Professor M. J. Fischer *October 5, 2006*

Linear Congruence Equations

Let $a, x \in \mathbf{Z}_n^*$. Recall that x is said to be an *inverse* of a modulo n if $ax \equiv 1 \pmod{n}$. It is easily seen that the inverse, if it exists, is unique modulo n, for if $ax \equiv 1 \pmod{n}$ and $ay \equiv 1 \pmod{n}$, then $x \equiv xay \equiv y \pmod{n}$. We denote this unique x, when it exists, by $a^{-1} \pmod{n}$ (or simply a^{-1} when the modulus n is clear from context).

Theorem 1 *Let $a \in \mathbf{Z}_n^*$. Then a^{-1} exists in $\mathbf{Z}_n^*$.*

Proof: Let $a \in \mathbf{Z}_n^*$ and consider the function $f_a(x) = ax \bmod n$. f_a is easily shown to be a one-one mapping from $\mathbf{Z}_n^*$ to $\mathbf{Z}_n^*$. Hence, f_a is also onto, so for some $x \in \mathbf{Z}_n^*$, $f_a(x) = 1$. Then $ax \equiv 1 \pmod{n}$, so $x = a^{-1} \pmod{n}$. ■

We showed in class how to use the Extended Euclidian algorithm to efficiently compute $a^{-1} \pmod{n}$ given a and n.

Here we consider the solvability of the more general linear congruence equation:

$$ax \equiv b \pmod{n} \tag{1}$$

where $a, b \in \mathbf{Z}_n^*$ are constants, and x is a variable ranging over $\mathbf{Z}_n^*$.

Theorem 2 *Let $a, b, n \in \mathbf{Z}_n^*$. Let $d = \gcd(a, n)$. If $d \mid b$ then $ax \equiv b \pmod{n}$ has d solutions $x_0, \ldots, x_{d-1}$, where*

$$x_t = \left(\frac{b}{d}\right)\bar{x} + \left(\frac{n}{d}\right)t \tag{2}$$

and $\bar{x} = (\frac{a}{d})^{-1} \pmod{(\frac{n}{d})}$. If $d \nmid n$, then $ax \equiv b \pmod{n}$ has no solutions.

Proof: Let $d = \gcd(a, n)$. Clearly if $ax \equiv b \pmod{n}$, then $d \mid b$, so there are no solutions if $d \nmid b$.

Now suppose $d \mid b$. Since $(\frac{a}{d})$ and $(\frac{n}{d})$ are relatively prime, $\bar{x}$ exists by Theorem 1. Multiplying both sides of (2) by a, we get

$$ax_t = b\left(\frac{a}{d}\right)\bar{x} + n\left(\frac{a}{d}\right)t \tag{3}$$

where now we are working over the integers. But $(\frac{a}{d})\,\bar{x} = 1 + \frac{kn}{d}$ for some k by the definition of $\bar{x}$, so substituting for $(\frac{a}{d})\,\bar{x}$ in (3) yields

$$ax_t = b + kn\left(\frac{b}{d}\right) + n\left(\frac{a}{d}\right)t \tag{4}$$

The quantities in parentheses are both integers, so it follows immediately that $ax_t \equiv b \pmod{n}$ and hence x_t is a solution of (1).

It remains to show that the d solutions above are distinct modulo n. But this is obvious since $x_0 < x_1 < \ldots < x_{d-1}$ and $x_{d-1} - x_0 = \frac{n}{d}(d-1) < n$. ■