MATHEMATICS OF COMPUTATION
Volume 66, Number 220, October 1997, Pages 1705–1708
S 0025-5718(97)00857-0

DENSITY OF CARMICHAEL NUMBERS WITH THREE PRIME FACTORS

R. BALASUBRAMANIAN AND S. V. NAGARAJ

ABSTRACT. We get an upper bound of $O(x^{5/14+o(1)})$ on the number of Carmichael numbers $\leq x$ with exactly three prime factors.

1. Introduction

A Carmichael number is a composite number n which satisfies the condition $a^n \equiv a \bmod n$ for every integer a. The smallest Carmichael number is 561. The Carmichael numbers have many interesting properties. For example, it is known that they are square-free and the product of at least three primes [5]. The reader may consult [4], [7], [8], [11] for more on Carmichael numbers.

The problem of proving the existence of infinitely many Carmichael numbers was a long-standing open problem until it was solved recently, by Alford, Granville and Pomerance [1]. They also gave a lower bound for the number of Carmichael numbers less than a given number x. Let $C(x)$ denote the number of Carmichael numbers up to x. They showed that $C(x) > x^{2/7}$ for all sufficiently large x.

Let $C_k(x)$ denote the number of Carmichael numbers up to x with k prime factors where $k \geq 3$. It is an open problem to show that the function $C_3(x)$ is unbounded. It is not known whether any of the functions $C_k(x)$ is unbounded. Pomerance et al. [9] proved that $C_3(x) = O(x^{2/3})$. Damgård et al. [3] improved this to $C_3(x) \leq (1/4)x^{1/2}(\log x)^{11/4}$ for all $x \geq 1$. An unpublished estimate of $O(x^{2/5+o(1)})$ for $C_3(x)$ was obtained by S. W. Graham. We show that for sufficiently large x, $C_3(x) = O(x^{5/14+o(1)})$. Granville (see [8]) has conjectured that $C_k(x) = x^{1/k+o_k(x)}$ for $x \to \infty$. Our upper bound for $C_3(x)$ comes very close to his conjectured value.

2. Proof of our bound

We state our result on the upper bound for $C_3(x)$ and give its proof. The proof is very similar to that in Damgård et al. [3].

Theorem 2.1. *Let $C_3(x)$ denote the number of Carmichael numbers up to x with exactly three prime factors. Then, for all sufficiently large x we have $C_3(x) = O(x^{5/14+o(1)})$.*

Proof. If n is a Carmichael number with three prime factors p, q, r with $2 < p < q < r$, then $n - 1 \equiv 0 \bmod p - 1$, $n - 1 \equiv 0 \bmod q - 1$, $n - 1 \equiv 0 \bmod r - 1$.

Received by the editor March 8, 1996 and, in revised form, August 7, 1996.
1991 *Mathematics Subject Classification.* Primary 11N25; Secondary 11Y11.
Key words and phrases. Carmichael number, primality testing.

Let $g = \gcd(p-1, q-1, r-1)$ and a, b, c be such that $p-1 = ga$, $q-1 = gb$, $r-1 = gc$; then $a < b < c$. The congruences given above imply that $gbc + b + c \equiv 0 \bmod a$, $gac + a + c \equiv 0 \bmod b$ and $gab + a + b \equiv 0 \bmod c$. These three congruences can be replaced by the single congruence $g(ab + ac + bc) + a + b + c \equiv 0 \bmod abc$ by observing that a, b, c are pair-wise coprime. This is true because $\gcd(a, b, c) = 1$ and $c \equiv 0 \bmod \gcd(a, b)$, $b \equiv 0 \bmod \gcd(a, c)$, $a \equiv 0 \bmod \gcd(b, c)$ implies that $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$. Hence, if a, b, c are given, then g is determined modulo abc.

We count the number N of quadruples (g, a, b, c) which satisfy the above conditions and $g^3abc \leq x$. Thus $C_3(x) \leq N$. We write $N = N_1 + N_2 + N_3$ where N_1 is the number of quadruples (g, a, b, c) such that $g > abc$, N_2 is the number of quadruples (g, a, b, c) such that $G < g \leq abc$ where $G = x^{3/14}$, N_3 is the number of quadruples (g, a, b, c) such that $g \leq G$ and $g \leq abc$ where G is as above. □

Estimate for N_1

If (a, b, c) are given, then the number of g with $g^3abc \leq x$, g in a particular residue class modulo abc and $g > abc$ is at most $(x/abc)^{1/3}/abc$, which is $x^{1/3}/(abc)^{4/3}$. Hence

$$N_1 \leq \sum_{a<b<c} \frac{x^{1/3}}{(abc)^{4/3}} < \frac{\zeta^3(4/3)x^{1/3}}{6}$$

where ζ is the Riemann zeta function. Thus $N_1 = O(x^{1/3})$.

Estimate for N_2

For each coprime triple (a, b, c) there is at most one g that satisfies the condition $g(ab + ac + bc) + a + b + c \equiv 0 \bmod abc$ and $g \leq abc$. If $g > G$ and $g^3abc \leq x$, then $abc \leq x/G^3$. Thus N_2 is at most the number of triples (a, b, c) with $a < b < c$ and $abc \leq x/G^3$. Hence,

$$\begin{aligned}
N_2 &\leq \sum_{1 \leq a < x^{1/3}/G} \quad \sum_{a<b<(x/aG^3)^{1/2}} \quad \sum_{b<c\leq x/abG^3} 1 \\
&< \sum_a \sum_b \frac{x}{abG^3} \quad < \quad \sum_a \frac{x}{aG^3} \ln\left(\left(\frac{x}{aG^3}\right)^{1/2}\right) \\
&< \frac{x}{2G^3}\left(1 + \ln\left(\frac{x^{1/3}}{G}\right)\right) \ln\left(\frac{x}{G^3}\right) \quad < \quad \frac{x}{6G^3}(\ln(x))^2 \\
&= O(x^{5/14+o(1)}), \text{ since } G = x^{3/14}.
\end{aligned}$$

Thus $N_2 = O(x^{5/14+o(1)})$.

Estimate for N_3

In this case $g \leq G$ and $g \leq abc$ where $G = x^{3/14}$. Let $g(ab+bc+ac)+a+b+c = \lambda abc$ where $\lambda \geq 1$ is a positive integer. Then $(\lambda a - g)bc = ga(b+c) + a + b + c$. We note that $6gbc \geq g(ab + bc + ac) + a + b + c = \lambda abc$ implies that $\lambda a \leq 6g$. We break the range for g, a, b as $G_1 \leq g \leq 2G_1$, $A \leq a \leq 2A$, $B \leq b \leq 2B$. We consider two cases: $B \geq Ax^{1/14}$ and $B < Ax^{1/14}$.

THE CASE $B \geq Ax^{1/14}$

We have,

$$\begin{aligned}
\mid \lambda a - g \mid &= \frac{ga(b+c)+a+b+c}{bc} \\
&= ga(1/c+1/b) + a/bc + 1/c + 1/b \\
&< 2ga/b + 3/b \quad (\text{since } 1/c < 1/b \text{ and } a < b < c) \\
&= O(G_1 A/B) \quad (\text{since } g \leq 2G_1, a \leq 2A, B \leq b) \\
&= O(x^{2/14}) \quad (\text{since } G_1 \leq G = x^{3/14} \text{ and } B \geq Ax^{1/14}).
\end{aligned}$$

We can fix g in $x^{3/14}$ ways since $g \leq G = x^{3/14}$. For a given value of g, λa has only $O(x^{2/14})$ choices since $\mid \lambda a - g \mid = O(x^{2/14})$. So we can fix g, a, λ in $O(x^{5/14+o(1)})$ ways. Now b, c have only $x^{o(1)}$ choices since $(g-\lambda a)bc + (b+c)(ga+1) + a = 0$ implies $[(g-\lambda a)b + 1 + ga][(g-\lambda a)c + 1 + ga] = (1+ga)^2 - (g-\lambda a)a$. We must ensure that $ga - \lambda a^2 \neq (ga+1)^2$. It is easily checked that this must be the case by looking, modulo a, at both sides of this inequality.

THE CASE $B < Ax^{1/14}$

Let $AJ \leq B \leq 2AJ$; then $J \leq x^{1/14}$. We consider the equality $g(ab+bc+ca) + a + b + c = \lambda abc$. We fix λ, a, b first and show that g, c have $x^{o(1)}$ choices by considering the equality $gc(a+b) + c(1-\lambda ab) + gab + a + b = 0$. This equality implies that $[\lambda ab - 1 - (a+b)g][ab + (a+b)c] = (\lambda ab - 1)ab + (a+b)^2$ which is positive. Thus, for fixed λ, a, b there are $\leq x^{o(1)}$ choices for g, c. Since $\lambda a \leq 6g \leq 12G_1$ there are $O(G_1)$ choices for λa. Now if we consider $G_1 \leq g$ and $g^3 abc \leq x$ we get

$$\begin{aligned}
abc &\leq x/g^3, \\
ab^2 &\leq x/g^3 \text{ since } c > b, \\
A(AJ)^2 &\leq x/G_1^3 \text{ since } A \leq a \leq 2A,\ B \leq b \leq 2B,\ AJ \leq B \leq 2AJ,\ G_1 \leq g, \\
A^3 J^2 &= O(x/G_1^3), \\
A &= O\left(\frac{x^{1/3}}{G_1 J^{2/3}}\right) \text{ and } B = O\left(\frac{x^{1/3} J^{1/3}}{G_1}\right).
\end{aligned}$$

Then since $B \leq b \leq 2B$ there are $O(x^{1/3} J^{1/3}/G_1)$ choices for b. Therefore to fix λ, a, b there are

$$O(G_1^{1+o(1)}(x^{1/3} J^{1/3}/G_1)) = O(x^{1/3+o(1)} J^{1/3}) = O(x^{1/3+o(1)} x^{1/42}) = O(x^{5/14+o(1)})$$

choices, since $J \leq x^{1/14}$. Once we fix λ, a, b then g, c have only $x^{o(1)}$ choices. Therefore to fix λ, a, b, g, c there are $O(x^{5/14+o(1)})$ choices.

We let the A, B, J run over powers of 2 and this introduces a factor of $x^{o(1)}$. Hence $N_3 = O(x^{5/14+o(1)})$. Hence $N = N_1 + N_2 + N_3 = O(x^{1/3}) + O(x^{5/14+o(1)}) + O(x^{5/14+o(1)}) = O(x^{5/14+o(1)})$.

Discussion. Our choices for parameters such as G were not arbitrary but optimal. We have used the optimal values for the parameters as this results in a shorter and clearer proof.

It would be best to make our bounds explicit and replace the $x^{o(1)}$ with a power of $\log x$. It is easy to see that these are two different problems. For the first problem we could use a result of Ramanujan [10] that states that there is an explicit constant K_α depending on α such that the number of divisors of n, $d(n) < K_\alpha n^\alpha$ for any positive number $0 < \alpha < 1$. For the second problem we need to consider the average of the divisor function over a polynomial on an interval. There are some results in this direction (see [6]), however, they depend on the coefficients of the polynomial in an unknown way.

Acknowledgements

We thank Prof. Carl Pomerance for providing his papers and informing us of the work of Prof. S. W. Graham. We also thank him for his valuable suggestions. We thank Prof. S. W. Graham for informing us of his work and for his helpful comments. Finally, we thank Prof. Mohan Nair for discussing with us and giving us his paper.

References

1. W.R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **140** (1994), 703–722. MR **95k:**11114
2. W.R. Alford, A. Granville, and C. Pomerance, *On the difficulty of finding reliable witnesses*, Lecture Notes in Comput. Sci. **877** (1994), 1–16. MR **96d:**11136
3. I. Damgård, P. Landrock, and C. Pomerance, *Average case error estimates for the strong probable prime test*, Math. Comp. **61** (1993), 177–194. MR **94b:**11124
4. A. Granville, *Primality testing and Carmichael numbers*, Notices Amer. Math. Soc. **39** (1992), 696–700.
5. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, New York, 1987. MR **88i:**94001
6. Mohan Nair, *Multiplicative functions of polynomial values in short intervals*, Acta Arith. (3) **62** (1992), 257–269. MR **94b:**11093
7. R.G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–392. MR **93m:**11137
8. C. Pomerance, *Carmichael numbers*, Nieuw Archief voor Wiskunde **11** (1993), 199–209. MR **94h:**11085
9. C. Pomerance, J.L. Selfridge, and S.S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003-1026. MR **82g:**10030
10. S. Ramanujan, *Highly Composite Numbers*, Proc. London Math. Soc. (2) **14** (1915), 347–409.
11. P. Ribenboim, *The Book of Prime Number Records (Second Edition)*, Springer Verlag, New York, 1989. MR **90g:**11127

Institute of Mathematical Sciences, Tharamani, Madras 600 113, India
E-mail address: `balu@imsc.ernet.in`

Institute of Mathematical sciences, Tharamani, Madras 600 113, India
E-mail address: `svn@imsc.ernet.in`