Math 445 Number Theory

September 24, 2004

Last time we found the result *"If p is an odd prime then $x^2 \equiv -1 \pmod p$ has a solution $\Leftrightarrow p \equiv 1 \pmod 4$"* useful. Now we will explore such equations more generally.

When does the equation $x^n \equiv a \pmod m$ have a solution?

We will find it useful to first deal with the warm-up problem *When does $nx \equiv a \pmod m$ have a solution?* For this, we have $nx \equiv a \pmod m \Leftrightarrow m|nx - a \Leftrightarrow a = nx - my$ for some $x, y \Leftrightarrow (n, m)|a$. Further, if $nx_0 \equiv a \pmod n$, then a complete set of incongruent solutions is given by (setting $k = (n, m)$)

$$x_0, x_0 + \frac{m}{k}, \ldots, x_0 + (k-1)\frac{m}{k}\ , \qquad \text{since } m|n\frac{m}{k} = m\frac{n}{k}$$

So there are in fact (n, m) solutions, if there are any.

Turning now to the main question, (*) $x^n \equiv a \pmod m$, we begin by supposing m is prime, so that there is a primitive root r mod m , i.e., $\text{ord}_m(r) = m - 1$. Then either $m|a$ (so $a \equiv 0$ and $x = 0$ solves (*)) or $(a, m) = 1$. In the latter case, $a = r^s$ for some s. Since $(a, m) = 1$, any possible solution to (*) must have $(x, m) = 1$, as well, and so we can write $x = r^t$ for some t. So the equation that we *really* wish to solve is

$$(**)\ (r^t)^n \equiv r^s \pmod m \qquad \text{(where we wish to solve for } t).$$

But this means we wish to solve $(r^{nt-s} \equiv 1 \pmod m$, which, since $\text{ord}_m(r) = m - 1$, means $m-1|nt-s$, i.e., $nt \equiv s \pmod{m-1}$. But as we have just seen, this has a solution (and we know how many) $\Leftrightarrow (n, m-1)|s$. Translating this back into information about a, we find that $s = (n, m-1)q$ so $a = r^s = r^{(n,m-1)q}$, so, mod m,

$$a^{\frac{m-1}{(n,m-1)}} = \left(r^{(n,m-1)q}\right)^{\frac{m-1}{(n,m-1}} = r^{(m-1)q} = (r^{m-1})^q \equiv 1^q = 1$$

Conversely, if $a^{\frac{m-1}{(n,m-1)}} \equiv 1$, then $r^{s\frac{m-1}{(n,m-1)}} \equiv 1$. Therefore $\text{ord}_m(b) = m - 1|s\dfrac{m-1}{(n,m-1)}$, so $(m-1)\dfrac{s}{(n,m-1)} = (m-1)y$, so $\dfrac{s}{(n,m-1)} = y$ is an integer. So $(n, m-1)|s$, which means (**) has a solution, and we can follow the argument back up from there to see that (*) has a solution. So we find:

If m is prime and $(a, m) = 1$, then

$$x^n \equiv a \pmod m \text{ has } \begin{cases} (n, m-1) \text{ solutions}, & \text{if } a^{\frac{m-1}{(n,m-1)}} \equiv 1 \\ 0 \text{ solutions}, & \text{if } a^{\frac{m-1}{(n,m-1)}} \not\equiv 1 \end{cases}$$

Specializing to $n = 2$, we have Euler's Criterion:

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

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

So for example, by checking that $13^2 = 169 \equiv -1 \pmod{17}$, so $13^8 \equiv 1 \pmod{17}$, we find that $x^2 \equiv 13 \pmod{17}$ has (two) solutions.