Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.1

Carmichael Numbers of the form $(6m+1)(12m+1)(18m+1)$

Harvey Dubner

449 Beverly Road
Ridgewood, New Jersey 07450
USA

hdubner1@compuserve.com

Abstract

Numbers of the form $(6m+1)(12m+1)(18m+1)$ where all three factors are simultaneously prime are the best known examples of Carmichael numbers. In this paper we tabulate the counts of such numbers up to 10^n for each $n \leq 42$. We also derive a function for estimating these counts that is remarkably accurate.

1 Introduction

Fermat's "Little Theorem" says that if a is any integer prime to N, and if N is prime, then

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

However, this is not a sufficient condition for a number to be prime since there are composite numbers known as Carmichael numbers which satisfy this congruence. Carmichael numbers meet the following criterion,

Korselt's criterion (1899). *A composite odd number N is a Carmichael number if and only if N is squarefree and $p-1$ divides $N-1$ for every prime p dividing N.*

Considerable progress has been made investigating Carmichael numbers in the past several years. Alford, Granville and Pomerance showed that there are infinitely many Carmichael numbers [1]. Löw and Niebuhr constructed Carmichael numbers with millions of components [6]. Balasubramanian and Nagaraj established an upper bound for the number of 3-component Carmichael numbers up to x that is a little more than $x^{1/3}$ [2]. Granville and Pomerance have developed several conjectures which seem to resolve some serious inconsistencies concerning the total number of Carmichael numbers [4]. These various conjectures are supported by counts of Carmichael numbers mostly done by Richard Pinch [8, 9]. However, in many cases the data is too limited to fully support some of the conjectures.

The main purpose of this paper is to supply accurate extended counts of an important family of 3-component Carmichael numbers. Chernick in 1939 [3] derived one-parameter expressions for Carmichael numbers which he called "Universal Forms," the most prominent of these being

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

$U_3(m)$ is a Carmichael number when the quantities in parentheses are simultaneously prime. There are indications that this family represents about 2.2% of the 3-component Carmichael numbers, more than any such family.

2 Search Method

The method used to search for and count numbers of the form (1) depends almost entirely on sieving. An array of 32,000,000 bits represents values of $q = 6m+1$ from $m = m_0$ to $m = m_0 + 31,999,999$. For each "small" prime from 5 to an appropriate maximum, each q is marked as composite when divisible by a small prime (i.e., the bit is turned on). With a slight program addition it can be determined if $r = 12m+1$ or $s = 18m+1$ has a factor, and if it does then q is also marked as composite even though q itself might actually be prime.

Typically, in the vicinity of $U_3 = 10^{41}$, about 18,000 numbers survive this sieving process which takes about 27 seconds on an Athlon/1.2 GHz computer. No additional tests are required since all three components of (1) must be prime and therefore the survivors are Carmichael numbers of the required form. The only additional processing needed is to determine the sizes of all the survivors and to do appropriate bookkeeping which takes about 1 second.

This process is repeated for the next block of 32,000,000 m's. It is easy to use multiple computers to get complete counts since the results for each block is independent of all other blocks. To extend the count from 10^{41} to 10^{42} took about 30 computer-days (Athlon/1.2 GHz). Compute time for each decade takes about 2.2 times as long as the previous decade. Thus, extending the count an additional decade takes about the same time as it took for all the previous counts.

3 Theoretical Count

It is interesting and important to try to estimate the the number of Carmichael numbers of the form $U_3(m)$ that are less than a given X. The famous Hardy-Littlewood conjectures [5] will be used as a model. We follow the theory as described in detail in Riesel's book [10, p. 60].

Consider a number of the form (1),

$$u = q \cdot r \cdot s, \quad \text{where} \quad q = 6m+1, \quad r = 12m+1, \quad s = 18m+1. \tag{2}$$

If q were chosen at random, by the Prime Number Theorem the probability of q being prime would be $1/\log q$ asymptotically. However in our case q can never be divisible by 2 or 3. When a number cannot be divided by a prime, p, the probability of the number being prime increases by the factor $p/(p-1)$. Thus the probability of q being prime is increased by the factor $(2/1)(3/2) = 3$ and becomes

$$P_q = \frac{3}{\log(6m+1)}. \tag{3}$$

As with q, r cannot have 2 or 3 as a factor, but its primality is also affected if q is prime. Normally the chance that a prime p will not divide r is $(p-1)/p$ because $(q \bmod p)$ has $(p-1)$ values which are not zero. However, since $r = q + 6m$ it is easy to show that if q is prime then $(r \bmod p)$ has only $(p-2)$ values which are not zero—thus dropping the probability that r is prime by the factor $(p-2)/(p-1)$. The correction factor, $C_r(p)$, for p is,

$$C_r(p) = \frac{p}{(p-1)} \cdot \frac{(p-2)}{(p-1)} = \frac{p(p-2)}{(p-1)(p-1)}$$

The full correction factor is the product of these for $p = 5, 7, 11, 13, \cdots \infty$,

$$C_r = \prod_5^\infty \frac{p(p-2)}{(p-1)(p-1)} \doteq .880216$$

and the probability of r being prime becomes,

$$P_r = 3 \cdot C_r \cdot \frac{1}{\log(12m+1)} = \frac{2.640648}{\log(12m+1)}\ . \tag{4}$$

Similarly, the full correction factor for s is

$$C_s = \prod_5^\infty \frac{p(p-3)}{(p-1)(p-2)} = .721604$$

and the probability of s being prime becomes,

$$P_s = 3 \cdot C_s \cdot \frac{1}{\log(18m+1)} = \frac{2.164812}{\log(18m+1)} \ . \tag{5}$$

For a given m the probability of q, r and s being prime simultaneously is,

$$P_{qrs} = P_q \cdot P_r \cdot P_s = \frac{17.14952}{\log(6m+1)\log(12m+1)\log(18m+1)} \ . \tag{6}$$

Summing this probability over all appropriate m gives an estimate for the number of such Carmichael numbers less than a given X. To facilitate the computation we replace the summation by integration, and replace the Carmichael number components with,

$$\log(6m+1)\log(12m+1)\log(18m+1) = \log^3(a_x m),$$

where a_x is determined by evaluating the above expression at $m = M = (X/1296)^{1/3}$, the maximum value of m corresponding to a given X.

The estimate now becomes,

$$E(X) = 17.14952 \sum_{m=1}^{M} \frac{1}{\log^3(a_x m)} \approx 17.14952 \int_1^M \frac{dm}{\log^3(a_x m)} \ . \tag{7}$$

To numerically evaluate $E(X)$, integrate by parts twice giving,

$$E(X) \approx \frac{17.14952}{2a_x} \left[\int^{a_x M} \frac{dx}{\log(x)} - \frac{a_x M}{\log(a_x M)} - \frac{a_x M}{\log^2(a_x M)} \right] \ . \tag{8}$$

The above integral term is the well-known logarithmic integral function, $L_i(x)$, which is easy to accurately evaluate numerically. Lower limits are omitted since they have negligible effect on the totals.

4 Results

Table 1 shows the actual counts of $(6m+1)(12m+1)(18m+1)$ Carmichael numbers and the estimated counts from Eq. (8). The errors and percentage errors are also shown. The estimates are remarkably close to the actual counts.

Although we do not know the exact probability distribution of the counts, we can make the reasonable assumption that they can be approximated by a Poisson distribution since this is true for almost all distributions of rare phenomena. We can then present the error as the number of standard deviations, which effectively normalizes the error. If $N(X)$ is the actual number of Carmichael numbers found up to X, and $E(X)$ is the estimated number then

$$\text{error in standard deviations} = \frac{N(X) - E(X)}{\sqrt{E(X)}} \ .$$

This is the last column in Table 1. Almost all these normalized errors are within one standard deviation, excellent results which support the accuracy of the theoretical estimating function over a wide range of of values.

X	actual	calculated	error	% error	error in stand. dev
10^{10}	10	14	-4	-40.00000	-1.07
10^{11}	16	21	-5	-31.25000	-1.09
10^{12}	25	34	-9	-36.00000	-1.57
10^{13}	50	54	-4	-8.00000	-0.54
10^{14}	86	89	-3	-3.48837	-0.32
10^{15}	150	149	1	0.66667	0.08
10^{16}	256	256	0	0.00000	0.00
10^{17}	436	447	-11	-2.52294	-0.52
10^{18}	783	793	-10	-1.27714	-0.36
10^{19}	1435	1422	13	0.90592	0.34
10^{20}	2631	2581	50	1.90042	0.98
10^{21}	4765	4729	36	0.75551	0.52
10^{22}	8766	8743	23	0.26238	0.25
10^{23}	16320	16290	30	0.18382	0.24
10^{24}	30601	30563	38	0.12418	0.22
10^{25}	57719	57706	13	0.02252	0.05
10^{26}	109504	109578	-74	-0.06758	-0.22
10^{27}	208822	209170	-348	-0.16665	-0.76
10^{28}	400643	401200	-557	-0.13903	-0.88
10^{29}	771735	772935	-1200	-0.15549	-1.37
10^{30}	1494772	1495205	-433	-0.02897	-0.35
10^{31}	2903761	2903388	373	0.01285	0.22
10^{32}	5658670	5657731	939	0.01659	0.39
10^{33}	11059937	11061388	-1451	-0.01312	-0.44
10^{34}	21696205	21692750	3455	0.01592	0.74
10^{35}	42670184	42665199	4985	0.01168	0.76
10^{36}	84144873	84141713	3160	0.00376	0.34
10^{37}	66369603	166363608	5995	0.00360	0.46
10^{38}	329733896	329724862	9034	0.00274	0.50
10^{39}	655014986	654988567	26419	0.00403	1.03
10^{40}	1303918824	1303921334	-2510	-0.00019	-0.07
10^{41}	2601139051	2601093060	45991	0.00177	0.90
10^{42}	5198859223	5198788710	70513	0.00136	0.98

Table 1: Count of $(6m+1)(12m+1)(18m+1)$ Carmichael Numbers up to X

5 Estimating $C_3(X)$ for large X

The 3-component Carmichael numbers can be expressed in the form

$$(am+1)(bm+1)(cm+1), \quad a<b<c, \quad a,b,c \text{ relatively prime in pairs.}$$

As shown in Ore's book [7, Ch. 14], $m = m_0 + k(abc)$, $k = 1, 2, 3\ldots$, where m_0 is the solution to the linear congruence

$$m_0(ab+ac+bc) \equiv -(a+b+c) \pmod{abc}.$$

Thus, for a given a, b, c it is easy to find all allowable values of m. All that remains is to test the three components for primality for each allowable m. In this way a "family" of Carmichael numbers is found corresponding to (a, b, c). Our 6–12-18 Carmichael numbers are the $(1, 2, 3)$ family.

From another project we found that part of the process of counting 3-component Carmichael numbers, $C_3(X)$ could be greatly speeded up if we counted by families. For example, finding all such numbers less than 10^{18}, took about 1100 hours using a Pentium III/550 MHz. However, we found 64.4% of them in about 4 hours by limiting the search to all families with $a = 1$, that is $(1, b, c)$. We repeated this for a wide range of X and found that the time improvement factor of about 300 was consistant and the ratios of Carmichael numbers found to $C_3(X)$ were remarkably similar. The results are shown in Table 2.

Having accurate values for $C_3(10^n)$ for large values of n is quite desirable to support various conjectures in [4]. Exhaustive searching is now used to obtain exact counts, but even with the continuing cost-performance improvement in computing hardware it takes much too long to extend the count for each additional decade. It seems we should consider sacrificing some accuracy in determining $C_3(10^n)$ if the upper limit of n can be extended in a practical manner.

Note the percentage columns of Table 2. The counts of $(1, a, b)$ are about 64.4% of the corresponding $C_3(10^n)$ for a wide range of n. Similarly the counts of $(1, 2, 3)$ are about 2.2% of $C_3(10^n)$, and appear to be closely correlated to counts of $(1, a, b)$. If we assume these correlations continue for larger values of n then the actual counts of the $(1, 2, 3)$ family possibly could be used to estimate $C_3(10^n)$ up to $n = 42$ with about 1% accuracy. Optimistically, this might even be extended for $n > 42$ by using the estimates from Eq. (8).

However, it must be remembered that all these results are heuristic, and although interesting they require more rigorous theory and study. One area for future research is to relate the above results to the conjectures and conclusions of the Granville and Pomerance paper [4].

X	$C_3(X)$	(1,2,3)	%	$(1,b,c)$	%
10^3	1				
10^4	7				
10^5	12				
10^8	84			59	70.24
10^9	172			122	70.93
10^{10}	335	10	2.985	227	67.76
10^{11}	590	16	2.712	403	68.31
10^{12}	1000	25	2.500	680	68.00
10^{13}	1858	50	2.691	1220	65.66
10^{14}	3284	86	2.619	2104	64.07
10^{15}	6083	150	2.466	3911	64.29
10^{16}	10816	256	2.368	6948	64.24
10^{17}	19539	436	2.331	12599	64.48
10^{18}	35586	783	2.200	22920	64.41
10^{19}	65309	1435	2.198	41997	64.32
10^{20}	120625	2631	2.182	77413	64.22

Table 2: Count of families of 3-component Carmichael numbers

6 Acknowledgements

The 3-component Carmichael number counts, $C_3(10^n)$, are taken from the Granville, Pomerance paper [4]. These counts were calculated by Richard Pinch, John Chick, Gordon Davies and Matthew Williams.

References

[1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math.* **140** (1994), 703–722. MR **95k**:11114

[2] R. Balasubramanian and S. V. Nagaraj, Density of Carmichael numbers with three prime factors, *Math. Comp.* **66** (1997), 1705–1708. MR**96d:**11110

[3] J. Chernick, On Fermat's simple theorem, *Bull. Amer. Math. Soc.*, **45** (1935), 269–274.

[4] A. Granville and C. Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (2002), 883–908.

[5] G. H. Hardy and J. E. Littlewood, Some problems on partitio numerorum III. On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1–70.

[6] G. Löh and W. Niebuhr, A new algorithm for constructing large Carmichael numbers, *Math. Comp.* **65**, (1996), 823–836.

[7] O. Ore, *Number Theory and Its History*, McGraw-Hill Book Company, Inc. 1948. Reprinted, Dover Publications, Inc., 1988.

[8] R. G. E. Pinch, The Carmichael numbers up to 10^{16}, to appear.

[9] R. G. E. Pinch, 3-component Carmichael numbers up to 10^{18}, private communication.

[10] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhäuser, 1994.

2000 *Mathematics Subject Classification*: 11A99
Keywords: Carmichael numbers

(Concerned with sequence A002997.)

Received August 12, 2002; revised version received September 16, 2002. Published in *Journal of Integer Sequences* September 23, 2002. Revised version, November 25, 2002.

Return to Journal of Integer Sequences home page.