CARMICHAEL NUMBERS

George Szekeres*

In a previous issue of **Parabola** (Vol 28 No 1, p26) David Tacon has written about prime numbers, that is integers greater than 1 which have only 1 and themselves as divisors. In particular he mentioned (and proved) Fermat's beautiful theorem that if p is a prime number and a is an integer not divisible by p then $a^{p-1}-1$ is always divisible by p. Another way of stating the theorem is that for any integer a and prime number p, $a^p - a$ is divisible by p. All you have to do is write $a^p - a = a(a^{p-1} - 1)$ and either the first or the second factor on the right hand side is divisible by p, depending on whether a is or is not divisible by p.

Here is a proof quite different from the one that David gave in his article. We use induction on a. For $a = 1$ the statement is obviously true since $1^p - 1 = 0$ is divisible by any non-zero integer (why?), hence also by p. Now suppose $a^p - a$ is divisible by p for some $a \geq 1$, we show that $(a+1)^p - (a+1)$ is divisible by p. Indeed by the binomial theorem $(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1$. Hence $(a+1)^p - a - 1 = a^p - a + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a$. Here $a^p - a$ is divisible by p by the induction hypothesis, and each of the binomial coefficients $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ is divisible by p for a prime number p (why?), hence the whole expression is divisible by p.

Fermat was to some extent anticipated by the ancient Chinese mathematicians who knew 2000 years before Fermat that if n is prime then n divides $2^n - 2$. They may even have thought according to some historians (though there is no real evidence for it) that the converse is also true: if n is a composite number (that is, not a prime number) then $2^n - 2$ is not divisible by n. For instance $2^4 - 2 = 14$ is not divisible by 4, $2^6 - 2 = 62$ is not divisible by $6, 2^8 - 2 = 254$ is not divisible by $8, 2^9 - 2 = 510$ is not divisible by 9 etc. However, if you are persistent enough – and with a programmable calculator it is a lot easier to be persistent than it would have been for the ancient Chinese – you will soon hit the number $n = 341 = 11 \times 31$ and verify that $2^{341} - 2$ is indeed divisible by 341.

* George is an Emeritus Professor in Pure Mathematics at the University of N.S.W.

I should mention here that for this check it is not necessary to calculate the huge number 2^{341} but replace at each step the number by its remainder "modulo" 341 – that is the remainder that you obtain when you divide the number by 341. For instance when you reach $2^9 = 512$, you replace it by 171, since $512 = 341 + 171$, or using the standard notation that David has introduced in his article, $2^9 = 512 \equiv 171 \bmod 341$. Next you replace 2^{10} by $2 \times 171 = 342 \equiv 1 \bmod 341$ and you are almost home: $2^{340} \equiv (1^{10})^{34} \equiv 1^{34} = 1 \bmod 341$, $2^{340} - 1$ is divisible by 341 and so is $2^{341} - 2$ divisible by 341. We were lucky to strike the remainder 1 already at the 10th step, which simplified the calculation enormously. Usually one is not quite so lucky, but in all cases the calculation of the residue of $2^n \bmod n$ is an extremely fast procedure, as explained by David in his second article (Vol.28, No2, p27).

The example of 341 shows that the Chinese congruence

$$2^n \equiv 2 \bmod n \tag{C}$$

cannot be reliably used as a "primality test" for n; a number n may well be composite and still satisfy (C). All right, you may say, why not try Fermat's more general congruence

$$a^n \equiv a \bmod n, \tag{F}$$

with several different "bases" a (not only 2). We call a composite number n a pseudoprime to base a (meaning: it behaves like a prime) if it satisfies Fermat's congruence (F). Surely the chances of n to be a pseudoprime for several bases simultaneously must be very slim indeed. To carry out the test for any base a is just as simple for the computer as $a = 2$, and here we have a good sporting chance for a fast, efficient and reliable primality test.

Unfortunately this stratagem doesn't work. Carmichael showed in 1910 that there are numbers which are pseudoprimes to **all** bases a. The first few that he found were

$$561 = 3 \times 11 \times 17,\ 1105 = 5 \times 13 \times 17,\ 1729 = 7 \times 13 \times 19.$$

How did he know that these were pseudoprimes to any base a? A few years earlier, in 1899, Korselt showed that a composite n is a pseudoprime to all bases if and only if the following two conditions hold:

(i) n is squarefree, that is n is not divisible by the square of any prime, and (ii) $p-1$ divides $n-1$ for all primes p which divide n. For instance in the case of 561, $3-1=2$ divides $561-1=560$, and so does $11-1=10$ and $17-1=16$.

It is not very "difficult" to verify (though quite sophisticated for the novice in number theory, as you will see) that n must have these properties if it is to be a pseudoprime to all bases. First, n must be squarefree, for if p^2 divides n then n cannot be a pseudoprime to base p since $p^n - p$ is certainly not divisible by p^2 (hence by n).

Secondly, if p is a prime divisor of n then $p-1$ must divide $n-1$. To prove this I must use a famous theorem of Euler and Gauss which states that modulo any prime number p there exists a "primitive root" a which has the property that $a,\ a^2, \cdots,\ a^{p-1}$ are congruent to the $p-1$ different non-zero residues modulo p. For instance if $p=5$ then 2 is a primitive root because $2^1=2,\ 2^2=4,\ 2^3=8 \equiv 3 \bmod 5$ and of course $2^4 \equiv 1 \bmod 5$ by Fermat. If $p=7$, then 2 is not a primitive root because $2^1=2,\ 2^2=4,\ 2^3=8\equiv 1$ mos 7 and from then on these 3 residues repeat cyclically: $2^4 \equiv 2,\ 2^5 \equiv 4,\ 2^6 \equiv 1 \bmod 7$, and only the residues 1,2 and 4 are among the powers of 2. On the other hand it is easy to verify that 3 is a primitive root mod 7; I leave the verification to you. A primitive root a is clearly characterised by the fact that

$$a^d \not\equiv \bmod p \text{ for } 1 \le d < p-1.$$

Proof of the existence of a primitive root modulo any prime number p is not at all easy and will not be attempted here; it is usually one of the first serious theorems that you learn in a course on number theory past High School Mathematics. You should do some experiments with various prime numbers such as 11, 13, 17 etc. and try to find a primitive root for each.

Now suppose that p is a prime divisor of n and a is a primitive root modulo p. Since n was assumed to be a pseudoprime to any base, it is a pseudoprime to this particular base a, hence $a^n - a$ (or $a^{n-1}-1$) is divisible by n and therefore divisible by p. So we have the two congruences

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

From here it follows that $p-1$ is a divisor of $n-1$. For if not, divide $p-1$ into $n-1$ and take the remainder,

$$n-1=k(p-1)+r$$

for some integer k and $0 \leq r < p-1$. But $a^{n-1}=a^{k(p-1)+r} \equiv a^r \bmod p$ (since $a^{p-1} \equiv 1 \bmod p$) unless $r=0$, and $n-1=k(p-1)$.

This proves the necessity of Korvelts condition (ii) for n to be a pseudoprime to all bases. The more difficult part of Korvelt's result is that conversely, if the conditions (i) and (ii) are satisfied then n is indeed a pseudoprime to all bases. I will be excused if I omit the proof; I am sure you found already the "easy" bit hard enough and at least got the flavour of the arguments.

Carmichael computed 15 such numbers which satisfied conditions (i) and (ii), and vaguely suggested that there may exist infinitely many of them. This became known ever since as Carmichael's conjecture and his numbers Carmichael numbers. The conjecture remained open for more than 80 years. Finally last year three American mathematicians, Alford, Granville and Pomerance (all three at the University of Georgia) settled the conjecture. Not only are there infinitely many Carmichael numbers but there are quite a lot of them – bad news for primality testing. To be more precise, if x is a very large number (and I mean very large, much larger than the number of atoms in the whole Universe) then there are more than $x^{2/7}$ Carmichael numbers under x.

The past two decades have been exceptionally rich in the settling of old unsolved problems. You may have heard that one of the most famous unsolved problems, Fermat's 350 years old conjecture that the equation

$$x^n+y^n=z^n$$

has no solution in non-zero integers x, y, z when $n>2$, has finally been laid to rest by a British mathematician, Andrew Wiles. His exceedingly difficult solution (a complete detailed proof may well fill the pages of several substantial books) is still under scrutiny but most mathematicians expect the proof to be correct: Fermat's equation has no solution.