Generalized Chinese Remainder Theorem

Harry J. Smith

March 23, 2005

Let a, b, r, and s be any four integers. Then there may be an integer N such that

$$N \equiv a \pmod{r}$$

and

$$N \equiv b \pmod{s}.$$

There is a solution if and only if $a \equiv b \pmod{d}$, where d = (r, s). Of course, if $d = 1$ there is a solution for any a and b as determined by the normal Chinese remainder theorem. Moreover, if an N exists it is uniquely determined modulo $M = rs/d$.

To determine N and M, first get all of the numbers nonnegative by replacing r with $|r|$, s with $|s|$, a with mod(a, r), and b with mod(b, s), where mod(a, r) is the common residue of $a \pmod{r}$. Now use the extended form of Euclid's algorithm to compute d, u and v such that

$$d = \mathrm{GCD}(r, s) = ru + sv.$$

Note that u and v may be zero or negative. Now if $b - a$ is not divisible by d there is no solution. If $d \mid (a - b)$ there is a solution. Let

$$p = r/d$$

and

$$q = a + up(b - a).$$

Then

$$M = ps$$

and

$$N = \mathrm{mod}(q, M).$$

To solve a set of simultaneous congruences such as

$$x \equiv a_i \pmod{m_i}$$

with $i = 1, ..., r$, solving the first two will reduce the number of congruences by one. Repeat this process if possible until there is only one congruence and you have the final answer.

References:

Knuth, The Art of Computer Programming Vol.2, Section 4.3.2, exercise 3. http://www-cs-faculty.stanford.edu/~knuth/taocp.html

PARI/GP Calculator http://pari.math.u-bordeaux.fr/

Eric W. Weisstein. "Chinese Remainder Theorem." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/ChineseRemainderTheorem.html

---

Notes:

If you are not familiar with some of the notation, I will explain: $N \equiv a \pmod{r}$ is a congruence and is read N is congruent to a modulo r and it means N and a have the same remainder when divided by r. This is an integer divide like 14/4 = 3 with a remainder of 2. http://mathworld.wolfram.com/Congruence.html

$d = (r, s)$ is read d is the greatest common divisor GCD of r and s and it means that $r \equiv 0 \pmod{d}$, $s \equiv 0 \pmod{d}$, and there is no larger number than d that evenly divides both r and s. http://mathworld.wolfram.com/GreatestCommonDivisor.html

N is uniquely determined modulo $M = rs/d$ means that there are an infinite number of solutions for N but they all have the same remainder when divided by M, and all numbers with this remainder when divided by M are solutions. Of course rs/d is r multiplied by s and divided by d.

$|r|$ is the absolute value of r. $|-7| = 7$, $|7| = 7$.
http://mathworld.wolfram.com/AbsoluteValue.html

$c = \text{mod}(a, r)$ is the common residue of a (mod r) means that $c \equiv a$ (mod r) and c is nonnegative and less than r, i.e. $0 \le c < r$. http://mathworld.wolfram.com/Mod.html http://mathworld.wolfram.com/CommonResidue.html

The normal Chinese remainder theorem is the same as this but it assumes that $(r, s) = 1$. In this form, it always has a solution for any a and b. The method presented to compute N and M will still work if $(r, s) = 1$.
http://mathworld.wolfram.com/ChineseRemainderTheorem.html

Euclid's algorithm is the oldest algorithm in the book (see Euclid's Elements, Book 7, Propositions 1 and 2). It is used to compute $d = \text{GCD}(r, s)$.
http://mathworld.wolfram.com/EuclideanAlgorithm.html The extended form of Euclid's algorithm also determines u and v such that $d = \text{GCD}(r, s) = ru + sv$.
http://mathworld.wolfram.com/ExtendedGreatestCommonDivisor.html

The | in $d \mid (a - b)$ says that d divides the difference a minus b, i.e. a minus b is divisible by d. http://mathworld.wolfram.com/Divide.html

$x \equiv a_i$ (mod m_i) with $i = 1, ..., r$, says that there is a set of r different congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

etc. …

$$x \equiv a_r \pmod{m_r}$$

and x represents the maximum set of integers that satisfies all of them. If while you are solving this set, taking two at a time, you find a pair that has no solution, then the set has no solution.

Here is a note I sent to John Hopkins:

John:

Around A.D. 100, the Chinese mathematician Sun-Tsu solved the following problem: There is a number that has a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7. Mathematicians write this as

$$x = 2 \pmod 3$$

$x = 3 \pmod 5$
$x = 2 \pmod 7$

The solution is $x = 23 \pmod{105}$, which says that 23 is the smallest number > 0 that satisfies the three equations and $x = 23 + 105*n$ with $n = 0, 1, 2, ...$ are all of the solutions > 0 (actually $-82 = 23 - 105$ is also a solution).

There are some problems like

$x = 2 \pmod 6$
$x = 3 \pmod 8$

that have no solutions, but

$x = 2 \pmod 6$
$x = 4 \pmod 8$

has the solution $x = 20 \pmod{24}$.

My calculator program, XICalc, can now solve all such problems that have a solution and tell you when there is no solution.

Look at http://www.cut-the-knot.org/blue/chinese.shtml

and

http://www.math.swt.edu/~haz/prob_sets/notes/node25.html

-Harry