Part Three of the relationships between quadratic partitions and cubic residues is explored by Mike Mudge.

This is the final part of the investigation of quadratic partitions and cubic residues, originally proposed by NV Meeres of Esher. The first two parts are to be found in *PCW* of June and August 1990 and have already generated considerable interest among readers. This presentation is, however, self-contained; the required mathematical concepts being defined and illustrated in Appendix A.

Throughout this work, p denotes a prime number congruent to unity modulo 6, and hence having the associated quadratic partitions (QPs) of the form $p = 3\times A^2 + B^2$ and $4p = 27\times C^2 + D^2 = 3\times E^2 + F^2$. Now consider the composite qr and ask when this is a cubic residue (CR) of p given that neither of its factors is. Firstly, the case when q is congruent to ±4 modulo 9, for example 5, 13, 23, 31 & 67, and $EF \equiv 0 \bmod 9$. Then it is found that 4q is a CR but that neither q nor 2q are. (Table 1.)

If EF or any factor of EF (whether prime or composite) is congruent to ±1 mod 9 it is a CR of p. Reference to the earlier articles will reveal this result for AB in $3\times A^2 + B^2$ and indicate that the factors of AB can be even or odd. However, those factors of EF can only be odd since both E and F are odd. (Table 2.)

The ultimate test of this analysis is whether or not it is capable of generating a complete set of CRs for a given (fairly small) p, hence PROJECT C. Design and implement a computer program which, given as input a prime $p \equiv 1 \bmod 6$, generates a complete set of cubic residues. (Using any method....) Test case p = 79, analysed by NV Meeres using the results of this series of articles thus: $79 = 3(5^2) + 2^2$; A = 5, B = 2, AB = 10. Thus one pair of CRs (10,69). The least multiple of $B \equiv \pm 2 \bmod 9$ is 8, hence (8,71). $4p = 316 = 27(1^2) + 17^2$; C = 1, D = 17, hence (1,78) & (17,62). The quotient of 1 + 17, on division by 6, is odd, therefore (12,67) are CRs.

Moreover 2,3 & 6 are all non-cubic which shows that 2 & 3 must have indices of the same sign mod 3. Hence $18 = 2\times 3^2$ will have an index of the same sign mod 3 as $12 = 2^2\times 3$, hence (18,61), and from 10 and 69 in turn (15,64); (46,33); (22,57) & (38,41) are CRs. Also, $4p = 316 = 3(7^2) + 13^2$; E = 7, F = 13, hence (14,65); (21,58); and finally (52,27) complete the set of CRs of 79.

Attempts at some or all of the above projects may be sent to Mike Mudge, 1 Dolboeth, Cwm Mabws, Llanrhystud, Dyfed SY23 5BB, tel 09746-548, to arrive by 1 January 1991. Any communications received will be judged, using suitable subjective criteria, and a prize will be awarded by *PCW* to the 'best' contribution arriving by the closing date. It would be appreciated if such submissions contained a brief description of the hardware used, details of programs, run times and a summary of the results obtained; together with suggestions for further work in this area.

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

Table 1: $4p = 3xE^2 + F^2$; $q \equiv \pm 4$ mod.9; $2q \equiv \pm 1 \bmod 9$

p	E	F	2q	Cubic Residues
61	5	13	10, 26	20, 52
151	5	23	10, 46	20, 92
367	13	31	26, 62	52, 124
547	PROJECT A: Design and implement a computer program to obtain a completed version of this table and to extend the list of p-values which respond to the above analysis.			
619				
1123				
1483				

Table 2: $4p = 3xE^2 + F^2$; EF or any factor congruent to ±1 mod 9

p	E	F	EF	Cubic Residues	
73	1	17	17	1, 17	
271	19	1	19	1, 19	
409	23	7	161	161	
613	19	37	703	19, 37	703 is also a CR of 613. Why?
751	PROJECT B: Design and implement a computer program to obtain a completed version of this table and to extend the list of p-values which respond to the above analysis.				
757					
877					
937					
1609	13	77	1001	14, 22, 52, 91, 308.	Illustrating all three ways of using E and F
1951					

APPENDIX A: Some pure mathematical concepts and their definitions.

(1) **Modulus & Congruence** Two integers m & n are said to be congruent modulo a third integer r if and only if (iff) they differ by a multiple of r. That is, m & n leave the same remainder on division by r. We write $m \equiv n(r)$, or $m \equiv n \bmod r$, for example $17 \equiv 65(4)$, $17 - 65 = -12\times 4$.

(2) **Quadratic Partition (QP)** A QP of a given integer, K, is simply an expression of K as the sum of multiples of two squares. For example, $68 = 3\times 4^2 + 5\times 2^2$ is a QP of 68.

(3) **Cubic Residue (CR)** If p greater than 2 does not divide, a, and there exists an integer n such that $a \equiv n^3(p)$, then a is a CR of p. For example, if p = 19 then $11 \equiv 5^3(19)$ and 11 is a CR of p.

(4) **Order** The order of an integer, a, modulo p is defined to be the smallest power of a which is congruent to 1 modulo p.

Review May 1990, Harshad Numbers

This problem, together with the 'Thought for the month . . . On Stanbury Primes' produced many detailed responses. Unfortunately space does not permit a detailed discussion of the results, which are expected to appear in *PCW* December 1990. However, the very worthy prizewinner is Richard Tobin, of 2FR 53 Spottiswoode Street, Edinburgh EH9 1DQ. Using a MIPS RS2030 workstation running at about 12 MIPS Richard found an almost complete list of the first H and NZH numbers for digit sums up to 500 (base 10). The omissions 275, 370, 385, 404 & 495 were attacked for about four days each without result! Any assistance would be greatly appreciated.

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

JJ Clessa's brainteasers.

This Month's Quickie

No answers, no prizes, for the quickie. In my golf club, 48% of the members are ladies. 25% of the lady members took part in the club tournament and 50% of the gentlemen. What percentage of the total membership took part?

Prize Puzzle, November 1990

A problem in permutations and combinations this month, simple to present and easy to solve — or is it? Get the micros working on it.

If every vertex of a regular octogon is connected with every other, how many triangles will be formed?

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

Winner, August

Loads and loads of entries to the August palindromic puzzle, proving that it was far too easy. You just can't win! Still, it wore out a few micros, we suspect. By the way, we received about a dozen late entries for the July puzzle, nine of which were from the same entrant. Really, Mr IH of Glasgow, if you're going to waste money on sending multiple entries, at least make sure they arrive in time! Since this month's winner comes from overseas, there's no excuse for any late entries from the UK. The correct solution(s) were:

1 A & B — 321123
2 B & C — 0110
3 A & C — 111111
4 A & B & C — 655666

and the winning card came from Norway — Mr SA Knudsen of Stabekk. Congratulations, Mr Knudsen, let's hope your prize gets to you OK. ■