Chinese Remaindering

CS255

Chris Pollett

Apr. 17, 2006.

Outline

- Algorithms for Modular Linear Equations
- The Chinese Remainder Theorem

Some Theorems

- Before giving our Modular-Linear-Equation-Solver algorithm we need to give a last couple theorems
- The first shows such equations have a solution:

Theorem. Let $d=\gcd(a,n)$ and suppose $d=ax' + ny'$ for some integers x' and y'. If $d \mid b$, then the equation $ax \equiv b \pmod{n}$ has as one of its solutions the value x_0 where $x_0 = x'(b/d) \bmod n$.

Proof: Suppose $x_0 = x'(b/d) \bmod n$. Then

$$\begin{aligned} ax_0 &\equiv ax'(b/d) \pmod{n} \\ &\equiv d(b/d) \pmod{n} \\ &\equiv b \pmod{n} \end{aligned}$$

The Second Theorem

- The second theorem gives the number of solutions

Theorem. Suppose $ax \equiv b \pmod{n}$ is solvable and that x_0 is a solution. Then this equation has exactly d solutions given by $x_i = x_0 + i(n/d)$, for i=0,1,..

Proof. Since $n/d > 0$ and $0 \leq i(n/d) < n$, the values x_0, x_1,..,x_d are all distinct. Each will be a solution since

$ax_i \equiv a(x_0 + i(n/d)) \equiv ax_0 + ai(n/d)) \equiv ax_0 \equiv b(\text{mod n})$

From our corollary of last day, the equation either has d solutions or no solutions so we must have all of them.

Modular Linear Equation Algorithm

- Given the above theorems we are now in position to give an algorithm for solving modular equations:

Modular-Linear-Equation-Solver(a, b, n)

1. $(d, x', y') =$ Extended-Euclid(a, n)
2. if $d \mid b$
   a) then $x_0 = x'(b/d) \bmod n$
   b) for $i = 0$ to $d - 1$
   c) do print $(x_0 + (i \cdot (n/d)) \bmod n$
   d) else print "no solutions"

About The Chinese Remainder Theorem

- This theorem goes back to Chinese text of at least 100A.D.
- It has two main uses:
  1. It tells us if n is the product of pairwise relatively prime numbers $n_0,..,n_k$ then the structure of $\mathbf{Z}_n$ behaves as that of the Cartesian product $\mathbf{Z}_{n_0} \times \mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_k}$
  2. It gives us efficient/parallel algorithms for certain operations like multiplication/division by allowing us to work modulo n_i rather than modulo n.

The Chinese Remainder Theorem

Theorem. Let $n = n_1 n_2 \cdots n_k$, where the n_i are pairwise relatively prime. Consider the correspondence $a \Leftrightarrow (a_1,..,a_k)$ where $a_i = a$ mod n_i. Then this is a bijection and preserves addition and product.

Proof. The preservation of plus and times is easy to check. Computing the a_i's from a is also easy. To compute a from $(a_1,..,a_k)$, let $m_i = n/n_i$, so gcd(m_i, n_i)=1. Compute $t_i = m_i^{-1}$ mod n_i using the extended Euclidean Algorithm. Let $c_i = m_i t_i$. Finally, compute a as $(a_0 c_0 + .. + a_k c_k)$. Notice

$a \equiv a_i c_i \equiv a_i\, m_i\, t_i \equiv a_i$ (mod $\mathrm{n_i}$)