Carmichael numbers with three prime factors

Notes by G.J.O. Jameson

The following notes are expository, not a research article. However, a few of the results, such as the internal inequalities (1.5, 2.13 and 2.14) and the estimations of $f_3(p)$ (1.7, 1.8) and $K_3(g)$ (2.15), may not have appeared explicitly elsewhere.

1. Results in terms of the smallest prime factor

Introductory

An integer n is a Carmichael number if it is composite but behaves like a prime in terms of Fermat's little theorem: $a^{n-1} \equiv 1 \mod n$ for all a coprime to n. Such numbers must be odd (consider $(-1)^{n-1}$). By Korselt's criterion, Carmichael numbers can be characterised as square-free numbers $n = p_1 p_2 \dots p_k$ such that $n \equiv 1 \mod (p_j - 1)$ for each j (see, e.g. [JJ], section 6). It follows easily that Carmichael numbers have at least three prime factors. Also, if p and q are prime factors of a Carmichael number n, then q cannot be congruent to $1 \mod p$, since this would imply that p divides n-1.

The following simple observation will be used constantly: if we write $n = p_j r_j$, then $n \equiv 1 \mod (p_j - 1)$ if and only if $q_j \equiv 1 \mod (p_j - 1)$.

Now let n = pqr, where p, q, r are prime and p < q < r. We use this notation consistently. Of course, $q \ge p+2$ and $r \ge q+2$. By the preceding remark, n is a Carmichael number if and only if

$$qr \equiv 1 \mod (p-1)$$
, $pr \equiv 1 \mod (q-1)$, $pq \equiv 1 \mod (r-1)$.

Given a pair of primes (p,q), it is easy to find all primes r > q such that pqr is a Carmichael number. First, list the primes r > q such that r - 1 divides pq - 1 (consider even divisors d > q of pq - 1 and check whether d + 1 is prime). Then check whether the other two conditions hold. By applying this procedure to appropriate pairs (p,q), one can rapidly detect all the Carmichael numbers less than 3000 (details are given in [Jam]):

$$3 \times 11 \times 17 = 561$$
 $5 \times 17 \times 29 = 2465$
 $5 \times 13 \times 17 = 1105$ $7 \times 13 \times 31 = 2821$
 $7 \times 13 \times 19 = 1729$

The set of prime factors p, q, r is much more illuminating than n itself, and from now on we will usually give the numbers only in factorised form.

Carmichael numbers with given p

We now show that there are only finitely many Carmichael numbers pqr for a given p, and describe a method for finding them. These results were originated by Beeger [Be] and Duparc [Du].

We restate the conditions above more explicitly: if (and only if) n = pqr is a Carmichael number, then there exist integers h_1 , h_2 , h_3 such that

$$qr - 1 = h_1(p - 1),$$
 (1)

$$pr - 1 = h_2(q - 1),$$
 (2)

$$pq - 1 = h_3(r - 1).$$
 (3)

The rough significance of these numbers is shown by the approximations $h_1 \approx qr/p$ (etc.) when p, q, r are large. Some simple inequalities:

1.1. We have $2 \le h_3 \le p - 1$.

Proof. Since r-1>q, we have $qh_3< pq$, hence $h_3< p$, so in fact $h_3\leq p-1$. Also, $h_3\neq 1$ since $r\neq pq$.

Similarly, $h_1 > r$ and $p < h_2 < r$.

1.2. We have $r \leq \frac{1}{2}(pq+1)$ and $r < n^{1/2}$.

Proof. Clearly,
$$r-1 \leq \frac{1}{2}(pq-1)$$
, so $r \leq \frac{1}{2}(pq+1)$. Hence $r^2 \leq \frac{1}{2}(pqr+r) < n$.

We can express q and r in terms of p, h_2 and h_3 :

1.3 PROPOSITION. We have

$$q - 1 = \frac{(p-1)(p+h_3)}{h_2h_3 - p^2}. (4)$$

Proof. By (2) and (3),

$$h_2(q-1) = p(r-1) + (p-1) = \frac{p}{h_3}(pq-1) + (p-1),$$

SO

$$h_2h_3(q-1) = p(pq-1) + h_3(p-1) = p[p(q-1) + (p-1)] + h_3(p-1),$$

hence

$$(h_2h_3 - p^2)(q-1) = (p+h_3)(p-1).$$

Once p, q and h_3 are known, r is determined by (3).

1.4 THEOREM. Let p be prime. Then there are only finitely many 3-factor Carmichael numbers with smallest prime factor p. Denote this number by $f_3(p)$. Then

$$f_3(p) \le (p-2)(\log p + 2).$$

Further, for any $\varepsilon > 0$, we have $f_3(p) < \varepsilon p \log p$ for sufficiently large p, so $f_3(p) = o(p \log p)$.

Proof. Choose h_3 satisfying $2 \le h_3 \le p-1$. Write $h_2h_3 - p^2 = \Delta$. We will work with Δ rather than h_2 . Once Δ is chosen, q is determined by (4) and then r by (3). By (4),

$$\Delta = \frac{(p-1)(p+h_3)}{q-1}.$$

Clearly, Δ is a positive integer, so $\Delta \geq 1$. Also, since p-1 < q-1, we have $\Delta < p+h_3$, so in fact $\Delta \leq p+h_3-1$. In addition, Δ must be congruent to $-p^2 \mod h_3$. Hence the number of choices for Δ is no more than

$$\frac{p+h_3-2}{h_3}+1=\frac{p-2}{h_3}+2.$$

It now follows that

$$f_3(p) \le \sum_{h=2}^{p-1} \left(\frac{p-2}{h} + 2\right) < (p-2)(\log p + 2).$$

This estimation took no notice of the fact that Δ also has to be a divisor of $(p-1)(p+h_3)$. We use the well-known fact that for any $\varepsilon > 0$, $\tau(n)/n^{\varepsilon} \to 0$ as $n \to \infty$, where τ is the divisor function. So the number of choices for Δ is also bounded by $\tau[(p-1)(p+h_3)]$, which is less than p^{ε} for large enough p (since $(p-1)(p+h_3) < 2p^2$). Using this bound for $h_3 \leq p^{1-\varepsilon}$ and the previous one for $h_3 > p^{1-\varepsilon}$, together with the elementary estimation $\sum_{y < n \leq x} \frac{1}{n} \leq \log x - \log y + 1$, we see that $f_3(p) \leq S_1 + S_2$, where $S_1 = p^{1-\varepsilon}p^{\varepsilon} = p$ and

$$S_2 \le \sum_{p^{1-\varepsilon} < h < p} \left(\frac{p}{h} + 2\right) \le p(\varepsilon \log p + 1) + 2p = \varepsilon p \log p + 3p,$$

so $f_3(p) < \varepsilon p \log p + 4p < 2\varepsilon p \log p$ for large enough p.

Note. There is a constant C_{ε} (which can be estimated) such that $\tau(n) \leq C_{\varepsilon} n^{\varepsilon}$ for all n. For example, $C_{1/2} = \sqrt{3}$. The method of 1.4 (with $p^{1-2\varepsilon}$ instead of $p^{1-\varepsilon}$) gives the bound $f_3(p) \leq 2\varepsilon p \log p + (3 + 2^{\varepsilon}C_{\varepsilon})p$ valid for all p. We return to give a more refined bound in Theorem 1.7.

The proof of Theorem 1.4 amounts to a procedure for finding the Carmichael numbers pqr with a given p. We choose h_3 , then search for possible values of Δ . They have to satisfy:

$$\Delta \le p + h_3 - 1,$$

$$\Delta \equiv -p^2 \mod h_3,$$

$$\Delta \text{ divides } (p - 1)(p + h_3).$$

We list the values of Δ satisfying these conditions. For each of them, q is defined by (4), in the form $q-1=(p-1)(p+h_3)/\Delta$. If q is prime, we continue, deriving r from (3). This r will be an integer, because the expression for $h_2(q-1)$ in the proof of 1.3 shows that h_3 divides p(pq-1); by Euclid's lemma, h_3 divides p(pq-1). The algebra of 1.3, in reverse, shows that we have ensured that (2) holds. We still have to check whether r is prime and whether $qr \equiv 1 \mod (p-1)$: if so, then pqr is a Carmichael number. Furthermore, this process will detect all Carmichael numbers of the form pqr. We set out the cases p=3, 5, 7.

Case p=3. The only value for h_3 is 2. We require Δ to be odd, no greater than 4, and a divisor of 10. The only choice is $\Delta=1$, giving q=11. By (3), 2(r-1)=32, so r=17. Clearly, $qr\equiv 1 \mod 2$. So $3\times 11\times 17$ is a Carmichael number, and it is the only one of the form 3qr.

We present the cases p=5 and p=7 in tabular form. A composite value of q or r, terminating the process, is indicated by c.

h_3	$5 + h_3$	$5^2 \bmod h_3$	Δ	q	r	$qr \bmod 4$	Carmichael number			
2	7	1	1	29	73	1	$5 \times 29 \times 73$			
3	8	1	2	17	29	1	$5 \times 17 \times 29$			
4	9	1	3	13	17	1	$5 \times 13 \times 17$			
h_3	$7 + h_3$	$7^2 \bmod h_3$	Δ	q	r	$qr \bmod 6$	Carmichael number			
2	9	1	1	55c						
			3	19	67	1	$7 \times 19 \times 67$			
3	10	1	2	31	73	1	$7 \times 31 \times 73$			
			5	13	31	1	$7 \times 13 \times 31$			
4	11	1	3	23	41	1	$7 \times 23 \times 41$			
5	12	4	1	73	103	1	$7 \times 73 \times 103$			
			6	13	19	1	$7 \times 13 \times 19$			
6	13	1								

These cases have a success rate that is quite untypical of larger numbers! In fact, 11 is already very different: there are no Carmichael numbers 11qr. The reader is invited to work through this for him/herself. There are ten admissible combinations of h_3 and Δ . Six cases have q prime, of which two also have r prime. Both then fail at the hurdle $qr \equiv 1 \mod 10$.

The 3-factor Carmichael numbers for all p up to 73 are listed in the Appendix.

Remark 1. If pqr is a Carmichael number and q-1 is a multiple of p-1, then so is r-1. This follows from (2) and the identity pr-1=(p-1)r+(r-1). We call Carmichael numbers "simple" if they have this property. Of the 83 numbers listed in the Appendix, 67 are simple. Clearly, the same comment applies to the numbers q and r generated by the process just described.

Remark 2. For all $p \geq 7$, p-1 is not a possible value for h_3 . For then $\Delta \equiv -1 \mod p-1$, so Δ is p-2 or 2p-3. It has to divide (p-1)(2p-1), so in either case, Euclid's lemma implies that it divides 2p-1. For p-2, this only occurs for p equal to 3 or 5, and for 2p-3, only for p=2. So in fact $h_3 \leq p-2$ for all Carmichael numbers except $3 \times 11 \times 17$ and $5 \times 13 \times 17$. (In similar fashion, one can show that the only ones with $h_3 = p-2$ are $5 \times 17 \times 29$, $7 \times 13 \times 19$ and $7 \times 73 \times 103$.)

Identity (4) also enables us to give bounds for q, r and n in terms of p. We give a rather detailed estimation which is nearly optimal, with the option of a weaker one that is much quicker.

1.5 PROPOSITION. If n = pqr is a Carmichael number, with p < q < r, then

$$q < 2p(p-1),$$
 $r < \frac{1}{2}p^2(p+1),$ $n < \frac{1}{2}p^4(p+1)^2.$

Moreover, for a given p, all but (at most) one of the Carmichael numbers pqr satisfy

$$r < \frac{1}{5}p^2(p+4), \qquad n < \frac{1}{5}p^4(p+4)^2.$$

Proof. By (4) and the fact that $h_3 \leq p-1$, we have

$$q \le (p-1)(p+h_3) + 1 \le (p-1)(2p-1) + 1 < 2p(p-1).$$

Next, we give a quick proof of weaker inequalities for r and n. By 1.2,

$$r \le \frac{1}{2}(pq+1) < p^2(p-1) + \frac{1}{2},$$

so in fact $r < p^2(p-1)$ (not equal, since r is prime!). Hence $n = pqr < 2p^4(p-1)^2$.

To prove the version stated, we retain h_3 (which we denote just by h) in the calculations. Firstly, since $h \ge 2$,

$$q \le (p-1)(p+h) + 1 \le p(p+h-1). \tag{5}$$

So by (3),

$$r \leq \frac{pq}{h} + 1$$
$$\leq \frac{1}{h} [p^2(p+h-1) - p] + 1$$

$$< \frac{1}{h}p^2(p+h-1)$$
 (6)

$$= p^2 \left(1 + \frac{p-1}{h} \right). \tag{7}$$

This estimate is largest when h=2, then assuming the value $\frac{1}{2}p^2(p+1)$.

Also, by (5) and (6),

$$qr < \frac{1}{h}p^3(p+h-1)^2.$$

Now $\frac{1}{h}(p+1-h)^2$ decreases with h for $0 < h \le p-1$, so again the greatest value of the bound occurs when h=2, giving $\frac{1}{2}p^3(p+1)^2$.

Now exclude the single case where $h_3=2$ and $\Delta=1$ (for which the estimation just given could be obtained more directly by writing q and r explicitly in terms of p). If $h_3=3$, then $p^2\equiv 1 \mod 3$ (note that $p\geq 5$), so $\Delta\equiv 2 \mod 3$, hence $\Delta\geq 2$. Similarly, if $h_3=4$, then $\Delta\geq 3$. Consider these two cases together. By (4), since $\Delta\geq 2$,

$$q \le \frac{1}{2}(p-1)(p+4) + 1 = \frac{1}{2}(p^2 + 3p - 2)$$

and by (3)

$$r < \frac{1}{3}pq + 1 < \frac{1}{6}(p^3 + 3p^2 - 2p + 6) \le \frac{1}{6}p^2(p+3).$$

So $n = pqr < \frac{1}{12}p^4(p+3)^2$.

Now consider the case $h_3=2$, with $\Delta>1$. Then $\Delta\geq 3$, and one finds similarly that $q<\frac{1}{3}(p^2+p+1), \ r<\frac{1}{6}p^2(p+2)$ and $n<\frac{1}{18}p^4(p+2)^2$.

Finally, consider $h_3 \geq 5$. By (7),

$$r < p^2 \left(1 + \frac{p-1}{5} \right) = \frac{1}{5} p^2 (p+4)$$

and the bound for qr is greatest when h = 5, becoming $\frac{1}{5}p^3(p+4)^2$.

The example $n = 5 \times 29 \times 73$ has $r > \frac{1}{2}p^3$ and $n > \frac{1}{2}p^6$, showing that the stated estimations are close to being optimal.

Closer estimation of $f_3(p)$

1.6 LEMMA. Let
$$F(x,y) = \sum_{x < n \le x+y} \tau(n)$$
. Then

$$F(x,y) \le y \log(x+y) + 2y + 2(x+y)^{1/2}.$$

If $0 < y \le x$, then $F(x, y) \le y \log x + 3y + 3x^{1/2}$.

Proof. This estimation could be deduced from known results, but we give a simple direct proof. For $n \leq x + y$, let $\tau_1(n)$ be the number of divisors j of n with $j \leq (x + y)^{1/2}$. Clearly, $\tau_1(n) \geq \frac{1}{2}\tau(n)$. Let $F_1(x,y) = \sum_{x < n \leq x + y} \tau_1(n)$. This is the number of pairs (j,n) with $j \leq (x + y)^{1/2}$, $x < n \leq x + y$ and j|n. For fixed j, the number of such pairs is no more than y/j + 1. So

$$F_1(x,y) \le \sum_{j \le (x+y)^{1/2}} \left(\frac{y}{j} + 1\right) \le y\left[\frac{1}{2}\log(x+y) + 1\right] + (x+y)^{1/2}.$$

Both the stated estimatons follow.

1.7 THEOREM. For all prime p, we have

$$f_3(p) \le p \log \log p + p \log \tau (p-1) + 13p.$$

Proof. By the proof of 1.4, $f_3(p) \leq S_1 + S_2$, where (with u to be chosen)

$$S_1 = \sum_{h \le p/u} \tau[(p-1)(p+h)] \le \sum_{h \le p/u} \tau(p-1)\tau(p+h),$$

$$S_2 = \sum_{p/u < h < p} \left(\frac{p}{h} + 2\right) \le p \sum_{p/u < h \le p} \frac{1}{h} + 2p \le p \log u + 3p.$$

By Lemma 1.6,

$$\sum_{h \le p/u} \tau(p+h) \le \frac{p}{u} \log p + \frac{3p}{u} + 3p^{1/2},$$

Take $u = \tau(p-1)\log p$. Since $\tau(p-1) < 2p^{1/2}$, we have (for $p \ge 3$)

$$S_1 \le p + \frac{3p}{\log p} + 3\tau(p-1)p^{1/2} < 10p.$$

The statement follows. (Also, it is clear that $S_1 < 2p$ for large enough p; the term 13p can then be replaced by 5p.)

For any $c > \log 2$, it is known that $\log \tau(n) \le c \log n/(\log \log n)$ for sufficiently large n [e.g. Ten, p. 82–83]. Hence:

1.8 COROLLARY. For sufficiently large
$$p$$
, we have $f_3(p) \leq p \frac{\log p}{\log \log p}$.

What we have really estimated is the number of integers q, r defined by the process described. We have not taken into account the need for q and r to be prime, or the condition $qr \equiv 1 \mod (p-1)$. Heuristically, one might expect the first two conditions to reduce the actual number by a factor like $(\log p)^2$. The third condition obviously reduces it further, but it is not even heuristically clear by how much.

An easy variation of the proof of 1.7 gives a bound for the number of "simple" Carmichael numbers pqr with given p. Denote this number by $f_3(p, 1)$.

1.9. We have $f_3(p,1) \le p(\log \log p + 10)$.

Proof. Recall that pqr is "simple" if p-1 divides q-1. Since

$$\frac{q-1}{p-1} = \frac{p+h_3}{\Delta},$$

this occurs iff Δ divides $p + h_3$. So in the proof of 1.7, we now take S_1 to be simply $\sum_{h < p/u} \tau(p+h)$. Putting $u = \log p$, we obtain the stated bound.

2. Results in terms of g, a, b, c

A rich algebra describing the structure of 3-factor Carmichael numbers was initiated in [DLP] and developed further in [BN] and [HBr]. The following is an attempt at a unified account of these results, with some slight simplifications.

For a Carmichael number n=pqr as above, let g(n)=g=(p-1,q-1,r-1), the gcd of p-1, q-1 and r-1. Obviously, g is even and $g \leq p-1$. Write

$$p-1 = ag, \quad q-1 = bg, \quad r-1 = cg,$$
 (8)

so that a < b < c (hence $b \ge 2$, $c \ge 3$ and $abc \ge 6$). Clearly, $abcg^3 < n$, so $g < n^{1/3}$.

2.1. We have g = (p-1, q-1) (etc.), hence a, b, c are pairwise coprime.

Proof. Let $(p-1, q-1) = g_0$. Now qr-1 is a multiple of (p-1), so of g_0 . But g_0 divides q-1, and qr-1 = (q-1)r + (r-1). So g_0 divides r-1, hence $g_0 = g$.

Hence a = 1 iff q - 1 is a multiple of p - 1 (that is, iff n is "simple").

Example. For $n = 7 \times 13 \times 19$, we have g = 6, a = 1, b = 2, c = 3.

The Appendix gives the values of g, a, b, c for the numbers listed.

Remark. A number of the form d = s(g+1) + 1 (with $s \ge 1$) is not a possible value for a, b, c, since gd + 1 = (gs + 1)(g + 1) is composite. Similarly for s(g-1) - 1.

There are a multitude of identities and inequalities linking these quantities. In the following results, the standing assumption is that n = pqr is a Carmichael number, with notation as above. Some of the statements can be expressed more simply with judicious use of the original p, q, r. We start by restating (1), (2), (3) in terms of the new quantities.

2.2. We have

$$h_1 a = bcg + b + c,$$
 $h_2 b = acg + a + c,$ $h_3 c = abg + a + b.$ (9)

Proof. (1) says $h_1 ag = (bg + 1)(cg + 1) - 1 = bcg^2 + bg + cg$. Similarly for (2), (3). \square

Note that h_3c can also be written as aq + b and as bp + a.

2.3 COROLLARY.
$$(h_3, a) = (h_3, b) = 1$$
 (etc.)

Proof. If d divides both h_3 and a, then it divides $h_3c - aq = b$, hence d = 1. Similarly for (h_3, b) .

However, h_3 and c need not be coprime: for $n = 5 \times 13 \times 17$, we have $c = h_3 = 4$.

The number k; Carmichael numbers with given (a, b, c)

2.4. *Let*

$$E = (bc + ca + ab)g + a + b + c.$$

Then there is an integer k such that E = kabc.

Proof. By 2.2, we have

$$E = a(b+c)g + a + (bcg + b + c) = a(b+c)g + a + h_1a,$$

so a divides E. Similarly for b and c. Since a, b, c are pairwise coprime, abc divides E. \square

2.5. If a, b, c are given, then there is only one possible choice for g mod abc.

Proof. Write bc+ca+ab=S. It is elementary that (S,a)=1 (etc.), so that (S,abc)=1. By 2.4, g has to satisfy $Sg\equiv -a-b-c \mod abc$. This determines g uniquely mod abc. \square

Conversely, suppose that a, b, c (pairwise coprime) are given, and that g satisfies $Sg \equiv -a - b - c \mod abc$, so that E is a multiple of abc. Let p, q, r be defined by (8) and let n = pqr. Then the algebra in 2.4 and 2.2, in reverse, shows that (9) holds for certain integers h_1 , h_2 , h_3 , and hence that (1), (2), (3) hold. So if p, q, r are prime, then n is a Carmichael number. This gives a procedure for searching for Carmichael numbers with specified a, b, c.

Example. (a, b, c) = (1, 2, 3). The condition for g is $11g \equiv -6 \mod 6$, hence $g = 0 \mod 6$. The first three cases that give three primes are:

$$g = 6 \hbox{:} \ \ 7 \times 13 \times 19; \qquad g = 36 \hbox{:} \ \ 37 \times 73 \times 103; \qquad g = 210 \hbox{:} \ \ 211 \times 421 \times 631.$$

In general, g = 6m, giving p = 6m + 1, q = 12m + 1, r = 18m + 1.

Example. (a, b, c) = (2, 3, 5). Then $31g \equiv -10 \equiv 20 \mod 30$, so $g \equiv 20 \mod 30$. The first three cases are:

$$g = 20$$
: $41 \times 61 \times 101$; $g = 50$: $101 \times 151 \times 251$; $g = 140$: $281 \times 421 \times 701$.

In general, g = 30m + 20, giving p = 60m + 41, q = 90m + 61, r = 150m + 101.

We now derive some inequalities involving k, a and g.

2.6 We have $g < ka \le 3g - 1$. In particular, $a \le 3g - 1$.

Proof. Recall that a < b < c and $g \ge 2$. By 2.4,

$$kab = g\left(a + b + \frac{ab}{c}\right) + \left(1 + \frac{a}{c} + \frac{b}{c}\right)$$

< $q(2a + b) + 3 < q(3b - 2) + 3 < 3bq$,

so ka < 3g, hence $ka \le 3g - 1$. Also, it is obvious that ka > g.

2.7 COROLLARY. We have $a < \sqrt{3}n^{1/6}$.

Proof. We have
$$a^2 < 3ag < 3p \le 3n^{1/3}$$
.

2.8 COROLLARY. We have $p < 3g^2$.

Proof. Since
$$g \ge 2$$
, we have $p = ag + 1 \le (3g - 1)g + 1 < 3g^2$.

Using 1.5, one could now write down bounds for q, r and n in terms of g. However, much stronger bounds actually apply, as we will see below.

Actually, $k \leq 2g$: since $a \geq 1$, $b \geq 2$, $c \geq 3$, we have

$$k = g\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right) + \frac{1}{bc} + \frac{1}{ca} + \frac{1}{ab} \le \frac{11}{6}g + 1 < 2g + 1.$$

We mention that of the 83 Carmichael numbers listed in the Appendix, just three have a > g. In each case, a = g + 1. A more extreme case of large a is $191 \times 421 \times 431$, for which g = 10 and a = 19. I do not know whether there are numbers with $a \ge 2g$.

The number j

2.9. Let j = ka - g. Then

$$jbc = a(b+c)q + a + b + c = p(b+c) + a,$$
 (10)

$$j = \frac{p + h_3}{b} = \frac{p + h_2}{c}. (11)$$

Proof. By 2.4,

$$jbc = (ka - g)bc = E - gbc = a(b + c)g + a + b + c = p(b + c) + a.$$

Also, by this expression and (9),

$$jbc = c(ag + 1) + (abg + a + b) = c(p + h_3),$$

so
$$jb = p + h_3$$
. Similarly, $jc = p + h_2$.

Of course, there are really three numbers $j_1 = ka - g$, $j_2 = kb - g$, $j_3 = kc - g$, with corresponding identities, but we will not use the others, so we write $j_1 = j$.

2.10. We have
$$j \leq \frac{2ag+1}{h}$$
, also $j \leq 2g-1$. If $a = 1$, then $j \leq g$.

Proof. By 1.2, $h_3 \leq p - 1 = ag$, hence

$$jb = p + h_3 \le 2ag + 1 < 2g(a+1) \le 2bg$$

hence j < 2g (this was also shown in 2.6). If a = 1, then $2j \le jb \le 2g + 1$, so $j \le g$. (More generally, $j \le (2ag + 1)/(a + 1)$.

Of the 83 Carmichael numbers with $p \le 73$, just one has j > g, namely $41 \times 61 \times 101$, for which g = 20, j = 22.

2.11. We have $(j, h_3) = 1$.

Proof. If d divides both j and h_3 , then it divides $jb - h_3 = p$. But clearly $(h_3, p) = 1$, hence d = 1.

2.12. We have $h_2h_3 = p^2 + ja$.

Proof. By (11) and (10),

$$h_2h_3 = (jc - p)(jb - p)$$
$$= p^2 + j^2bc - jp(b + c)$$
$$= p^2 + ja. \square$$

Recall that $h_2h_3 - p^2$ is the Δ of section 1, so 2.12 says that $\Delta = ja$. Together with the identity $jb = p + h_3$ (11), this amounts to a restatement of (4):

$$(p-1)(p+h_3) = (ag)(jb) = (ja)(bg) = \Delta(q-1).$$

Inequalities in terms of a and g

In 1.5, we gave bounds for q, r and n in terms of p (= ag + 1). We now show how stronger bounds for all the other quantities can be given in terms of a and g, with derived versions in terms of g alone. Better constants, and simpler algebra, are achieved by making exceptions of one or two of the early Carmichael numbers. We will use our listings of the numbers with p equal to 3 or 5 in section 1.

2.13 PROPOSITION. Write $n_1 = 3 \times 11 \times 17$, $n_2 = 5 \times 13 \times 17$, $n_3 = 5 \times 29 \times 73$. Then the following inequalities hold for all 3-factor Carmichael numbers with the exceptions stated:

all except
$$n_1$$
: $b \le 2ag$, $q \le 2ag^2 + 1$, $n < 3a^4g^6$;
all except n_1 , n_3 : $c < a^2g^2$, $r < a^2g^3$.

Proof. Note first that since n_1 is the only Carmichael number with p=3, we have $ag \geq 4$ for all n except n_1 . Our starting point is the identity $jb=p+h_3$ (11). As noted on p. 5, for all n except n_1 and n_2 , we have $h_3 \leq p-2$, hence $jb \leq 2ag$, so $b \leq 2ag$ and $q \leq 2ag^2 + 1$. This also holds for n_2 (for which ag = 4, b = 3).

Our listings show that $c < a^2g^2$ for the numbers with $p \le 5$ except n_1 and n_3 . So assume now that $ag = p - 1 \ge 6$. By (9),

$$c = \frac{pb+a}{h_3} \le \frac{p(p+h_3)+a}{h_3} = p + \frac{p^2+a}{h_3}.$$

This is largest when $h_3 = 2$, giving (since a < p and $ag \ge 6$)

$$2c < p^2 + 2p + a < p^2 + 3p = (ag + 1)(ag + 4) < 2a^2g^2$$

hence $c < a^2g^2$, so $r \le (a^2g^2 - 1)g + 1 < a^2g^3$ and

$$n = pqr < (ag+1)(2a^2g^2+1)a^2g^3 < 3a^4g^6.$$

Calculation shows that this inequality also holds for n_3 .

If j = 1 and $h_3 = 2$, then it is clear from the expressions above that b > ag and $c > \frac{1}{2}a^2g^2$, showing that the estimations for b and c are not far from being optimal. However, by writing the bound for bc in terms of h_3 , one can show that in fact $n < a^4g^6$ for large enough ag.

We now establish bounds in terms of g only. We have already seen (2.8) that $p < 3g^2$. By 2.13 and the inequality a < 3g, we have at once

$$b<6g^2, \quad q<6g^3, \quad c<9g^4, \quad r<9g^5, \quad n<162g^{10}$$

(without any exceptions). The reader may be inclined to settle for these estimates. However, once more, the constants can be greatly improved with a bit more attention to what is happening. The basic point is that $a \leq g+1$ (instead of 3g-1) unless $j \geq 2$, which essentially halves the estimates for b and c.

2.14. We have in all cases

$$b \le 2g(g+1), \quad g < 2g(g+1)^2, \quad c < g^2(g+1)^2, \quad r < g^3(g+1)^2, \quad n < 2g^4(g+1)^6.$$

Proof. Suppose first that $a \leq g+1$. This occurs, in particular, if j=1, since ka=g+j. Then $p < (g+1)^2$, and the stated bounds follow from 2.13. One can check that they also hold for n_1 and n_3 .

We will show that the same bounds, or smaller ones, apply for all other values of j. If j=2, then a divides g+2. Also, $a \neq g+2$, since $g(g+2)+1=(g+1)^2$, which is not prime. So in fact a < g, and the stated bounds apply.

Now suppose that $3 \le j \le g-1$ (so $g \ge 4$). Then $a \le 2g-1$, so $p \le 2g^2-g+1 \le 2g^2-3$. We now write c in terms of both h_3 and j:

$$c = \frac{pb+a}{h_3} = \frac{p(p+h_3)+ja}{jh_3} = \frac{p}{j} + \frac{p^2+ja}{jh_3}.$$

This bound is greatest when $h_3 = 2$, giving

$$c \le \frac{p}{j} + \frac{p^2 + ja}{2j} = \frac{a}{2} + \frac{p(p+2)}{2j}.$$
 (12)

So for $3 \le j \le g - 1$, we take j = 3 in this bound, obtaining

$$6c \le p(p+2) + 3a \le (2g^2 - 3)(2g^2 - 1) + 6g - 3 = 4g^4 - 8g^2 + 6g < 4g^4,$$

hence $c < \frac{2}{3}g^4$, $r < \frac{2}{3}g^5$, $n < \frac{16}{9}g^{10}$.

Finally, suppose that $j \ge g$ (also $g \ge 4$). Then $a \le 3g-1$ and $p \le 3g^2-g+1 \le 3g^2-3$. Further, $b \le 2a$, so $q < 6g^2$. By (12),

$$2gc \le ag + p(p+2) < 3g^2 + (3g^2 - 3)(3g^2 - 1) < 9g^4,$$

so $c < \frac{9}{2}g^3$, hence $r < \frac{9}{2}g^4$ and $n < 81g^8$. Note that these bounds are in terms of lower powers of g. Provided that $g \ge 8$, they are smaller than the ones stated. Now we resort to the listing of Carmichael numbers with small g in the next sub-section: we see that in fact $a \le g+1$ (so the stated bounds hold) for all the 13 numbers with $g \le 6$.

Carmichael numbers with given g

It is clear from 2.14 (or 2.8 and 1.5) that there are only finitely many 3-factor Carmichael numbers with a given value of g. Denote this number by $K_3(g)$.

Let

$$L(x) = \frac{\log x}{\log \log x},$$

and $M(x) = e^{L(x)} = x^{1/\log \log x}$. Note that $M(x) = o(x^{\varepsilon})$ for all $\varepsilon > 0$ and $(\log x)^k = o(M(x))$ for all k > 0.

As already mentioned, for any $\alpha > \log 2$, we have $\log \tau(m) \leq \alpha L(m)$, so that $\tau(m) \leq M(m)^{\alpha}$, for all large enough m.

2.15 THEOREM. For sufficiently large g, we have

$$K_3(g) \le g M(g)^4,$$

hence $K_3(g) \ll g^{1+\varepsilon}$ for all $\varepsilon > 0$.

Proof. With g fixed, we choose a < 3g, then j < 2g satisfying $j \equiv -g \mod a$. The number of choices of j is no more than 2g/a + 1, so the number of pairs (a, j) is no more than

$$\sum_{a \le 3g} \left(\frac{2g}{a} + 1 \right) \le 2g(\log 3g + 1) + 3g$$
$$\le 2g(\log g + 4).$$

(Alternatively, choose j first, then a, which has to be a divisor of g+j. The number of pairs (j,a) is bounded by $S_{\tau}(3g) - S_{\tau}(g)$, which leads to a similar estimate. Also, by allowing for the requirement that ag + 1 must be prime, one could replace the $\log g$ factor by $Cg/\phi(g)$, for some ineffective constant C.)

Given a choice of h_3 , b (hence q) is now defined by (11) and r by (3). By 2.12, the number of possible choices for h_3 is bounded by $\tau(p^2 + ja)$ (actually, no more than half this number, because $h_3 \leq p$). Now (for $g \geq 4$) $p^2 + ja \leq 9g^4 + 6g^2 \leq 10g^4$. If g is large enough, then for all $m \leq 10g^4$,

$$\log \tau(m) \le \frac{\frac{7}{10}(4\log g + \log 10)}{\log \log g} < 3L(g),$$

so $\tau(m) \leq M(g)^3$. Also, $2(\log g + 4) \leq M(g)$. Hence $K_3(g) \leq gM(g)^4$.

For an "effective" version of this result, start from the fact that $\log \tau(m) \leq L(m) + C_1$ for a constant C_1 which can certainly be estimated. This leads to $\tau(m) \leq C_2 M(g)^5$ for all $m \leq 10g^4$, where $C_2 = e^{C_1}$, hence to $K_3(g) \leq C_3 g M(g)^5 (\log g + 4)$.

This estimate, or indeed stronger ones, may exist in the literature, but at the time of writing I am not aware of references for it.

Again, the proof amounts to a procedure for finding the 3-factor Carmichael numbers for a particular g. The process is clearly more complex than the one for fixed p in section 1. However, quite a lot of choices are eliminated by the conditions that have to be satisfied (some of which were not exploited in the proof). We restate them here:

- (C1) ag + 1 must be prime.
- (C2) $j \le 2g 1$ (and $j \le g$ if a = 1), also $j \equiv -g \mod a$.
- (C3) $2 \le h_3 \le p-1$, $h_3 \equiv -p \mod j$ and h_3 divides $p^2 + ja$.
- (C4) b > a and (a, b) = 1.

Example. We show that there are exactly two 3-factor Carmichael numbers with g = 2. We tabulate the process, listing possible choices of a, j and then h_3 . The symbol * means either that no choice of the number concerned is possible, or that one of the conditions is violated.

a p j
$$p^2 + ja$$
 h_3 b q r Carmichael number

1 3 1 10 2 5 11 17 $3 \times 11 \times 17$
2 11 *
2 5 2 29 *
3 7 1 52 2 9*
4 11 23 41 $7 \times 23 \times 41$

5 11 3 136 4 5*

The starred cases for b fail condition (C4). The first one, if continued, would lead to $7 \times 19 \times 67$, which is a Carmichael number, but with g = 6.

The 3-factor Carmichael numbers with $g=4,\,6$ and 8 are:

$$g = 4$$
: $5 \times 13 \times 17$, $5 \times 17 \times 29$, $5 \times 29 \times 73$.
 $g = 6$: $7 \times 13 \times 19$, $7 \times 13 \times 31$, $7 \times 19 \times 67$, $7 \times 31 \times 73$, $7 \times 73 \times 103$, $19 \times 43 \times 409$, $43 \times 271 \times 5827$, $43 \times 433 \times 643$.
 $g = 8$: $17 \times 41 \times 233$, $41 \times 73 \times 137$.

Note that this procedure requires the factorisation of p^2+ja , whereas the corresponding

quantity in the procedure in section 1 was $(p-1)(p+h_3)$, already given in factorised form. Of course, $p^2 + ja$ can be large compared with g (recall that our bound for it is $10g^4$). By way of illustration, the case g = 12, a = 26, j = 14 gives $p^2 + ja = 168,029$ (which happens to be prime). The investigation is greatly facilitated by an instant factorisation service, such as "Factoris", available at http://wims.unice.fr/wims.cgi.

Once j > g, the possible range for h_3 is restricted from below by $h_3 = jb - p \ge j(a+1) - p$. In the specific case just mentioned, this gives $h_3 \ge 361$ (while p = 409).

3. The number of 3-factor Carmichael numbers not greater than x

Let $C_3(x)$ be the number of 3-factor Carmichael numbers not greater than x. Extensive computations of $C_3(x)$ have been performed in [Pi]. Some of the values are as follows. In each case, we record the α such that $C_3(x) = x^{\alpha}$.

$$x$$
 10^9 10^{12} 10^{15} 10^{18} $C_3(x)$ 172 $1,000$ $6,083$ $35,586$ α 0.248 0.250 0.252 0.253

It is fairly clear what these figures suggest. What estimations have actually been proved?

No useful *lower* bound is known, since it has not been proved there are infinitely many 3-factor Carmichael numbers, though this seems compellingly likely. However, a lot of progress has been made in establishing *upper* bounds. We start with some quick estimations that do not use the results of section 2. The reader is at liberty to ignore these and proceed directly to the stronger estimate given in Theorem 3.7.

We denote by P(y) the set of primes $p \leq y$ and by $P^*(y)$ the set of primes p > y. Our Theorem 1.4 gives at once:

3.1. We have
$$C_3(x) \ll x^{2/3}$$
.

Proof. By Chebyshev's estimate, $\theta(x) =: \sum_{p \in P(x)} \log p \le cx$, where $c \le \log 4$. By Theorem 1.4, for a suitable constant C,

$$C_3(x) \le \sum_{p \in P(x^{1/3})} f_3(p) \le C \sum_{p \in P(x^{1/3})} p \log p \le C x^{1/3} \theta(x^{1/3}) \le C c x^{2/3}.$$

Next we give a variation of an argument from [Pom] leading to the estimate $x^{2/3}/(\log x)^{4/3}$. The improvement is only slight, but we include it because the method introduces some interesting ideas and extends easily to numbers with more prime factors. Let $P^+(n)$ denote the largest prime factor of n.

3.2 LEMMA. Let C(x,p) be the number of Carmichael numbers (with any number of prime factors) $n \le x$ with $P^+(n) = p$. Then $C(x,p) \le x/[p(p-1)]$.

Proof. If n is a Carmichael number with p as a prime factor, then $n \equiv 0 \mod p$ and $n \equiv 1 \mod (p-1)$, hence $n \equiv p \mod p(p-1)$. Each interval of length p(p-1) contains one number n satisfying this condition. However, the first such n is p, which is not a Carmichael number.

3.3 LEMMA. There is a constant $C \leq 5$ such that for all y > 4,

$$\sum_{p \in P^*(y)} \frac{1}{p(p-1)} \le \frac{C}{y \log y}.$$

Proof. This follows by Abel summation from the prime number theorem in the weak form $\pi(x) \leq 2x/\log x$ (we omit the details).

3.4 LEMMA. Let $D_3(y)$ be the number of 3-factor Carmichael numbers n with $P^+(n) \le y$. Then $D_3(y) \le \frac{1}{4}\pi(y)^2$.

Proof. Let $g_3(r)$ be the number of 3-factor Carmichael numbers with $P^+(n) = r$. For each prime p < r, there is a unique q < r (which may or may not be prime, or distinct from p) such that $pq \equiv 1 \mod r - 1$. Hence $g_3(r) \leq \frac{1}{2}(\pi(r) - 1)$. Now let $r_1 < r_2 < \ldots < r_k$ be the primes not greater than y, so that $\pi(y) = k$. Then

$$2D_3(y) \le \sum_{j=2}^k [\pi(r_j) - 1] = \sum_{j=2}^k (j-1) = \frac{1}{2}(k-1)k.$$

3.5. We have
$$C_3(x) \ll \frac{x^{2/3}}{(\log x)^{4/3}}$$
.

Proof. Let $y = x^{1/3} (\log x)^{\alpha}$, where α is to be chosen. By 3.4,

$$D_3(y) \le \frac{1}{4}\pi(y)^2 \le \frac{y^2}{(\log y)^2} = \frac{9x^{2/3}}{(\log x)^{2-2\alpha}}.$$

Meanwhile, by 3.2 and 3.3, the number of (all) Carmichael numbers $n \le x$ with $P^+(n) \ge y$ is no more than

$$\frac{Cx}{y\log y} < \frac{3Cx^{2/3}}{(\log x)^{1+\alpha}}.$$

Take $\alpha = \frac{1}{3}$ to obtain the stated result.

Note on numbers with more prime factors. This method can be extended to establish the same estimate $x^{2/3}/(\log x)^{4/3}$ for $C_4(x)$. Also, 3.2 and 3.3 (without 3.4) show quite easily

that $C_k(x) \ll x^{1-1/k}/\log x$ for any $k \geq 3$. However, it is shown in [GP] that $C_k(x) \ll x^{2/3}(\log x)^{r(k)}$, where $r(k) = \frac{1}{3}(2^{k-2} - 1)$.

We now show how a much stronger bound for $C_3(x)$ can be obtained using the algebra of section 2. The basic method was introduced in [DLP], where the bound obtained was $x^{1/2}(\log x)^{11/4}$. A fairly small modification of their method actually gives a bound of the form $x^{2/5+\varepsilon}$ (cf. [Gra]). By a further development of the method, [BN] reduced the estimate to $x^{5/14+\varepsilon}$. We give the version of their proof presented in [HBr], with some slight modifications and corrections. It uses the following (seemingly rather technical) further algebraic identity. The point is that the right-hand side is in terms of a, b and k, while the left-hand side is the product of two factors that are linear in g and c respectively.

3.6 LEMMA. We have

$$[abk - (a+b)g - 1](bc + ca + ab) = ka^2b^2 + a^2 + b^2 + ab.$$

Proof. Write bc + ca + ab = S. By 2.4, gS + a + b + c = kabc. Multiply by a + b and rearrange as far as possible in terms of S:

$$g(a+b)S + (a+b)(a+b+c) = kabc(a+b),$$

$$g(a+b)S + S + a^2 + b^2 + ab = kab(S-ab),$$

$$[kab - g(a+b) - 1]S = ka^2b^2 + a^2 + b^2 + ab.$$

Recall that for large enough x, we have $\tau(m) \leq M(x)$ (or even $M(x)^{7/10}$) for all $m \leq x$; the definition of M(x) was given before Theorem 2.15.

3.7 THEOREM. We have $C_3(x) \ll x^{5/14} M(x)$.

Proof. Call a quadruple (a, b, c, g) "suitable" if it satisfies all the required conditions. We will estimate the number of suitable quadruples with $abcg^3 \leq x$. Consider the "dyadic cell" formed by restricting a, b, c, g to chosen intervals (A, 2A], (B, 2B], (C, 2C] and (G, 2G] respectively, where A, B, C, G are numbers of the form 2^r . Let N(A, B, C, G, x) be the number of suitable quadruples in this cell. Of course, we only need to consider cells that contain at least one suitable (a, b, c, g), so they will satisfy $ABCG^3 \leq x$ and $A \leq B \leq C$, also $A \leq 6G$ (since a < 3g).

We will show that, for a positive value μ to be found, we always have $N(A, B, C, G, x) \ll (ABCG^3)^{\mu}$. One way to complete the proof (cf. [HBr]) is then to use the fact the total number of cells is $\ll (\log x)^4$, since each of the variables is bounded by x. However, this extra

log factor is superfluous. For if A_0 is the largest value of A occurring, then the others are of the form $A_0/2^j$ $(j \ge 1)$ (similarly for B, C, G), and summation over all the cells gives

$$C_3(x) \ll S_1^3 S_2 (A_0 B_0 C_0 G_0^3)^{\mu} \le S_1^3 S_2 x^{\mu},$$

where $S_1 = \sum_{j=0}^{\infty} 2^{-\mu j}$, $S_2 = \sum_{j=0}^{\infty} 2^{-3\mu j}$.

To do this, we establish three different bounds for N(A, B, C, G, x):

(1)
$$ABC + G$$
, (2) $\left(\frac{AG^2}{B} + AG\right) M(x)$, (3) $BGM(x)$

(each possibly multiplied by a constant).

(1) Choose a, b, c freely within the cell: there are at most ABC choices. (Note: if, for example, A = B, then half of these choices would be excluded by the condition a < b.) Then, by 2.5, g is fully determined mod abc, so the number of choices of g is no more than

$$\frac{G}{abc} + 1 \le \frac{G}{ABC} + 1.$$

Multiply by ABC to obtain estimate (1).

(2) (Compare the proof of 2.15.) We define the quadruple by choosing g, a, j and h_3 in that order: then b is defined by (11) and c by (9). Choose g and a freely (AG choices). Then by 2.10, j must satisfy

 $j < \frac{3ag}{h} \le \frac{6aG}{B}$

(note that b has not yet been chosen, but B has!). Also, $j \equiv -g \mod a$, so the number of choices for j is no more than 6G/B+1. Hence the number of choices for (g, a, j) is estimated (ignoring constants) by $AG^2/B + AG$. In each case, the number of choices for h_3 is bounded by $\tau(p^2 + ja)$, which (for large enough x) is less than M(x), since $p^2 + ja < x$.

(Note. Alternatively, choose j, then a: the number of choices of the pair is estimated by $\sum_{j \leq AG/B} \tau(g+j) \ll AG \log G/B$. This gives an extra $\log G$ factor, but no term AG.)

(3) This is where we use Lemma 3.6. We choose a, b and k, consistent with the other conditions, and let $V = k^2 a^2 b^2 + a^2 + b^2 + ab$. By Lemma 3.6, a chosen factorisation of V will now determine g and c. Since ka < 3g, it is clear that $V \ll g^2 b^2 < x$, so again $\tau(V) \ll M(x)$.

Choose a and b freely (AB choices). Then k has to satisfy $ka < 3g \le 6G$, so the number of choices for k is at most $6G/a \le 6G/A$. Hence the number of choices of (a, b, k) is at most 6BG. Hence (3).

We now combine these estimates to obtain the required statement. If AG is the larger term in (2) (in other words, if G < B), we simply note that $AG \le (ABCG^3)^{1/3}$. Similarly

if G is the larger term in (1). So we now work with ABC from (1) and $AB^{-1}G^2$ from (2). Consider

$$(ABC)^{\alpha} (AB^{-1}G^{2})^{\beta} (BG)^{1-\alpha-\beta} = A^{\alpha+\beta}B^{1-2\beta}C^{\alpha}G^{1-\alpha+\beta},$$

where $\alpha, \beta > 0$ and $\alpha + \beta \leq 1$. We want the smallest μ such that this expression is not greater than $(ABCG^3)^{\mu}$. The following at least indicates how to derive it (instead of just being presented with the answer). Equating the combined powers of A, B and C and the power of G to 3μ gives $1 + 2\alpha - \beta = 1 - \alpha + \beta = 3\mu$, hence $3\alpha = 2\beta$. Also, $6\mu = 2 + \alpha$, so we want α to be as small as possible. Since A is smaller than all the other variables, we must have $\alpha + \beta \geq \mu$. Substitution leads to $7\alpha \geq 1$, so we take $\alpha = \frac{1}{7}$ and $\beta = \frac{3}{14}$. The expression becomes

$$A^{5/14}B^{8/14}C^{1/7}G^{15/14} \le (ABCG^3)^{5/14}$$

(of course, we have wasted a factor of $(BC^{-1})^{3/14}$.)

Note 1. An alternative ending, closer to the original proof in [BN], is to consider cases, as follows. Write $ABCG^3 = X$. With α , δ to be chosen:

Case 1: $G > X^{\alpha}$. Then $ABC \leq X^{1-3\alpha}$.

Case 2: $G \leq X^{\alpha}$ and $B > AX^{\delta}$. Then $AB^{-1}G^2 \leq X^{2\alpha-\delta}$.

Case 3: $G \leq X^{\alpha}$ and $B \leq AX^{\delta}$. Then $B^3G^3 \leq X^{\delta}AB^2G^3 \leq X^{1+\delta}$, so $BG \leq X^{(1+\delta)/3}$.

Choose α and δ to make all three equal, that is

$$1 - 3\alpha = 2\alpha - \delta = \frac{1}{3} + \frac{1}{3}\delta.$$

Solving this, we find $\alpha = \frac{3}{14}$ and $\delta = \frac{1}{14}$, making all three estimates equal to $X^{5/14}$.

Note 2. The estimate $x^{2/5}M(x)$ can be derived from bounds (1) and (2), in the weaker form $G^2M(x)$, by observing that $(ABC)^{2/5}(G^2)^{3/5} \leq x^{2/5}$. This, in essence, was the method of [DLP], but the result obtained there was weaker because it only used the fact that a divides $(g+j)(1+h_3)$ instead of g+j.

Note 3. In estimation (2), [HBr] has an algebraic error: its formula (9), in our notation, has $p^2 - ja$ instead of $p^2 + ja$, leading to an unnecessary discussion of the possibility of this quantity being 0.

The method lends itself well to giving bounds for the number of Carmichael numbers of special kinds. We already saw in the proof that the bound $x^{1/3}M(x)$ applies to the numbers satisfying $b \geq g$. Another special type for which this estimation applies is the set of numbers satisfying $b^2 \leq ac$: this only needs the bound BG, since $B^2 \leq AC$ gives $(BG)^3 \leq ABCG^3$. A more interesting example is:

3.8. Let $C_3(x, 1)$ be the number of 3-factor Carmichael numbers not greater than x with a = 1. Then $C_3(x, 1) \ll x^{1/3}M(x)$.

Proof. The variable A is now replaced by 1. Again the result is immediate if G is the larger term in (1) or (2). Otherwise, the product of the three bounds, without M(x), is

$$(BC)(B^{-1}G^2)(BG) = BCG^3 \le x. \qquad \Box$$

A further application is the following estimation of the partial sums of $f_3(p)$, to be compared with the bounds for individual values given in Theorems 1.4 and 1.7.

3.9. For any
$$\varepsilon > 0$$
, we have $\sum_{p \le P} f_3(p) \ll P^{3/2+\varepsilon}$.

Proof. The numbers considered now satisfy $AG \leq P$. Either AG is the larger term in (2), or we have

$$(AB^{-1}G^2)^{1/2}(BG)^{1/2} = A^{1/2}G^{3/2} \le P^{3/2}.$$

By 1.5, all the numbers considered are less than P^6 , so the M(x) factors can be replaced by a power of M(P). This time, we do need to multiply by the number of cells, which is $\ll (\log P)^4$.

The bound for $C_3(x)$ has been strengthened further in [HBr] to $x^{7/20+\varepsilon}$: this is the best estimate currently known. It is obtained by establishing the following further bound for $C_3(A, B, C, G, x)$:

$$AG + A^{1/2}BCx^{\varepsilon} + A^2B^{1/2}C^{1/2}x^{\varepsilon}.$$

Apart from the x^{ε} terms, this is essentially a strengthening of bound (1). The proof uses analytic methods, and is considerably longer and more delicate than any of the proofs given above. We will not reproduce it here: interested readers are referred to [HBr]. Unlike any of the estimations we have given, it takes account of the fact that a, b, c have to be pairwise coprime.

It is conjectured in [GP], with heuristic reasoning, that the true bound is $Kx^{1/3}/(\log x)^3$ for a certain specified K. Heath-Brown's exponent $\frac{7}{20}$ is tantalisingly close to $\frac{1}{3}$.

REFERENCES

- [BN] R. Balasubramanian and S.V. Nagaraj, Density of Carmichael numbers with three prime factors, *Math. Comp.* **66** (1997), 1705–1708.
- [Be] N.G.W.H. Beeger, On composite numbers n for which $a^{n-1} \equiv 1 \mod n$ for every a prime to n, Scripta Math. 16 (1950), 133–135.
- [Car] R.D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, American Math. Monthly 19 (1912), 22–27.
- [DLP] I. Damgård, P. Landrock and C. Pomerance, Average case error estimates for the strong probable prime test, *Math. Comp.* **61** (1993), 177–194.
 - [Du] H.J.A. Duparc, On Carmichael numbers, Simon Stevin 29 (1952), 21–24.
- [Gra] S.W. Graham, Carmichael numbers with three prime factors, unpublished preprint.
- [GP] Andrew Granville and Carl Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (2001), 883–908.
- [HBr] D.R. Heath-Brown, Carmichael numbers with three prime factors, Hardy-Ramanujan J. 30 (2007), 6–12.
- [Jam] G.J.O. Jameson, Finding Carmichael numbers, at www.maths.lancs.ac.uk/~jameson
 - [JJ] G.A. Jones and J.M. Jones, *Elementary Number Theory*, Springer (1998).
- [Rib] P. Ribenboim, The New Book of Prime Number Records, Springer (1995).
 - [Pi] R.G.E. Pinch, The Carmichael numbers up to 10¹⁸, at www.chalcedon.demon.co.uk/rgep/carpsp.html.
- [Pom] Carl Pomerance, Two methods in elementary number theory, Number Theory and Applications (Banff, 1988; R.A. Mollin, ed.), NATO Adv. Sci. Ser. C 265 (1989), 135–161.
- [Ten] G. Tenenbaum, Introduction to Analytic and Probablistic Number Theory, Cambridge Univ. Press (1995).

March 2010

Appendix: Carmichael numbers with three prime factors for $p \le 73$

pqr	g	a,b,c	h_3	j	pqr	g	a,b,c	h_3	j
$3 \times 11 \times 17$	2	1, 5, 8	2	1	$43\times127\times211$	42	1, 3, 5	26	23
					$43 \times 127 \times 1093$	42	1, 3, 26	5	16
$5 \times 13 \times 17$	4	1, 3, 4	4	3	$43 \times 127 \times 2731$	42	1, 3, 35	2	15
$5 \times 17 \times 29$	4	1, 4, 7	3	2	$43 \times 211 \times 337$	42	1, 5, 8	27	14
$5 \times 29 \times 73$	4	1, 7, 18	2	1	$43 \times 211 \times 757$	42	1, 5, 18	12	11
					$43 \times 271 \times 5827$	6	7, 45, 971	2	1
$7 \times 13 \times 19$	6	1, 2, 3	5	6	$43 \times 433 \times 643$	6	7, 72, 107	29	1
$7 \times 13 \times 31$	6	1, 2, 5	3	5	$43 \times 547 \times 673$	42	1, 13, 16	35	6
$7 \times 19 \times 67$	6	1, 3, 11	2	3	$43 \times 631 \times 1597$	42	1, 15, 38	17	4
$7 \times 23 \times 41$	2	3, 11, 20	4	1	$43 \times 631 \times 13567$	42	1, 15, 323	2	3
$7 \times 31 \times 73$	6	1, 5, 12	3	2	$43 \times 3361 \times 3907$	42	1, 80, 93	37	1
$7 \times 73 \times 103$	6	1, 12, 17	5	1	45 1151 1000	4.0	1 05 10	20	0
					$47 \times 1151 \times 1933$	46	1, 25, 42	28	3
$13 \times 37 \times 61$	12	1, 3, 5	8	7	$47 \times 3359 \times 6073$	46	1, 73, 132	26	1
$13 \times 37 \times 97$	12	1, 3, 8	5	6	$47 \times 3727 \times 5153$	46	1, 81, 112	34	1
$13 \times 37 \times 241$	12	1, 3, 20	2	5	F2 70 F00	oc	0 0 00	-	20
$13 \times 61 \times 397$	12	1, 5, 33	2	3	$53 \times 79 \times 599$	26	2, 3, 23	7	20
$13 \times 97 \times 421$	12	1, 8, 35	3	2	$53 \times 157 \times 521$	52	1, 3, 10	16	23
	_				$53 \times 157 \times 2081$	52	1, 3, 40	4	19
$17 \times 41 \times 233$	8	2, 5, 29	3	4	F0 14F1 2000	F 0	1 05 96	41	4
$17 \times 353 \times 1201$	16	1, 22, 75	5	1	$59 \times 1451 \times 2089$	58	1, 25, 36	41	4
$19 \times 43 \times 409$	6	3, 7, 68	2	3	$61 \times 181 \times 1381$	60	1, 3, 23	8	23
$19 \times 199 \times 271$	18	1, 11, 15	$\overline{14}$	3	$61 \times 181 \times 5521$	60	1, 3, 92	2	21
		, , -			$61 \times 241 \times 421$	60	1, 4, 7	35	24
$23 \times 199 \times 353$	22	1, 9, 16	13	4	$61 \times 271 \times 571$	30	2, 9, 19	29	10
		, - , -			$61 \times 277 \times 2113$	12	5, 23, 176	8	3
$29 \times 113 \times 1093$	28	1, 4, 39	3	8	$61 \times 421 \times 12841$	60	1, 7, 214	2	9
$29 \times 197 \times 953$	28	1, 7, 34	6	5	$61 \times 541 \times 3001$	60	1, 9, 50	11	8
		, ,			$61 \times 661 \times 2521$	60	1, 11, 42	16	7
$31 \times 61 \times 211$	30	1, 2, 7	9	20	$61 \times 1301 \times 19841$	20	3, 65, 992	4	1
$31 \times 61 \times 271$	30	1, 2, 9		19	$61 \times 3361 \times 4021$	60	1, 56, 67	51	2
$31 \times 61 \times 631$	30	1, 2, 21	3	17					
$31\times151\times1171$	30	1, 5, 39	4	7	$67 \times 331 \times 463$	66	1, 5, 7	48	23
$31 \times 181 \times 331$	30	1, 6, 11	17	8	$67 \times 331 \times 7393$	66	1, 5, 112	3	14
$31 \times 271 \times 601$	30	1, 9, 20	14	5	$67 \times 2311 \times 51613$	66	1, 35, 782	3	2
$31\times991\times15361$	30	1, 33, 512	2	1					
					$71 \times 271 \times 521$	10	7, 27, 52	37	4
$37 \times 73 \times 109$	36	1, 2, 3	25	31	$71 \times 421 \times 491$	70	1, 6, 7	61	22
$37 \times 73 \times 181$	36	1, 2, 5	15	26	$71 \times 421 \times 4271$	70	1, 6, 61	7	13
$37 \times 73 \times 541$	36	1, 2, 15	5	21	$71 \times 631 \times 701$	70	1, 9, 10	64	15
$37\times109\times2017$	36	1, 3, 56	2	13	$71 \times 631 \times 4481$	70	1, 9, 64	10	9
$37\times613\times1621$	36	1, 17, 45	14	3	$71 \times 701 \times 5531$	70	1, 10, 79	9	8
					$71 \times 911 \times 9241$	70	1, 13, 132	7	6
$41 \times 61 \times 101$	20	2, 3, 5	25	22	79 157 0000	10	C 10 101	-	c
$41 \times 73 \times 137$	8	5, 9, 17	22	7	$73 \times 157 \times 2293$	12	6, 13, 191	5	6
$41 \times 101 \times 461$	20	2, 5, 23	9	10	$73 \times 379 \times 523$	18	4, 21, 29	53	6
$41 \times 241 \times 521$	40	1, 6, 13	19	10	$73 \times 601 \times 21937$	24 72	3, 25, 914	2	$\frac{3}{6}$
$41 \times 241 \times 761$	40	1, 6, 19	13	9	$73 \times 937 \times 13681$	72	1, 13, 190	5	O
$41 \times 881 \times 12041$	40	1, 22, 301	3	2					
$41 \times 1721 \times 35281$	40	1, 43, 882	2	1					