Math 445 Number Theory

September 17, 2004

Fermat numbers $2^{2^n}+1$; known prime only for $n=0,1,2,3,4$. Part of the interest in them is

Fact (Gauss): A regular n-gon can be constructed by compass and straight-edge $\Leftrightarrow$ $n=2^k d$ where d is a product of distinct Fermat primes.

So the fact that we know of only 5 Fermat primes means we only know of 32 regular n-gons with an odd number of sides that can be so constructed. If there is another one, it has more than a billion sides!

Lucas' Theorem has a rather strong converse:

Theorem: If p is prime, then there is an a with $(a,p)=1$ so that for every prime q with $q|n-1$, $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$.

Note that $a^{p-1}\equiv 1 \pmod{p}$ is always true, because p is prime. In effect, what this theorem says is that $\mathrm{ord}_p(a)=p-1$ (which in the language of groups says that the group of units in $\mathbb{Z}_p$ is cyclic, when p is prime). In order to prove this theorem, 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 $\underline{\text{all}}$ 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.

This in turn will allow us to find our a ....