Hardy-Ramanujan Journal
Vol. 30 (2007) 6-12

Carmichael Numbers With Three Prime Factors

D.R. Heath-Brown
Mathematical Institute, Oxford

A Carmichael number (or absolute pseudo-prime) is a composite positive integer n such that $n|a^n - a$ for every integer a. It is not difficult to prove that such an integer must be square-free, with at least 3 prime factors. Moreover if the numbers $p = 6m + 1$, $q = 12m + 1$ and $r = 18m + 1$ are all prime, then $n = pqr$ will be a Carmichael number. However it is not currently known whether there are infinitely many prime triplets of this form. Indeed it is not known whether or not there are infinitely many Carmichael numbers with 3 prime factors. None the less it was proved by Alford, Granville and Pomerance [1] that there are infinitely many Carmichael numbers.

Let $C_3(x)$ denote the number of Carmichael numbers $n \leq x$ having $\omega(n) = 3$. It has been conjectured by Granville and Pomerance [3] that

$$C_3(x) \sim c\frac{x^{1/3}}{(\log x)^3},$$

with an explicit positive constant c. Various upper bounds approximating this have been given, the best available in the literature being the estimate

$$C_3(x) \ll_\varepsilon x^{5/14+\varepsilon},$$

for any fixed $\varepsilon > 0$, due to Balasubramanian and Nagaraj [2]. The goal of the present paper is to improve this as follows.

Theorem *For any fixed $\varepsilon > 0$ we have*

$$C_3(x) \ll_\varepsilon x^{7/20+\varepsilon}.$$

Note that $1/3 < 7/20 < 5/14$. Indeed

$$\frac{\frac{7}{20} - \frac{1}{3}}{\frac{5}{14} - \frac{1}{3}} = \frac{7}{10}.$$

Thus our results reduces the previous excess in the exponent by 30%.

Suppose that $n = pqr$ is counted by $C_3(x)$, where $p < q < r$. We write $m = (p - 1, q - 1, r - 1)$ and $p = 1 + am$, $q = 1 + bm$, $r = 1 + cm$. Since $p - 1 = am$ divides $n - 1 = abcm^3 + (ab + ac + bc)m^2 + (a + b + c)m$, we must have

$$a|(ab + ac + bc)m + a + b + c. \tag{1}$$

Thus $(a, b)|c$, and since we know that $(a, b, c) = 1$ we deduce that a and b are coprime. Similarly a and c are coprime, and also b and c. In analogy to (1) we see likewise that both b and c divide $(ab + ac + bc)m + a + b + c$. Since a, b and c have been shown to be coprime in pairs we conclude that the product abc divides $(ab + ac + bc)m + a + b + c$. We may therefore write

$$(ab + ac + bc)m + a + b + c = abck, \tag{2}$$

say, for some integer k. We proceed to divide the available ranges for a, b, c, m and k into $O((\log x)^5)$ dyadic ranges $(A, 2A]$, $(B, 2B]$, $(C, 2C]$, $(M, 2M]$ and $(K, 2K]$. We shall write $C_3(x; A, B, C, M, K)$ for the corresponding contribution to $C_3(x)$. Since $2 \le p < q < r$ we may suppose that

$$1 \le A \le B \le C. \tag{3}$$

Moreover, since $pqr \le x$ we will have

$$M^3 ABC \le x. \tag{4}$$

Finally we observe from (2) that

$$ABCK < abck = (ab + ac + bc)m + a + b + c \ll BCM,$$

whence

$$K \ll M/A. \tag{5}$$

To prove our result we give three different bounds for $C_3(x; A, B, C, M, K)$. The first two are completely elementary, and appear in a slightly different form in the work of Balasubramanian and Nagaraj [2].

For our first estimate we count the 5-tuples (a, b, c, m, k) according to the values of a, b and k. We multiply (2) by $a + b$ and re-write the answer as

$$\{abk - 1 - (a + b)m\}\{(a + b)c + ab\} = N_1, \text{ with } N_1 = a^2b^2k + a^2 + b^2 + abk.$$

One readily sees that $N_1 = O(x)$ by (3), (4) and (5). Hence the number of possible divisors of N_1 is $O_\varepsilon(x^\varepsilon)$. Moreover, given a, b and k, each pair of divisors determines c and m uniquely. We therefore conclude that

$$C_3(x; A, B, C, M, K) \ll_\varepsilon x^\varepsilon ABK \ll_\varepsilon x^\varepsilon BM, \tag{6}$$

by (5).

For our second estimate we substitute $h = ak - m$ into (2), to deduce that

$$hbc = ma(b + c) + a + b + c. \tag{7}$$

It follows that

$$h \ge 1 \quad \text{and} \quad h \ll (BC)^{-1}.MAC = MAB^{-1}. \tag{8}$$

We proceed to count solutions according to the values of h and m, there being $O(M^2AB^{-1})$ such pairs. Given h and m we have $ak = h + m$. However $h + m$ has $O_\varepsilon(x^\varepsilon)$ divisors, since $h + m \ll x$, by (3), (4) and (8). Thus we have $O_\varepsilon(x^\varepsilon M^2AB^{-1})$ possible 4-tuples (a, m, k, h). For each such 4-tuple we multiply (7) by h to obtain

$$\{hb - ma - 1\}\{hc - ma - 1\} = N_2 \quad \text{with} \quad N_2 = (ma + 1)^2 - ha. \tag{9}$$

If $N_2 = 0$ then $a = 1$, since $a | N_2 - 1$. We would then have $h = (m + 1)^2$. However if $N_2 = 0$ then (9) would imply $hb - ma - 1 = 0$ or $hc - ma - 1 = 0$. However, since we must have $a = 1$ and $h = (m + 1)^2$ these would entail either $(m + 1)^2 b = m + 1$ or $(m + 1)^2 c = m + 1$, which are impossible for $m \ge 1$. Thus we must have $N_2 \ne 0$ in (9). However it is also clear that $N_2 \ll x$, by (3), (4)

and (8). Thus N_2 has $O_\varepsilon(x^\varepsilon)$ pairs of divisors, and each such pair determines b and c, once the 4-tuple (a,m,k,h) has been specified. It therefore follows that

$$C_3(x;A,B,C,M,K) \ll_\varepsilon x^{2\varepsilon}M^2AB^{-1}. \tag{10}$$

We proceed to present a new estimate.

Lemma *For any fixed $\varepsilon > 0$ we have*

$$C_3(x;A,B,C,M,K) \ll_\varepsilon MA + x^\varepsilon A^{1/2}BC + x^\varepsilon A^2B^{1/2}C^{1/2}. \tag{11}$$

Before proving this we show how the theorem follows. We consider three cases. If

$$\max\{MA\,,\,A^{1/2}BC\,,\,A^2B^{1/2}C^{1/2}\} = MA$$

in (11), then it suffices to observe that $MA \le (M^3ABC)^{1/3} \ll x^{1/3}$, by (3) and (4), so that $C_3(x;A,B,C,M,K) \ll x^{1/3}$. If

$$\max\{MA\,,\,A^{1/2}BC\,,\,A^2B^{1/2}C^{1/2}\} = A^{1/2}BC,$$

then (11), in conjunction with (6) and (10), yields

$$\begin{aligned} C_3(x;A,B,C,M,K) &\ll_\varepsilon x^{2\varepsilon}\min\{BM\,,M^2AB^{-1}\,,\,A^{1/2}BC\} \\ &\ll_\varepsilon x^{2\varepsilon}(BM)^{11/20}(M^2AB^{-1})^{1/4}(A^{1/2}BC)^{1/5} \\ &= x^{2\varepsilon}(M^3ABC)^{7/20}(BC^{-1})^{3/20} \\ &\le x^{2\varepsilon+7/20}, \end{aligned}$$

by (3) and (4). Finally, if

$$\max\{MA\,,\,A^{1/2}BC\,,\,A^2B^{1/2}C^{1/2}\} = A^2B^{1/2}C^{1/2},$$

then (6), (10) and (11) yield

$$\begin{aligned} C_3(x;A,B,C,M,K) &\ll_\varepsilon x^{2\varepsilon}\min\{BM\,,M^2AB^{-1}\,,\,A^2B^{1/2}C^{1/2}\} \\ &\ll_\varepsilon x^{2\varepsilon}(BM)^{3/4}(M^2AB^{-1})^{3/20}(A^2B^{1/2}C^{1/2})^{1/10} \\ &= x^{2\varepsilon}(M^3ABC)^{7/20}(BC^{-1})^{3/10} \\ &\le x^{2\varepsilon+7/20}, \end{aligned}$$

by (3) and (4). Thus $C_3(x;A,B,C,M,K) \ll_\varepsilon x^{2\varepsilon+7/20}$ in every case. The theorem then follows on replacing ε by $\varepsilon/3$ and summing over the $O(\log x)^5$ sets of dyadic ranges for A,B,C,M and K.

We turn now to the proof of the lemma. From (2) we have

$$a(b+c)m + a + b + c \equiv 0 \pmod{bc}. \tag{12}$$

For coprime positive integers u and v we now define $\overline{u}^{(v)}$ by the conditions $0 \le \overline{u}^{(v)} < v$ and $u\overline{u}^{(v)} \equiv 1 \pmod v$. Where the context is clear we shall write $\overline{u}$ for $\overline{u}^{(v)}$. Since a, b and c are coprime in pairs we may now re-write (12) as $m \equiv -\overline{(b+c)} - \overline{a} \pmod{bc}$, where the inverses are taken modulo bc. For a given triple (a,b,c), each solution m of this congruence, with m in the range $M < m \le 2M$, corresponds to at most value of k. We now write $r := -\overline{(b+c)} - \overline{a}$

for brevity, and observe, using the familiar transformation formula for the theta-function, that

$$\begin{aligned}\#\{m\in(M,2M]: m\equiv r \pmod{bc}\}&\\ \leq\ & e^4 \sum_{\substack{m\in\mathbb{Z}\\ m\equiv r \pmod{bc}}} \exp\{-m^2M^{-2}\}\\ =\ & e^4\sum_{n\in\mathbb{Z}}\exp\{-(r+nbc)^2M^{-2}\}\\ =\ & e^4\sqrt{\pi}\frac{M}{bc}\sum_{n\in\mathbb{Z}} e(\frac{rn}{bc})\exp\{-(\pi nM/bc)^2\}\\ =\ & e^4\sqrt{\pi}\frac{M}{bc}\sum_{n\in\mathbb{Z}} e_{bc}(-n\overline{(b+c)}-n\overline{a})\exp\{-(\pi nM/bc)^2\}.\end{aligned}$$

Here we use the standard notations $e(t):=\exp(2\pi it)$ and $e_q(t):=\exp(2\pi it/q)$.

We may now deduce that

$$\begin{aligned}&C_3(x;A,B,C,M,K)\\ &\quad\leq\ e^4\sqrt{\pi}\sum_{a,b,c}\frac{M}{bc}\sum_{n\in\mathbb{Z}} e_{bc}(-n\overline{(b+c)}-n\overline{a})\exp\{-(\pi nM/bc)^2\}\\ &\quad=\ e^4\sqrt{\pi}\sum_{b,c}\frac{M}{bc}\sum_{n\in\mathbb{Z}} e_{bc}(-n\overline{(b+c)})\exp\{-(\pi nM/bc)^2\}\sum_a e_{bc}(-n\overline{a})\\ &\quad\ll\ \frac{M}{BC}\sum_{b,c}\sum_{n\in\mathbb{Z}}\exp\{-(\pi nM/bc)^2\}\Big|\sum_a e_{bc}(-n\overline{a})\Big|\\ &\quad\ll\ \frac{M}{BC}\sum_{b,c}\sum_{n\in\mathbb{Z}}\exp\{-(\pi nM/4BC)^2\}\Big|\sum_a e_{bc}(-n\overline{a})\Big|\\ &\quad\ll\ MA+\frac{M}{BC}\sum_{b,c}\sum_{n=1}^{\infty}\exp\{-(\pi nM/4BC)^2\}\Big|\sum_a e_{bc}(-n\overline{a})\Big|,\end{aligned}$$

where the variables a,b,c are restricted to be coprime in pairs, and to lie in the intervals $A<a\leq 2A$, $B<b\leq 2B$ and $C<c\leq 2C$. At this point we combine the variables b and c, writing $bc=f$, say. Thus f lies in the range $BC<f\leq 4BC$, and is coprime to a. Moreover each available value of f arises at most $d(f)\ll_\varepsilon x^\varepsilon$ times, so that

$$\begin{aligned}&C_3(x;A,B,C,M,K)\\ &\ll_\varepsilon\ MA+x^\varepsilon\frac{M}{BC}\sum_{BC<f\leq 4BC}\sum_{n=1}^{\infty}\exp\{-(\pi nM/4BC)^2\}\Big|\sum_{\substack{A<a\leq 2A\\(a,f)=1}} e_f(-n\overline{a})\Big|.\end{aligned}$$

We proceed to apply Cauchy's inequality, whence

$$C_3(x;A,B,C,M,K)\ll_\varepsilon MA+x^\varepsilon\frac{M}{BC}S_1^{1/2}S_2^{1/2},\tag{13}$$

where

$$S_1:=\sum_{BC<f\leq 4BC}\sum_{n=1}^{\infty}\exp\{-(\pi nM/4BC)^2\}$$

and

$$S_2 := \sum_{BC<f\le 4BC} \sum_{n=1}^{\infty} \exp\{-(\pi nM/4BC)^2\} \Big| \sum_{\substack{A<a\le 2A \\ (a,f)=1}} e_f(-n\overline{a}) \Big|^2.$$

Since

$$\sum_{n=1}^{\infty} \exp\{-n^2 t^{-2}\} \ll t \tag{14}$$

uniformly for $t > 0$, we trivially have

$$S_1 \ll B^2 C^2 M^{-1}. \tag{15}$$

To handle S_2 we expand the square, and rearrange the sum to produce

$$S_2 = \sum_{n=1}^{\infty} \exp\{-(\pi nM/4BC)^2\} \sum_{A<a_1,a_2\le 2A} S_3(a_1,a_2;n), \tag{16}$$

with

$$S_3(a_1,a_2;n) := \sum_{\substack{BC<f\le 4BC \\ (f,a_1a_2)=1}} e_f(n(\overline{a_1}-\overline{a_2})).$$

To deal with this last sum we observe that

$$\overline{a_1}-\overline{a_2} \equiv (a_2-a_1)\overline{a_1a_2} \pmod f.$$

Moreover we have

$$a_1a_2\overline{a_1a_2}^{(f)} + f\overline{f}^{(a_1a_2)} \equiv 1 \pmod{a_1a_2f},$$

whence

$$\frac{\overline{a_1a_2}^{(f)}}{f} = -\frac{\overline{f}^{(a_1a_2)}}{a_1a_2} + \frac{1}{a_1a_2f} + v$$

for some integer v. It follows that

$$e_f(n(\overline{a_1}-\overline{a_2})) = e_f(n(a_2-a_1)\overline{a_1a_2}) = e_{a_1a_2}(n(a_1-a_2)\overline{f}^{(a_1a_2)})e\Big(\frac{n(a_2-a_1)}{a_1a_2f}\Big).$$

We may therefore write

$$S_3(a_1,a_2;n) = \sum_{\substack{BC<f\le 4BC \\ (f,g)=1}} e_g(r\overline{f}^{(g)})e(\delta/f),$$

where we have written $g := a_1a_2$, $r := n(a_1-a_2)$ and $\delta := n(a_2-a_1)/a_1a_2$ for brevity. An elementary estimate for $S_3(a_1,a_2;n)$ will suffice for our purposes. By partial summation we have

$$S_3(a_1,a_2;n) \ll \Big(1+\frac{|\delta|}{BC}\Big) \max_{BC<F\le 4BC} \Big| \sum_{\substack{BC<f\le F \\ (f,g)=1}} e_g(r\overline{f}^{(g)}) \Big|.$$

Moreover, on writing

$$c_g(r) = \sum_{\substack{0<f\le g\\(f,g)=1}} e_g(r\overline{f}^{(g)}) = \sum_{d|g,\, d|r} \mu(g/d)d \ll_\varepsilon (g,r)g^\varepsilon$$

for the Ramanujan sum, we have

$$\begin{aligned}\sum_{\substack{BC<f\le F\\(f,g)=1}} e_g(r\overline{f}^{(g)}) &= [\frac{F-BC}{g}]c_g(r) + O(g)\\ &\ll_\varepsilon \frac{BC}{g}(g,r)g^\varepsilon + g.\end{aligned}$$

Thus, on recalling the definitions of g, r and δ, we deduce from (3) that

$$\begin{aligned}S_3(a_1,a_2;n) &\ll (1+\frac{n}{ABC})\{\frac{BC}{A^2}\big(a_1a_2, n(a_1-a_2)\big)A^{2\varepsilon}+A^2\}\\ &\ll \frac{BC}{A^2}\big(a_1a_2, n(a_1-a_2)\big)A^{2\varepsilon}+A^2+\frac{n}{ABC}\{BCA^{2\varepsilon}+A^2\}\\ &\ll \frac{BC}{A^2}\big(a_1a_2, n(a_1-a_2)\big)A^{2\varepsilon}+A^2+nA^{-1+2\varepsilon},\end{aligned}$$

in view of the fact that $\big(a_1a_2, n(a_1-a_2)\big) \le a_1a_2$.

We are now ready to perform the summation over n in (16).We begin by noting that $\big(a_1a_2, n(a_1-a_2)\big) \le \big(a_1a_2,(a_1-a_2)\big)(a_1a_2,n)$. If we now classify integers n according to the value of (a_1a_2,n) we find, using (14), that

$$\begin{aligned}&\sum_{n=1}^{\infty}\big(a_1a_2, n(a_1-a_2)\big)\exp\{-(\pi nM/4BC)^2\}\\ &\qquad\le \big(a_1a_2,(a_1-a_2)\big)\sum_{d|a_1a_2} d\sum_{n:d|n}\exp\{-(\pi nM/4BC)^2\}\\ &\qquad= \big(a_1a_2,(a_1-a_2)\big)\sum_{d|a_1a_2} d\sum_{s=1}^{\infty}\exp\{-(\pi sdM/4BC)^2\}\\ &\qquad\ll_\varepsilon \big(a_1a_2,(a_1-a_2)\big)\sum_{d|a_1a_2} d\frac{BC}{dM}\\ &\qquad\ll_\varepsilon \big(a_1a_2,(a_1-a_2)\big)\frac{BC}{M}x^\varepsilon,\end{aligned}$$

since the number of divisors of a_1a_2 is $\ll_\varepsilon (a_1a_2)^\varepsilon \ll_\varepsilon x^\varepsilon$. Thus

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{BC}{A^2}\big(a_1a_2, n(a_1-a_2)\big)A^{2\varepsilon}&\exp\{-(\pi nM/4BC)^2\}\\ &\ll_\varepsilon \big(a_1a_2,(a_1-a_2)\big)B^2C^2A^{-2}M^{-1}x^{2\varepsilon}.\end{aligned}$$

A second application of (14) shows that

$$\sum_{n=1}^{\infty}A^2\exp\{-(\pi nM/4BC)^2\} \ll A^2BCM^{-1},$$

while the bound

$$\sum_{n=1}^{\infty} n \exp\{-n^2 t^{-2}\} \ll t^2,$$

which holds uniformly for $t > 0$, implies that

$$\sum_{n=1}^{\infty} nA^{-1+2\varepsilon} \exp\{-(\pi nM/4BC)^2\} \ll A^{-1}B^2C^2M^{-2}x^{\varepsilon}.$$

On combining these bounds we find that

$$\begin{aligned}\sum_{n=1}^{\infty} \exp\{-(\pi nM/4BC)^2\} & S_3(a_1, a_2; n) \\ &\ll_{\varepsilon} \big(a_1a_2, (a_1 - a_2)\big)B^2C^2A^{-2}M^{-1}x^{2\varepsilon} \\ &\qquad + A^2BCM^{-1} + A^{-1}B^2C^2M^{-2}x^{\varepsilon}.\end{aligned}$$

To complete our bound for S_2 we must investigate

$$\sum_{A < a_1, a_2 \le 2A} \big(a_1a_2, (a_1 - a_2)\big).$$

When $a_1 = a_2$ we have $\big(a_1a_2, (a_1 - a_2)\big) = a_1a_2 \ll A^2$, while for $a_1 \neq a_2$ we have $\big(a_1a_2, (a_1 - a_2)\big) \le |a_1 - a_2| \le A$. It follows that the sum above is $O(A^3)$. We therefore deduce from (16) and (3) that

$$\begin{aligned} S_2 &\ll_{\varepsilon} AB^2C^2M^{-1}x^{2\varepsilon} + A^4BCM^{-1} + AB^2C^2M^{-2}x^{\varepsilon} \\ &\ll_{\varepsilon} AB^2C^2M^{-1}x^{2\varepsilon} + A^4BCM^{-1}. \end{aligned}$$

If we combine this with (13) and (15), we deduce that

$$C_3(x; A, B, C, M, K) \ll_{\varepsilon} MA + x^{2\varepsilon}A^{1/2}BC + x^{\varepsilon}A^2B^{1/2}C^{1/2},$$

and the lemma follows on replacing ε by $\varepsilon/2$.

References

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

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

[3] A. Granville and C. Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.,* 71 (2002), 883–90.

Mathematical Institute,
24–29, St. Giles',
Oxford
OX1 3LB
UK

rhb@maths.ox.ac.uk

Received on 26-03-07
Accepted on 02-04-07