Math 445 Number Theory

September 29, 2004

Last time: If m is an odd prime and $(a,m)=1$, then

$$x^2 \equiv a \pmod{m} \text{ has } \begin{cases} 2 \text{ solutions,} & \text{if } a^{\frac{m-1}{2}} \equiv 1 \\ 0 \text{ solutions,} & \text{if } a^{\frac{m-1}{2}} \equiv -1 \end{cases}$$

The only fact we really needed to know about the prime m, though, was that there was a primitive root, b, mod m. This, it turns out, is true somewhat more generally, and will allow us to extend our result above, suitably modified. What is in fact true is:

Theorem: If p is an odd prime and $k \geq 1$, then $m = p^k$ has a primitive root, i.e., there is an integer b with $\text{ord}_{p^k}(b) = \Phi(p^k) = p^{k-1}(p-1)$.

To see this, start with a primitive root b modulo p , i.e., $\text{ord}_p(b) = p-1$, and consider the collection of integers

$$A = \{b + pk : 0 \leq k \leq p-1\}$$

We claim that for all but at most one $a \in A$, $\text{ord}_{p^2}(a) = p(p-1)$. To see this, note that since $(a,p) = (b,p) = 1$, $(a,p^2) = 1$, so $a^{\Phi(p^2)} = a^{p(p-1)} \equiv 1 \pmod{p^2}$ by Euler's Theorem, so $\text{ord}_{p^2}(a) | p(p-1)$. But $a^k \equiv 1 \pmod{p^2}$ implies $a^k \equiv 1 \pmod{p}$ and $a \equiv b \pmod{p}$, so $p-1 | \text{ord}_{p^2}(a)$, so $\text{ord}_{p^2}(a) = p-1$ or $p(p-1)$. Our claim asserts that there is at most one a where it is $p-1$.

So, suppose there are two!

Suppose $(b+k_1p)^{p-1} \equiv 1 \equiv (b+k_2p)^{p-1}$, mod p^2 with $0 \leq k_2 < k_1 \leq p-1$. Then $p^2 | (b+k_1p)^{p-1} - (b+k_2p)^{p-1} = [(b+k_1p)-(b+k_2p)] \cdot [(b+k_1p)^{p-2} + (b+k_1p)^{p-3}(b+k_2p) + \cdots + (b+k_1p)(b+k_2p)^{p-3} + (b+k_2p)^{p-2}] = p(k_1-k_2)(\text{stuff})$

So $p | (k_1-k_2)(\text{stuff})$, so $p | (k_1-k_2)$ or $p | (\text{stuff})$. But $0 < k_1 - k_2 < p-1$, so the first is impossible. And, mod p ,

$$\begin{aligned} \text{stuff} &= (b+k_1p)^{p-2} + (b+k_1p)^{p-3}(b+k_2p) + \cdots + (b+k_1p)(b+k_2p)^{p-3} + (b+k_2p)^{p-2} \\ &\equiv (b)^{p-2} + (b)^{p-3}(b) + \cdots + (b)(b)^{p-3} + (b)^{p-2} = (p-1)b^{p-2} \end{aligned}$$

and since $p \not| (p-1)$, $p \not| b$, p can't divide this stuff, either. This gives us a contractiction, so there is at most one value of $0 \leq k \leq p-1$ for which $\text{ord}_{p^2}(b+kp) = p-1$. So for all of the others, $\text{ord}_{p^2}(b+kp) = p(p-1)$, i.e., $b+kp$ is a primitive root modulo p^2 .

Next time we will see that we get all other higher powers for free......