Thursday, October 10

What do we know about which moduli have primitive roots?

- Group Work Tue:
  - $m = 1, 2, 4$ do have primitive roots
  - only other possibilities are: p^k, $2p^k$ for odd primes p
- Mini-lecture Tue:
  - primes p do have primitive roots

Today: look at p^k for odd p.

Some data when $p = 5$.

- The $\phi(\phi(5)) = 2$ primitive roots (mod 5) are $\{2, 3\}$.
- The $\phi(\phi(25)) = 8$ primitive roots (mod 25) are $\{2, 3, 8, 12, 13, 17, 22, 23\}$.

missing 7, 18

Note: $7^4 = 2401 \equiv 1 \pmod{25}$

$18^4 \equiv (-7)^4 \equiv 1 \pmod{25}$.

Still, we observe:

- every primitive root (mod 25) is a primitive root (mod 5) as well;
- most (but not all) lifts of the primitive roots (mod 5) are also primitive roots (mod 25).

— True in general.

Theorem: If g is a primitive root $(\text{mod } p^2)$, then g is also a primitive root $(\text{mod } p)$.

Starting observation: Suppose $a^k \equiv 1 \pmod p$. Then $a^{kp} - 1 = (a^k - 1)((a^k)^{p-1} + (a^k)^{p-2} + \cdots + (a^k)^2 + a^k + 1)$; and both factors are multiples of p, so $a^{kp} \equiv 1 \pmod{p^2}$.

Contrapositive: if $a^{kp} \not\equiv 1 \pmod{p^2}$, then $a^k \not\equiv 1 \pmod p$.

Proof of theorem: Suppose g is a primitive root $(\text{mod } p^2)$, so g has order $\phi(p^2) = p(p-1)$.

Thus $g^p, g^{2p}, \ldots, g^{(p-2)p} \not\equiv 1 \pmod{p^2}$.

By the observation, $g, g^2, \ldots, g^{p-2} \not\equiv 1 \pmod p$, so g is a primitive root $(\text{mod } p)$. ✓

Lemma: If a has order $h \pmod m$ and $d \mid m$, then the order of $a \pmod d$ divides h.

Proof: a has order $h \pmod m$

$\Rightarrow a^h \equiv 1 \pmod m$

$\Rightarrow a^h \equiv 1 \pmod d$

$\Rightarrow h$ is a multiple of the order of $a \pmod d$. ✓

Proposition: If g is a primitive root $\pmod{p^r}$ with $r \geq 2$, then

$$g^{p^{r-2}(p-1)} \not\equiv 1 \pmod{p^r}. \quad (*)$$

Moreover, if g is a primitive root $\pmod{p^{r-1}}$ and $(*)$ holds, then g is also a primitive root $\pmod{p^r}$.

Proof: If g is a primitive root $\pmod{p^r}$, then g has order $\phi(p^r) = p^{r-1}(p-1) > p^{r-2}(p-1)$, and so $(*)$ holds (definition of order).

- Suppose g is a primitive root $\pmod{p^{r-1}}$ and $(*)$ holds. The order of $g \pmod{p^r}$:
  - divides $\phi(p^r) = p^{r-1}(p-1)$ (Euler's thm)
  - is a multiple of $\phi(p^{r-1}) = p^{r-2}(p-1)$ (previous lemma).

Thus the order $\pmod{p^r}$ must be either $p^{r-2}(p-1)$ or $p^{r-1}(p-1)$ (no intermediate divisors since p is prime).

But it can't be $p^{r-2}(p-1)$ by $(*)$. //

Theorem: Primitive roots exist $\pmod{p^2}$ for every prime p.

Proof: Let g be a primitive root $\pmod p$. We'll show that of the p lifts $g+tp \pmod{p^2}$ $(0 \le t \le p-1)$, all but one of them is a primitive root $\pmod{p^2}$. By Proposition, it suffices to show that there's a unique $0 \le t \le p-1$ such that $(*)$ fails, that is,

$$(g+tp)^{p-1} \equiv 1 \pmod{p^2}. \quad (**)$$

Let $f(x) = x^{p-1} - 1$. Then g is a root of $f(x) \pmod p$; and $f'(g) = (p-1)g^{p-2} \not\equiv 0 \pmod p$, so g is a nonsingular root. By Hensel's lemma, there is exactly one solution to $(**)$. //

Theorem: Let p be an odd prime, and let g be a primitive root $\pmod{p^r}$ for $r \ge 2$. Then g is also a primitive root $\pmod{p^{r+1}}$.

Corollary: Let p be an odd prime. Any primitive root $\pmod{p^2}$ is a primitive root $\pmod{p^k}$ for every $k \in \mathbb{N}$.

Proof of Theorem: Let g be a primitive root (mod p^r). By Proposition,

$$g^{p^{r-2}(p-1)} \not\equiv 1 \pmod{p^r};$$

and we want to show (*)

$$g^{p^{r-1}(p-1)} \not\equiv 1 \pmod{p^{r+1}},$$

so that g will be a primitive root (mod p^{r+1}). require $p \neq 2$

~~Now~~ $\cancel{g^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}}$ ~~by Euler's thm,~~

~~so~~ $\cancel{g^{p^{r-1}(p-1)} = 1 + np^r}$

Now $g^{p^{r-2}(p-1)} \equiv 1 \pmod{p^{r-1}}$ by Euler's thm;

so $g^{p^{r-2}(p-1)} = 1 + np^{r-1}$ for some $n \not\equiv 0 \pmod p$. Then by the binomial theorem,

$$g^{p^{r-1}(p-1)} = (1+np^{r-1})^p = \sum_{k=0}^{p} \binom{p}{k} (np^{r-1})^k .$$

Look at this (mod p^{r+1}):

- When $k \geq 3$, $k(r-1) \geq r+1$ (check), so $\binom{p}{k} n^k (p^{r-1})^k \equiv 0 \pmod{p^{r+1}}$.
- When $k=2$, $\binom{p}{2}(np^{r-1})^2 = \frac{p-1}{2} p \cdot n^2 p^{2(r-1)} = n \frac{p-1}{2} p^{2r-1}$; and $2r-1 \geq r+1$ (check). So $\binom{p}{2}(np^{r-1})^2 \equiv 0 \pmod{p^{r+1}}$.

Therefore

$$g^{p^{r-1}(p-1)} \equiv \sum_{k=0}^{1} \binom{p}{k}(np^{r-1})^k = 1 + p \cdot np^{r-1} = 1 + np^r \not\equiv \cancel{0}\, 1 \pmod{p^{r+1}}$$

since $n \not\equiv 0 \pmod p$. Thus (*) holds. //

Summary: Primitive roots exist precisely for $m = 1, 2, 4, p^k, 2p^k$ for odd primes p.

Exercise: Let p be odd. Show that if $(a, 2p^k)$, then the order of $a \pmod{2p^k}$ equals the order of $a \pmod{p^k}$.

In particular, since $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$, every primitive root $\pmod{p^k}$ is also a primitive root $\pmod{2p^k}$.

Group theory formulation: Let

- C_m be the cyclic group of order m (a complete residue system $\pmod m$, under $+$)
- M_m be the "multiplicative group" $\pmod m$: reduced residue system $\pmod m$, under $\times$. (size $\phi(m)$).

We now know how to find the group structure of M_m for any $m \geq 2$:

- Chinese remainder theorem — if $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, then
$$M_m \cong M_{p_1^{r_1}} \times M_{p_2^{r_2}} \times \cdots \times M_{p_k^{r_k}}.$$
- If p is odd, then primitive roots exist $\pmod{p^k}$; so $M_{p^k} \cong C_{\phi(p^k)}$
$$= C_{p^{k-1}(p-1)}.$$
- When $p = 2$:
$$M_{2^k} \cong \begin{cases} C_1, & \text{if } k=1, \\ C_2, & \text{if } k=2, \\ C_{2^{k-2}} \times C_2, & \text{if } k \geq 3. \end{cases}$$

Lemma: Suppose m has primitive roots and $(a,m)=1$. The number of solutions of $x^n \equiv a \pmod{m}$ equals

$$\begin{cases} d, & \text{if } a^{\phi(m)/d} \equiv 1 \pmod{m}, \\ 0, & \text{otherwise,} \end{cases}$$

where $d = (n, \phi(m))$.

(Special case: if $(n, \phi(m)) = 1$ then always exactly 1 solution.)

Proof: Let g be a primitive root $\pmod{m}$, and write $a \equiv g^b \pmod{m}$ and $x \equiv g^y \pmod{m}$. $(1 \le y \le \phi(m))$. Then

$$x^n \equiv a \pmod{m} \iff (g^y)^n \equiv g^b \pmod{m}$$

$$\iff g^{yn-b} \equiv 1 \pmod{m} \iff y\cancel{m}n - b \equiv 0 \pmod{\phi(m)}$$

$$\iff y\cancel{m}n \equiv b \pmod{\phi(m)}.$$

The number of solutions to this linear congruence is known from an earlier theorem. //

↳ Thu Sep 26

Special case $n=2$, $m=p$ odd:

Euler's criterion: Suppose $p \nmid a$.

The number of solutions of $x^2 \equiv a \pmod{p}$ is

$$\begin{cases} 2, & \text{if } a^{(p-1)/2} \equiv 1 \pmod{p}, \\ 0, & \text{if } a^{(p-1)/2} \equiv -1 \pmod{p}. \end{cases}$$

$\left[\left(a^{(p-1)/2}\right)^2 \equiv 1 \pmod{p} \right.$ by Fermat, so $\left. a^{(p-1)/2} \equiv \pm 1 \pmod{p}. \right]$