Carmichael Numbers

Carl Pomerance[1]
Department of Mathematics, University of Georgia,
Athens, Georgia 30602, U.S.A.

This is an elaborated version of the *Beeger Lecture* (see: Mededelingen van het Wiskundig Genootschap, januari 1992, pp. 3-4), which was delivered by the author on April 22, 1992, during the 28th Nederlands Mathematisch Congres in Delft.

1. Introduction

Early in 1992, W. R. 'Red' Alford, Andrew Granville and I [2] proved that there are infinitely many Carmichael numbers. These are composite integers n for which $a^n \equiv a \bmod n$ for every integer a. It had long been conjectured that there are indeed infinitely many of these integers n, but the problem had remained open for most of this century. (Carmichael gave the first examples in 1910.) In this paper we shall discuss this new theorem and several other results concerning Carmichael numbers.

2. Fermat's 'little theorem'

Part of the basic landscape of elementary number theory is the 'little theorem' of Fermat, which asserts that $a^p \equiv a \bmod p$ for all integers a and all primes p. There are many simple proofs; here is one of them. For a given prime p, it is only necessary to verify the congruence for $a = 0, 1, \ldots, p-1$. It is trivially true for $a = 0$, and the truth for the remaining values of a now follows by induction from the identity $(a+1)^p \equiv a^p + 1 \bmod p$. This identity looks like a poor student's mistaken version of the binomial theorem, but the coefficients of the missing terms are each divisible by p, thus justifying the student's 'mistake'.

Fermat's little theorem is not an isolated mathematical curiosity. To the contrary, it has been generalized by Euler and Lagrange and in the latter form it now stands as perhaps the first example of a nontrivial consequence of the axioms of group theory.

From Fermat's little theorem one easily sees that if p is prime and a is an integer, then $a^{2p-1} \equiv a^p a^{p-1} \equiv a a^{p-1} \equiv a^p \equiv a \bmod p$, and similarly $a^k \equiv a \bmod p$ for every positive integer k with $k-1$ divisible by $p-1$. Suppose

[1]Supported in part by an NSF grant

p, q are distinct primes and k is a positive integer with $k-1$ divisible by both $p-1$ and $q-1$. Then $a^k \equiv a \bmod pq$ for every integer a. This identity is the backbone of the RSA cryptosystem, a very practical application of Fermat's little theorem, see [21].

How easy is it to verify Fermat's little theorem numerically? For small values of a and p this is of course very easy. Take $a = 2$, $p = 5$, for example. We have $2^5 = 32$ and clearly $32 \equiv 2 \bmod 5$. It is less obvious that this is relatively easy to compute for larger numbers, but nevertheless true. Let us check the Fermat congruence for $a = 3$ and $p = 161$. We do not want to actually compute the power 3^{161} nor do we have to, since we are only interested in its residue mod 161. Further we can reach high powers of 3 mod 161 by successive squaring:

$$3^2 \equiv 9 \bmod 161, 3^4 \equiv 81 \equiv -80 \bmod 161, 3^8 \equiv -40 \bmod 161,$$

$$3^{16} \equiv -10 \bmod 161, 3^{32} \equiv -61 \bmod 161, 3^{64} \equiv 18 \bmod 161, 3^{128} \equiv 2 \bmod 161.$$

Since $161 = 128 + 32 + 1$ (every positive integer can of course be written as a sum of distinct powers of 2, since it can be written in binary), we have

$$\begin{aligned} 3^{161} \equiv 3^{128+32+1} \equiv 3^{128}3^{32}3 &\equiv (2)(-61)(3) \bmod 161 \\ &\equiv (39)(3) \bmod 161 \\ &\equiv -44 \bmod 161. \end{aligned}$$

Whoops! Have we made an error and shouldn't the result be 3? No, there is no error, but why doesn't Fermat's little theorem apply here? It is because, as the reader probably already knows, 161 is not prime; it is $7 \cdot 23$.

This example illustrates one of the principal modern applications of Fermat's little theorem. Namely if you are presented with a large integer n and if for some integer a you see that $a^n \not\equiv a \bmod n$, then you have discovered that n is composite. It is interesting that this proof of compositeness appears to reveal nothing about the prime factorization of n.

I invite the reader to try another example – this time to compute the residue of 2^{341} mod 341. If you do it correctly you will get the answer 2. What can be concluded and in particular have we proved that 341 is prime? It is reported in L. E. Dickson's 'History of the Theory of Numbers that Leibniz would have answered 'yes'. That is, he believed that if $2^n \equiv 2 \bmod n$ and n is an integer larger than 1, then n is prime. However, 341 is $11 \cdot 31$, so Leibniz was wrong.

A composite integer n for which $a^n \equiv a \bmod n$ is called a pseudoprime to the base a. It was proved in 1903 by Malo that there are infinitely many pseudoprimes to the base 2, and Cipolla did the same for every base a in the same year. Here is Cipolla's proof for $a = 2$. If p is a prime with $p \geq 5$, then $n = (4^p - 1)/3$ is a pseudoprime base 2. Indeed, n is the product of $2^p - 1$ and $(2^p + 1)/3$, so that n is composite. In addition, by Fermat's little theorem, $p \mid n - 1$. Since also $2 \mid n - 1$ we have $2p \mid n - 1$, so that $2^{2p} - 1 \mid 2^{n-1} - 1$. But $2^{2p} - 1 = 3n$, hence $n \mid 2^{n-1} - 1$, which implies that n is a pseudoprime to the base 2.

3. KORSELT'S CRITERION

One can still wonder though if the converse of Fermat's little theorem might be true. That is, if n is an integer exceeding 1 with $a^n \equiv a \bmod n$ for all integers a, must n be prime?

In 1899, KORSELT [15] gave an equivalent criterion for such an integer. Namely, a positive integer n satisfies $a^n \equiv a \bmod n$ for all integers a if and only if n is squarefree and $p-1 \mid n-1$ for every prime $p \mid n$. However Korselt left open the question of whether any composite numbers n satisfy this criterion.

It is very easy to prove Korselt's criterion. Suppose $a^n \equiv a \bmod n$ for every integer a. We first prove n must be squarefree. Suppose not and $k^2 \mid n$ for some integer $k > 1$. We let $a = k$, so that $k^n \equiv k \bmod n$. Since $k^2 \mid n$, this congruence is true mod k^2, so that $k^n \equiv k \bmod k^2$ which contradicts $k^n \equiv 0 \bmod k^2$. Thus n is squarefree. Suppose p is a prime dividing n. It is well known that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of residues mod p relatively prime to p is a cyclic group of order $p-1$; this is the so-called theorem on the primitive root. Suppose a is an integer such that $a \bmod p$ is a cyclic generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Since $a^n \equiv a \bmod n$, we have $a^n \equiv a \bmod p$, and since a and p are coprime, we have $a^{n-1} \equiv 1 \bmod p$. Since the order of $a \bmod p$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is $p-1$, we have $p-1 \mid n-1$. This proves one-half of Korselt's criterion.

For the other half, assume n is squarefree and $p-1 \mid n-1$ for every prime $p \mid n$. Suppose p is some prime dividing n and a is an integer. As remarked above, $a^k \equiv a \bmod p$ for any positive integer k with $p-1 | k-1$ and so in particular for $k = n$. Thus we have shown that $a^n - a$ is divisible by every prime factor of n and since n is squarefree it follows that $a^n - a$ is divisible by n. Thus Korselt's criterion is proved.

In 1910, CARMICHAEL [6] discovered a criterion essentially equivalent to Korselt's criterion and actually gave some examples of composite numbers n which satisfy it. The first example is $n = 561$ and indeed it is easy to check that 561 has the prime factorization $3 \cdot 11 \cdot 17$ and that 560 is divisible by each of $2, 10$ and 16. Thus the converse of Fermat's little theorem is not true, since 561 is a counter-example. We now call such counter-examples 'Carmichael numbers' after Carmichael, of course. It is curious that Korselt apparently overlooked this simple example; otherwise we might call them 'Korselt numbers'.

4. CHERNICK'S THEOREM AND THE PRIME k-TUPLES CONJECTURE

Perhaps the converse of Fermat's little theorem is 'almost true' and there are only finitely many Carmichael numbers. In 1939, CHERNICK [7] showed that if $6m+1$, $12m+1$, $18m+1$ are all prime for the same positive integral value of m, then the product of these three primes is a Carmichael number. For example, when $m = 1$ we have the primes $7, 13$ and 19, so Chernick claims that $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number, and indeed it is.

We leave it to the reader to supply the simple argument that the numbers described by Chernick satisfy Korselt's criterion.

One consequence of the prime k-tuples conjecture in analytic number theory is that there are infinitely many integers m such that $6m+1$, $12m+1$, $18m+1$ are simultaneously prime. Thus this conjecture and Chernick's theorem imply

there are infinitely many Carmichael numbers. Although Carmichael himself suggested this was true in 1912, Chernick gave perhaps the first 'evidence' for this.

Maybe the reader has already heard of the prime k-tuples conjecture. This asserts that if a_i, b_i are integers with $a_i > 0$ for $i = 1, 2, \ldots, k$ and if the number of solutions of

$$(a_1x + b_1)(a_2x + b_2)\ldots(a_kx + b_k) \equiv 0 \bmod p$$

is less than p for every prime p, then there are infinitely many integers m such that $a_1m + b_1$, $a_2m + b_2, \ldots, a_km + b_k$ are all prime numbers. It is easy to check that

$$(6x + 1)(12x + 1)(18x + 1) \equiv 0 \bmod p$$

has no solutions if $p = 2$ or 3 and of course for $p > 3$ it has at most 3, which is less than p, solutions. Thus the prime k-tuples conjecture implies that Chernick's hypothesis holds infinitely often and so there are infinitely many Carmichael numbers.

However, the prime k-tuples conjecture is a notorious unsolved problem. It is a generalization of the prime twins conjecture, which is the case of the two linear expressions x and $x + 2$. Although Chernick's theorem lent credence to the conjecture that there are infinitely many Carmichael numbers, it did not seem like a promising line of attack.

5. The theorems of Beeger and Duparc

In 1950, N. G. W. H. Beeger [4] proved that if $p < q < r$ are primes and pqr is a Carmichael number, then $q < 2p^2$ and $r < p^3$. Thus there are only finitely many Carmichael numbers with three prime factors with one of these primes given. Duparc [9] later generalized this result to show that if $n = mqr$ is a Carmichael number where q, r are primes, then $q < 2m^2$ and $r < m^3$. Thus there are only finitely many Carmichael numbers if all but two prime factors are fixed. The case $m = 1$ shows that every Carmichael number has at least three prime factors, a result first shown by Carmichael himself in [6].

Here is a proof of Duparc's theorem. Suppose $n = mqr$ is a Carmichael number where $q < r$ are primes. Then

$$1 \equiv n = mqr \equiv mq \bmod (r - 1), \quad 1 \equiv n \equiv mr \bmod (q - 1),$$

so that

$$C := \frac{mq - 1}{r - 1}, \quad D := \frac{mr - 1}{q - 1}$$

are integers with $1 \le C < m < D$. We have

$$D(q - 1) = mr - 1 = m\left(\frac{mq - 1}{C} + 1\right) - 1,$$

so that

$$CD(q - 1) = m^2q - m + mC - C.$$

We conclude that

$$(CD - m^2)(q-1) = m^2 - m + mC - C = (m+C)(m-1) > 0.$$

Thus

$$q - 1 \le (m+C)(m-1) < m^2 + (C-1)m, \tag{1}$$

which with $C < m$ proves that $q < 2m^2$. But from (1),

$$r - 1 = \frac{mq-1}{C} < \frac{m^3 + (C-1)m^2}{C} \le m^3,$$

so that $r < m^3$. This concludes the proof of Duparc's theorem.

Duparc's theorem was recently used by Pinch [17] in his calculation of all of the Carmichael numbers up to 10^{15}. In case you are curious, Pinch found there are 105,212 Carmichael numbers up to this point.

Can one show that there are only finitely many Carmichael numbers if all but three prime factors are fixed? Probably not, for this would imply that there are only finitely many Carmichael numbers with just three prime factors and as we have seen, this would contradict the prime k-tuples conjecture.

6. The Erdős heuristic and the Erdős theorem

Let $C(x)$ denote the number of Carmichael numbers n with $n \le x$. In 1956, Erdős [11] published a proof of the theorem

$$C(x) \le x^{1 - c \log\log\log x / \log\log x}$$

for some positive constant c and all sufficiently large x. This upper bound on the one hand is a *small* function of x since it is eventually smaller than $x/(\log x)^k$ for any fixed k. On the other hand, it is a *large* function of x since it is eventually larger than $x^{1-\epsilon}$ for any fixed $\epsilon > 0$.

Could it really be that $C(x) > x^{1-\epsilon}$ for all large x? In the same paper, Erdős gave a heuristic argument for this seemingly implausible assertion. In particular, this gave another heuristic argument, completely different than Chernick's, for the infinitude of the set of Carmichael numbers.

Erdős's heuristic went sort of like this. Suppose L is the least common multiple of the integers $1, 2, 3, \ldots, m$, where m is some large integer. Let $\mathcal{P}$ denote the set of primes p with $p > m$ and $p - 1 \mid L$. Erdős first assumed that $\mathcal{P}$ is very large, that is, L has many divisors of the form $p - 1$. Now suppose n is the product of the primes in some subset of $\mathcal{P}$ with cardinality greater than 1. If $n \equiv 1 \bmod L$, then n is a Carmichael number. Indeed n is composite, squarefree, and if p is a prime factor of n, then $p \in \mathcal{P}$, so that $p - 1 \mid L$, so that $p - 1 \mid n - 1$. That is, n satisfies Korselt's criterion and is therefore a Carmichael number.

How many such numbers n are there? In other words, how many subsets of $\mathcal{P}$ have their product being 1 mod L? Well if we say the "probability" that a random subset of $\mathcal{P}$ has product 1 mod L is about $1/L$ or greater (it should

be greater since all such products are already known to be coprime to L), then there should be about $2^{|\mathcal{P}|}/L$ or more Carmichael numbers created in this way. Indeed, $\mathcal{P}$ has $2^{|\mathcal{P}|}$ subsets in all, so that at least $2^{|\mathcal{P}|}/L$ of them should have this special property.

In particular, it is not unreasonable to assume that $|\mathcal{P}| > 2^{(1-\epsilon)\log L/\log\log L}$ (since L has about $2^{\log L/\log\log L}$ divisors in all, and the "probability" that a divisor is 1 less than a prime should be at least $1/\log L$). Thus Erdős would have us believe that there are at least $2^{2^{(1-2\epsilon)\log L/\log\log L}}$ Carmichael numbers composed only of primes p with $p-1 \mid L$.

By refusing to use the larger primes $p \in \mathcal{P}$, Erdős was able further to quantify this argument to get $C(x) > x^{1-\epsilon}$. In [19], [20], [22], Erdős's argument was further refined to give for any $\epsilon > 0$, numbers $x_0(\epsilon)$ and $x_1(\epsilon)$ with

$$C(x) \le x^{1-(1-\epsilon)\log\log\log x/\log\log x} \quad \text{for all} \quad x \ge x_0(\epsilon)$$

unconditionally and

$$C(x) \ge x^{1-(1+\epsilon)\log\log\log x/\log\log x} \quad \text{for all} \quad x \ge x_1(\epsilon)$$

heuristically. That is, there should be a "Carmichael number theorem" that

$$C(x) = x^{1-(1+o(1))\log\log\log x/\log\log x} \quad \text{for} \quad x \to \infty.$$

We are half done with the proof, but probably this is the easy half!

7. Connections to combinatorial group theory

Let us examine the second heuristic assumption of Erdős more closely. Let $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$, so that the p_i's are the primes with $p_i - 1 \mid L$ and $p_i \nmid L$. We may view $\mathcal{P}$ as a sequence of (distinct) elements in the group $(\mathbb{Z}/L\mathbb{Z})^*$ of reduced residues modulo L. We would like to assert that there is a subsequence of this sequence whose product is the group identity 1 mod L. In fact we would like to assert there are many such subsequences.

One can ask more generally when a given sequence $g_1, \ldots, g_k$ of elements in a finite group G has a "null subsequence", that is, a nonempty subsequence with product the identity of G. In particular, how large must k be to *guarantee* the existence of a null subsequence?

It is easy to see that if $k \ge |G|$ (where $|G|$ denotes the order of G), then there must be a null subsequence in $g_1, \ldots, g_k$. Indeed, if not, then there are only $|G| - 1$ possible values for the $k \ge |G|$ products $g_1, g_1g_2, \ldots, g_1g_2\cdots g_k$, and so two of them must be equal. Say $g_1g_2\cdots g_i = g_1g_2\cdots g_j$ where $i < j$. But then $g_{i+1}, \ldots, g_j$ is a null subsequence.

If G is cyclic, then this estimate cannot be improved. Indeed for $G = \langle g \rangle$, a sequence consisting of $|G| - 1$ copies of g has no null subsequence.

Let us define by $n(G)$ the length of the longest sequence of elements of G which contains no null subsequence. Thus for a finite cyclic group G we have $n(G) = |G| - 1$.

In the late 1960's Kruyswijk (see [3]) and Olson [16] independently obtained an exact formula for $n(G)$ when G is a finite abelian p-group. They proved that if $G \cong (\mathbb{Z}/p^{\alpha_1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p^{\alpha_t}\mathbb{Z})$, then $n(G) = p^{\alpha_1} + \ldots + p^{\alpha_t} - t$.

So far no one has been able to find a general formula for $n(G)$, not even for the case of G abelian, but VAN EMDE BOAS and KRUYSWIJK [10] were able to find a beautiful inequality for this case. They showed that if G is a finite abelian group, then

$$n(G) \le \lambda(G) \log |G|,$$

where $\lambda(G)$ denotes the maximal order of an element of G (that is, the order of the largest cyclic subgroup of G).

Let us try to apply the van Emde Boas–Kruyswijk inequality to the group G of the last section. Recall that L is the least common multiple of $1, 2, \dots, m$ and $G = (\mathbb{Z}/L\mathbb{Z})^*$. We have $|G| = \varphi(L)$ where φ is Euler's function. What can we say about $\lambda(G)$? Well this is either the least common multiple of $\{\varphi(q) : q \le m,$ q is a prime or a power of a prime$\}$ or is one-half of this least common multiple. It is an interesting and fairly difficult problem to estimate $\lambda(G)$, but it is almost certainly true that $\lambda(G)$ is about $\exp(m \log\log m / \log m)$. (Using some "big guns" from analytic number theory one can show $\lambda(G) \ge e^{m^{2/3}}$ for all large m, but we cannot prove much more.) If $\lambda(G)$ is really as large as we think it is, then we have no hope to use combinatorial group theory to force the existence of a null subsequence of $p_1, p_2, \dots, p_k$. Indeed, these are the primes p with $p - 1 \mid L$, $p \nmid L$. There cannot be more such primes than L has divisors, and the number of divisors of L is about $2^{\log L / \log\log L}$, which is about $\exp(cm/\log m)$, with $c = \log 2$. Thus we are too short by a factor $\log\log m$ in the exponent. (We cannot even exploit the fact that $p_1, p_2, \dots, p_k$ is a sequence of *distinct* group elements, since it is easy to show that every nontrivial finite group G has a sequence of at least $[\sqrt{\lambda(G)}]$ distinct group elements with no null subsequence.)

Obviously I wouldn't have brought up this issue of combinatorial group theory if it was not to be of help. Can the reader spot an idea?

8. A NEW IDEA

It is clear that $G = (\mathbb{Z}/L\mathbb{Z})^*$, with L the least common multiple of the integers up to m, is just the wrong group to use, since the value of $\lambda(G)$ is just too large (in all likelihood). We would like to replace L with some integer N, say, where for $G = (\mathbb{Z}/N\mathbb{Z})^*$ we have $\lambda(G)$ being a fairly small function of N. Let us abbreviate the more complicated expression $\lambda((\mathbb{Z}/N\mathbb{Z})^*)$ by just $\lambda(N)$, which is the usual notation used.

What is known about the order of magnitude of the arithmetic function $\lambda(N)$ and how it compares to $\tau(N)$ the number of divisors of N? It is shown in [12] that the average order of $\lambda(N)$ is a little larger than $N/\log N$ and that the normal order of $\lambda(N)$ (what is true for most values of N) is about $N/(\log N)^{\log\log\log N}$. On the other hand, it is well-known that $\tau(N)$ on average is about $\log N$ and is normally about $(\log N)^{\log 2}$. So average or normal values of N will be of no help, since for these values of N we have $\lambda(N)$ much bigger than $\tau(N)$.

Might it be true that there are *no* large values of N with $\lambda(N) < \tau(N)$? Well occasionally $\lambda(N)$ is fairly small. It was shown in [1], [12] that there are infinitely many N with $\lambda(N) < (\log N)^{c \log\log\log N}$ for some positive constant

c. On the other hand it is a classical theorem that the maximal order of $\tau(N)$ is about $2^{\log N/\log\log N}$. So the minimal order of $\lambda(N)$ is actually quite a bit *smaller* than the maximal order of $\tau(N)$, so there is still a glimmer of hope.

Suppose we take L as before, namely the least common multiple of the integers up to m, and we let N be the product of the primes $p < m^2$ with $p-1 \mid L$. It is possible to show using the tools of analytic number theory (for example, see [18]) that the primes $p < m^2$ with $p-1 \mid L$ comprise at least a certain fixed positive proportion of all of the primes $p < m^2$ as $m \to \infty$. Thus N has at least $c_1 m^2/\log m$ distinct prime factors for some positive constant c_1, and so $\tau(N) > 2^{c_1 m^2/\log m}$. Well, what can we say about $\lambda(N)$? Since every prime $p \mid N$ has $p-1 \mid L$, we also have $\lambda(N) \mid L$. Since L is about e^m, we have that $\lambda(N)$ is at most about e^m and this is enormously smaller than $2^{c_1 m^2/\log m}$. We did it! We found an infinite set of numbers N with $\lambda(N)$ much smaller than $\tau(N)$.

But we are not out of the woods yet. It is not really $\tau(N)$ that interests us, but rather the number of divisors of N which are 1 less than a prime. Can we show this is almost as big as $\tau(N)$? This is close to Erdős's first heuristic assumption and it is a hurdle standing squarely in our path.

9. There are infinitely many Carmichael numbers

Early in 1992, W. R. "Red" Alford, Andrew Granville and I found a way to get over this last hurdle.

The proof in [1], [12] that $\lambda(N) < (\log N)^{c \log\log\log N}$ infinitely often, strongly uses a much earlier result of Prachar [23]. What Prachar did was show the existence of integers M with a great number of divisors of the form $p-1$, with p prime. Then (as in the last section), the product of these primes p is a large number N with $\lambda(N)$ small, since $\lambda(N) \mid M$.

Of course the trouble with existence proofs is that they just assert that somewhere there is an example. The particular number N that you hold dear, even if by all rights it "should be" an example, very well may not be.

What Alford, Granville and I were able to do was modify Prachar's proof to show that if N is the number of the last section (so that N is the product of the primes $p < m^2$ such that $p-1$ divides the least common multiple of the integers up to m), then there is some number k coprime to N such that kN has at least $\tau(N)^{c_2}$ divisors of the form $p-1$ with p prime, $p \nmid N$ and $p \equiv 1 \bmod k$. Here c_2 is some absolute positive constant and the above assertion holds for all sufficiently large values of the parameter m.

Let us see if the van Emde Boas–Kruyswijk inequality is now of use to us. Let G be the subgroup of $(\mathbb{Z}/(kN\mathbb{Z}))^*$ consisting of those residues congruent to 1 mod k. Then from the above paragraph, we have a set of $\tau(N)^{c_2}$ elements in the group G. From the last section we see that

$$\tau(N)^{c_2} > 2^{c_1 c_2 m^2/\log m},$$

so we have a rather long list of group elements. What can we say about $\lambda(G)$? Since G is isomorphic to $(\mathbb{Z}/(N\mathbb{Z}))^*$, $\lambda(G)$ is just $\lambda(N)$, and as we saw in the last section, $\lambda(N)$ is at most about e^m. It remains to estimate $\log|G|$. But

$|G| = \varphi(N) < N$ and N is at most the product of *all* the primes up to m^2, which is about e^{m^2}. Thus $\log|G|$ is at most about m^2.

In particular, we have for all large m that

$$\lambda(G)\log|G| < e^{2m}.$$

Thus comparing this inequality with the one displayed above, we see that the van Emde Boas–Kruyswijk inequality now guarantees us that we can make many Carmichael numbers from the primes p with $p-1 \mid kN$, $p \nmid N$, $p \equiv 1 \bmod k$. Repeating the argument for a larger m we get many more Carmichael numbers and there is no limit. We have proved there are infinitely many Carmichael numbers!

10. Further results and unsolved problems

So we have $C(x)$, the number of Carmichael numbers up to x, unbounded. But can we say anything interesting about the rate of growth of $C(x)$ as $x \to \infty$? By refining the argument in the previous section, Alford, Granville and I were able to prove $C(x) > x^{2/7}$ for all sufficiently large x.

The exponent $2/7$ arises from two other constants implicit in the above discussion. One of these constants is related to the number c_2 in the Prachar argument, which in turn is related to a paper of Huxley [14] on estimates for the number of zeros of certain Dirichlet L-functions in certain regions of the critical strip.

The other constant we took as "2" in the above discussion: we let N be the product of the primes $p < m^2$ such that $p-1$ divides the least common multiple of the integers up to m. We cited [18] as saying there are a positive proportion of all of the primes $p < m^2$ with this property. Using a result of Friedlander [14], we may replace m^2 with m^c for c any number below $2\sqrt{e}$.

Using both the Huxley and Friedlander results, we get $C(x) > x^c$ for all sufficiently large x, for any

$$c < \frac{5}{12}\left(1 - \frac{1}{2\sqrt{e}}\right) = .290306\ldots .$$

In particular, $c = 2/7$ works.

Is there any hope to prove Erdős's conjecture that for each $\varepsilon > 0$, $C(x) \geq x^{1-\varepsilon}$ for all large x, depending on the choice of ε? This is probably a very hard problem, but we can at least reduce it to another in analytic number theory that is widely believed. Suppose that for each $\delta > 0$ and for all sufficiently large x, depending on the choice of δ, and for each integer d in the range $1 \leq d \leq x^{1-\delta}$, the number of primes $p \leq x$ with $p \equiv 1 \bmod d$ exceeds $x/(10d\log x)$. Then Erdős's conjecture follows.

It is safe to say that we shall never "use up" mathematics. With every new advance, many new questions are suggested. Not only is Erdős's "$x^{1-\varepsilon}$" conjecture still open, although perhaps more clearly in focus, we can ask if the proof of the existence of infinitely many Carmichael numbers can be carried over to other Carmichael-like numbers. For example, are there infinitely many

squarefree composite integers n such that $p+1 \mid n+1$ for every prime $p \mid n$? That is, we have just changed the two minus signs in Korselt's criterion to plus signs. This problem is open.

BEEGER [5] was the first to prove there are infinitely many even pseudoprimes. These are even numbers $n > 2$ that satisfy $2^n \equiv 2 \bmod n$. Let $B(x)$ denote the number of even pseudoprimes up to x. Do we have $B(x) > x^c$ for some positive constant c and all large x? This problem too is open.

Let $C_k(x)$ denote the number of Carmichael numbers up to x with exactly k distinct prime factors. We have seen that Chernick's theorem and the prime k-tuples conjecture imply that $C_3(x)$ is unbounded. In particular a strong form of the prime k-tuples conjecture implies that $C_3(x) > cx^{1/3}/(\log x)^3$ for some positive constant c and all sufficiently large x. However we still cannot even prove unconditionally that $C_3(x)$ is unbounded, nor can we prove *any* of the functions $C_k(x)$ is unbounded.

What should we conjecture to be the true order of magnitude for $C_3(x)$? A simple argument (see [22]) gives $C_3(x) < cx^{2/3}$ for all large x. A result in [8] gives $C_3(x) \le \frac{1}{4}x^{1/2}(\log x)^{11/4}$ for all $x \ge 1$. What is the "correct" exponent on x? That is, is there a number c_3 such that $C_3(x) = x^{c_3+o(1)}$ for $x \to \infty$? Granville has conjectured that $c_3 = 1/3$, so in some sense Chernick's theorem would be most of the story. In fact, Granville conjectures that for each integer $k \ge 3$, we have $C_k(x) = x^{1/k+o_k(1)}$ for $x \to \infty$. He may be right. It might appear that this conjecture is antithetical to Erdős's "$x^{1-\epsilon}$" conjecture, but there is no superficial reason why they both cannot be true.

REMARK. Recently, S.W. GRAHAM ('Carmichael numbers with three prime factors,' to appear) has shown that $C_3(x) \le x^{2/5+o(1)}$ for $x \to \infty$.

REFERENCES

1. L. M. ADLEMAN, C. POMERANCE and R. S. RUMELY, 1983, *On distinguishing prime numbers from composite numbers*, Annals Math. 117, pp. 173-206.
2. W. R. ALFORD, A. GRANVILLE AND C. POMERANCE, *There are infinitely many Carmichael numbers*, Annals Math. (to appear).
3. P. C. BAAYEN, 1968, *Een combinatorisch probleem voor eindige abelse groepen*, in Colloquium Discrete Wiskunde, MC Syllabus 5, Mathematisch Centrum, Amsterdam, pp. 76-108.
4. N. G. W. H. BEEGER, 1950, *On composite numbers n for which* $a^{n-1} \equiv 1 (\bmod n)$ *for every a prime to n*, Scripta Math. 16, pp. 133-135.
5. N. G. W. H. BEEGER, 1951, *On even numbers m dividing* $2^m - 2$, Amer. Math. Monthly 58, pp. 553-555.
6. R. D. CARMICHAEL, 1910, *Note on a new number theory function*, Bull. Amer. Math. Soc. 16, pp. 232-238.
7. J. CHERNICK, 1939, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. 45, pp. 269-274.

8. I. DAMGÅRD, P. LANDROCK and C. POMERANCE, 1993, *Average case error estimates for the strong probable prime test*, Math. Comp. 61, pp. 177-194.
9. H. J. A. DUPARC, 1952, *On Carmichael numbers*, Simon Stevin 29, pp. 21-24.
10. P. VAN EMDE BOAS and D. KRUYSWIJK, 1969, *A combinatorial problem on finite abelian groups* III, Report ZW 1969-008, Mathematisch Centrum, Amsterdam, 32 p.
11. P. ERDŐS, 1956, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4, pp. 201-206.
12. P. ERDŐS, C. POMERANCE and E. SCHMUTZ, 1991, *Carmichael's lambda function*, Acta Arith. 58, pp. 363-385.
13. J. B. FRIEDLANDER, 1989, *Shifted primes without large prime factors*, in Number Theory and Applications (ed. R. A. Mollin), Kluwer, Dordrecht, NATO ASI, pp. 393-401.
14. M. N. HUXLEY, 1975, *Large values of Dirichlet polynomials*, Acta Arith. 26, 435-444.
15. A. KORSELT, 1899, *Problème chinois*, L'intermédiare des mathématiciens 6, pp. 142-143.
16. J. OLSON, 1969, *A combinatorial problem on finite abelian groups*, I, J. Number Theory 1, 8-10.
17. R. G. E. PINCH, 1993, *The Carmichael numbers up to* 10^{15}, Math. Comp. 61, pp. 381-391.
18. C. POMERANCE, 1980, *Popular values of Euler's function*, Mathematika 27, pp. 84-89.
19. C. POMERANCE, 1981, *On the distribution of pseudoprimes*, Math. Comp. 37, pp. 587-593.
20. C. POMERANCE, 1989, *Two methods in elementary analytic number theory*, in Number Theory and Applications (ed. R. A. Mollin), Kluwer, Dordrecht, NATO ASI, 135-161.
21. C. POMERANCE, 1990, *Cryptology and computational number theory – an introduction*, in Cryptology and Computational Number Theory (ed. C. Pomerance), Proc. Symp. Appl. Math. 42, Amer. Math. Soc., Providence, 1-12.
22. C. POMERANCE, J. L. SELFRIDGE and S. S. WAGSTAFF, JR., 1980, *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35**, 1003-1026.
23. K. PRACHAR, 1955, *Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form* $p - 1$ *haben*, Monatsh. Math. **59**, 91-97.