§17 Applications of primitive roots.

Definition: Let p be prime. An integer a is a primitive root mod p if $\mathrm{ord}_p(a) = p-1$.

Q: How to find a primitive root?

A: Trial and error works quite well for findind primitive roots.

From previous lectures: there are $\varphi(p-1)$ primitive roots mod p. (In particular, we have at least one).

Let the prime factorization of $p-1$ be

$$p-1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_d^{\alpha_d}$$

Then

$$\frac{\varphi(p-1)}{p-1} = \frac{(p-1)\cdot\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_d}\right)}{p-1}$$

$$= \frac{(q_1-1)(q_2-1)\cdots(q_d-1)}{q_1\cdot q_2\cdot \cdots \cdot q_d}$$

probability that a random $a \in \{1, 2, \dots, p-1\}$ is a primitive root.

In principle this ratio can be arbitrarily close to 0 (if factorization of $p-1$ has plenty of small prime factors). But in practise it is usually relatively big. It is rare that one needs to check >10 candidates to find a primitive root.

Q: Given $a \in \{1, 2, \dots, p-1\}$ how to check that it is a prim. root mod p?

a is a prim root mod p. if and only if $a^d \not\equiv 1 \pmod{p}$ for any proper divisor d of $p-1$.

This requires prime factorization of $p-1$ $\longrightarrow$ might be difficult.

Important property of prim. roots: If a is a prim. root mod p then $\{a^0, a^1, \dots, a^{p-2}\}$ is a reduced set of residues mod p.
I.e. $\{a^0, a^1, \dots, a^{p-2}\}$ modulo p is $\{1, 2, 3, \dots, p-1\}$ in a different order.

Example: $p = 11$. $a = 2$.

$$
\begin{array}{lll}
2^0 \equiv a^0 \equiv 1 & 2^4 \equiv 5 & 2^8 \equiv 3 \\
2^1 \equiv a^1 \equiv 2 & 2^5 \equiv 10 & 2^9 \equiv 6 \\
2^2 \equiv 4 & 2^6 \equiv 9 & 2^{10} \equiv 1 \equiv 2^0. \\
2^3 \equiv 8 & 2^7 \equiv 7 &
\end{array}
$$

Proposition. Let p be prime, a be a prim root mod p, $d \mid p-1$, $\ell = \frac{p-1}{d}$.
Then the elements from $\{a^0, a^1, \dots, a^{p-2}\}$ which have order d are exactly those which are $a^{k\ell}$, and $\gcd(k, d) = 1$, $k \in \{0, 1, \dots, d-1\}$

Proof.

$$\operatorname{ord}_p(a^i) = \min\{j \in \mathbb{Z}^+ : a^{ij} \equiv 1 \pmod p\}$$
$$= [a \text{ is a prim root}]$$
$$= \min\{j \in \mathbb{Z}^+ : p-1 \mid ij\}$$

Then $\operatorname{ord}_p(a^i) = d \iff p-1 \mid d \cdot i$ and $\nexists j < d$ with $p-1 \mid ij$.

$\iff e \mid i$ and $\nexists j < d$ with $\frac{p-1}{e} \mid \left(\frac{i}{e}\right) j$

$\iff i = ke$ and $\nexists j < d$ with $d \mid kj$.

$\iff i = ke$ and $\gcd(d, k) = 1$ $\boxtimes$

Another property: p is prime, a is a prim root, $p-1 = d \cdot e$. Then the elements from $\{a^0, a^1, \dots, a^{p-2}\}$ which are solutions of $x^d \equiv 1 \pmod p$ are those of the form $x \equiv a^{ke} \pmod p$, $k \in \{0, 1, \dots, d-1\}$

Proof - EX.

Example: $x^5 \equiv 1 \pmod{11}$, $(p = 11, d = 5, e = 2)$.

Solutions are:

$x \equiv 2^0$ or 2^2 or 2^4 or 2^6 or $2^8 \pmod{11}$

$\equiv 1$ or 4 or 5 or 9 or $3 \pmod{11}$.

Consider, which values $c \in \{a^0, a^1, \dots, a^{p-2}\}$ have d'th root (i.e. the equation $x^d \equiv c \pmod{p}$ has solutions).

Let $c \equiv a^k \pmod{p}$, $x \equiv a^i \pmod{p}$

Then

$$a^{id} \equiv a^k \pmod{p} \iff id \equiv k \pmod{p-1}$$

Now, $d \mid p-1$. $\Rightarrow d \mid k$. $\Rightarrow k = d \cdot l$.

and $i \equiv l \pmod{\frac{p-1}{d}}$ or $i \equiv l \pmod{e}$.

Therefore $c \equiv a^k \pmod{p}$ has d'th root mod p if and only if $c \equiv a^{d \cdot l}$, and $l \in \{0, 1, \dots, e-1\}$.

In that case all solutions of

$$x^d \equiv c \pmod{p} \text{ are}$$

$x \equiv a^{l+me} \pmod{p}$ and $m \in \{0, 1, \dots, d-1\}$.