END ZONE

NUMBERS COUNT

Mike Mudge looks at the importance of the Fermat Quotient.

Definition. Two integers a and b are said to be congruent modulo a third integer c if, and only if, c is a factor of a−b.

This is written a≡b(mod c) or a≡b(c).

For example:

23≡17(mod 3) since 23−17=6=2×3,

16688=96(mod 17) since

16688−96=16592=976×17.

Consider the congruence:

$a^{N-1}\equiv 1 \pmod{N^2}$ . . . (1)

This was investigated, for odd N and a=2,3,4 . . . 99 by DH and Emma Lehmer from 1960 to 1967. Their investigation extended earlier work including that of Fröberg, Kravitz, Pearson, Riesel, Hausner & Sachs and Kloss.

There are found to be two distinct problems; the first in which N is restricted to prime values, p=3,5,7,11,13,17. . . while the second considers composite(non-prime) values of N.

Readers should be aware that the Fermat Quotient is closely connected with Fermat's Last Theorem — through the criterion of Wieferich (1909)–and with Catalan's Conjecture through the work of Inkeri (1964); for these reasons alone it is worthy of both theoretical and empirical study.

(i) Some results when N=p a prime

In 1962 the highest published search limit for a=2 was 200183 due to Pearson; by 1963 the Lehmers had searched to 2^{22} for 2≤a≤10 and found the new solutions p=1006003 for a=3 and p=534851 for a=6, also p=3152573 for a=6.

In 1964 Riesel extended a to 150 finding all solutions p<500000 for 2≤a≤10 and p<10000 for 11≤a≤150.

In 1965 Kloss published solutions including p=1747591 for a=13, p=2481757 for a=23 and p=1025273 for a=41.

The latest results known to the author are due to Brillhart, Tonascia and Weinberger and include the search limits shown in Fig 1.

Their discoveries include: p=53471161 for a=5, p=56598313 for a=10, p=1284043 for a=18 and p=63061489 for a=19.

The totality of known solutions to $a^{p-1}\equiv 1 \pmod{p^2}$ where p is prime are shown in Fig 2.

(ii) Some results when N is composite (non-prime)

There are theoretical results providing a strong characterisation of the primes which divide a composite solution of congruence (1) above.

These are to be found in AOL Atkin's and BJ Birch's *Computers in Number Theory*, Academic Press 1971; but they are beyond the scope of this article.

Known solutions of $a^{N-1}\equiv 1 \pmod{N^2}$, N odd and composite are shown in Fig 3.

Readers are invited to investigate the Fermat Quotient, above, determining all possible solutions for N both prime and composite for a specified set of values of a: reproducing as many as possible of the particular results quoted. It is hoped that such investigations will lead to some statement regarding the prime factors of composite N solutions.

The results of these investigations, which must arrive by 1 March 1987, may be submitted to Mike Mudge, 'Square Acre', Stourbridge Road, Penn, Nr Wolverhampton, Stafford shire WV4 5NF, tel (0902) 892141. It would be appreciated if such submissions contained a brief summary of results; together with thoughts relating to this problem, in a form suitable for future publication in *PCW*.

Submissions will be judged using suitably vague criteria, and a prize will be awarded to the 'best' contribution received. Please note that submissions can only be returned if a suitable stamped addressed envelope is provided.

Mike Mudge welcomes correspondence on any subject within the areas of number theory and other computational mathematics. Particularly welcome are suggestions for future 'Numbers Count' articles: all letters will be answered after a sufficient length of time!

Isolated readers can be put in contact with others sharing common interests: however, greater efficiency regarding published problems should result from contacting the prize-winner directly.

June review: PAPs

The state of the art regarding Primes in Arithmetic Progression (PAPs) is to be found in the paper by Paul A Pritchard, *Mathematics of Computation*, volume 45, number 171, July 1985, pages 263–267, 'Long Arithmetic Progressions of Primes: Some Old, Some New'. This contains the results of 14000 hours of computer time on a DEC VAX-11/780 (or rather two such systems) at Cornell University, and reports that no PAPs of length greater than 19 are known. There is also an interesting comparison of statistically predicted and experimentally observed PAPs of given length.

Tables 1, 2 and 3 are reproduced from the above paper in the hope of encouraging interested readers to experiment in this field.

The June prize-winner, in a problem which attracted an encouraging and varied response, is Hugh Spence of 22 Orissa Road, Plumstead, London SE18, who programmed his Tatung Einstein in Pascal. Hugh presented detailed flow charts in addition to his Pascal coding, run times and output; I feel sure that he would be happy to discuss his work in detail with any interested readers. Furthermore, I am convinced that Hugh, together with fellow PAP enthusiasts would benefit from a sight of the paper referred to above.

a	2	3	5	6,7,10,11,12,13	14,15,17,18,19,20	21,34	29,47,50
p	3.10^9	2^{30}	2^{29}	2^{28}	2^{27}	2^{29}	2^{28}

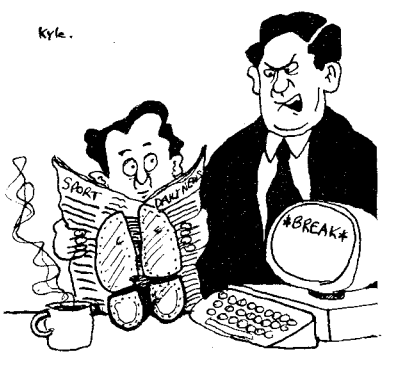
Fig 1

a	p	a	p
2	1093, 3511	3	11, 1006003
15	29131	17	3, 46021, 48947

Fig 2

a	N	a	N	a	N
26	15, 1065	68	133	80	9
82	9, 45	99	35,65,	146	91
			1729	148	451

Fig 3



'No, Jenkins, that's not what it means!'

NUMBERS COUNT

END ZONE

m	PAP of length m with minimal last term (k=0,1,2. . ., m−1)	last term	estimated last term
2	2,3	3	2
3	3,5,7	7	2
4	5,11,17,23	23	2
5	5,11,17,23,29	29	29
6	7+30k	157	92
7	7+150k	907	497
8	199+210k	1669	1406
9	199+210k	1879	5086
10	199+210k	2089	24310
11	110437+13860k	249037	177300
12	110437+13860k	262897	829800
13	4943+60060k	725663	5582000
14	31385539+420420k	36850999	2.332×10^{7}
15	115453391+4144140k	173471351	1.137×10^{8}
16	53297929+9699690k	198793279	6.793×10^{8}
17	3430751869+87297210k	4827507229	5.774×10^{9}
18	4808316343+717777060k	17010526363	3.303×10^{10}
19	8297644387+4180566390k	83547839407	2.564×10^{11}
20	?	?	1.261×10^{12}

Table 1 The known PAPs with minimum last term

n	common difference	first term	last term	discovery
12	30030	23143	353473	VA Golubev, 1958 (see [8])
12	13860	110437	262897	E Karst, 1967 ([8])
13	60060	4943	725663	VN Seredinskij, 1963 (see [8])
14	223092870	2236133941	5136341251	SC Root, 1969 (see [7])
14	420420	31385539	36850999	PA Pritchard, 1983
15	223092870	2236133941	5359434121	SC Root, 1969 (see [7])
15	4144140	115453391	173471351	PA Pritchard, 1983
16	223092870	2236133941	5582526991	SC Root, 1969 (see [7])
16	9699690	53297929	198793279	S Weintraub, 1976 ([12])
17	87297210	3430751869	4827507229	S Weintraub, 1977 ([13])
18	9922782870	107928278317	276615587107	PA Pritchard, 1981 ([11])
18	717777060	4808316343	17010526363	PA Pritchard, 1983
19	4180566390	8297644387	83547839407	PA Pritchard, 1984

Table 2 Some PAPs and their discoverers

length	first term	common difference	last term
18	4808316343	717777060	17010526363
19	8297644387	4180566390	83547839407
18	64158606367	2735312580	110658920227
18	2518035911	7536659130	130641241121
18	115936060313	3103900800	168702373913
18	98488875263	5169934770	186377766353
18	170263333103	5063238180	256338382163
18	107928278317	9922782870	276615587107
18	51565746467	13889956080	287694999827

Table 3 The known PAPs of length at least 18

DIARY DATA

Readers are strongly advised to check details with exhibition organisers before making arrangements, in order to avoid wasted journeys due to cancellations, printers' errors, and so on.

PC & SYSTEMS EXHIBITION
NEC, Birmingham — Evan Steadman & Partners (0799) 26699 **25-27 November**

PC USER NORTH EXHIBITION
GMex, Manchester — EMAP International (01) 608 1161 **21-28 November**

ATARI CHRISTMAS SHOW
New Horticultural Hall, London — Database Publications (061) 456 8835 **28-30 November**