Math 445 Number Theory

October 00, 2004

We have seen (because there is a primitive root mod p^k for p an odd prime):

Theorem: If p is an odd prime, $k \geq 1$, and $(a,p)=1$, then the equation

$$x^n \equiv a \pmod{p^k} \text{ has a solution} \Leftrightarrow a^{\frac{\Phi(p^k)}{(n,\Phi(p^k))}} \equiv 1 \pmod{\Phi p^k}$$

But what about $p=2$? This case is a bit different, since for $k \geq 3$ there is no primitive root mod 2^k. But we can almost manage it:

Proposition: 5 has order $2^{k-2} = \Phi(2^k)/2 \bmod 2^k$.

This is because $\mathrm{ord}_{16}(5) = 4 = 2{\cdot}\mathrm{ord}_8(5)$, and so our earlier result tells us that it will keep rising by a factor of 2 ever afterwards.

This in turn implies that

Proposition: If $k \geq 3$ and $(a, 2^k) = 1$ (i.e., a is odd), then $a \equiv 5^j$ or $a \equiv -5^j \bmod 2^k$, for some $1 \leq j \leq 2^{k-2}$

This is because the integers $5^j : 1 \leq j \leq 2^{k-2}$ are all distinct mod 2^k, as are the $-(5^j) : 1 \leq j \leq 2^{k-2}$, and they are distinct from one another, because mod 4, $5^j \equiv 1^j = 1$, and $-(5^j) \equiv -(1^j) \equiv -1 \equiv 3$, so the two collections have nothing in common. But together they account for $2^{k-2} + 2^{k-2} = 2^{k-1} = \Phi(2^k)$ of the elements relatively prime to 2^k, i.e., all of them.

In particular, the representation of such an a is unique. With this in hand, we can show:

Theorem: If n is odd and $(a,2)=1$, then for every $k \geq 1$, $x^n \equiv a \pmod{2^k}$ has a solution.

To see this, note that $a \equiv \pm 5^j$ by the above result. If $a \equiv 5^j$, then as in the case of an odd prime, we simply assume that the solution x (since it also must have $(x,2)=1$) is $x = 5^r$ for some r, and solve $5^{nr} \equiv 5^j \pmod{2^k}$ by solving $nr \equiv j \bmod \mathrm{ord}_{2^k}(5) = 2^{k-2}$ for r, which we can do, since $(n, 2^{k-2}) = 1$. If $a \equiv -(5^j)$, then we just solve $y^n \equiv 5^j$ first; then since n is odd, $x = -y$ will solve our equation; $x^n = (-y)^n = -y^n \equiv -(5^j) \equiv a$.

For even exponents, things are slightly more complicated.

Theorem: If $k \geq 3$, $(a,2)=1$ and $n = 2^m \cdot d$ with d odd, $m \geq 1$, then $x^n \equiv a \pmod{2^k}$ has a solution $\Leftrightarrow a \equiv 1 \pmod{2^{m+2}}$.

($\Rightarrow$): If $x^n \equiv a \pmod{2^k}$ has a solution, then $(x,2)=1$, so $x \equiv \pm 5^j \bmod 2^k$ for some j . We may assume that $m \leq k-2$, otherwise $x^n = (x^{2^{k-2}})^s \equiv 1^s = 1$ for all x, so only $a \equiv 1$ will have a solution. So, since n is even, $a \equiv (\pm 5^j)^n = 5^{jn} = 5^{jd2^m} \equiv (5^{dj})^{2^m} \bmod 2^k$, so this is also true mod 2^{m+2}. So $a \equiv x^n \equiv (5^{4dj})^{2^m} = y^{2^m} \equiv 1 \bmod 2^{m+2}$, since all (odd) integers have order, mod 2^{m+2}, dividing 2^m .

($\Leftarrow$): If $a \equiv 1 \pmod{2^{m+2}}$, then $a = 1 + N2^{m+2}$, so $a^{2^{k-m-2}} = (1+N2^{m+2})^{2^{k-m-2}} = 1 + N2^k +$ higher powers of $2 \equiv 1 \pmod{2^k}$. But $a \equiv \pm 5^j \pmod{2^k}$, and we must have $\pm 1 = 1$, since $a \equiv 1 \pmod 4$. So $a \equiv 5^j \pmod{2^k}$, so $a^{2^{k-m-2}} = 5^{j \cdot 2^{k-m-2}} \equiv 1 \pmod{2^k}$, so $2^{k-2} | j \cdot 2^{k-m-2}$, so $2^m | j$. So $j = 2^m c$, and so we really wish to solve the equation $x^{2^m d} = (x^{2^m})^d \, equiv (5^{2^m})^c = 5^{2^m c}$. If we instead solve $x^d \equiv 5^c$, which, from the theorem above, we can, since d is odd, then $x^{2^m d} = (x^d)^{2^m} \, equiv (5^c)^{2^m} = 5^{2^m c} \equiv a$, as desired!