PURSUITS

All mod cons

Mike Mudge investigates the Chinese remainder theorem (CRT).

Definition
A is said to be congruent to B modulo m, if and only if A−B is an integer multiple of m. This relationship is written A≡B(mod m) or simply A≡B(m). Alternatively, we may say that A and B leave the same remainder when divided by m; the remainder is called the residue of A (or B) modula m. For example, 32≡17(5); also 982≡−143(9).

Historical note
A simple example, taken from a whole family of ancient Chinese puzzles, asks for a number which leaves a remainder 1 when divided by 3, a remainder 2 when divided by 5, and a remainder 3 when divided by 7.

A solution is therefore sought to the three simultaneous congruences: $x\equiv1(3)$; $x\equiv2(5)$; $x\equiv3(7)$...!

The Chinese Remainder theorem
Let $m_1,m_2,...m_r$ be pairwise relatively prime integers. Then the system of simultaneous congruences: $x\equiv a_1(m_1)$; $x\equiv a_2(m_2)$;...$x\equiv a_r(m_r)$ has a unique solution modulo $M=m_1m_2...m_r$.

Constructively, if $M_k=M/m_k$ for k=1,2,...r and if further y_k is defined by $M_ky_k\equiv1(m_k)$ then the required solution is $x=a_1M_1y_1+a_2M_2y_2+...a_rM_ry_r$.

For complete proof see, for example, KH Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley 1984.

Example
To solve the three simultaneous congruences ! above: $a_1=1$, $a_2=2$, $a_3=3$: $M=3.5.7=105$, $M_1=105/3=35$, $M_2=105/5=21$, $M_3=105/7=15$.

Solve $35y_1\equiv1(3)$, thus $2y_1\equiv1(3)$ or $y_1\equiv2(3)$; similarly from $21y_2\equiv1(5)$ find $y_2\equiv1(5)$ and from $15y_3\equiv1(7)$ find $y_3\equiv1(7)$. Hence from CRT $x\equiv1.35.2+2.21.1+3.15.1\equiv157\equiv52(105)$.

Example
To solve the three simultaneous congruences $x\equiv1(5)$, $x\equiv2(6)$ and $x\equiv3(7)$ use $a_1=1$, $a_2=2$, $a_3=3$, $m_1=5$, $m_2=6$ and $m_3=7$ to yield $M=210$, $M_1=42$, $M_2=35$, $M_3=30$, $y_1=3(5)$, $y_2\equiv5(6)$, $y_3\equiv4(7)$ and hence $x\equiv206(210)$.

Multi-length addition
Suppose that the word size of a computer is only 100, but that we wish to do arithmetic with integers as large as 10^6. First find pairwise relatively prime integers less than 100 with a product greater than 10^6; say 99, 98, 97 and 95. Convert integers less than 10^6 into quadruplets consisting of their least positive residues modulo the above integers. (**Note** This requires multi-precision operations but is only carried out once for all.)

Finally carry out the required arithmetic operations on the members of the appropriate quadruplets (to the appropriate modulus), and combine the results using the CRT.

Example To add x=123684 and y=413456 on a computer of word size 100 using the moduli suggested above:
$x\equiv33(99)$, $y\equiv32(99)$ hence $x+y\equiv65(99)$
$x\equiv8(98)$, $y\equiv92(98)$ hence $x+y\equiv2(98)$
$x\equiv9(97)$, $y\equiv42(97)$ hence $x+y\equiv51(97)$
$x\equiv89(95)$, $y\equiv16(95)$ hence $x+y\equiv10(95)$...!!

Solving II by CRT using $M=89403930$, $M_1=903070$, $M_2=912288$, $M_3=921690$, $M_4=941094$ yields $y_1\equiv37(99)$, $y_2\equiv38(98)$, $y_3\equiv24(97)$, $y_4\equiv4(95)$ hence by CRT, $x+y\equiv537140$ (89403930) and by 'order of magnitude test' x+y=537140.

Readers who doubt the usefulness of this approach should consult D Knuth, *The Art of Computer Programming: Semi-Numerical Algorithms*, Volume 2 (2nd edition, Addison-Wesley 1981).

Problem
Readers are invited to write computer programs to:
1) Solve systems of linear congruences of the type found in the CRT. Test case: $x\equiv2,3,4,5\&6$ moduli 11,12,13,17&19. Answer $x\equiv150999(554268)$.
2) Carry out multi-precision addition and multiplication using the CRT.

Attempts at either or both of these projects may be sent to Mike Mudge, 'Square Acre', Stourbridge Road, Penn, South Staffordshire WV4 5NF, tel: (0902) 892141, by 1 May 1989.

Review, September

Rare and very rare primes generated an above average response, probably due to the omission of the 'square' on the modulus in the Wilson Primes: ...p_W^2... sorry!

Sierpinski Primes: if there are only finitely many then there are infinitely many composite Fermat Numbers. Reg Bond pointed out that the given bound of 3×10^{10} is at least 4.137×10^{10}.

Best general reference once again, *The Book of Prime Number Records* by Paulo Ribenboim, Springer-Verlag 1988. I do have a list of 850 prime numbers with more than 1000 digits constructed by Samuel Yates, if any reader is interested — 15 have more than 10,000 digits.

This month's prizewinner is John C McCarthy of 168 Fairholme Drive, Mansfield, Notts NG19 6DU, whose work shows that success can be achieved in interpretive Superbasic on a QL.

Mike Mudge welcomes correspondence on any subject within the areas of number theory and other computational mathematics. Particularly welcome are suggestions, either general or specific, for future Numbers Count articles. All letters will be answered in due course.

LEISURE LINES

Brainteasers courtesy of JJ Chessa.

Quickie
Which is the odd one out in the following set?

HIJACK CANOPY THIRST
MONDAY DEFEAT
STUPID SIGHING

No prizes, so don't send answers.

Prize Puzzle
Very simple this month — perhaps.

What is the smallest number that can be written using only the digits 3,5 and 7 such that both the number and also the sum of its digits are exactly divisible by 3,5 and 7?

Answer on postcards (or backs of envelopes) to: *PCW* Prize Puzzle March, *PCW* Editorial, VNU House, 32-32 Broadwick Street, London W1A 2HG, to arrive not later than last post on 31 March 1989.

Good Luck!

Winners

Because of the Xmas holiday and advanced publishing deadlines, the winners of the November and December prize puzzles are announced in this issue.

November 1988
101 entries — mostly correct. The winner was RT Deadill of Southampton with the correct solution of £47.41 starting wage.

December 1988
The Christmas crossword attracted about 150 entries. The winner was Mr Mark Gill of Abingdon, Oxfordshire and the solution is shown alongside.

Our congratulations to both winners and their prizes are on their way. To all the near misses, keep trying!