Mike Mudge poses some problems relating to the primitive roots of (safe) prime numbers.

The area of investigation this month has been suggested by PS Brady of Wrexham, Clwyd who sees it as 'the topic which interests me most at present (and probably for some time to come)'; thus there is obviously much scope for investigative computing here.

Some mathematical prerequisites

A **prime number**, p, is an integer (whole number) which is only exactly divisible by itself and unity (one), for example, 2,3,5,...31,..613... A **safe prime number** is a prime of the form $2p + 1$, for example, $7 = 2\times3 + 1$, $83 = 2\times41 + 1$, $503 = 2\times251 + 1$.

Two integers a & b are said to be **coprime** if and only if (iff) they have no common divisor (factor) other than unity. We write (a,b)=1. (In general (a,b) denotes the highest common factor (HCF) of a&b.) 16 and 57 are coprime while (96,172) = 4.

Two integers a & b are said to be **congruent modulo** a third integer,m, iff their difference is exactly divisible by m; alternatively iff they each leave the same remainder on division by m. We write $a \equiv b(m)$, for example, $80 \equiv 25\ (11)$ because $80 - 25 = 55 = 5\times11$.

If there exists an integer × such that $\times^2 \equiv a(m)$ where (a,m)=1 then a is called a **quadratic residue** modulo m. In this investigation m will be replaced by a prime, possibly a safe prime,p. For example, 13 is quadratic residue modulo 23 because $6^2 \equiv 13(23)$.

The **Legendre Symbol** (a/p),read symbol of a with respect to p, is defined for integers, a, which are not divisible by p. It is equal to 1 if a is a quadratic residue modulo p and to −1 if a is a quadratic non-residue modulo p.

The **Jacobi Symbol** (a/P), where $P = p_1p_2p_3....$ (notice that some factors may be repeated), and where (a,P)=1, is defined thus: $(a/P) = (a/p_1)(a/p_2)(a/p_3).....$ for example $(219/383) = -(383/219) = -(164/219) = -(41/219) = -(219/41) = -(14/41) = (2/41)(7/41) = -(7/41) = -(41/7) = -(-1/7) = 1$ hence 219 is a quadratic residue modulo 383.

NOTE Many simple properties of L & J symbols are illustrated in this numerical example.

Euler's Function, $\emptyset(a)$ is defined for all positive integers,a, as the number of integers in 0,1,2,...a−1 which are coprime with a. For example, $\emptyset(4) = 2$, $\emptyset(5) = 4$, $\emptyset(6)=2$.

If a&m are positive integers such that (a,m)=1 then k is the *smallest* integer such that $a^k \equiv 1(m)$ is called the **exponent** to which a belongs modulo m. For example, 7 belongs to exponent 2 modulo 4.

If, however, $k = \emptyset(m)$ the a is called a **primitive root** modulo m. For example, 3 is a primitive root to moduli 17, 289 & 578.

The Investigation

Mr Brady is concerned with the 'uniqueness' of the sequence of residues (remainders) r_i, generated when any primitive root g_j of a prime (safe or otherwise) is raised to the power of all of the integers less than p, with reduction modulo p: that is, $r_i \equiv g_j^k (p)$ where $1 \leq i, k \leq p-1$ & $r_i < p$. .....(**)

He observes that EM Burton *et al*, *Elementary Number Theory*, state that the above operation generates all the residues modulo p in *some* order, not that each primitive root of a prime number generates a unique sequence from all others. There are (p−1)! permutations of the integers less than p, but only a maximum of (p−3)/2 primitive roots, this being attained for safe primes.

To identify the primitive roots of a safe prime number it is only necessary to compute the Legendre Symbols of all the integers less than p−1. Those integers ,i, which are quadratic non-residues, that is, for which (i/p) = −1 are primitive roots.

Project A Write and implement a program to generate safe primes.

Project B Write and implement a program to determine the (p−3)/2 primitive roots of the safe primes from **A** above.

Project C Investigate the sequence generated by (**) above with particular reference to the observation regarding EM Burton *et al*.

Attempts at some, or all, of the above projects may be sent to Mike Mudge, 1 Dolboeth, Cwm Mabws, Llanrhystud, Dyfed SY23 5BB, tel (Nebo) 09746-548 to arrive by 1 November 1990.

Review March 1990

This investigation proved to be the most popular since that of Palindromic Numbers in February 1985 . . . why? Many of the submissions have been forwarded to the proposer, Michael Meierruth in Milan. Despite a degree of ambiguity regarding 'odd diagonals' as distinct from 'normal diagonals', efforts worthy of mention include: Paul Cleary, who identified a readily soluble subset (4n+6) (4n+6) reaching 1450 × 1450 in 3.9secs on an Atari 520; and Robin Merson with a most detailed and professionally presented analysis.

The selection of a prize-winning entry has proved to be difficult. But within the spirit of Numbers Count in particular, and empirical number theory in general, it is Antonio Key of 134 Astwood Road, Worcester WR3 8EZ who, having used Quick Basic (v4.5) on an Advent 286/20 for a search program, discarded this having observed a pattern, made an empirical conjecture of an analytic solution and attempted to verify this up to N=32766. Albeit, it must be said, not for the most general problem.

Details of state-of-the-art and other solutions from Michael Meierruth, Via Treviso 33, 20127 Milan, Italy.

Mike Mudge welcomes correspondence on any subject within the areas of number theory and computational mathematics. Particularly welcome are suggestions for future Numbers Count articles.

LEISURE LINES

Brainteasers courtesy of JJ Clessa.

Sep 90

This month's quickie

No answers, no prizes. Look at the following series of letters:

T E L H B

What letter in the alphabet comes next?

Prize Puzzle

There are five consecutively numbered houses in a street, each with a front door of a different colour, and inhabited by men of different nationalities, different occupations, each playing a different sport and each preferring a different drink.

1 The Englishman lives in the house with the red door.
2 The Spaniard's sport is golf.
3 Beer is drunk in the house with the green door.
4 The Ukranian drinks vodka.
5 The number of the house with the green door is one more than the number of the house with the ivory door.
6 The Teacher's sport is tennis.
7 The Accountant lives in the house with the yellow door.
8 The man in the middle house drinks gin.
9 The Norwegian lives in the lowest numbered house.
10 The Solicitor lives in the house next to the hiker.
11 The Accountant lives in the house next to the jogger.
12 The Doctor drinks rum.
13 The Dentist is Japanese.
14 The Norwegian lives next to the house with the blue door.

Now, who drinks whisky, and whose sport is swimming?

Answers on postcards or backs of sealed envelopes — no letters please. Send to: September Prize Puzzle, *PCW* Editorial, VNU House, 32-34 Broadwick Street, London W1A 2HG, to arrive not later than 30 September 1990.

Winner, June 1990

A very good response to the logic problem in the June issue — exactly 125 entries were received, most of which were correct. As usual we had to draw our winner from the heap and the lucky card came from Mr Stephen Lambert of Hull. Congratulations, Stephen, your prize is on its way. To the other 124 entries, keep puzzling, it could be your turn next.

The correct solution was as follows. The pairings were:
Albert-Celia : Barry-Betty : Charlie-Alice.
Albert bought 32 — Celia bought 31
Barry bought 12 — Betty bought 9
Charlie bought 8 — Alice bought 1 ■