Carmichael numbers with three prime factors

Notes by G.J.O. Jameson

These notes are expository, not a research article. However, the estimations of $f_3(p)$ (1.6, 1.7, 3.7) and $K_3(g)$ (2.17), may not have appeared explicitly elsewhere, and some of the internal inequalities have appeared only in the arXiv article [Ch].

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: $a^{n-1} \equiv 1 \bmod n$ 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 $n \equiv 1 \bmod (p_j - 1)$ 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 $1 \bmod p$, 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 $n \equiv 1 \bmod (p_j - 1)$ if and only if $r_j \equiv 1 \bmod (p_j - 1)$.

We refer to Carmichael numbers with three prime factors as C_3-numbers. Let $n = pqr$ be such a number, where p, q, r are prime and $p < q < r$. We use this notation consistently. Of course, $q \geq p + 2$ and $r \geq q + 2$. By the preceding remark, n is a Carmichael number if and only if

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

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 [Jam1]):

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

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 C_3-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

$$qr - 1 = h_1(p-1), \tag{1}$$
$$pr - 1 = h_2(q-1), \tag{2}$$
$$pq - 1 = h_3(r-1). \tag{3}$$

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 $h_3 \le p-1$. Also, $h_3 \ne 1$ since $r \ne pq$. □

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

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

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

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

1.3 PROPOSITION. *We have*

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

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

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

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 C_3-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 $h_2 h_3 - p^2 = \Delta$. 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 $\Delta \ge 1$. Also, since $p-1 < q-1$, we have $\Delta < p + h_3$, so in fact $\Delta \le p + h_3 - 1$. 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 $h_3 \le p^{1-\varepsilon}$ and the previous one for $h_3 > p^{1-\varepsilon}$, together with the elementary estimation $\sum_{y<n\le x} \frac{1}{n} \le \log x - \log y + 1$, we see that $f_3(p) \le S_1 + S_2$, 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 $\tau(n) \le C_\varepsilon n^\varepsilon$ 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 $f_3(p) \le 2\varepsilon p \log p + (3 + 2^\varepsilon C_\varepsilon)p$ valid for all p. We return to give a more refined bound in Theorem 1.6.

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:

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

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

Δ 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 $pq-1$. 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 $qr \equiv 1 \bmod (p-1)$: 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, $qr \equiv 1 \bmod 2$. 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	$qr \bmod 4$	C_3-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	$qr \bmod 6$	C_3-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* C_3-numbers with $p = 11$. 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 $qr \equiv 1 \bmod 10$.

The C_3-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 C_3-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 $\Delta \equiv -1 \bmod p-1$, 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 C_3-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 $7\times 73\times 103$.)

Closer estimation of $f_3(p)$

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

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

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

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

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

Both the stated estimations follow. □

1.6 THEOREM. *For all prime p, we have*

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

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

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

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

By Lemma 1.5,

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

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:

1.7 COROLLARY. *For sufficiently large p, we have* $f_3(p) \le p\dfrac{\log p}{\log\log p}$. □

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 $qr \equiv 1 \bmod (p-1)$. 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 1.6 gives a bound for the number of simple C_3-numbers with given p. Denote this number by $f_3(p,1)$.

1.8. *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 1.6, we now take S_1 to be simply $\sum_{h\le p/u}\tau(p+h)$. Putting $u = \log p$, we obtain the stated bound. □.

Bounds for q, r and n in terms of p

First, we state some non-optimal bounds that follow at once from (4). Since $h_3 \le p-1$, we have

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

Hence, by 1.2,

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

so in fact $r < p^2(p-1)$, and $n = pqr < 2p^4(p-1)^2$.

We now derive optimal estimates, at the cost of greater complication. The case of r is simplest, and we deal with it first. We can express r in terms of p, h_3 and Δ:

1.9. *We have $r = r(h_3, \Delta)$, where*

$$r(h, \Delta) = (p-1)\left(\frac{p^2}{h\Delta} + \frac{p}{\Delta} + \frac{1}{h}\right) + 1. \tag{5}$$

Proof. By (3) and (4),

$$\begin{aligned} h_3(r-1) &= pq - 1 \\ &= p(q-1) + (p-1) \\ &= (p-1)\left(\frac{p(p+h_3)}{\Delta} + 1\right). \end{aligned}$$

The stated identity follows. □

1.10 COROLLARY. *For a given p, we have $r \le r_1(p)$, where*

$$r_1(p) = \tfrac{1}{2}(p-1)(p+1)^2 + 1 = \tfrac{1}{2}(p^3 + p^2 - p + 1).$$

Equality only occurs in the case $h_3 = 2,\ \Delta = 1$.

Proof. Clearly, the largest possible value of r occurs when $(h_3, \Delta) = (2, 1)$, giving

$$r - 1 = (p-1)(\tfrac{1}{2}p^2 + p + \tfrac{1}{2}) = \tfrac{1}{2}(p-1)(p+1)^2. \qquad \square$$

Of course, the pair $(h_3, \Delta) = (2, 1)$ does not always generate prime q and r (and hence a Carmichael number). The first few values of p for which it does are 3, 5, 31, 41, 83. Chick [Ch, p. 7] reports that there are just 178 such values less than 132,425.

Next, we consider the problem of finding a bound for $n = pqr$; clearly, this equates to finding a bound for qr. The result is given in [Ch], with a slightly different method, and attributed to J. D. Swift. Recall that $q = q(h_3, \Delta)$, where

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

We regard $q(h, \Delta)$ and $r(h, \Delta)$ as functions of positive real variables. Clearly, both decrease with Δ for fixed h. For fixed Δ, $q(h, \Delta)$ increases with h. However, we have:

1.11 LEMMA. *For fixed Δ, $q(h, \Delta)r(h, \Delta)$ decreases with h for $0 < h \le p - 1$.*

Proof. Write q, r for $q(h, \Delta)$ and $r(h, \Delta)$. Since $qr = (q-1)r + r$ and r decreases with h, it is sufficient to show that $(q-1)r$ decreases with h. Now

$$\begin{aligned} \frac{\Delta}{(p-1)^2}(q-1)(r) &= (p+h)\left(\frac{p^2+\Delta}{h\Delta} + \frac{p}{\Delta} + \frac{1}{p-1}\right) \\ &= Ah + \frac{B}{h} + C, \end{aligned}$$

where

$$A = \frac{p}{\Delta} + \frac{1}{p-1}, \qquad B = \frac{p^3}{\Delta} + p.$$

By differentiation, one sees that $Ah + B/h$ decreases with h when $Ah^2 \leq B$. This is satisfied, since

$$Ah^2 \leq A(p-1)^2 < \frac{p^3}{\Delta} + p - 1 < B. \qquad \square$$

1.12 PROPOSITION. *For a given p, we have $n \leq n_1(p)$, where*

$$n_1(p) = \tfrac{1}{2}p(p^5 + 2p^4 - p^3 - p^2 + 2p - 1).$$

Equality only occurs in the case $h_3 = 2$, $\Delta = 1$. In particular, $n < \frac{1}{2}p^5(p+2)$.

Proof. By the Lemma, the greatest possible value of n occurs when $(h_3, \Delta) = (2, 1)$. In this case, we have $r - 1$ as in 1.10 and $q - 1 = (p-1)(p+2)$. With some of the algebraic details suppressed, this gives

$$\begin{aligned} 2(qr-1) &= 2(q-1)(r-1) + 2(q-1) + 2(r-1) \\ &= (p-1)[(p-1)(p+1)^2(p+2) + 2(p+2) + (p+1)^2] \\ &= (p-1)(p^4 + 3p^3 + 2p^2 + p + 3) \\ &= p^5 + 2p^4 - p^3 - p^2 + 2p - 3, \end{aligned}$$

and hence the stated expression $n_1(p)$. $\square$

The case $(h_3, \Delta) = (2, 1)$ is a highly special outlier. In all other cases, much smaller bounds apply to r and n, as we now show.

1.13. *In all cases except $(h_3, \Delta) = (2, 1)$, we have $r \leq r_2(p)$ and $n \leq n_2(p)$, where*

$$r_2(p) = \tfrac{1}{5}(p^3 + 4p^2 - 4p + 4) < \tfrac{1}{5}p^2(p+4),$$

$$n_2(p) = \tfrac{1}{5}p(p^5 + 8p^4 + 8p^3 - 28p^2 + 32p - 16) < \tfrac{1}{5}p^4(p+4)^2.$$

Proof. Recall that $\Delta \equiv -p^2 \bmod h_3$. If $h_3 = 2$, this implies that Δ is odd. We are excluding the case $(2, 1)$, so $\Delta \geq 3$. If $h_3 = 3$, then $p^2 \equiv 1 \bmod 3$ (note that $p \geq 5$), so $\Delta \equiv 2 \bmod 3$, hence $\Delta \geq 2$. Similarly, if $h_3 = 4$, then $\Delta \geq 3$.

Consider all cases with $\Delta = 1$. As just shown, we then have $h_3 \geq 5$. By Lemma 1.11, for all such cases, $r \leq r(5, 1)$ and $qr \leq q(5, 1)r(5, 1)$. Now

$$r(5, 1) - 1 = \tfrac{1}{5}(p-1)(p^2 + 5p + 1),$$

hence $r(5, 1) = r_2(p)$. Routine, but tedious, algebra shows that $pq(5, 1)r(5, 1)$ equates to the stated expression for $n_2(p)$.

Now consider cases with $\Delta \geq 2$. Since the combination $(2,2)$ does not occur, the greatest values, among such cases, for both r and n are given by either $(3,2)$ or $(2,3)$. For both of these,

$$r - 1 \leq (p-1)\left(\frac{p^2}{6} + \frac{p+1}{2}\right) = \tfrac{1}{6}(p-1)(p^2+3p+3) < r(5,1) - 1,$$

so the previous bound $r_2(p)$ applies. Also, since $q(h,\Delta)$ increases with h and decreases with Δ, both $q(3,2)$ and $q(2,3)$ are less than $q(5,1)$, so the bound $n \leq n_2(p)$ also applies. □

The case $(h_3, \Delta) = (5,1)$ requires $p^2 \equiv -1 \bmod 5$, hence p congruent to 2 or 3 mod 5. The first two Carmichael numbers generated by $(5,1)$ are $7 \times 73 \times 103$ and $17 \times 53 \times 1201$. There are no others with $p < 100$.

We now return to the question of bounds for q. This is rather more tricky, because $q(h,\Delta)$ increases with h. Recall that (4) gives at once $q \leq 2p(p-1)$. The optimal bound, due to Duparc [Du], is as follows; it is actually only slightly stronger.

1.14 PROPOSITION. *We have $q \leq q_1(p)$, where*

$$q_1(p) - 1 = (p-1)[2p - (p - \tfrac{3}{4})^{1/2} + \tfrac{1}{2}].$$

Proof. If $\Delta \geq 2$, then (4) gives the stronger inequality $q - 1 < p(p-1)$, so assume that $\Delta = 1$. Write $p - h_3 = s$, so that $1 \leq s \leq p-2$ and $q - 1 = (p-1)(2p-s)$. We want a lower bound for s. Write also $t = h_2 - p - s$. Then

$$1 = \Delta = h_2 h_3 - p^2 = (p+s+t)(p-s) - p^2 = t(p-s) - s^2,$$

so $t(p-s) = s^2 + 1$. Hence $t > 0$: since it is an integer, $t \geq 1$. Rewrite the identity again as $s^2 + ts = tp - 1$. With t chosen, this gives $s = s(t) = -\frac{t}{2} + M(t)$, where

$$M(t) = \left(\frac{t^2}{4} + tp - 1\right)^{1/2}.$$

Now

$$s'(t) = -\frac{1}{2} + \frac{\frac{t}{2} + p}{2M(t)} > 0,$$

since $M(t) < \frac{t}{2} + p$. Since $t \geq 1$, we have

$$s \geq s(1) = -\tfrac{1}{2} + (p - \tfrac{3}{4})^{1/2},$$

and hence the stated bound for $q - 1$. □

For the bound $q_1(p)$ to be attained, we require $t = 1$, so that $p = s^2 + s + 1$: then $h_3 = s^2 + 1$, and one can (if desired) write q and r in terms of s. For p to be prime, s cannot

(for example) be congruent to 1 mod 3, unless $s = 1$. The first three values of s that actually generate a Carmichael number are 1, 2 and 6, giving respectively $3 \times 11 \times 17$, $7 \times 73 \times 103$ and $43 \times 3361 \times 3907$. The next example is $s = 90$, and Chick [Ch, p. 7] reports that there are just 12 cases up to 3654.

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

A rich algebra describing the structure of C_3-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. The notation largely follows [DLP].

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

$$p - 1 = ag, \quad q - 1 = bg, \quad r - 1 = cg, \tag{6}$$

so that $a < b < c$ (hence $b \geq 2$, $c \geq 3$ and $abc \geq 6$). 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").

Note that p does not divide b, since it does not divide $q - 1$.

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 $s \geq 1$) 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 C_3-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*

$$h_1 a = bcg + b + c, \qquad h_2 b = acg + a + c, \qquad h_3 c = abg + a + b. \tag{7}$$

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

Note that $h_3 c$ can also be written as $aq + b$ and as $bp + a$.

2.3 COROLLARY. *We have $c < abg$.*

Proof. $h_3 \geq 2$ and $a + b < 2b < abg$. □

2.4. *We have $(h_3, a) = (h_3, b) = 1$ (etc.)*

Proof. If d divides both h_3 and a, then it divides $h_3 c - aq = b$, 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 $c = h_3 = 4$.

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

Proof. By the first two identities in (7), $qc \equiv -b \bmod a$ and $pc \equiv -a \bmod b$. This determines c mod a and mod b, hence mod ab. (Alternatively, $h_3 c \equiv a + b \bmod ab$, and $(h_3, ab) = 1$). □

Note that abg is the lowest common multiple $[p-1, q-1]$, and 2.5 equates to the statement that r is determined mod $[p-1, q-1]$.

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

2.6 PROPOSITION. *Let*

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

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

Proof. We have

$$\begin{aligned} n - 1 &= (ag+1)(bg+1)(cg+1) - 1 \\ &= abcg^3 + (bc + ca + ab)g^2 + (a + b + c)g \\ &= abcg^3 + Eg. \end{aligned}$$

Now $n - 1$ is a multiple of $p - 1 = ag$, hence a divides E. Similarly for b and c. Since a, b, c are pairwise coprime, abc divides E. □

Clearly, $n - 1 = abcg(g^2 + k)$. An alternative proof of 2.6 is as follows: by 2.2,

$$E = a(b + c)g + a + (bcg + b + c) = a(b + c)g + a + h_1 a,$$

so a divides E. Similarly for b and c.

2.7. *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 2.6, g has to satisfy $Sg \equiv -a - b - c \bmod abc$. This determines g uniquely mod abc. (Alternatively, (7) shows that g is determined mod each of a, b, c.) □

Conversely, suppose that a, b, c (pairwise coprime) are given, and that g satisfies $Sg \equiv -a - b - c \bmod abc$, so that E is a multiple of abc. Let p, q, r be defined by (6) and let $n = pqr$. Then the algebra in 2.6 and 2.2, in reverse, shows that (7) 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 $11g \equiv -6 \bmod 6$, hence $g = 0 \bmod 6$. The first three cases that give three primes are:

$$g = 6\text{:}\ \ 7 \times 13 \times 19; \qquad g = 36\text{:}\ \ 37 \times 73 \times 109; \qquad g = 210\text{:}\ \ 211 \times 421 \times 631.$$

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

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

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

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

2.8 PROPOSITION. *We have $g < ka \leq 3g - 1$. In particular, $a \leq 3g - 1$.*

Proof. Recall that $a < b < c$ and $g \geq 2$. By 2.6,

$$\begin{aligned} kab &= g\left(a + b + \frac{ab}{c}\right) + \left(1 + \frac{a}{c} + \frac{b}{c}\right) \\ &< g(2a + b) + 3 \leq g(3b - 2) + 3 < 3bg, \end{aligned}$$

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

2.9 COROLLARY. *We have $p < 3g^2$.*

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

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

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

2.11 COROLLARY. *We have* $abg < (3n)^{1/2}$

Proof. $(abg)^2 < (abg)(3bg^2) = 3ab^2g^3 < 3n.$ □

By 2.9 and 1.4, there are only finitely many C_3-numbers with a given value of g. Below, we will give an estimation of this number and a procedure for finding them.

By 2.9 and the inequalities from section 1, we have $q < 2(3g^2)^2$, $r < \frac{1}{2}(3g^2)^3$ and $n < \frac{1}{2}(3g^2)^6$. However, much stronger bounds actually apply, as we will see below.

Note 1. Actually, $k \le 2g$: since $a \ge 1$, $b \ge 2$, $c \ge 3$, we have

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

Note 2. Of the 83 C_3-numbers listed in the Appendix, just three have $a > g$. In each case, $a = g + 1$. A more extreme case of large a is the number $191 \times 421 \times 431$, with $g = 10$ and $a = 19$. One might be tempted to conjecture that a never exceeds $2g$, but Chick [Ch, p. 15] reports computations showing that there are C_3-numbers with this property, though only eleven with $n < 10^{24}$. The smallest one is defined by $(a, b, c, g) = (1049, 1841, 2304, 518)$.

The case $g = 2$. By 2.9, if $g = 2$, then $p \le 11$. From our listings in section 1 (including the empty case $p = 11$), it is easily seen that there are only two C_3-numbers with $g = 2$:

$$3 \times 11 \times 17, \qquad 7 \times 23 \times 41.$$

So all other C_3-numbers have $g \ge 4$; recall that this means that $(p-1, q-1) \ge 4$, and similarly for other pairs. For example, twin primes cannot occur among the factors (we remark that no such statement holds for 4-factor Carmichael numbers). Another consequence is:

2.12. *Suppose that* $p > 7$ *and* $p = 2k + 1$, *where* k *is prime. Then all* C_3*-numbers* pqr *(with* $p < q < r$*) are simple.*

Proof. We have $ag = 2k$. By the above, $g \ne 2$. Since g is even, $g = 2k$. □

The number j

2.13. *Let* $j = ka - g$. *Then*

$$jbc = a(b + c)g + a + b + c = p(b + c) + a, \tag{8}$$

$$j = \frac{p + h_3}{b} = \frac{p + h_2}{c}. \tag{9}$$

Proof. By 2.6,

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

Also, by this expression and (7),

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

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 $j_1 = j$.

By 2.8, $j \leq 2g - 1$. Further, we have:

2.14. *We have* $j \leq \dfrac{2ag+1}{b}$. *If* $a = 1$, *then* $j \leq g$.

Proof. By 1.2, $h_3 \leq p - 1 = ag$, hence $jb = p + h_3 \leq 2ag + 1$. If $a = 1$, then $2j \leq jb \leq 2g + 1$, so $j \leq g$. □

Of course, it also follows that $b \leq 2ag + 1$.

Of the 83 C_3-numbers with $p \leq 73$, just one has $j > g$, namely $41 \times 61 \times 101$, for which $g = 20$, $j = 22$.

2.15. *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 $d = 1$. □

2.16. *We have* $h_2 h_3 = p^2 + ja$.

Proof. By (9) and (8),

$$\begin{aligned} h_2 h_3 &= (jc - p)(jb - p) \\ &= p^2 + j^2 bc - jp(b + c) \\ &= p^2 + ja. \qquad \square \end{aligned}$$

Recall that $h_2 h_3 - p^2$ is the Δ of section 1, so 2.16 says that $\Delta = ja$. Together with the identity $jb = p + h_3$, this amounts to a restatement of (4):

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

If so inclined, the reader could now proceed to the first part of section 3.

Carmichael numbers with given g

We have seen that there are only finitely many C_3-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 $\log\tau(m) \le \alpha L(m)$, so that $\tau(m) \le M(m)^\alpha$, for all large enough m.

2.17 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 $j \equiv -g \bmod a$. The number of choices of j is no more than $2g/a + 1$, so the number of pairs (a, j) is no more than

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

(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.)

Given a choice of h_3, b (hence q) is now defined by (9) and r by (3). By 2.16, the number of possible choices for h_3 is bounded by $\tau(p^2 + ja)$ (actually, no more than half this number, because $h_3 \le p$). Now (for $g \ge 4$) $p^2 + ja \le 9g^4 + 6g^2 \le 10g^4$. If g (and hence p) is large enough, then we have

$$\log\tau(p^2 + ja) \le \frac{\frac{7}{10}(4\log g + \log 10)}{\log\log g} < 3L(g),$$

so $\tau(p^2 + ja) \le M(g)^3$. Also, $2(\log g + 4) \le M(g)$. Hence $K_3(g) \le gM(g)^4$. □

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.

The proof amounts to a procedure for finding the C_3-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) $j \equiv -g \bmod a$ and $j \leq (2ag + 1)/(a + 1)$.

(C3) $2 \leq h_3 \leq p - 1$, $h_3 \equiv -p \bmod j$ and h_3 divides $p^2 + ja$.

(C4) $b > a$ and $(a, b) = 1$.

When $j > g$, the possible range for h_3 is also restricted from below by $h_3 = jb - p \geq j(a + 1) - p$, since $b \geq a + 1$.

We have already identified the numbers with $g = 2$, using the listings from section 1. We illustrate the process just described by tabulating the case $g = 4$ (the reader may care to set out the case $g = 2$ in similar style). We list the possible choices of a, j and then h_3. The symbol $-$ means that no choice of the number concerned is possible, and $*$ that one of the conditions is violated.

a	p	j	$p^2 + ja$	h_3	b	q	r	C_3-number
1	5	1	26	2	7	29	73	$5 \times 29 \times 73$
		2	27	3	4	17	29	$5 \times 17 \times 29$
		3	28	4	3	13	17	$5 \times 13 \times 17$
		4	29	$-$				
3	13	2	175	5	$9*$			
				7	10	41	$77*$	
4	17	4	305	$-$				
7	29	3	862	$-$				
9	37	5	1414	$-$				
10	41	6	1741	$-$				

The starred case for b fails condition (C4). If continued, it would lead to $13 \times 37 \times 97$, which is a Carmichael number, but with $g = 12$.

We record the complete list of C_3-numbers with $g = 6$ and $g = 8$:

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

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

quantity in section 1 was $(p-1)(p+h_3)$, already given in factorised form. This rapidly leads to large numbers: if a is close to $3g$, then $p^2 + ja$ is of the order $9g^4$. However, in these cases, there are only a small number of candidate values for h_3, and it may be easier simply to check these instead of factorising $p^2 + ja$. For example, the case $g = 12$, $a = 34$, $j = 22$ gives $p^2 + ja = 168,029$. This number happens to be prime, but the only candidate values for h_3 are 361, 383 and 405. The process is greatly facilitated by an instant factorisation service, such as "Factoris", available at `http://wims.unice.fr/wims.cgi`.

Inequalities in terms of a and g

In section 1, we gave bounds for q, r and n in terms of p $(= ag + 1)$. We now give some bounds in terms of a and g separately. Once a and g are chosen , the other numbers are determined by h_3 and j. We retain the notation p where it simplifies expressions.

We give bounds that are optimal, but rather complicated (though not hard to derive), and also some more simply stated inequalities. For these, we need to make exceptions of a few early Carmichael numbers: for this purpose, write

$$n_1 = 3 \times 11 \times 17, \quad n_2 = 5 \times 29 \times 73, \quad n_3 = 7 \times 23 \times 41, \quad n_4 = 7 \times 73 \times 103.$$

We will use the listings in the Appendix up to $p = 13$.

We have already seen in 2.14 that $b \leq 2ag + 1$. In fact, since $h_3 \leq p - 2$ for all n except n_1 and $5 \times 13 \times 17$, (Remark 2, p. 5), we have $b \leq 2ag$ for all n except n_1. We give an optimal estimation for b later.

Coresponding to the result for r (1.10), we have:

2.18. *For all C_3-numbers, we have $c \leq C(a, g)$, where*

$$C(a, g) = \tfrac{1}{2}(a^2g^2 + 4ag + a + 3).$$

Equality holds when $j = 1$ and $h_3 = 2$. Further, $c \leq \frac{1}{2}ag(ag+6)$, with strict inequality except for n_1.

Proof. By (7) and (9),

$$c = \frac{pb + a}{h_3} = \frac{p(p + h_3)}{jh_3} + \frac{a}{h_3} = \frac{p^2}{jh_3} + \frac{p}{j} + \frac{a}{h_3}. \tag{10}$$

This is greatest when $j = 1$ and $h_3 = 2$, giving $c = \frac{1}{2}(p^2 + a) + p$, which equates to $C(a, g)$ when $ag + 1$ is substituted for p.

Now $a+3 \le 4a \le 2ag$, hence $c \le \frac{1}{2}(a^2g^2+6ag) = \frac{1}{2}ag(ag+6)$. Equality holds only when $a=1$ and $g=2$, hence only for n_1. □

2.19 LEMMA. *For a given combination of (a,g,j), qr is maximised by taking $h_3=2$.*

Proof. We have

$$qr = (bg+1)(cg+1) = bcg^2 + (b+c)g + 1.$$

We show that $b+c$ and bc are maximised by taking $h_3=2$. Now

$$jb = p + h_3, \qquad jc = \frac{p^2+ja}{h_3} + p,$$

so $j(b+c) = F_1(h_3)$ and $j^2bc = F_2(h_3)$, where

$$F_1(h) = 2p + h + \frac{p^2+ja}{h},$$

$$F_2(h) = (2p^2+ja) + ph + \frac{p(p^2+ja)}{h}.$$

Recall that $Ah + B/h$ decreases (strictly) with h when $Ah^2 \le B$. Hence both functions decrease on the interval $2 \le h \le p$, so attain their greatest values at $h=2$, as stated. □

2.20 PROPOSITION. *For all C_3-numbers, we have $n \le N(a,g)$, where*

$$N(a,g) = (ag+1)(ag^2+3g+1)[gC(a,g)+1].$$

Equality holds when $j=1$ and $h_3=2$. Also,

$$n \le \tfrac{1}{2}ag^3(ag+1)(ag+4)(ag+6),$$

and $n < a^4g^6$ in all cases except n_1, n_2, n_3 and n_4.

Proof. Note that $p = ag+1$ is given, so the problem is to maximise qr. For fixed h_3, b and c (hence q and r) are clearly maximised by taking $j=1$. By the Lemma, qr is then maximised by taking $h_3=2$. This gives $r = gC(a,g)+1$ and $b = ag+3$, hence $q = ag^2+3g+1$, leading to the stated expression $N(a,g)$.

Now $ag^2+3g+1 < g(ag+4)$. For $n \ne n_1$, 2.18 gives $cg+1 < \frac{1}{2}ag^2(ag+6)$, and hence the second stated inequality for n. It is easily checked that this inequality also holds for n_1. For $x \ge 16$, $(1+\frac{1}{x})(1+\frac{4}{x})(1+\frac{6}{x}) < 2$, hence $n < a^4g^6$ when $ag \ge 16$, (so $p \ge 17$). Using our list, one can check that this inequality holds for all n with $p \le 13$ except the four stated. □

The full expression for $N(a,g)$ is complicated and not very illuminating. The two leading terms are $\frac{1}{2}a^4g^6 + 4a^3g^5$.

The first few cases having $j = 1$ and $h_3 = 2$ are n_1, n_2 and

$$31 \times 991 \times 15361, \quad 41 \times 1721 \times 35281, \quad 43 \times 271 \times 5827.$$

We now show that an adaptation of the proof of 1.14 gives an optimal estimation of b.

2.21. *We have*

$$b \leq 2ag + \tfrac{5}{2} - (ag + \tfrac{5}{4} - a)^{1/2}.$$

Proof. If $j \geq 2$, then $b \leq ag$, so we assume that $j = 1$. Then $b = p + h_3$ and $h_2h_3 - p^2 = a$. As in 1.14, we put $s = p - h_3$ and $t = h_2 - p - s$ to obtain $b = 2p - s$ and $a = h_2h_3 - p^2 = t(p - s) - s^2$, so that $s^2 + ts = tp - a$, hence

$$s = s(t) = -\frac{t}{2} + \left(\frac{t^2}{4} + tp - a\right)^{1/2}.$$

As before, we deduce that $s \geq s(1)$, and hence the stated inequality for b. Equality holds in cases when $t = 1$, as exhibited previously. □

Inequalities in terms of g

We now establish bounds in terms of g only. We already have $a < 3g$ and $p < 3g^2$. This could be substituted into the results just obtained to give (for example) $b \leq 6g^2$ and $n < 81g^{10}$. However, we are now no longer regarding a as given, and we use the fact that $a \leq g + j$ to derive better (in some cases, optimal) estimates by paying attention to j.

2.22. *For all C_3-numbers, we have $b \leq 2g(g + 1)$.*

Proof. For all n except n_1 and $5 \times 13 \times 17$, we have $h_3 \leq p - 2$, hence $jb \leq 2p - 2 = 2ag \leq 2g(g + j)$, so $b \leq 2g^2/j + 2g \leq 2g(g + 1)$. This is also satisfied by the two numbers excepted. □

2.23. *We have $c \leq C(g)$, where*

$$C(g) = \tfrac{1}{2}(g^4 + 2g^3 + 5g^2 + 5g + 4),$$

with equality (only) when $j = 1$, $h_3 = 2$ and $a = g + 1$. In all cases, $c < \frac{1}{2}g^3(g + 4)$.

Proof. By (10), with $h_3 = 2$ but j still variable,

$$2c \leq \frac{p(p + 2)}{j} + a.$$

Substituting $p = ag + 1$ and $a \leq g + j$, we have $2c \leq F_3(j)$, where

$$F_3(j) = \frac{1}{j}(g^2 + gj + 1)(g^2 + gj + 3) + g + j = Aj + \frac{B}{j} + C,$$

with $A = g^2+1$ and $B = (g^2+1)(g^2+3)$. Then $F_3(1)$ equates to $2C(g)$, so we have to show that $F_3(j) < F_3(1)$ for $1 < j < 2g$. Now $F_3(j)$ decreases (strictly) with j when $j^2 < g^2+3$, and subsequently increases. So we just have to show that $F_3(2g) < F_3(1)$. Now

$$F_3(2g) = \frac{1}{2g}(3g^2+1)(3g^2+3) + 3g = \tfrac{9}{2}g^3 + 9g + \frac{3}{2g},$$

so for $g \geq 2$,

$$F_3(1) - F_3(2g) > g^4 - \tfrac{5}{2}g^3 + 5g^2 - 4g > g^4 - \tfrac{5}{2}g^3 + 3g^2 > g^2(g-\tfrac{5}{4})^2 > 0.$$

For $g \geq 4$, it is easily checked that $5g^2+5g+4 < 2g^3$, so $c < \frac{1}{2}g^3(g+4)$. This is also satisfied by the two C_3-numbers with $g = 2$. □

An example where $c = C(g)$ is $43 \times 271 \times 5827$, for which $j = 1$, $h_3 = 2$, $g = 6$ and $a = 7$.

2.24 PROPOSITION. *We have $n \leq N(g)$, where*

$$N(g) = (g^2+g+1)(g^3+g^2+3g+1)[gC(g)+1],$$

with equality (only) when $j = 1$, $h_3 = 2$ and $a = g+1$. Further,

$$n < \tfrac{1}{2}g^4(g+1)^5(g+4).$$

Proof. The choice of h_3 does not affect p, and by Lemma 2.19, qr is maximised (for any fixed j) by taking $h_3 = 2$. So we fix $h_3 = 2$. By 2.23, c (hence q) is then maximised by the combination $j = 1$, $a = g+1$. We show that pq (though not p and q separately) is also maximised by this combination. The resulting values are $p = g^2+g+1$ and $q = (p+2)g+1 = g^3+g^2+3g+1$, hence the stated expression $N(g)$ for n.

Now $pq = (ag+1)(bg+1) = abg^2 + (a+b)g + 1$. We will show that $a+b$ and ab are both maximised by the combination stated. We have $a \leq g+j$, so $p \leq g^2+gj+1$ and (with $h_3 = 2$)

$$b = \frac{p+2}{j} \leq g + \frac{g^2+3}{j}.$$

So $a+b \leq F_4(j)$ and $ab \leq F_5(j)$, where

$$F_4(j) = j + \frac{g^2+3}{j} + 2g, \qquad F_5(j) = gj + \frac{g(g^2+3)}{j} + 2g^2 + 3.$$

As in the previous proof, $F_4(j)$ and $F_5(j)$ decrease when $j^2 < g^2+3$ and then increase, so we have to show that $F_k(2g) < F_k(1)$ for $k = 4, 5$. Now $F_4(1) = g^2+2g+4$ and $F_4(2g) = \frac{9}{2}g + \frac{3}{2g}$, so for $g \geq 2$,

$$F_4(1) - F_4(2g) > g^2 - \tfrac{5}{2}g + 3 > (g-\tfrac{5}{4})^2 > 0.$$

Also, $F_5(1) = g^3 + 2g^2 + 4g + 3$ and $F_2(2g) = \frac{9}{2}g^2 + \frac{9}{2}$, hence

$$F_5(1) - F_5(2g) > g^3 - \tfrac{5}{2}g^2 + 3g > 0.$$

Of course, equality occurs when $j = 1$ and $a + g + 1$.

In the expression for $N(g)$, the product of the first two factors is less than $(g+1)^5$, and by 2.23, $gC(g) + 1 < \frac{1}{2}g^4(g+4)$. □

The inequality $a < 3g$ has been improved by Chick to $a < 3g - (g/2)^{1/2}$ [Ch, Theorem 4.1]. A slightly simplified version of the proof is given in [Jam2].

A closer estimation of b can be obtained by the method of 1.14 and 2.21, taking $j = 1$ and $a = g + 1$. The case $t = 1$ would imply $s^2 + s = g^2$, which is not possible in integers. Taking $t = 2$, we obtain the bound

$$b \le 2g(g+1) + 3 - (2g^2 + g + 2)^{1/2},$$

but I do not know whether this case can actually occur.

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}	10^{21}
$C_3(x)$	172	1,000	6,083	35,586	224,763
α	0.248	0.250	0.252	0.253	0.255

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. First, we mention a very quick estimation derived from our Theorem 1.4 together with Chebyshev's estimate for prime numbers. We denote by $P(y)$ the set of primes $p \le y$.

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,

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

We now show how progressively better estimates can be obtained by applying increasing amounts of the algebra of section 2.

Let us call a quadruple (a, b, c, g) "admissible" if it generates a Carmichael number and $abcg^3 \le x$. We have to estimate the number of admissible quadruples. To do this, we consider the "dyadic cells" 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 admissible quadruples in this cell. If this number is non-zero, then we must have $A \le B \le C$, and $ABCG^3 \le x$. Also, for example, the inequality $a < 3g$ translates into $A \le 6G$. Suppose that $2^R \le x < 2^{R+1}$, so that $R \le (\log x)/(\log 2)$. Since each of a, b, c, g is bounded by x, the number of dyadic intervals required for each of them is not more than R , so the total number of dyadic cells is no more than R^4 (this is actually an overestimate, since, for example, $a < \sqrt{3} x^{1/6}$ and $g < x^{1/3}$). We aim to establish an upper bound of the form x^μ or $x^\mu M(x)^\alpha$ applying to each dyadic cell.

We start with a quick estimate using only the elementary results 2.3, 2.5 and the inequality $a < 3g$. As far as I know, this method has not appeared elsewhere.

3.2. *We have* $C_3(x) \ll x^{1/2} (\log x)^4$.

Proof. In a given dyadic cell, choose a, b and g freely: there are ABG choices (of course, some could be excluded, for example any with $a > b$). By 2.5, c is then determined mod ab, so the number of possible choices of c is bounded by

$$\frac{C}{ab} + 1 \le \frac{C}{AB} + 1.$$

It follows that

$$N = N(A, B, C, G, x) \le ABG \left(\frac{C}{AB} + 1 \right) = CG + ABG.$$

By 2.11, any admissible quadruple satisfies $abg \le (3x)^{1/2}$, hence if $N \ne 0$, we have $ABG \le (3x)^{1/2}$. Also, by 2.3, $c < abg$, so $(cg)^2 < (abg^2)(cg) = abcg^3 < x$, hence $CG \le x^{1/2}$. So $N < 3x^{1/2}$. The result follows (with a constant no more than $3/(\log 2)^4$). $\square$

By parting with the dyadic cell method, but proving some further lemmas, one can replace $(\log x)^4$ by $(\log x)^2$; we return to this below.

The first estimation of this type was presented in [DLP]. The next result essentially encapsulates their method, translated into the language of dyadic cells. It uses 2.7, 2.13 and 2.15. Our presentation follows [HBr], with some slight modifications and corrections. Actually, [DLP] obtained the weaker bound $x^{1/2}(\log x)^{11/4}$, because it only used the fact that a divides $(g+j)(1+h_3)$ instead of $g+j$.

As before, write $L(x) = (\log x)/(\log\log x)$ and $M(x) = e^{L(x)}$. By the result quoted previously, for large enough x, we have $\tau(m) \le M_1(x)$ for all $m \le x$, where $M_1(x) = M(x)^{7/10})$.

3.3 PROPOSITION. *We have* $C_3(x) \ll x^{2/5}M(x)$.

Proof. We establish two further bounds for $N(A,B,C,G,x)$:

$$H_1 = ABC + G, \quad H_2 = \left(\frac{AG^2}{B} + AG\right) M_1(x),$$

(each possibly multiplied by a constant).

(1) Choose a, b, c freely within the cell: there are at most ABC choices. Then, by 2.7, 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 the estimate H_1.

(2) (Compare the proof of 2.17.) 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 2.14, j must satisfy

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

(note that b has not yet been chosen, but B has!). Also, $j \equiv -g \bmod a$, so the number of choices for j is no more than $6G/B+1$. Hence the number of choices for (g,a,j) is bounded by $6AG^2/B + AG$. 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 $M_1(x)$, since $p^2 + ja < x$.

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

For present purposes, we only use H_2 in the weaker form $G^2M_1(x)$. If G is the larger term in H_1, we simply note that $G \le x^{1/3}$. If ABC is the larger term, we combine it with H_2 by observing that $(ABC)^{2/5}(G^2)^{3/5} \le x^{2/5}$. Hence $N \ll x^{2/5}M_1(x)$. We finish by observing that $M_1(x)(\log x)^4 \ll M(x)$. □

Note. In the estimation of H_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.

By a further development of the method, [BN] reduced the estimate to $x^{5/14+\varepsilon}$. The proof 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..

3.4 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 2.6, $gS + a + b + c = kabc$. Multiply by $a + b$ and rearrange as far as possible in terms of S:

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

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

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

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

Proof. Using Lemma 3.4, we establish the further bound $H_3 = BGM_1(x)$ for N. We choose a, b and k, consistent with the other conditions, and let $V = k^2a^2b^2 + a^2 + b^2 + ab$. By Lemma 3.4, a chosen factorisation of V will now determine g and c. Since $ka < 3g$, it is clear that $V \ll g^2b^2 < x$, so $\tau(V) \ll M_1(x)$.

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

We now combine these estimates to find a value μ such that in all cases we have $N(A, B, C, G, x) \ll x^{\mu} M(x)^{7/10}$.

If AG is the larger term in H_2 (in other words, if $G < B$), we simply note that $AG \leq (ABCG^3)^{1/3}$. Similarly if G is the larger term in H_1. So we now work with ABC from H_1 and $AB^{-1}G^2$ from H_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 $\alpha + \beta \le 1$. 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 $\alpha + \beta \ge \mu$. Substitution leads to $7\alpha \ge 1$, 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. 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 $ABC \le X^{1-3\alpha}$.
Case 2: $G \le X^\alpha$ and $B > AX^\delta$. Then $AB^{-1}G^2 \le X^{2\alpha-\delta}$.
Case 3: $G \le X^\alpha$ and $B \le AX^\delta$. Then $B^3G^3 \le X^\delta AB^2G^3 \le X^{1+\delta}$, so $BG \le X^{(1+\delta)/3}$.

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

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

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

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 $b \ge g$. Another special type for which this estimation applies is the set of numbers satisfying $b^2 \le ac$: this only needs the bound BG, since $B^2 \le AC$ gives $(BG)^3 \le ABCG^3$. A more interesting example is:

3.6. *Let $C_3(x,1)$ be the number of simple 3-factor Carmichael numbers not greater than x. 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 H_1 or H_2. Otherwise, the product of the three bounds, without $M_1(x)$, is

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

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.

3.7 PROPOSITION. *For any $\varepsilon > 0$, we have $\sum_{p \le P} f_3(p) \ll P^{3/2}M(P)^4$.*

Proof. The numbers considered now satisfy $AG \le P$. Combine H_2 and H_3. Either AG is the larger term in H_2, or we have

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

By 2.18, $b < 2p$ and $c < p^2$, so the number of cells is $\ll (\log P)^4$. Also, $p^2 + ja < 2p^2$ and (in 3.5) $V \ll g^2b^2 \ll p^4$, so the number of divisors of these quantities can be estimated by $M(P)^3$ (as in 2.17). □

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 H_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 $\frac{1}{3}$.

Non-dyadic versions of the proofs. A non-dyadic version of the proof of Proposition 3.3, closer to the style of [DLP] and [BN], is as follows.

3.8 LEMMA. *The number of integer triples (i, j, k) with $ijk \le y$ is no more than $y(\log y + 1)^2$.*

Proof. For each (i, j) with $ij \le y$, there are at most $y/(ij)$ values of k with $ijk \le y$. The statement now follows from

$$\sum_{ij \le y} \frac{1}{ij} \le \sum_{i \le y} \frac{1}{i} \sum_{j \le y} \frac{1}{j} \le (\log y + 1)^2.$$

(Of course, more accurate estimations are possible; the main term is really $\frac{1}{2}y(\log y)^2$.) □

Proof of Proposition 3.3. We estimate the number of admissible quadruples (a, b, c, g). For a number G to be chosen later, let N_1 be the number of such quadruples with $g > G$, and N_2 the number with $g \le G$.

To estimate N_1, consider the triples (a, b, c) with $a < b < c$ and $abc \le x/G^3$. By 2.7, for each triple, g is determined mod abc. Also, $g \le (x/abc)^{1/3}$. So the number of choices for

g is no more than

$$\frac{x^{1/3}}{(abc)^{4/3}} + 1.$$

The contribution of the +1 term is the number of such triples, which is estimated by Lemma 3.8: since $\log(x/G^3) + 1 < \log x$ (given $G \geq 2$) and the Lemma counts each triple 6 times, this number is no more than $x(\log x)^2/(6G^3)$. The contribution of the first term (ignoring the upper bound on abc) is no more than

$$x^{1/3} \sum_{a<b<c} \frac{1}{(abc)^{4/3}} \leq \tfrac{1}{6} x^{1/3} \zeta(\tfrac{4}{3})^3 < 8x^{1/3}.$$

To estimate N_2, we can apply Theorem 2.17 (ignoring the restriction $abcg^3 \leq x$):

$$N_2 \leq \sum_{g \leq G} K_3(g) \ll \sum_{g \leq G} gM(g)^4 \ll G^2 M(G)^4.$$

Now take $G = x^{1/5}$. Then $M(G)^4 \leq M(x)$. Also, $(\log x)^2 \ll M(x)$. So both N_1 and N_2 are dominated by $x^{2/5}M(x)$. □

Sketch of non-dyadic proof of 3.2, with $(\log x)^2$ *instead of* $(\log x)^4$. Let $C_3^*(x)$ be the number of 3-factor Carmichael numbers in $(x/2, x]$. Given a triple (a, b, g) with $ab^2g^3 \leq x$, c is determined mod ab and $c \leq x/abg^3$, so the number of choices of c is no more than

$$\frac{x}{a^2b^2g^3} + 1.$$

Since $a < 3g$, $abg < (3x^{1/2}$. By Lemma 3.8, the number of such triples is estimated by $x^{1/2}(\log x)^2$. Since $c < abg$, we have $(abg^2)^2 > abcg^3 > x/2$. The result now follows, given the following fact (we omit the proof, but it is not hard):

$$\sum_{abg^2 > y} \frac{1}{a^2b^2g^3} \ll \frac{(\log y)^2}{y}. \qquad \square$$

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 $a^{n-1} \equiv 1 \bmod n$ 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.

[Ch] J.M. Chick, Carmichael number variable relations: three-prime Carmichael numbers up to 10^{24}, arXiv:0711.2915v2[math.NT].

[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.

[Jam1] G.J.O. Jameson, Finding Carmichael numbers, *Math. Gazette* **95** (2011), 244–255.

[Jam2] G.J.O. Jameson, An inequality for Carmichael numbers due to J.M. Chick, 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 10^{18}, 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).

December 2011

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

pqr	g	a, b, c	h_3	j
$3 \times 11 \times 17$	2	1, 5, 8	2	1
$5 \times 13 \times 17$	4	1, 3, 4	4	3
$5 \times 17 \times 29$	4	1, 4, 7	3	2
$5 \times 29 \times 73$	4	1, 7, 18	2	1
$7 \times 13 \times 19$	6	1, 2, 3	5	6
$7 \times 13 \times 31$	6	1, 2, 5	3	5
$7 \times 19 \times 67$	6	1, 3, 11	2	3
$7 \times 23 \times 41$	2	3, 11, 20	4	1
$7 \times 31 \times 73$	6	1, 5, 12	3	2
$7 \times 73 \times 103$	6	1, 12, 17	5	1
$13 \times 37 \times 61$	12	1, 3, 5	8	7
$13 \times 37 \times 97$	12	1, 3, 8	5	6
$13 \times 37 \times 241$	12	1, 3, 20	2	5
$13 \times 61 \times 397$	12	1, 5, 33	2	3
$13 \times 97 \times 421$	12	1, 8, 35	3	2
$17 \times 41 \times 233$	8	2, 5, 29	3	4
$17 \times 353 \times 1201$	16	1, 22, 75	5	1
$19 \times 43 \times 409$	6	3, 7, 68	2	3
$19 \times 199 \times 271$	18	1, 11, 15	14	3
$23 \times 199 \times 353$	22	1, 9, 16	13	4
$29 \times 113 \times 1093$	28	1, 4, 39	3	8
$29 \times 197 \times 953$	28	1, 7, 34	6	5
$31 \times 61 \times 211$	30	1, 2, 7	9	20
$31 \times 61 \times 271$	30	1, 2, 9	7	19
$31 \times 61 \times 631$	30	1, 2, 21	3	17
$31 \times 151 \times 1171$	30	1, 5, 39	4	7
$31 \times 181 \times 331$	30	1, 6, 11	17	8
$31 \times 271 \times 601$	30	1, 9, 20	14	5
$31 \times 991 \times 15361$	30	1, 33, 512	2	1
$37 \times 73 \times 109$	36	1, 2, 3	25	31
$37 \times 73 \times 181$	36	1, 2, 5	15	26
$37 \times 73 \times 541$	36	1, 2, 15	5	21
$37 \times 109 \times 2017$	36	1, 3, 56	2	13
$37 \times 613 \times 1621$	36	1, 17, 45	14	3
$41 \times 61 \times 101$	20	2, 3, 5	25	22
$41 \times 73 \times 137$	8	5, 9, 17	22	7
$41 \times 101 \times 461$	20	2, 5, 23	9	10
$41 \times 241 \times 521$	40	1, 6, 13	19	10
$41 \times 241 \times 761$	40	1, 6, 19	13	9
$41 \times 881 \times 12041$	40	1, 22, 301	3	2
$41 \times 1721 \times 35281$	40	1, 43, 882	2	1
$43 \times 127 \times 211$	42	1, 3, 5	26	23
$43 \times 127 \times 1093$	42	1, 3, 26	5	16
$43 \times 127 \times 2731$	42	1, 3, 35	2	15
$43 \times 211 \times 337$	42	1, 5, 8	27	14
$43 \times 211 \times 757$	42	1, 5, 18	12	11
$43 \times 271 \times 5827$	6	7, 45, 971	2	1
$43 \times 433 \times 643$	6	7, 72, 107	29	1
$43 \times 547 \times 673$	42	1, 13, 16	35	6
$43 \times 631 \times 1597$	42	1, 15, 38	17	4
$43 \times 631 \times 13567$	42	1, 15, 323	2	3
$43 \times 3361 \times 3907$	42	1, 80, 93	37	1
$47 \times 1151 \times 1933$	46	1, 25, 42	28	3
$47 \times 3359 \times 6073$	46	1, 73, 132	26	1
$47 \times 3727 \times 5153$	46	1, 81, 112	34	1
$53 \times 79 \times 599$	26	2, 3, 23	7	20
$53 \times 157 \times 521$	52	1, 3, 10	16	23
$53 \times 157 \times 2081$	52	1, 3, 40	4	19
$59 \times 1451 \times 2089$	58	1, 25, 36	41	4
$61 \times 181 \times 1381$	60	1, 3, 23	8	23
$61 \times 181 \times 5521$	60	1, 3, 92	2	21
$61 \times 241 \times 421$	60	1, 4, 7	35	24
$61 \times 271 \times 571$	30	2, 9, 19	29	10
$61 \times 277 \times 2113$	12	5, 23, 176	8	3
$61 \times 421 \times 12841$	60	1, 7, 214	2	9
$61 \times 541 \times 3001$	60	1, 9, 50	11	8
$61 \times 661 \times 2521$	60	1, 11, 42	16	7
$61 \times 1301 \times 19841$	20	3, 65, 992	4	1
$61 \times 3361 \times 4021$	60	1, 56, 67	51	2
$67 \times 331 \times 463$	66	1, 5, 7	48	23
$67 \times 331 \times 7393$	66	1, 5, 112	3	14
$67 \times 2311 \times 51613$	66	1, 35, 782	3	2
$71 \times 271 \times 521$	10	7, 27, 52	37	4
$71 \times 421 \times 491$	70	1, 6, 7	61	22
$71 \times 421 \times 4271$	70	1, 6, 61	7	13
$71 \times 631 \times 701$	70	1, 9, 10	64	15
$71 \times 631 \times 4481$	70	1, 9, 64	10	9
$71 \times 701 \times 5531$	70	1, 10, 79	9	8
$71 \times 911 \times 9241$	70	1, 13, 132	7	6
$73 \times 157 \times 2293$	12	6, 13, 191	5	6
$73 \times 379 \times 523$	18	4, 21, 29	53	6
$73 \times 601 \times 21937$	24	3, 25, 914	2	3
$73 \times 937 \times 13681$	72	1, 13, 190	5	6