Primitive Roots

Recall that if p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. More generally, if m and a are relatively prime, then by Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. However there may be smaller exponents which take a to 1.

For example

$$3^4 \equiv 1 \pmod{16}$$
$$9^3 \equiv 1 \pmod{13}$$

The smallest such exponent taking a fixed a to the congruence class of 1 modulo m is called the order of a modulo m, and is denoted $e_m(a)$, provided there is some x such that $a^x \equiv 1 \pmod{m}$.

$$e_m(a) = \min\{x \geq 1 \mid a^x \equiv 1 \pmod{m}\}.$$

Notice $e_m(a)$ exists precisely when $\gcd(a,m)=1$: If a and m are relatively prime, then we know $a^{\varphi(m)} \equiv 1 \pmod{m}$ and so $e_m(a) \leq \varphi(m)$. On the other hand, if $a^x \equiv 1 \pmod{m}$, then $a^x - 1 = my \Rightarrow a \cdot (a^{x-1}) + m(-y) = 1 \Rightarrow \gcd(a,m) = 1$.

Before going any further, let's determine what possible exponents x satisfy $a^x \equiv 1 \pmod{m}$.

Lemma

Suppose a and m are relatively prime. Then $a^x \equiv 1 \pmod{m}$ iff $e_m(a) \mid x$. In particular, $x \mid \varphi(m)$.

Pf

- First suppose $e_m(a) \mid x$, so $x = k \cdot e_m(a)$. Then

$$a^x = a^{k \cdot e_m(a)} = \left[a^{e_m(a)}\right]^k \equiv 1^k \equiv 1 \pmod{m}.$$

- Suppose $a^x \equiv 1 \pmod{m}$. By the division algorithm, we may write

$$x = q \cdot e_m(a) + r$$

where $0 \leq r < e_m(a)$. Then

$$a^x = a^{q\, e_m(a) + r} = \left[a^{e_m(a)}\right]^q \cdot a^r \equiv a^r \pmod{m}$$

But we've assumed $a^x \equiv 1 \pmod{m}$, thus $a^r \equiv 1 \pmod{m}$. If $r \neq 0$, this would contradict that $e_m(a)$ is the smallest exponent taking a to 1. Hence $r = 0$, and $e_m(a) \mid x$. □

So $\varphi(m)$ gives us an upper bound for the orders $e_m(a)$. If in fact $e_m(a) = \varphi(m)$, then we say a is a primitive root modulo m.

We will show that every prime has primitive roots, but first we need some lemmas to help with the proof.

Lemma

Suppose $\gcd(a,m) = 1$. Then if $e_m(a) = k$, $a^i \equiv a^j \pmod m$ iff $i \equiv j \pmod k$.

Pf.

- Suppose $a^i \equiv a^j \pmod m$. WLOG, suppose $i \geq j$. Note

$$\begin{aligned} & a^i \equiv a^j \pmod m \\ \Rightarrow\ & a^{i-j} a^j \equiv a^j \pmod m \\ \Rightarrow\ & a^{i-j} \equiv 1 \pmod m \end{aligned}$$

  But our previous lemma then tells us $e_m(a) = k \mid i-j$. That is $i \equiv j \pmod k$.

- Now suppose $i \equiv j \pmod k$. Thus

$$\begin{aligned} & k \mid i-j \\ \Rightarrow\ & qk = i-j \\ \Rightarrow\ & i = qk + j \end{aligned}$$

Note

$$\begin{aligned} a^i = a^{qk+j} = (a^k)^q a^j &\equiv 1^q a^j \pmod k \\ &\equiv a^j \pmod k. \end{aligned}$$

□

Another way to phrase this is that:

Cor.

If $\gcd(a,m)=1$ and $e_m(a)=k$, then

$$a, a^2, a^3, \ldots, a^{k-1}, a^k$$

are all incongruent modulo m □

Notice if m is prime and if a is a primitive root modulo p (so $e_p(a) = \varphi(p) = p-1$), then

$$a, a^2, a^3, \ldots, a^{p-2}, a^{p-1}$$

are incongruent modulo m. This observation will be important in proving the following theorem.

Thm (Primitive Root Theorem)

If p is prime, then there are $\varphi(p-1)$ primitive roots modulo p. □

~~$\varphi(p)=p-1$~~

To prove the primitive root theorem we will show that primitive roots are solutions to a certain polynomial congruence equation, and then count the number of

solutions.

First recall a theorem we proved a while back: if $f(x)$ is a polynomial of degree d, then $f(x) \equiv 0 \pmod{p}$ has at most d incongruent solutions. Now consider a specid type of polynomial congruence:

w/integer coefficients →

<u>Lemma</u>

If p is prime and $d \mid p-1$, then

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d incongruent solutions

<u>Pf</u>

As $d \mid p-1$, $p-1 = dq$ for some q. Now consider the polynomial

$$x^{p-1} - 1$$

and note this polynomial factors as

$$(x^d - 1) \cdot \left(x^{d(q-1)} + x^{d(q-2)} + x^{d(q-3)} + \dots + x^d + 1 \right)$$

Note the right-hand factor is a polynomial of degree $d(q-1) = dq - d = p - d - 1$, and so has at most $p-d-1$ solutions. However, by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ for each $1 \le a < p$ — that is, $x^{p-1} - 1 \equiv 0 \pmod{p}$

has exactly $p-1$ solutions. The only way the two equal polynomials,

$$(x^d-1)(x^{d(q-1)}+\cdots+x^d+1) = x^{p-1}-1$$

can have the same number of roots, $p-1$, is if x^d-1 has d solutions. □

We now prove a general result which will have the primitive root theorem as a corollary.

Theorem

If p is prime and $d \mid p-1$, then there are exactly $\varphi(d)$ values of a, $1 \le a < p$, such that $e_p(a) = d$.

Pf

Let $d \mid p-1$, and let $\Psi(d)$ be the number of values in $1 \le a < p$ such that $e_p(a) = d$

$$\Psi(d) = \#\{\, a \mid 1 \le a < p,\ e_p(a) = d \,\}.$$

So we want to show $\Psi(d) = \varphi(d)$.

Notice that every integer $1 \le a < p$ has some order $e_p(a)$, and each order must divide $p-1$. Hence if $d_1, d_2, \ldots, d_r$ are the divisors of $p-1$, then

$$\psi(d_1) + \psi(d_2) + \cdots + \psi(d_r) = p-1 = \varphi(p)$$

However, we've also seen in the last lecture that for any number N, if $\Delta_1, \Delta_2, \ldots, \Delta_s$ are the divisors of N, then $N = \varphi(\Delta_1) + \cdots + \varphi(\Delta_s)$. Applying that result to $N = p-1$ we have

$$\psi(d_1) + \cdots + \psi(d_r) = \varphi(d_1) + \cdots + \varphi(d_r)$$

We want to show that $\psi(d_i) = \varphi(d_i)$ for each d_i. Because of the sum above it suffices to just show $\psi(d_i) \leq \varphi(d_i)$. — if any $\psi(d_i) < \varphi(d_i)$, we'd have

$$\sum \psi(d_i) < \sum \varphi(d_i)$$

which we know can't be true, and we're forced to conclude that $\psi(d_i) = \varphi(d_i)$, provided we can prove $\psi(d_i) \leq \varphi(d_i)$.

- <u>Case 1</u> $\psi(d_i) = 0$
  If $\psi(d_i) = 0$, then obviously $\psi(d_i) \leq \varphi(d_i)$
- <u>Case 2</u> $\psi(d_i) > 0$
  There then exists at least one a st. $e_p(a) = d_i$
  Hence $a, a^2, a^3, \ldots, a^{d_i}$ are incongruent by an earlier lemma and its corollary

Notice that each of these is a solution to

$$x^{d_i} - 1 \equiv 0 \pmod{p}$$

However we know there are exactly d_i solutions to this equation, so $a, a^2, \ldots, a^{d_i}$ must be all of the solutions.

Note that even though each a^k, $1 \leq k \leq d_i$, is congruent to 1 when raised to the d_i power, it is <u>not</u> necessarily the case that each a^k has order d_i — there may be a smaller exponent j st. $(a^k)^j \equiv 1 \pmod{p}$. However, the order of a^k must divide d_i since the order divides all exponents taking a^k to 1.

Thus a^k has order d_i precisely when k and d_i are relatively prime. That is, $\varphi(d_i)$ of the a^k have order d_i — and these are the <u>only</u> values having order d_i. Thus $\varphi(d_i) = \psi(d_i)$, which is what we wanted to show. □

Applying the above theorem to $d = p-1$ gives the primitive root theorem.

More generally, we may ask how many primitive roots are there modulo a composite number m. Herein lies a problem: not all numbers have primitive roots! For example, there are no primitive roots modulo 8:

a	$e_8(a)$	
1	1	$1^1 \equiv 1 \pmod 8$
2	(Not rel. prime)	
3	2	$3^2 = 9 \equiv 1 \pmod 8$
4	(Not rel. prime)	
5	2	$5^2 = 25 \equiv 1 \pmod 8$
6	(Not rel. prime)	
7	2	$7^2 = 49 \equiv 1 \pmod 8$

The largest order modulo 8 is 2, yet $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$. So if we want to count the primitive roots of m, we first have to know if m has any primitive roots.

Fact

m has primitive roots if and only if $m = 1$, $m = 2$, $m = 4$, $m = p^k$ or $m = 2p^k$ where p is an odd prime.

Pf

Exercise for those who've had abstract algebra:

- The congruence classes modulo m form a ring $\mathbb{Z}/m\mathbb{Z}$
- If m has prime factorization $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, then $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $[\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}] \times \cdots \times [\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}]$
- The units of any ring R form a groups under multiplication, $R^\times$
- As groups, (has order $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$)

$$[\mathbb{Z}/m\mathbb{Z}]^\times \cong [\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}]^\times \times \cdots \times [\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}]^\times$$

- The product of two finite cyclic groups G and H is cyclic iff the orders are relatively prime
- Finally, show $[\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}]^\times$ is cyclic iff $p_i^{\alpha_i} = 1, 2, 4, p, p^k$ for p an odd prime. □

Theorem

If $\gcd(a,m) = 1$ and the positive integers less than and relatively prime to m are $a_1, a_2, \ldots, a_{\varphi(m)}$, then provided b is a primitive root of m,

$$\{b, b^2, b^3, \ldots, b^{\varphi(m)}\} = \{a_1, \ldots, a_{\varphi(m)}\}$$

Pf

Note $b^i \not\equiv b^j \pmod m$, and there are exactly $\varphi(m)$ incongruent elements relatively prime to m. □

Theorem

If m has a primitive root, then it has exactly $\varphi(\varphi(m))$ of them

Pf

Suppose a is a primitive root of m. By the previous result, all the other primitive roots must be contained in

$$\{a, a^2, \ldots, a^{\varphi(m)}\}$$

Each a^k will be a primitive root precisely when $\gcd(k, \varphi(m)) = 1$, and there are $\varphi(\varphi(m))$ such numbers.

□