Math 445 Number Theory

October 4, 2004

Proposition: If f is a polynomial with integer coefficients and $(M,N)=1$, then the congruence equation $f(x)\equiv 0 \pmod{MN}$ has a solution $\Leftrightarrow$ the equations $f(x)\equiv 0 \pmod{M}$ and $f(x)\equiv 0 \pmod{N}$ both do.

The direction ($\Rightarrow$) is immediate; $MN|f(x)$ implies $M|f(x)$ and $N|f(x)$, since $M,N|MN$. The point to ($\Leftarrow$) is that the solutions we know of to each of the two equations might be *different*: $f(x_1)\equiv 0 \pmod{M}$ and $f(x_2)\equiv 0 \pmod{N}$. What we wish to show is that a single number solves *both*, since then $M|f(x_0)$ and $N|f(x_0)$, and then $(M,N)=1$ implies that $MN|f(x_0)$.

To do this, we use the fact that f is a polynomial, since then if $a\equiv b \pmod{n}$, then $f(a)\equiv f(b)b \pmod{n}$. So if we suppose that we have found a and b with $f(a)\equiv 0 \pmod{M}$ and $f(b)\equiv 0 \pmod{N}$, then any x satisfying both $x\equiv a \pmod{M}$ and $x\equiv b \pmod{N}$ will satisfy both $f(x)\equiv 0 \pmod{M}$ and $f(x)\equiv 0 \pmod{N}$ simultaneously, as desired. So it is enough to show that for any a,b , there is an x which simultaneously satisfies

$$x\equiv a \pmod{M} \quad \text{and} \quad x\equiv b \pmod{N}$$

But since $(M,N)=1$, this is true by the Chinese Remainder Theorem. In fact, finding x is a matter of solving $x=a+Mi$, $x=b+Nj$, so we need $a+Mi=b+Nj$, so $b-a=Mi-Nj$. But since $(M,N)=1$, we can use the Euclidean algorithm to write $1=MI_0+NJ_0$, and then $i=(b-a)I_0, j=-(b-a)J_0$ will work, allowing us to solve for x. In fact, since the only other I,J which will work are $I=I_0+kN, J=J_0-kM$, we find that our solution x is unique modulo MN .

For any pair of solutions a,b to $f(a)\equiv 0 \pmod{M}$ and $f(b)\equiv 0 \pmod{N}$ there is a unique corresponding x mod MN (with $x\equiv a \pmod{M}$ and $x\equiv b \pmod{N}$) satisfying $f(x)\equiv 0 \pmod{MN}$. Iintroducing the notation $S(n)=$ the number of solutions, mod n, to the equation $f(x)\equiv 0 \pmod{n}$, we then have shown that $S(MN)=S(M)S(N)$ whenever $(M,N)=1$. So by induction, whenever $N_1,\dots N_k$ are relatively prime, $S(N_1\cdots N_k)=S(N_1)\cdots S(N_k)$.

So if $N=p_1^{k_1}\cdots p_r^{k_r}$ is the prime factorization of the odd number N, then for any $(a,N)=1$ (so $(a,p_i)=1$ for each i) we have $x^n\equiv a \pmod{N}$ has solutions $\Leftrightarrow$ $x^n\equiv a \pmod{p_i^{k_i}}$ does for every i , and we know how to determine when that occurs.

Quadratic Residues: If $x^2\equiv a \pmod{n}$ has a solution, a is a *quadratic residue* modulo n . If it doesn't, a is a *quadratic non-residue* modulo n . Euler's Criterion gives us a test: if p is a prime, then a is a quadratic residue mod n $\Leftrightarrow$ $a^{\frac{p-1}{2}}\equiv 1 \pmod{p}$. But this may require a lot of calculation if p is large; our next task is to find a quicker way.

To talk about things in a compact manner, we introduce the *Legendre symbol*; for p an odd prime,

$$\left(\frac{a}{p}\right)=\begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases}$$

By Euler's criterion, this really means $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod{p}$, but our goal is to find a *quicker* way to compute it!