Math 445 Number Theory

September 22-24, 2008

One tool that we need to add to our toolbox is the existence of *primitive roots of 1 mod a prime* p: that is, the existence of integers a for which $\mathrm{ord}_p(a) = p-1$. In the language of groups, this says that the group of units in $\mathbb{Z}_p$ is cyclic, when p is prime. In order to prove this, we need a bit of machinery:

Lagrange's Theorem: If $f(x)$ is a polynomial with integer coefficients, of degree n, and p is prime, then the equation $f(x) \equiv 0 \pmod{p}$ has at most n mutually incongruent solutions, unless $f(x) \equiv 0 \pmod{p}$ for <u>all</u> x.

To see this, do what you would do if you were proving this for real or complex roots; given a solution a, write $f(x) = (x-a)g(x) + r$ with r=constant (where we understand this equation to have coefficients in $\mathbb{Z}_p$) using polynomial long division. This makes sense because $\mathbb{Z}_p$ is a *field*, so division by non-zero elements works fine. Then $0 = f(a) = (a-a)g(a)+r = r$ means $r = 0$ in $\mathbb{Z}_p$, so $f(x) = (x-a)g(x)$ with $g(x)$ a polynomial with degree $n-1$. Structuring this as an induction argument, we can assume that $g(x)$ has at most $n-1$ roots, so f has at most (a and the roots of g, so) n roots, because, *since* p *is prime*, if $f(b) = (b-a)g(b) \equiv 0 \pmod{p}$, then either $b - a \equiv 0$ (so a and b are congruent mod p), or $g(b) = 0$, so b is among the roots of g.

This in turn leads us to

Corollary: If p is prime and $d|p-1$, then the equation $x^d - 1 \equiv 0 \pmod{p}$ has *exactly* d solutions mod p.

This is because, writing $p-1 = ds$, $f(x) = x^{p-1}-1 \equiv 0$ has exactly $p-1$ solutions (namely, 1 through $p-1$), and $x^{p-1} = (x^d-1)(x^{d(s-1)} + x^{d(s-2)} + \cdots + x^d + 1) = (x^d-1)g(x)$. But $g(x)$ has *at most* $d(s-1) = (p-1)-d$ roots, and $x^d - 1$ has at most d roots, and together (since p is prime) they make up the $p-1$ roots of f. So in order to have enough, they both must have *exactly* that many roots.

We introduce the notation $p^k||N$, which means that $p^k|N$ but $p^{k+1} \not| N$.

For each prime p_i dividing $n-1$, $1 \le i \le s$, we let $p_i^{k_i}||n-1$. Then the equation (*) $x^{p_i^{k_i}} \equiv 1 \pmod{n}$ has $p_i^{k_i}$ solutions, while (†) $x^{p_i^{k_i-1}} \equiv 1 \pmod{n}$ has only $p_i^{k_i-1} < p_i^{k_i}$ solutions; pick a solution, a_i to (*) which is not a solution to (†) . [In particular, $\mathrm{ord}_n(a_i) = p_i^{k_i}$.] Then set $a = a_1 \cdots a_s$. Then a computation yields that, mod n, $a^{\frac{n-1}{p_i}} \equiv a_i^{\frac{n-1}{p_i}} \not\equiv 1$, since otherwise $\mathrm{ord}_n(a_i)|\dfrac{n-1}{p_i}$, and so $\mathrm{ord}_n(a_i)|\gcd(p_i^{k_i}, \dfrac{n-1}{p_i}) = p_i^{k_i-1}$, a contradiction. So $p_i^{k_i}||\mathrm{ord}_n(a)$ for every i, so $n-1|\mathrm{ord}_n(a)$, so $\mathrm{ord}_n(a) = n-1$.

This result is fine for theoretical purposes (and we will use it many times), but it is somewhat less than satisfactory for computational purposes; this process of *finding* such an a would be very laborious.