Mike Mudge investigates the relationships between Quadratic Partitions and Cubic Residues.

This research area has been suggested by NV Meeres of Esher, who explored it in considerable detail in 1982. Although certain pure mathematical concepts are required these are carefully defined, with simple numerical examples, in Appendix A.

The objects of interest are those prime numbers, p, congruent to unity modulo 6. That is, 7, 13, 19, 31, 37, 43, 61, 67, 73. . . The overall task, *to be considered in several stages*, is to attempt to use quadratic partitions of p, and related integers, to generate the complete set of cubic residues of p.

Notice that each p has a unique quadratic partition of the form: $3\times A^2 + B^2$. For example, $7 = 3\times 1^2 + 2^2$, $13 = 3+2^2 + 1^2$, $19 = 3\times 1^2 + 4^2$ . . . Each p has $(p-1)/6$ pairs of cubic residues; $(R_1, p-R_1)$, $(R_2, p-R_2)$ . . . while the remaining integers less than $p-1$ fall equally into two sets of pairs depending upon whether their indices are congruent to $+1$ or -1 modulo 3. For example, the cubic residues of 19 are (1,18), (7,12), (8,11). The remaining integers less than 18 are (2,17),(3,16), (5,14) with index congruent to $+1$ mod 3 and (4,15), (6,13) (9,10) with index congruent to -1 mod 3.

In attempting to identify the sequence $R_1, R_2, \ldots$ and hence to generate the complete set of cubic residues of p, many famous mathematicians were led to study the quadratic partition $4p = 27C^2 + D^2$, for which C×D and its factors are always cubic residues of p. For example, p=19, $4p=76=27\times 1^2+7^2$; C×D=1×7. p=307,$4p=1228=27\times 6^2 + 16^2$;C×D=96. The cubic residues of 307 include all of the factors of 96, and indeed of 96^2 (reduced modulo 307 when appropriate).

Now, if two primes are both cubic residues of p their product is also, but a composite, qr, may also be a cubic residue when neither of its factors is. For example, 10 is a cubic residue of 37 although 2 & 5 are not.

The case when qr = 10 leads to the conjecture that 10 is a cubic residue of p if and only if A×B (recall $p=3\times A^2+B^2$) is divisible by 10. For example, (p,A,B): (73,4,5), (79,5,2), (103,1,10), (349,10,7) . . .

Two further observations of NV Meeres are:

(a) Any integer congruent to ± 1 mod 9 is a cubic residue (CR) of p if (though not only if) it is a factor of A×B. For example (p,A,B:CR's): (67,1,8;1,8), (97,4,7;28), (181,2,13;26) . . .

(b) The least multiples of A and B congruent to ± 1 mod 9 are cubic residues of p. For example, (p,A,B:CR's): (61,2,7;8,28), (271,5,14;10,28), (421,10,11;10,44) . . .

Enough theory for this month!

Project A Design and implement a computer program to obtain the primes, p, congruent to unity modulo 6 together with the associated quadratic partitions $p = 3\times A^2 + B^2$ and $4\times p = 27\times C^2 + D^2$.

Project B Design and implement a computer program to verify that C×D and its factors are indeed CR's of p.

Project C Design and implement a computer program to test both the conjecture regarding the existence of a CR of 10 and A×B (the late Professor Goodstein of Leicester University verified this for p less than 10000 in 1964), also the observations (a) & (b) due to NV Meeres above.

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 August 1990.

APPENDIX A Some pure mathematical concepts and definitions.

(i) Modulus & Congruence Two integers m & n are said to be congruent modulo a third integer r if and only if they differ by a multiple of r. That is, m & n leave the same remainder on division by r. We write m = n(r), for example, 17=65(4), because $17-65 = -48 = -12\times 4$.

(ii) Quadratic Partition A quadratic partition of a given integer,K, is simply an expression of two squares. For example, $68 = 3\times 4^2 + 5\times 2^2$ is a quadratic partition of 68.

(iii) 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 cubic residue of p. For example, if p = 19 then $11 \equiv 5^3(19)$ and 11 is a CR of p. Notice that $11 - 125 = -114 = -6\times 19$.

(iv) Order The order of a modulo p is the smallest power of a which is congruent to 1 modulo p.

Review, December 1989, 'Some famous integer sequences'

This problem area proved to be popular. Among the submissions worthy of special mention are the following: Jim Waterton who, although restricted by the single precision arithmetic of his QL, did an in-depth study; Gareth Suggett, who computed up to R_{25}, B_{26}, E_{25} and S(13,13) with very substantial factorisation; Luis Lampreia and three fellow Portugese students who generated a detailed submission using Basic on a Philips MSX–2; and Frank Webster's achievements include S(100,4), 158 digits in 11 seconds, and R_{100}, also 158 digits in 2.4 seconds using both Basic and Assembler on an Acord Electron.

Readers are also encouraged to read 'Micromaths: some discoveries about tan x' by Adrian Oldknow, *Teaching Mathematics and its Applications*, vol 8, no 3, 1989, pp135-141.

The very worthy prizewinner this month is WE Thomson of Woodhaven, Leiston Road, Aldeburgh, Suffolk IP15 5PX. This submission 'turned out to be more of an exercise in algebra than in number-crunching'. Mr Thomson 'first came upon subfactorials in a practical problem about 50 years ago'. Space does not permit details of the balance between algebra and computing, but these are available on request.

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

LEISURE LINES

Brainteasers courtesy of JJ Clessa.

This Month's Quickie

No answers, no prizes, and no tricks this month. Using each of the digits 1-6, make a 6-digit number whose:

1. First and last digits are odd.
2. Second digit is twice the fourth.
3. 5th digit is twice the 2nd.
4. 3rd digit is one more than the last.

Prize Puzzle

This shouldn't be too difficult. Even if you can't do it, you've still got a one in six chance of being correct if you make a guess!

Albert, Barry and Charlie are married to Alice, Betty and Celia, but not necessarily respectively. One day the three couples went to the Post Office to buy stamps. Each man spent 63p more than his wife. Each person bought as many stamps as they paid in pence per stamp. Albert bought 23 more stamps than Betty and Barry bought 11 more stamps than Alice.

Who is married to who?

When you have completed the puzzle, write the solution on a postcard or the back of a sealed envelope — no letters please — and post it to: June Prize Puzzle, *PCW* Editorial, VNU House, 32-34 Broadwick Street, London W1A 2HG, to arrive not later than 30 June 1990.

Winner, March 1990

A good response to our number problem — about 150 entries, practically all of them containing the correct solution which was 9^{21} or, if you prefer to be longwinded: 109,418,989,131,512,359,209.

Despite the relatively high number of entries, we pulled out our first ever triple winner, Mr G Langley of Canterbury who, if our records are correct, was a winner in December 1985 as well as November 1986. We assure you that he is neither a relative, nor anyone we know!

Congratulations, Mr Langley, another prize is on its way to you. Perhaps the Post Office will soon be able to offer us a quantity discount for prizes sent to your address. Meanwhile, our condolences to all the others who lost this time, and do keep trying.