a universal form (1) from any given Carmichael number of k prime factors. In the latter construction, the b_i of (1) are the prime divisors of the given Carmichael number. We will explain why this method is unlikely to produce a Carmichael number n of the form (1) with $m>0$ for which $\phi(n) \mid n-1$.

Suppose that (1) is a universal form with $k\geq 3$ and positive integers a_i and b_i. (The a_i and b_i are positive integers in Chernick's [3] constructions.) Assume that m is a positive integer for which each of the k factors in (1) is prime. Suppose that the value n of (1) for this m satisfies $\phi(n)\mid n-1$. Then

$$2\leq(n-1)/\phi(n)<n/\phi(n)=\prod_{i=1}^{k}(1+(a_i m+b_i-1)^{-1})$$

$$\leq \prod_{i=1}^{k} (1+(a_i m)^{-1}),$$

and we have

$$\log 2 < \sum_{i=1}^{k} 1/(a_i m) = \frac{1}{m} \sum_{i=1}^{k} \frac{1}{a_i}.$$

Hence

$$m < \frac{1}{\log 2} \sum_{i=1}^{k} \frac{1}{a_i}. \tag{2}$$

This shows that k must be large and the a_i small in order for there to be even one positive value of m for which (1) satisfies $\phi(n) \mid n-1$. However, the a_i in Chernick's construction are rather large.

Pomerance [7] has shown that if $\phi(n) \mid n-1$ and n has exactly k prime factors, then $n < k^{2^k}$. This inequality shows that for any form (1) there are only finitely many values of m for which each factor $a_i m + b_i$ is prime and the value n of (1) satisfies $\phi(n) \mid n-1$. Indeed, any such m must be less than

$$(k^{2^k} / \prod_{i=1}^{k} a_i)^{1/k}.$$

But this inequality is not as sharp as (2).

Where, then, should one look for composite n with $\phi(n) \mid n-1$? Of the four methods which Yorinaga [10] describes, the one best suited for this purpose seems to be his Method III, which is a direct search of square-free numbers whose prime factors are drawn from a small set of specified primes.

Acknowledgments. The author thanks Carl Pomerance for supplying Theorem 2. He is grateful to John Selfridge and Marvin Wunderlich for the use of their prime proving program. Most of the calculations for this paper were performed at the Computer Center of Northern Illinois University.

Table 1

Some m with $6m+1$, $12m+1$, and $18m+1$ all prime.

925968953850065	925968953854121	925968953858280	925968953858935
925968953862470	8550768560768681	8550768560769871	8550768560772035
8550768560773876	8550768560778451	8550768560778845	8550768560784495
8550768560790456	8522851273339146	8522851273349646	8522851273351855
8522851273354456	8522851273354481	8522851273355841	8522851273360266
8522851273361266	8522851273362166	8522851273365081	9510693751419300
9510693751424610	9510693751425636	9510693751431925	9510693751437311
9510693751439811	9510693751443160	9510693751445145	9510693751446670

1	17460813	84297126	18283788	96431395	52776760
1	44492282	01171123	49553264	82414660	41285720
1	47699719	59277571	73633936	51396213	79085480
3	74373319	56845198	89317764	04948781	96178490
11	72784255	93238765	61052131	96981236	70218170

Table 2

Some m with $rm+1$ prime for $r=6$, 12, 18, and 36.

32016531278336	61778652920320	85863288288256	90269095925760
103431922671616	118520551937536	129949692862976	161980645770240
169850734699520	216684974643200	223486317857280	265131346677760
266728027023360	295903497402880	334697679219200	353997424132096
385291843847680	421490647515136	437534194639360	461654369021440
475388910342656	486800024231936	574050879246336	621204455259136
633936693369856	643140267916800	654783157985280	699233193632256
702524415376896	736415243357696	737581335068160	739685862775296
754305789101056	763983732228096	776497070614016	795558858649600
836065608901120	841031284775936	852887923987456	894056008936960
899392011640320	909703476323840	929150012816896	944238127024640
967402868490240	983535005620736	986882883764736	998857986356736
1030750388614656	1043477476143616	1059843449686016	1088689282832896
1095598273205760	1106344962048000	1116054323723776	1169865026661376
1193982625752576	1205393739641856	1306023230777856	1321446647858176
1322785799115776	1354937790694400	1362512236230656	1403765305779200
1414525386134016	1442750574178816	1462047228742656	1464455125715456
1470256741009920	1501147355115520	1508618273958400	1509151874228736
1545486653254656	1673159273921536	1751929181009920	1773132065883136

1792219606827520	1801169257693696	1809600760034816	1822868658648576
1830869572354560	1888188336528896	1906817475696640	1924754376675840
2066467998278656	2083233141907456	2112382859378176	2138835732239360
2142585870818816	2148426115476480	2166236827202560	2175095827829760
2179822001652736	2185026149463040	2199783081263616	2210482899811840
2227701809693696	2243652646346240	2249277081628160	2287863179941376
2382514905886720	2441625557455360	2445149070437376	2452372761355776
2453639804468736	2538052173875200	2538312793312256	2555296836665856
2555404483824640	2578461063073280	2636155304657920	2643268773126656
2650929748436480	2678782034361856	2679827087400960	2713705038927360
2735582650011136	2823647296943616	2869157837374976	2893743624348160
2922247458866176	2925749854462976	2931026625476096	2948193514482176
2964201522592256	2967904275819520	2987343086439936	3001344427896320
3025560403099136	3108466742398976	3168630172879360	3308430353358336
3310023943354880	3383736494213120	3385928066752000	3428237520619520
3446635913724416	3448363418846720	3450902655654400	3530119118181376
3535083763939840	3560463770620416	3563559270258176	3567890909518336
3576095271203840	3583617695864320	3584503595927040	3606803039656960
3621359098768896	3632146477207040	3666974711068160	3710376603326976
3741987783820800	3788807087077376	3935631630960640	3936582428353536
3959970705067520	3970616957565440	3974616899360256	3982594635448320
3990800027250176	3998677842052096	4050268129192960	4061221356363776
4066149948049920	4073945868601856	4082287235762176	4083383794611880
4129656621150720	4138572793235456	4150642666531840	4175937688613376
4197083402029056	4213116647989760	4226696115680000	4236354012658176
4248918856861696	4256968914989056	4296618394541056	4306064561488896
4338412275174400	4385030190684160	4415990852701696	4437986412107776
4501734647493120	4505101067731456	4542511803287040	4547937941171200
4584636351269376	4636121566542336	4642665380668416	4695870375191040
4746652536053760	4748040617838080	4759328632823296	4811835723517440
4813342783740416	4876534756295680	4880601655653376	4904476662343680
4915367567475200	4928195606406656	5026233839859200	5051147203832320
5085605110864896	5111138604881920	5118006905658880	5138730786428416
5154962329786880	5173535842671616	5195858464019456	5259158598791680
5259586097077760	5275234079522816	5306431153243136	5424418104910336
5427191178129920	5433943590817280	5434177942287360	5445534975068160
5446454353912320	5501347194077696	5519438612509696	5534992854366720
5625257314768896	5633322610746880	5635267470419456	5681568110092800
5695256296178176	5699654893001216	5700130806755840	5772772551666176
5815980266992640	5820567375108096	5857218399854080	5901642167534080
5916135904606720	5980883867911680	5993430685079040	6008671256506880

6012150474485760	6042469374016000	6097102109802496	6104042518724096
6128507782084096	6142290738873856	6155241361651200	6188231352882176
6190755137944576	6239237048993280	6265693012203520	6327389255815680
6375784637090816	6398408052413440	6450480949065216	6458907300824576
6564022948673536	6735964304509440	6744748621701120	6772837319329280
6774179560935936	6782886619401216	6830758186511360	6859936232181760
6861252720879616	6868731365595136	6914154346136576	6957444985829376
6960110411890176	6993462489018880	7021889064810496	7056691030704640
7060052300361216	7077739398125056	7085552315596800	7175425331785216
8550768560766141	8522851273346280	8522851273364036	

Table 3

Some m with $rm+1$ prime for $r=6$, 12, 18, 36, and 72.

28606846153216	109975736797696	116267172417536	292710136711680
322647893191680	327652198429696	743849593070080	975610320524800
1214425284758016	1693385608493056	1725800279741440	1734716451826176
1810081824371200	2583838270430720	2600188792227840	3112589268039680
3132846506101760	3318031037758976	3437393194756096	3570092268162560
3709980008531456	3783406187043840	4888937357173760	5924788881963520
6044097472910336	6461039126615040	6865524613391360	6877409580802560

REFERENCES

[1] P. T. BATEMAN and R. A. HORN: A heuristic formula concerning the distribution of prime numbers. Math. Comp. **16** (1962). 363—367.

[2] J. BRILLHART and J. L. SELFRIDGE: Some factorizations of $2^n \pm 1$ and related results. Math. Comp. **21** (1967), 87—96.

[3] J. CHERNICK: On Fermat's simple theorem. Bull. Amer. Math. Soc. **45** (1939), 269—274.

[4] P. ERDÖS: On pseudoprimes and Carmichael numbers. Publ. Math. Debrecen. **4** (1956), 201—206.

[5] M. KISHORE: On the equation $k\phi(M) = M - 1$. Not. Amer. Math. Soc. **22** (1975), A—501—A—502.

[6] D. H. LEHMER: On Euler's totient function. Bull. Amer. Math. Soc. **38** (1932), 745—757.

[7] C. POMERANCE: On composite n for which $\phi(n) | n-1$, II. Pacific J. Math. **69** (1977), 177—186.

[8] J. L. SELFRIDGE and M. C. WUNDERLICH: An efficient algorithm for testing large numbers for primality. Proc. Fourth Manitoba Conference on Numerical Math. (1974), 109—120.

[9] S. WEINTRAUB: Seventeen primes in arithmetic progression. Math. Comp. **31** (1977), 1030.

[10] M. YORINAGA: Numerical Computation of Carmichael numbers. Math. J. Okayama Univ. **20** (1978), 151—163.

[11] J.R. HILL: Large Carmichael numbers with three prime factors. Not. Amer. Math. Soc. **26** (1979), A—374.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
URBANA, IL 61801 U. S. A.
AND
DEPARTMENT OF MATHEMATICAL SCIENCES
NORTHERN ILLINOIS UNIVERSITY
DEKALB, IL 60115 U. S. A.

(*Received July 24, 1979*)