14 Primitive roots mod p and Indices

Fix an odd prime p, and $x \in \mathbb{Z}$. By little Fermat:

$$x^{p-1} \equiv 1 \ (mod\ p) \text{ if } x \not\equiv 0 \ (mod\ p)$$

E.g.

	x	x^2	x^3	x^4
	1	1	1	1
$p = 5$	2	-1	3	1
	3	-1	2	1
	4	1	-1	1

2 and 3 are called "primitive roots mod 5" since no smaller power than $p-1$ is $\equiv 1$.

Definition: Let $x \in \mathbb{Z}$, $p \not| x$. Then the *exponent* of x (relative to p) is the smallest integer r among $\{1, 2, \ldots, p-1\}$ such that $x^r \equiv 1$ (mod p). One writes $r = e_p(x)$.

When $p = 5$, $e_5(1) = 1$, $e_5(2) = 4 = e_5(3)$, $e_5(4) = 2$.

Definition: x is a *primitive root mod* p iff $e_p(x) = p - 1$.

Again, when $p = 5$, 2 and 3 are primitive roots.

Claim: For any x prime to p,

$$e_p(x) | (p-1).$$

Proof: Since $1 \leq e_p(x) \leq p-1$, by definition, it suffices to show that

$$d = \gcd(e_p(x), p-1) \geq e_p(x).$$

Suppose $d < e_p(x)$. Since d is the gcd of $e_p(x)$ and $p-1$, we can find $a, b \in \mathbb{Z}$ such that $ae_p(x) + b(p-1) = d$. Then

$$x^d = x^{ae_p(x)+b(p-1)} = (x^{e_p(x)})^a (x^{p-1})^b$$

But

$$x^{p-1} \equiv 1 \text{ (mod } p\text{) by Little Fermat,}$$

and

$$x^{e_p(x)} \equiv 1 \text{ (mod } p\text{) by definition of } e_p(x).$$

Thus

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

Since we are assuming that $d < e_p(x)$, we get a contradiction as $e_p(x)$ is the smallest such number in $\{1, 2, \ldots, p-1\}$.

$\Rightarrow d \geq e_p(x)$.

Since $d = \gcd(e_p(x), p-1),\ d | e_p(x) \Rightarrow d = e_p(x)$. Hence the claim.

Two natural questions

1. Are these primitive roots mod p?

2. If so, how many?

For $p = 5$, the answers are (1) yes, and (2) two.

Theorem: Fix an odd prime p. Then
(i) $\exists$ primitive roots mod p
(ii) $\#\{$primitive roots mod $p = \varphi(p-1)$.

Proof: For every (positive) divisord of $p-1$, put

$$\psi(d) = \#\{x \in \{1, \ldots, p-1\} | e_p(x) = d\}$$

Both (i) and (ii) will be proved if we show

$$\psi(p-1) = \varphi(p-1). \qquad (*)$$

We will in fact show that

$$\psi(d) = \varphi(d) \quad \forall d | (p-1)$$

Every x in $\{1, \ldots, p-1\}$ has an exponent, and by the claim above this exponent is a divisor of d. Consequently

$$(p-1) = \sum_{d|(p-1)} \psi(d) \qquad (1)$$

Recall that we proved last week

$$p-1 = \sum_{d|(p-1)} \varphi(d) \qquad (2)$$

Consequently,

$$\sum_{d|(p-1)} \psi(d) = \sum_{d|(p-1)} \varphi(d) \tag{3}$$

It suffices to show that

$$\psi(d) \leq \varphi(d) \quad \forall d|(p-1) \tag{A}$$

Proof of (A): Pick any $d|(p-1)$. If $\psi(d) = 0$, we have nothing to prove. So assume that $\psi(d) \neq 0$. Then

$$\exists a \in \{1, \dots, p-1\} \text{ such that } e_p(a) = d.$$

Consider

$$Y = \{1, a, \dots, a^{\mathrm{d}-1}\}$$

Then $(\mathrm{d}^j)^\alpha \equiv 1 \pmod{p}$. Further, Y supplies d distinct solutions to the congruence

$$x^d \equiv 1 \pmod{p}.$$

We proved earlier (LaGrange) that, given any polynomical $f(x)$ with integral coef's f degree n, there are at most n solutions mod p of $f(x) \equiv 0 \pmod{p}$. So $x^d - 1 \equiv 0 \pmod{p}$ has at most d solutions mod p. Consequently, Y is exactly the set of solutions to this congruence and $\#Y = d$. Hence

$$\psi(d) = \#\{a^j \in Y | e_p(a^j) = d\}.$$

Proof of claim: Let $r = \gcd(j, d)$. Then, by the proof of the earlier claim,

$$e_p(a^j) = \frac{d}{r}.$$

So $r = 1$ iff $e_p(a^j) = d$. This proves the claim.

Thanks to the claim, we have:

$$\psi(d) = \#\left\{ a^j \in Y \middle| \begin{matrix} j \in \{0, 1, \dots, d-1\} \\ (j, d) = 1 \end{matrix} \right\} \leq \varphi(d) \text{ for all } d|(p-1).$$

In fact we see that $\psi(d) = 0$ or $\varphi(d)$, which certainly proves (A), and hence the Theorem.

2 is a primitive root module the following primes < 100:

$$3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83$$

Artin's Conjecture

There are infinitely many primes with 2 as a primitive root.

More generally, for any non-square a, are there infinitely many primes with a a prime root?

Claim:

$$e_p(a^j) = d \text{ iff } (j, d) = 1.$$

This cannot be true if a is a perfect square. Indeed if $a = b^2$, since $b^{(p-1)} \equiv 1 \pmod p$, if $p \not| b$, we have

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

So, for any odd $p \not| a$, $e_p(a) | (\frac{p-1}{2})$. Similarly, $a = -1$ is a bad case, because

$$(-1)^2 = 1 \text{ and } e_p(-1) = 2 \text{ or } 1, \ \forall p \text{ odd}.$$

So we are led to the following

Generalized Artin Conjecture. Let a be an integer which is not -1 and not a perfect square. Then $\exists$ infinitely many primes such that $e_p(a) = p - 1$.

Here is a positive result in this direction:

Theorem: (Gupta, Murty, and Heath-Brown) There are at most three pairwise relatively prime a's for which there are possibly a finite number of primes such that $e_p(a) = p - 1$.

Problem: no one has any clues as to the nature and size of these three possible exceptions, or whether they even exist. Is 2 an exception?

Indices

Fix an odd prime y and a primitive root a mod p. We can consider

$$Y = \{a^j | 0 \leq j < p - 1\}.$$

Then each element of Y is in $(\mathbb{Z}/p)^*$ and we get $p - 1$ distinct elements. But $\#(\mathbb{Z}/p)^* = p - 1$. So Y gives a set of reps. for $(\mathbb{Z}/p)^*$.

Consequently, given any integer b prime to p, we can find a *unique* $j \in \{0, 1, \ldots, p-2\}$ such that $b \equiv a^j \pmod{p}$.

This (unique) j is called the **index** of b mod p relative to a, written $I_p(b)$ or $I(b)$. Properties: $I(ab) = I(a+b)$, $I(ka) = kI(a)$.