NUMBERS COUNT

Mike Mudge looks at the construction of tables of primitive roots and indices in number theory.

This topic is fundamental to many primality-testing algorithms, also to the solution of various types of linear and non-linear congruence.

Definition D1. Two positive integers b and c are said to be congruent modulo m if, and only if, they differ by an integer multiple of m.

We write $b = c \pmod m$ meaning $b = c + km$ where $k = 0, +1, +2, \ldots$. For example, $13 = 98 \pmod 5$ because $13 = 98 + (-17)(5)$.

Definition D2. Euler Phi-function $\phi(n)$ is defined to be the number of positive integers not exceeding the given positive integer n which are relatively prime to n (that is which share no common factor, other than 1 with n). For example, $\varphi(4) = 2$, $\varphi(12) = 4$, $\varphi(p) = p - 1$ where p is prime.

Definition D3. Let a and m be relatively prime positive integers, then the least positive integer, x, such that $a^x = 1 \pmod m$ is called the *order* of a *modulo* m. We write $x = \mathrm{ord}_m a$. For example, $\mathrm{ord}_7 2 = 3$, $\mathrm{ord}_7 3 = 6$, $\mathrm{ord}_{17} 5 = 16$.

Definition D4. If r and n are relatively prime integers, and if further $\mathrm{ord}_n r = \varphi(n)$, then r is called a primitive root modulo m. For example, 2 is a primitive root modulo 9.

Now when an integer possesses a primitive root, it usually has many primitive roots.

Theorem T1. If a positive integer, m, has a primitive root then it has a total of $\varphi(\varphi(m))$ incongruent primitive roots.

Theorem T2. The positive integer n possesses a primitive root if, and only if, $n = 2, 4, p^t$, or $2p^t$, where p is an odd prime and t is an integer.

Problem A. Write a computer program to:

(i) find primitive roots modulo powers of a given odd prime; and

(ii) find primitive roots modulo twice the powers of a given odd prime.

Test. 7, 13, 17 and 19 are all the incongruent primitive roots modulo 22.

5 is a primitive root moduli 23, 529, 1058.

3 is a primitive root moduli 17, 289, 578.

Definition D5. Let m be a positive integer with primitive root r. If a is a positive integer which is relatively prime to m, then the unique integer, x, with $1 \leq x \leq \varphi(m)$ and $r^x = a \pmod m$ is called the *index* of a to the *base* r *modulo* m: we write $x = \mathrm{ind}_r a$ and do not display the base explicitly since it is assumed to be fixed at a known value.

For example, modulo 7. $\mathrm{ind}_3 1 = 6$, $\mathrm{ind}_3 2 = 2$, $\mathrm{ind}_3 3 = 1$, $\mathrm{ind}_3 4 = 4$, $\mathrm{ind}_3 5 = 5$ and $\mathrm{ind}_3 6 = 3$. However, a change of primitive root from 3 to 5 yields $\mathrm{ind}_5 1 = 6$, $\mathrm{ind}_5 2 = 4$, $\mathrm{ind}_5 3 = 5$, $\mathrm{ind}_5 4 = 2$, $\mathrm{ind}_5 5 = 1$ and $\mathrm{ind}_5 6 = 3$.

Problem B. Write a computer program to construct a table of indices modulo a particular primitive root of an integer.

Test. The table of indices modulo 23 with respect to the primitive root 5 includes: $\mathrm{ind}_5 1 = 22$, $\mathrm{ind}_5 2 = 2, \ldots \mathrm{ind}_5 7 = 19, \ldots \mathrm{ind}_5 22 = 11$.

Readers are invited to submit their attempts on problems A(i) and (ii) and B to : Mike Mudge, 'Square Acre', Stourbridge Road, Penn, Wolverhampton, Staffordshire WV4 5NF. Tel: (0902) 892141.

Submissions, which must reach me by 1 May, will be judged using suitably vague criteria. A prize will be awarded for the best entry received.

Please note that submissions can only be returned if a suitable stamped addressed envelope is provided.

Expanded reviews of previous problems together with, subject to the approval of the contributor, copies of detailed programs from the winning entry may also be requested. However, in the interests of efficiency, interested readers are urged to contact the prize-winner directly.

A triad of curiosities — August review

(1) Powers of 10 that can be factorised in a manner which contains no zeros: 10^{18} and the example of 10^{33} quoted are the only known examples below 10^{5000} and greater than 10^{10}, below which several trivial cases occur. This subject was the basis of the puzzler in *Computer Weekly* (July 1985) and of some subsequent correspondence, after the *PCW* material had been submitted.

(2) The digit patterns in 2^n can be readily examined to show for example that the tens digits appear periodically as do the hundreds digits and so on — the period is always $4 \times 5^{n-1}$ where n is the position of the digit counting from the right. Despite this periodicity it has been proved that there exist arbitrary length strings of zeros. However, no string of nine zeros has been found up to 2^{60000}. More work is needed . . .

For further discussion of these matters and of (3) the reader is referred to *Excursions in Number Theory* by Ogilvy and Anderson, and encouraged to experiment further, preferably in a strictly interactive mode on a PC with the consequence of multiplying a number by its 'reverse'.

No submission worthy of a prize was received; however, a piece of work relating to the determination of Palindromic Primes has come to the surface. Using an Olivetti M20 running PCOS-Basic generating and storing 249400 primes, a sieve approach to a linear array of 150000 bits representing 150000 contiguous integers, and storing the primes themselves 100 7-digit numbers in 107 bytes of random access file. This work, by Russell Lavelle-Langham of 31 Risby House, Barleycorn Way, Limehouse, London E14 8DF, is worthy of a suitable reward as the approach should encourage many other readers.