A Christmas Miscellany

There's something for everyone this month as Mike Mudge presides over a wide variety of mathematical problems for you to pore over. Plus, feedback from readers, both positive and negative.

Seasons Greetings to all readers of this first extended version of Numbers Count. The one hundred and fortieth column represents the first attempt to satisfy *your* requests for a greater variety of subject matter each month and more detailed information on responses to previous problems.

The various problems posed represent a subset of those suggested by *PCW* readers over the past few years. Experience shows that such material is likely to prove very popular and the selection is intended to appeal to all known, and hopefully many unknown, interest groups.

Don Hunter (February/March 1989), Saffron Walden

Problem H_1. Factorise 13292975656219311750605021691 7.

Suggestion: Use Knuth's Algorithm E and Exercise 12, Art of Computer Programming vol 2, 2nd Edition, p381 etc. Don goes on: "The pleasant thing about a problem like this is that the manufacturers' packages are seldom of any use." Comments, please.

Problem H_2. (a) Investigate the solution of: $ax^2 + bx + c = y^2$ in the particular cases a = 1, b = 0 and (much) more interestingly a = 1549, b = 0 c = 1.

(b) As above when a = 91894770302976, b = 287722528867021824, c = 256527596541064768.

How does this lead to the factors of $2^{79} - 1$?

It is believed that a set of 30 simultaneous integer equations were solved by a mechanical means in 200 micro-seconds over 50 years ago, a time significantly reduced by Lehmer using delay-line techniques, c. 1 micro-second per set.

Tom Napier (March 1989), Pa, USA

Problem N_1. Recall The Fibonacci Numbers, satisfying the linear recurrence relation $F_n = F_{n-1} + F_{n-2}$ where $F_0 = F_1 = 1$.

Their analytic form is given by $F_n = (Z^n - (-Z)^{-n})/(5)^{1/2}$, where $Z = (1 + 5^{1/2})/2$.

Tom's first observation is that the definition can be extended to negative n by writing $F_N = F_{N+2} - F_{N+1}$ from which it can be seen that the absolute value is the same as that of the corresponding positive number but that the signs alternate. The second observation is that replacing $(-Z)^{-n} = (-1)^n(Z)^{-n}$ by $(\cos(n\ PI))\ (Z)^{-n}$ enables a function of a continuous variable to be defined by replacing the integer n by the continuous variable, x say. Some correspondence with the Fibonacci Quarterly suggested to Tom that this extension was original. Is this the only "simple" function which replaces $(-1)^n$ to yield an F_x satisfying the original additive property of F_n? Supply graphs of this, and any other suitable F_x, making a reasoned choice of the "best" or most natural extension.

Problem N_2. In general it is required to determine which physical taps on a shift register must be combined with exclusive OR-gates to create a series delayed by a specific number of clock pulses. In particular, given a 23-bit shift register wired to generate the maximal length (2^{23}-1) sequence, how does one generate a sequence in phase with this but delayed by 2^{22} clock periods? Tom has a tap combination to do this but seeks an algorithm. Also, how is the time delay associated with a given tap combination determined algebraically or computationally?

Albert Debono (February 1988), Malta

Problem D_1. Construct a computer program to express each PRIME NUMBER as a difference of two integers whose prime power decomposition (i.e. whose resolution into prime factors) includes only primes smaller than the given number.

e.g. $5 = 3^2-2^2$, $7 = 5^2-2.3^2$... not an easy task since a decomposition of $29 = 3.11.13^2.19.23-2^{12}.5.7.17$....

Problem D_2. Given two sets of positive integers $A..(a_1,a_2...a_n)$ and $B..(b_1,b_2...b_k)$ define A+B to be the set (a_i+b_j) and A-B to be the set (a_i-b_j) taken over all possible pairs (i,j).

NOTE. Repeated elements are NOT ALLOWED in these sets. Conway conjectured that the number of elements in A-A is never less than the number of elements in A+A. This is known to be false, one counter-example being provided by A..(1,2,3,5,8,9,13,15,16). Verify this result, attempt to find other counter-examples and investigate generalisations relating to (A+A)-A compared with A+(A-A) and other natural combinations. The good news is that long computer runs and/or multiple precision are not likely to be needed here.

Problem D_3. Given the unique prime factorisation of a positive integer, n, in the form $n = {}_{p1}{}^{n1}{}_{p2}{}^{n2}.....{}_{pk}{}^{nk}$ where, of course, the n_k are called the multiplicity of the factors pk. Define an iterative sequence thus f(1) = 2, $f(n) = 1+e_1p_1+e_2p_2+....e_kp_k$, f_2=f(f(n),f_3=f(f(f(n)).. What happens to the sequence of functions (f_N) for various n? This problem is completely solved, reference Mathematical Reviews 50(1975) number 220; but what happens to either the iterates of g(n) = f(n) - 1 or of h(n) = 1 + 2(g(n))?

R.K. Guy, Unsolved Problems in Number Theory, Page 129

Problem G_1. MacMahon's "prime numbers of measurement" are obtained from the sequence of positive integers by excluding all the sums or TWO or MORE consecutive earlier members of the sequence, thus: 1,2,4,5,8,10,14,15,16,21,22,... Jeff Lagarias considers an "easier" sequence formed by excluding the sums of TWO or THREE consecutive earlier members: 1,2,4,5,8,10,12,14,15,16,... and asks if this contains 60% of all positive integers in the limit.

Systematically extend from Lagarias towards MacMahon, investigating the apparent density of the sequence at each stage.

Responses to some, or all, of the above problems may be sent to Mike Mudge, 22 Gors Fach, Pwll-Trap, St Clears, Carmarthen, Dyfed SA33 4AQ, tel (0994) 231121, to arrive by 1 February 1995. Any communications received will be judged, using suitable subjective criteria, and a prize in the form of a £25 book token, or equivalent overseas voucher, will be awarded by Mike Mudge to the "best" contribution arriving by the closing date.

Such contributions should contain a brief description of the hardware used, details of coding, run times and a summary of the results obtained; all in a form suitable for publication in *PCW*. Additionally, readers' comments upon the general, or specific, nature of this month's column would be most valuable

Please note that material can only be returned if a suitable stamped addressed envelope is enclosed.

Feedback from readers

In problem A of "In the prime of life", June 1994, several readers found that the value of 337* - 1 had been omitted from the list of primes; research showed this omission to go back to the original paper "Primes of the Form n!±1 and 2.3.5.....p± 1" by J.P. Buhler, R.E. Crandall and M.A. Penk, Mathematics of Computation, vol. 38, no. 158. April 1982, pp329-643. Professor Richard E Crandall, Vollum Professor of Science at Reed College, Portland, Oregon, acknowledges the omission (a correction was published later in 1982) and refers interested readers to his new book, Projects in Scientific Computation, ISBN 0-387-97808-9, Springer-Verlag 1994, with a long section on number theoretic computations. Searches of the type suggested in Numbers Count have been carried out upto at least 10^{1000}. Many readers have indicated the value of UBasic and also Mathcad in number theoretic research projects: any detailed experiences (good or bad) with these software packages would be reported on in future Numbers Count columns.

This month's prizewinner is John McCarthy of 17 Mount Street, Mansfield, Notts NG19 7AT. John uses Borland C++ version 3.1 on an Amstrad PC2386 20MHz 386DX. He first wrote a C++ class to implement manipulation of positive integers of up to 100,004 decimal digits, followed by a probabilistic primality testing routine "having similarity to Rabin's Algorithm". John refers, in passing, to discovering bugs in the Borland clock() and delay functions and the Timer class... Any readers share this experience?

Attempts at problems D, E, F, G, & H were very minimal and further submissions on these matters are encouraged. The result in F, namely that 40585 = 4!+0!+5!+8!+5! is due to Leigh James, 1964; while in G the use of (consecutive) renders 10! unique, apart from the trivial 1!=0!x1! and 2!=0!x1!x2! = 1!x2!, but what happens if (consecutive) is excluded?

Returning now to the topic of Interval Analysis, *PCW* April 1994, reviewed, briefly, in October's *PCW*. Eldon Hansen invites consideration of the problem of inversion of the Hilbert Segment or order 3 **(Fig 1)** known to be **(Fig 2)**.

Consider 1/2, 1/4 & 1/5 to be represented by their exact decimal equivalents while 1/3 is represented by the interval (0.33333 33333, 0.33333 33334). NOTE: In theory, we could invert 3H and use exact decimal representation throughout, however this is not possible in general. If this computation is carried through, the inverse is found to be as **Fig 3** for one particular algorithm. Readers are invited to write a matrix inversion routine in interval arithmetic and compare their results with the above. Notice that the introduction of an interval (non-trivial) for 1/3 was based upon a decimal representation; for a binary representation, different criteria may be needed? Alternatively, since there is only one interval in the approximation to H, the two "extreme" matrices can be inverted using a library programme to produce the "extremes" of the inverse? Such a luxury is not available in any "real-world" calculation where more than one piece of input data has an error bound, or experimental error or degree of uncertainty associated with it, which may be amenable to interval representation.

1

$$H = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & 1/5 \end{bmatrix}$$

2

$$H^{-1} = \begin{bmatrix} 9 & -36 & 30 \\ -36 & 192 & -180 \\ 30 & -180 & 180 \end{bmatrix}$$

3

$$H^{-1} + 10^{-7} \begin{bmatrix} (-8,8) & (-20,30) & (-40,30) \\ (-50,60) & (-200,100) & (-200,200) \\ (-40,40) & (-100,200) & (-200,200) \end{bmatrix}$$

PCW Contributions Welcome

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.