Using similar techniques, we can show that

$$\cos A = \frac{m^2 + n^2}{4mn} \quad \text{and} \quad \cos B = \frac{(m^2 + n^2)(m^4 + n^4 - 10m^2n^2)}{16m^3n^3}.$$

Hence

$$\cos 3A = \cos A(4\cos^2 A - 3) = \frac{(m^2 + n^2)(m^4 + n^4 - 10m^2n^2)}{16m^3n^3} = \cos B.$$

The given restrictions on m and n show that $0 < A < \frac{1}{4}\pi$, whence $3A$ lies between 0 and π. Since B also lies in this range we conclude that $B = 3A$.

Acknowledgement

The author is grateful to the referee for suggesting improvements in original draft.

M. N. DESHPANDE

Institute of Science, Nagpur - 440 001, India

86.65 The prime factors of $2^n + 1$

The puzzle set by John Parkes in his letter in the November 2001 *Gazette* has several points of interest. The table below shows the prime factorisation of $2^n + 1$ for $n = 1, 2, \dots, 16$.

n	$2^n + 1$	n	$2^n + 1$
1	**3**	9	$3^3 \times$ **19**
2	**5**	10	$5^2 \times$ **41**
3	3^2	11	$3 \times$ **683**
4	**17**	12	$17 \times$ **241**
5	$3 \times$ **11**	13	$3 \times$ **2731**
6	$5 \times$ **13**	14	$5 \times$ **29** $\times$ **113**
7	$3 \times$ **43**	15	$3^2 \times 11 \times$ **331**
8	**257**	16	**65537**

Each bold entry denotes the first appearance of a given prime in the table. The puzzle was to show that if a prime p makes its first appearance at index n, then $p \equiv 1 \pmod{n}$. Thus, for example, $p = 11$ appears first when $n = 5$, and we note that $11 \equiv 1 \pmod{5}$.

Certainly n is the least positive integer such that

$$2^n \equiv -1 \pmod{p}. \qquad (1)$$

By the pigeonhole principle, the values of $2^1, 2^2, 2^3, \dots, 2^{p+1}$ cannot all be distinct modulo p. Thus we may let s, t be positive integers such that $s < t$ and $2^s \equiv 2^t \pmod{p}$. Since $2^{t-s} \equiv 1 \pmod{p}$, there is a least positive integer d such that

$$2^d \equiv 1 \pmod{p}. \qquad (2)$$

I claim that if r is any positive integer such that $2^r \equiv 1 \pmod{p}$, then d divides r. To see this, let h be the highest common factor of r and d. We can use Euclid's algorithm to find integers a and b such that $h = ra + db$. Then

$$2^h \equiv (2^r)^a . (2^d)^b \equiv 1^a . 1^b \equiv 1 \pmod{p}.$$

From the definition of d, $d \leqslant h$. But h divides d, so that $h = d$. It follows that d divides r, as claimed.

From (1), $2^{2n} \equiv 1 \pmod{p}$. Thus d divides $2n$. Each prime factor of $2^n + 1$ is odd, so that (1) and (2) show that $d \neq n$. If $d < n$, then $2^{n-d} \equiv -1 \pmod{p}$, contradicting the definition of n. Thus d is a divisor of $2n$ that exceeds n. Hence $d = 2n$.

By Fermat's little theorem, $2^{p-1} \equiv 1 \pmod{p}$. Our earlier result shows that d divides $p - 1$. But $d = 2n$, so that n divides $(p - 1)$ and $p \equiv 1 \pmod{n}$ as desired.

Group theory illuminates the argument. The non-zero integers modulo p form a group, F_p^*, of order $(p - 1)$ under multiplication modulo p. We could have deduced that d divides $(p - 1)$ from the fact that the order of an element divides the order of the group. Indeed, Fermat's little theorem is itself a consequence of this fact.

The argument also enables us to characterise those primes that appear as factors of some value of $2^n + 1$. They are precisely the odd primes p for which the order, d, of 2 in F_p^* is even. We have seen that this condition is necessary for p to be a factor of some value of $2^n + 1$, because $d = 2n$. Thus $p = 7$ can never be a factor, as successive powers of 2 (mod 7) are 2, 4, 1, so that $d = 3$. Similarly the order of 2 (mod 23) is 11, so that 23 cannot be a factor of $2^n + 1$. Conversely, when d is even, there is a positive integer, n such that $d = 2n$. Hence $2^{2n} \equiv 1 \pmod{p}$. Since p is prime, either $2^n \equiv 1 \pmod{p}$ or $2^n \equiv -1 \pmod{p}$. The first possibility is ruled out by the definition of d and the fact that $n < d$. Thus $2^n \equiv -1 \pmod{p}$ and p is a factor of $2^n + 1$.

Readers can explore what happens when $2^n + 1$ is replaced by $a^n + 1$ for some integer $a > 2$ or by $a^n - 1$ for some integer $a \geqslant 2$.

K. ROBIN McLEAN

Department of Education, University of Liverpool, Liverpool L69 3BX

Editor's note: Similar proofs of Parkes' conjecture were received from Nick Lord, Martin Griffiths and Wim de Jong.