Finding Carmichael numbers

G. J. O. JAMESON

Introduction

Recall that Fermat's 'little theorem' says that if p is prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \bmod p$.

This theorem gives a possible way to detect primes, or more exactly, non-primes: if for some positive $a \leqslant n - 1$, a^{n-1} is *not* congruent to 1 mod n, then, by the theorem, n is *not* prime. A lot of composite numbers can indeed be detected by this test, but there are some that evade it. In other words, there are numbers n that are composite but still satisfy $a^{n-1} \equiv 1 \bmod n$ for all a coprime to n. Such numbers might be called 'false primes', but in fact they are called *Carmichael numbers* in honour of R. D. Carmichael, who demonstrated their existence in 1912 [1] – so the year 2012 marks their centenary. (Composite numbers that satisfy the stated condition for one particular a are called *a-pseudoprimes*. They are the subject of a companion article [2].)

It is easy to see that every Carmichael number is odd: if $n (\geqslant 4)$ is even, then $(n-1)^{n-1} \equiv (-1)^{n-1} = -1 \bmod n$, so is not congruent to 1 mod n.

There is a pleasantly simple description of Carmichael numbers, due to Korselt:

Theorem 1: A number n is a Carmichael number if, and only if, $n = p_1 p_2 \dots p_k$, a product of (at least two) distinct primes, and $p_j - 1$ divides $n - 1$ for each j.

Proof ('if' part): Let n be as stated, and let $\gcd(a, n) = 1$. By Fermat's theorem, for each j, we have $a^{p_j - 1} \equiv 1 \bmod p_j$. Since $p_j - 1$ divides $n - 1$, $a^{n-1} \equiv 1 \bmod p_j$. In other words, $a^{n-1} - 1$ is a multiple of each p_j. It follows that it is a multiple of n, so $a^{n-1} \equiv 1 \bmod n$.

We leave out the proof of the converse, that every Carmichael number is of this form. It can be found in many textbooks on number theory, for example [3, section 6].

At this point, some texts simply state that 561 (= 3 × 11 × 17) is a Carmichael number, and invite the reader to verify it. This is indeed easily done using Theorem 1. But how was it found? Is it the first Carmichael number? More generally, how might one detect all the Carmichael numbers up to a certain magnitude N? We will show how this can be done very quickly for $N = 3000$ (this value is chosen because it is just large enough to produce several examples and to illustrate the principles involved; of course, the reader may choose to extend the search). We then go on to show how one can find all the Carmichael numbers of certain types, such as those having three prime factors, with the smallest one given.

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

For numbers within the range considered, these investigations require only minimal numerical calculations, and we hope to convince the reader that they offer an entertaining and instructive piece of detective work, easily carried out with bare hands. Of course, a search up to seriously large numbers has to be a computer exercise, and this has been very efficiently undertaken by Pinch [4, 5]; the methods, greatly refining those used here, are described in [4].

We conclude with a brief account of some recent research topics. For any readers whose interest has been stimulated, further information about Carmichael numbers can be found in [6] and [7].

We record here some easy consequences of Theorem 1 which we shall use constantly.

Lemma: Let $n = pu$, where p is prime. Then $p - 1$ divides $n - 1$ if, and only if, it divides $u - 1$.

Proof: $(n-1)-(u-1) = n-u = pu-u = (p-1)u$. The statement follows.

Proposition 1: A Carmichael number has at least three prime factors.

Proof: Suppose that n has two prime factors: $n = pq$, where p, q are prime and $p > q$. Then $p - 1 > q - 1$, so $p - 1$ does not divide $q - 1$. By the lemma, $p - 1$ does not divide $n - 1$. So n is not a Carmichael number.

Proposition 2: Suppose that n is a Carmichael number and that p and q are prime factors of n. Then q is not congruent to 1 mod p.

Proof: Suppose that $q \equiv 1 \bmod p$, so that p divides $q - 1$. Since $q - 1$ divides $n - 1$, it follows that p divides $n - 1$. But this is not true, since p divides n.

The Carmichael numbers up to 3000

We start by considering numbers with three prime factors: $n = pqr$, with $p < q < r$. By Theorem 1 and the lemma, we have to discover triples (p, q, r) that fit together as follows:

(1) $p - 1$ divides $qr - 1$ (equivalently, $qr \equiv 1 \bmod p - 1$);

(2) $q - 1$ divides $pr - 1$;

(3) $r - 1$ divides $pq - 1$.

Given a pair of primes (p, q) with $p < q$, the following procedure will detect all the primes $r > q$ such that pqr is a Carmichael number. Consider the even divisors (if there are any) d of $pq - 1$ with $q < d < pq - 1$ and check whether $d + 1 (= r)$ is prime (we exclude $d = pq - 1$ since it would give $r = pq$). Then we have ensured (3), and we check whether (1) and (2) hold.

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

We do this for all pairs of primes (p, q) for which $pqr < 3000$ for at least some primes $r > q$. However, because of Proposition 2, we leave out any combination that has $q \equiv 1 \bmod p$ (for example, (3,7), (3,13), (5,11)).

The results are best presented in tabular form, as follows. In each case, we only list the values of d for which r is prime; the reader can easily check that none have been missed.

(p, q)	$pq - 1$	d	r	(1)	(2)	Carmichael number
(3,5)	14	–				
(3,11)	32	16	17	yes	yes	$3 \times 11 \times 17 = 561$
(3,17)	50	–				
(3,23)	68	–				
(5,7)	34	–				
(5,13)	64	16	17	yes	yes	$5 \times 13 \times 17 = 1105$
(5,17)	84	28	29	yes	yes	$5 \times 17 \times 29 = 2465$
		42	43	no		
(5,19)	94	–				
(7,11)	76	–				
(7,13)	90	18	19	yes	yes	$7 \times 13 \times 19 = 1729$
		30	31	yes	yes	$7 \times 13 \times 31 = 2821$
(7,17)	118	–				
(11,13)	142	–				

Note on checking (1) *and* (2): To check whether $qr \equiv 1 \bmod p - 1$, we do not need to calculate qr; all we need is the values of q and r mod $p - 1$. For example, $17 \equiv 1$ and $29 \equiv 1 \bmod 4$, hence $17 \times 29 \equiv 1 \bmod 4$.

It is not hard to check that these really are the only pairs (p, q) that need to be considered: for example, (3,29) cannot occur with 31, and $3 \times 29 \times 37 = 3219$.

What about numbers with four prime factors? The very first candidate, bearing in mind excluded combinations, is $3 \times 5 \times 17 \times 23 = 5865$, well outside our range (of course, this is a bit of an evasion; we come back later for a more resolute look at these numbers).

So the complete list of Carmichael numbers below 3000 is as seen in the table. Note that to show that 561 is the first one, only the cases (3,5), (3,11) and (5,7) are needed.

From now on, we will usually present Carmichael numbers by stating the prime factors without multiplying them out, since it is really the factors themselves that are of interest.

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

Carmichael numbers pqr with given p

What we have been doing is finding the Carmichael numbers of form pqr for a given (p, q). We now establish a much more striking fact: there are only finitely many Carmichael numbers of the form pqr for a given p. Furthermore, we can give an upper bound for the number of them and describe a systematic way of finding them. These results were originated by Beeger [8] and Duparc [9].

We restate the previous (1), (2), (3) more explicitly: $n = pqr$ is a Carmichael number if and only if there are integers h_1, h_2, h_3 such that

$$qr - 1 = h_1(p - 1), \tag{4}$$

$$pr - 1 = h_2(q - 1), \tag{5}$$

$$pq - 1 = h_3(r - 1). \tag{6}$$

The rough size of these numbers is shown by the approximations $h_1 \approx qr/p$, etc., when p, q, r are large.

Proposition 3: We have $2 \leqslant h_3 \leqslant p - 1$.

Proof: Since $r - 1 > q$, we have $qh_3 < pq$, hence $h_3 < p$. Since both are integers, $h_3 \leqslant p - 1$. Also, $h_3 \neq 1$ since $r \neq pq$ (r is prime!). So $h_3 \geqslant 2$.

The essential point is that we can express q and r in terms of p, h_2 and h_3 as follows.

Proposition 4: We have

$$q - 1 = \frac{(p - 1)(p + h_3)}{h_2h_3 - p^2}. \tag{7}$$

Proof: By (5) and (6),

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

so

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

hence

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

Once p, q and h_3 are known, r is determined by (6).

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

Theorem 2: 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

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

Moreover, for any $\varepsilon > 0$, we have $f_3(p) < \varepsilon p \log p$ for sufficiently large p, so in fact

$$\frac{f_3(p)}{p \log p} \to 0 \text{ as} p \to \infty.$$

Proof: Choose h_3 satisfying $2 \leqslant h_3 \leqslant p-1$. Write $h_2h_3 - p^2 = \Delta$. We will work with Δ rather than h_2. When Δ is chosen, q is determined by (7) and then r by (6). By (7),

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

Clearly, Δ is a positive integer, so $\Delta \geqslant 1$. Also, since $p - 1 < q - 1$, we have $\Delta < p + h_3$, so in fact $\Delta \leqslant p + h_3 - 1$, and Δ must lie in an interval of length $p + h_3 - 2$. In addition, Δ must be congruent to $-p^2 \bmod h_3$, so each block of length h_3 contains only one possible value for Δ. Hence the number of choices for Δ is no more than

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

We now sum over the possible values of h_3 and use the well-known fact that $\sum_{h=2}^{p} \frac{1}{h} < \log p$ to obtain

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

The reader is at liberty not to bother with the second half of the proof! For those bothering, the point is that the bounds just found 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 $\tau(n)$ is the number of divisors of n. 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 n (since $(p-1)(p+h_3) < 2p^2$). Using this bound for $h_3 \leqslant p^{1-\varepsilon}$ and the previous one for $h_3 > p^{1-\varepsilon}$, together with the elementary inequality

$$\sum_{y<n\leqslant x} \frac{1}{n} \leqslant \log x - \log y + 1,$$

we see that $f_3(p) \leqslant S_1 + S_2$, where $S_1 = p^{1-\varepsilon}p^{\varepsilon} = p$ and

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

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

so $f_3(p) < \varepsilon p \log p + 4p < 2\varepsilon p \log p$ for large enough p. Of course, we can now replace 2ε by ε.

Note: Using known bounds for the divisor function, the bound can be refined to show that $f_3(p) \leqslant (p \log p)/(\log \log p)$ for large enough p (see [7]). This still makes no allowance for the need for q and r to be prime. Because of the prime number theorem, which says that the number of primes less than N is approximated by $N/\log N$, one might expect these conditions to reduce the bound for $f_3(p)$ by a factor like $(\log p)^2$; however, as far as I know, no such result has been proved.

The proof of Theorem 2 also amounts to a procedure for finding the Carmichael numbers pqr for a given p. We choose h_3, then search for possible values of Δ. They have to satisfy:

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

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

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

For example, when $h_3 = 2$, the second condition restricts Δ to odd values.

We list the values of Δ satisfying these conditions. For each of them, q is defined by $q - 1 = (p-1)(p+h_3)/\Delta$. Of course, q may or may not be prime. If it is, we continue, deriving r from (6). (The r defined this way will always be an integer: by the expression for $h_2(q-1)$ in the proof of Proposition 4, h_3 divides $p(pq-1)$; now, by Euclid's lemma, h_3 divides $pq - 1$). The algebra of Proposition 4, taken in reverse, shows that we have ensured that (5) is satisfied. We still have to check whether r is prime and whether $qr \equiv \bmod (p-1)$: if both these things happen, then pqr is a Carmichael number. Furthermore, this process will detect all Carmichael numbers of the form pqr.

We now work through the cases $p = 3,5,7$. First, take $p = 3$. 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 (6), $2(r-1) = 32$, 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 with $p = 3$.

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	$5 \times 13 \times 17$

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

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

These cases have a success rate that is quite untypical of larger numbers! In fact, even $p = 11$ is very different: there are *no* Carmichael numbers $11qr$. The reader is invited to work through this for himself or herself: there are ten admissible combinations of h_3 and Δ; six cases have q prime, then two have r prime. The remaining combinations fail at the hurdle $qr \equiv 1 \bmod 10$.

At the risk of spoiling the fun, we now list the 3-factor Carmichael numbers pqr for all p up to 61, grouped by p, then ordered by q and r in turn.

3 × 11 × 17

5 × 13 × 17
5 × 17 × 29
5 × 29 × 73

7 × 13 × 19
7 × 13 × 31
7 × 19 × 67
7 × 23 × 41
7 × 31 × 73
7 × 73 × 103

13 × 37 × 61
13 × 37 × 97
13 × 37 × 241
13 × 61 × 397
13 × 97 × 421

17 × 41 × 233
17 × 353 × 1201

19 × 43 × 409
19 × 199 × 271

23 × 199 × 353

29 × 113 × 1093
29 × 197 × 953

31 × 61 × 211
31 × 61 × 271
31 × 61 × 631
31 × 151 × 1171
31 × 181 × 331
31 × 271 × 601
31 × 991 × 15361

37 × 73 × 109
37 × 73 × 181
37 × 73 × 541
37 × 109 × 2017
37 × 613 × 1621

41 × 61 × 101
41 × 73 × 137
41 × 101 × 461
41 × 241 × 521
41 × 241 × 761
41 × 881 × 12041
41 × 1721 × 35281

43 × 127 × 211
43 × 127 × 1093
43 × 127 × 2731
43 × 211 × 337
43 × 211 × 757
43 × 271 × 5827
43 × 433 × 643
43 × 547 × 673
43 × 631 × 1597
43 × 631 × 13567
43 × 3361 × 3907

47 × 1151 × 1933
47 × 3359 × 6073
47 × 3727 × 5153

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

53 × 79 × 599
53 × 157 × 521
53 × 157 × 2081

59 × 1451 × 2089

61 × 181 × 1381
61 × 181 × 5521
61 × 241 × 421
61 × 271 × 571
61 × 277 × 2113

61 × 421 × 12841
61 × 541 × 3001
61 × 661 × 2521
61 × 1301 × 19841
61 × 3361 × 4021

Remark: 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 $pr - 1 = (p - 1)r + (r - 1)$. It is very common for Carmichael numbers to have this property, at least in the early stages: of the 69 numbers listed above, 57 have it. The same comment applies to the q and r generated by the process we have described.

Another consequence of Proposition 4 is that we can give bounds for q, r and n in terms of p:

Proposition 5: If pqr is a Carmichael number, with $p < q < r$, then

$$q < 2p(p-1), \qquad r < p^2(p-1), \qquad n < 2p^4(p-1)^2 \;\left(< 2p^6\right).$$

Proof: By (7) and the fact that $h_3 \leqslant p - 1$, we have

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

Now by (6),

$$r = \frac{1}{h_3}(pq-1) + 1 \leqslant \frac{1}{2}(pq-1) + 1 = \frac{1}{2}(pq+1) < p^2(p-1) + \frac{1}{2},$$

so in fact $r < p^2(p - 1)$ (equality doesn't occur, since r is prime!). Hence $n = pqr < 2p^4(p-1)^2$.

With a bit more care, one can improve these bounds to $r < \frac{1}{2}p^2(p+1)$ and $n < \frac{1}{2}p^4(p+1)^2$, which are close to being optimal (see [7]).

Carmichael numbers pqr with given r

Now let us vary the problem and ask how one might find all the Carmichael numbers pqr for a given r (of course, the results for all $r \leqslant 71$ could be read off from our list, but that would really be cheating!). A very different method is appropriate. Because of Proposition 2, we only need to consider primes $p < r$ that do not divide $r - 1$. For such p, (3) demands q such that $pq \equiv 1 \bmod (r-1)$. By elementary number theory, there is exactly one integer $q < r - 1$ that satisfies this, found either by applying the Euclidean algorithm to obtain an expression $xp + y(r-1) = 1$ or (more quickly when the numbers are small) by simply trying the numbers $k(r-1) + 1$ ($k = 1,2, \ldots$) in turn until a multiple of p is found. If q is prime and different from p, we now check whether (1) and (2) are satisfied. We do this for successive p, but of course leave out any prime that has already appeared as the q corresponding to an earlier p. We set out the result for the case $r = 19$:

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

p	q	(1)	(2)	Carmichael number
5	11	yes	no	
7	13	yes	yes	$7 \times 13 \times 19$
17	17			

Four prime factors

Now consider numbers with four prime factors: $n = pqrs$, with $p < q < r < s$. The requirements are now: $p - 1$ divides $qrs - 1$ and three similar conditions. The analogy with the first problem we considered for 3-factor numbers is: given (p, q, r) find the $s\,(> r)$ such that $pqrs$ is a Carmichael number. To solve this, observe that $s - 1$ must be a divisor of $pqr - 1$ and s must satisfy the three other congruence conditions. We identify the numbers s that satisfy all these conditions, and check whether they are prime. We work through two examples.

Example: $(p, q, r) = (7,11,13)$. Then $pqr = 1001$, so $s - 1$ must be a divisor of 1000. The congruence condition for 6 will be implied by the one for 12, so we can leave it out. The other two are:

$7 \times 13 \times s \equiv 1 \bmod 10$; since $7 \times 13 = 91 \equiv 1 \bmod 10$, this is equivalent to $s \equiv 1 \bmod 10$;

$7 \times 11 \times s \equiv 1 \bmod 12$; since $77 \equiv 5 \bmod 12$, this is equivalent to $5s \equiv 1 \bmod 12$, hence to $s \equiv 5 \bmod 12$.

This pair of conditions is equivalent to $s \equiv 41 \bmod 60$ (found by considering 5, 17, 29, 41 until we find a number congruent to 1 mod 10). So $s - 1$ is congruent to 40 mod 60 and a divisor of 1000. The only numbers satisfying this are 40 and 100. Since 41 and 101 are prime, these two values of s are the solution to our problem. (In fact, $7 \times 11 \times 13 \times 41 = 41\,041$ is the smallest 4-factor Carmichael number.)

If pqr is itself a Carmichael number, then the congruence conditions equate to s being congruent to 1 mod $p - 1$, $q - 1$ and $r - 1$, since (for example) $qr \equiv 1 \bmod (p - 1)$.

Example: $(p, q, r) = (7,13,19)$ (a particularly rewarding example). By the previous remark, s is congruent to 1 mod 6, 12 and 18, hence congruent to 1 mod 36. Also, $s - 1$ must divide $pqr = 1729 - 1 = 48 \times 36$. So the possible values for s are of the form $36k + 1$, where k is a divisor of 48. We list these values, indicating by * those that are prime, thereby giving a Carmichael number:

$$37^*,\ 73^*,\ 109^*,\ 145,\ 217,\ 289,\ 433^*,\ 577^*,\ 865.$$

Now for the second problem, to find the Carmichael numbers $pqrs$ for given (p, q). All we have to do is substitute pq for p in our previous reasoning. It doesn't make any difference that pq is not prime until the final step, where of course the congruences for $p - 1$ and $q - 1$ must be checked separately. We define h_4 by $h_4(s - 1) = pqr - 1$, from which it follows that

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

$2 \leqslant h_4 \leqslant pq - 1$. Clearly, h_4 cannot be a multiple of p or q. Nor can it be congruent to 1 mod p (or q), since then s would be a multiple of p (or q). Proposition 4 becomes $r - 1 = (pq - 1)(pq + h_4) / \Delta$, where $\Delta = h_3 h_4 - p^2 q^2$, so that

$$\Delta = \frac{(pq - 1)(pq + h_4)}{r - 1} < p(pq + h_4).$$

Of course, Δ also has to divide $(pq - 1)(pq + h_4)$. This limits the number of possible values for it to $(pq)^{\varepsilon}$ (for any given $\varepsilon > 0$) for large enough pq, so the number of Carmichael numbers of this form is bounded by $(pq)^{1+\varepsilon}$.

The reader may care to work through the first case, $(p, q) = (3, 5)$. By the remarks above, the only relevant values of h_4 are 2, 8, 14. Also, because of the exclusions given by Proposition 4, the smallest possible value for r is 17, so in fact $\Delta < 15 + h_4$. You should discover quite quickly that there is only one resulting Carmichael number, $3 \times 53 \times 47 \times 89$.

How many Carmichael numbers?

There are just 43 Carmichael numbers up to 10^6, whereas there are 78 498 primes – so the original idea of using the Fermat property to detect primes is not so bad after all! As mentioned above, Pinch [4, 5] has computed the Carmichael numbers up to 10^{18} (more recently, even to 10^{21}). Some of his results are as follows. Here, $C(x)$ denotes the number of Carmichael numbers up to x, and $C_3(x)$ the number with three prime factors.

x	10^6	10^7	10^8	10^{19}	101^{12}	10^{15}	10^{18}
$C(x)$	43	105	255	646	8 241	105 212	1 401 644
$C_3(x)$	23	47	84	172	1 000	6 083	35 586

It was an unsolved problem for many years whether there are infinitely many Carmichael numbers. The question was resolved in 1994 in a classic article by Alford, Granville and Pomerance [10]. Here it was shown, using sophisticated methods, not only that the answer is yes, but that in fact $C(x) > x^{2/7}$ for sufficiently large x. Harman [11] has improved the $\frac{2}{7}$ to 0.33.

There is a very wide gap between these estimates and the known *upper* bounds for $C(x)$. These involve the following rather unwieldy expressions: write $\log_2(x) = \log\log x$, etc., and $l(x) = \exp(\log x \log_3 x / \log_2 x)$. Erdős [12] obtained the upper bound $x / l(x)^{1-\varepsilon}$ for some $c > \frac{1}{2}$, valid for large enough x. It was improved to $x / l(x)^{1-\varepsilon}$ in [13]. Erdős conjectured (with reasons) that $C(x)$ is *not* bounded above by x^{a} for any $\alpha < 1$. This is a very bold conjecture in view of the computed values (Pinch's largest figure is only slightly more than $x^{1/3}$), but it is still regarded as a serious possibility. The question is discussed in depth in [14].

For 3-factor Carmichael numbers, the situation is just the reverse. As yet, nobody has come near to proving that there are infinitely many of them, though this seems compellingly likely in view of Pinch's calculations. One approach to this problem is deceptively enticing. Suppose, for some n, that

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

$p = 6n + 1$, $q = 12n + 1$ and $r = 18n + 1$ are all prime. It is easily verified that (1), (2) and (3) hold, for example

$$(6n + 1)(12n + 1) = 72n^2 + 18n + 1 \equiv 1 \bmod 18n.$$

So pqr is a Carmichael number. This occurs, for example, for $n = 1$ and $n = 6$. Are there infinitely many values of n for which it occurs? Unfortunately, this question is unsolved: it is a typical example of a whole family of questions about prime numbers that sound simple but stoutly resist solution.

In contrast, a lot of progress has been made on upper bounds. We remark first that the estimation $C_3(x) \leqslant Cx^{2/3}$ (for some constant C) follows easily from our Theorem 2, together with Chebyshev's well-known estimate for prime numbers, which states the following: let $P(x)$ denote the set of primes not greater than x, and let $\theta(x) = \sum_{p \in P(x)} \log p$. Then $\theta(x) \leqslant cx$ for all x, where c is a constant not greater than $\log 4$. If $n = pqr \leqslant x$, then $p < x^{1/3}$, so by Theorem 2 (in the form $f_3(p) \leqslant 2p \log p$), we have

$$C_3(x) \leqslant \sum_{p \in P(x^{1/3})} 2p \log p \leqslant 2x^{1/3}\theta\left(x^{1/3}\right) \leqslant 2cx^{2/3}.$$

However, much stronger results are known. Following methods developed in [15], it was shown in [16] that, for any $\varepsilon > 0$, $C_3(x) < x^{5/14} + \varepsilon$ for large enough x, and the $\frac{5}{14}$ has been further reduced to $\frac{7}{20}$ in [17]. In [14], it is conjectured, with heuristic reasoning, that the true bound is $Kx^{1/3}/(\log x)^3$ for a certain specified K.

The starting point for all these methods is to consider the gcd g of $p - 1, q - 1$ and $r - 1$ and to write

$$p - 1 = ag, \qquad q - 1 = bg, \qquad r - 1 = cg.$$

There is an intricate algebra relating these quantities and the h_j, and one finds, for example, that there are only finitely many 3-factor Carmichael numbers with a given value of g. A gentle exposition of these results can be seen in [7].

References

1. R. D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, *American Math. Monthly* **19** (1912), pp. 22-27.

2. G. J. O. Jameson, Finding pseudoprimes (to appear in a future *Gazette*).

3. G. A. Jones and J. M. Jones, *Elementary number theory*, Springer (1998).

4. R. G. E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comp.* **61** (1993) pp. 381-391.

5 R. G. E. Pinch, The Carmichael numbers up to 10^{18}, at
www.chalcedon.demon.co.uk/rgep/carpsp.html

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press

6. P. Ribenboim, *The new book of prime number records*, Springer (1995).

7. G. J. O. Jameson, Carmichael numbers with three prime factors, at www.maths.lancs.ac.uk/~jameson

8. 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) pp. 133-135.

9. H. J. A. Duparc, On Carmichael numbers, *Simon Stevin* **29** (1952) pp. 21-24.

10. W. R. Alford, Andrew Granville and Carl Pomerance, There are infinitely many Carmichael numbers, *Annals of Math.* **140** (1994) pp. 703-722.

11. Glyn Harman, On the number of Carmichael numbers up to x, *Bull. London Math. Soc.* **37** (2005) pp. 641-650.

12. P. Erdős, On pseudoprimes and Carmichael numbers, *Pub. Math. Debrecen* **4** (1956) pp. 200-206.

13. 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) pp. 135-161.

14. Andrew Granville and Carl Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (2001) pp. 883-908.

15. I. Damgård, P. Landrock and C. Pomerance, Average case error estimates for the strong probable prime test, *Math. Comp.* **61** (1993) pp. 177-194.

16. R. Balasubramanian and S. V. Nagaraj, Density of Carmichael numbers with three prime factors, *Math. Comp.* **66** (1997) pp. 1705-1708.

17. D. R. Heath-Brown, Carmichael numbers with three prime factors, *Hardy-Ramanujan J.* **30** (2007) pp. 6-12.

G. J. O. JAMESON

Dept. of Mathematics and Statistics, Lancaster University, Lancaster LA1 4YF

e-mail: *g.jameson@lancaster.ac.uk*

https://doi.org/10.1017/S0025557200002965 Published online by Cambridge University Press