§15. Primitive roots and discrete logarithms

From yesterday, let p be prime, $d \in \mathbb{Z}^+$ and $c \in \mathbb{Z}$. Then the equation

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

has at most d solutions modulo p.

Example: $p=13$, $d=3$, (note $(-x)^3 = -x^3$)

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 \pmod{13}$	0	1	8	1	12	8	8	5	5	1	12	5	12

three ones　　　　three 5's

Theorem. Let p be prime, $d \in \mathbb{Z}^+$ where $d \mid p-1$. For any $c \not\equiv 0 \pmod{p}$ the number of solutions of $x^d \equiv c \pmod{p}$ is either 0 or d.

Proof. $p-1 = d \cdot e$ where $e \in \mathbb{Z}$.

Consider the function

$$f : \{1,2,3,\dots,p-1\} \longrightarrow \{1,2,3,\dots,p-1\}$$
$$x \longmapsto x^d$$

Let c be in the range (or image) of f i.e. $c \equiv x^d \pmod{p}$ for some x.

FLT $\Rightarrow \underline{c^e} \equiv x^{de} \equiv x^{p-1} \equiv \underline{1} \pmod{p}$

Yesterday's Theorem $\Rightarrow$ there are $\leq e$ elements in the range of f.

For any c in the range, the number of x from the domain of f such that $x^d \equiv c \pmod{p}$ is $\leq d$.

In total we have $\leq e \cdot d$ elements in the domain of f.

On the other hand there are exactly $p-1 = d \cdot e$ elements in the domain. $\Rightarrow$ both "$\leq$" signs are in fact equalities.

$\Rightarrow$ There are $e = \frac{p-1}{d}$ elements c in the range of f, for each of them the equation

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

has exactly d solutions. $\boxtimes$

Recall: for a s.t. $\gcd(a,p)=1$, the $\mathrm{ord}_p(a)$ is the minimal $d \in \mathbb{Z}^+$ s.t.

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

We know:

(a) $a^d \equiv a^{d'} \pmod{p} \Longleftrightarrow d \equiv d' \pmod{\mathrm{ord}_p(a)}$

(Ex!)

In particular

(b) $a^d \equiv 1 \pmod{p} \Longleftrightarrow \mathrm{ord}_p(a) \mid d$

(c) FLT $\Rightarrow a^{p-1} \equiv 1 \pmod p \Longrightarrow \mathrm{ord}_p(a) \mid p-1$.

Example: $p = 13$

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ord}_{13}(a)$	1	12	3	6	4	12	12	4	3	6	12	2

Only need to check the divisors of 12.

$2^4 \equiv 3 \pmod{13}$, $2^6 \equiv 12 \pmod{13}$

Notice: for any $d \mid 12$ the number of occurrencies of d is exactly $\varphi(d)$.

Theorem: Let p be prime and $d \mid p-1$. The number of values $a \in \{1, 2, \dots, p-1\}$ with $\mathrm{ord}_p(a) = d$ is $\varphi(d)$

Proof. Denote $F(d) := \#\{a \in \{1, 2, \dots, p-1\} : \mathrm{ord}_p(a) = d\}$

By the previous theorem:

$$d = \#\{a \in \{1, 2, \dots, p-1\} : a^d \equiv 1 \pmod p\}$$

$$[\text{by (b)}] = \#\{a \in \{1, 2, \dots, p-1\} : \mathrm{ord}_p(a) \mid d\}$$

$$= \sum_{e \mid d} F(e)$$

Möbius inversion formula:

$$F(d) = \sum_{e \mid d} \mu\left(\frac{d}{e}\right) \cdot e = [\text{property of Euler } \varphi\text{-function}]$$

$$= \varphi(d)$$

$\boxtimes$

Definition. Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. a is called a <u>primitive root modulo m</u> if $\gcd(a, m) = 1$ and $\mathrm{ord}_m(a) = \varphi(m)$.

If $m = p$ is prime then it is equivalent to $a \not\equiv 0 \pmod p$, $\mathrm{ord}_p(a) = p-1$.

Corollary: Primitive roots mod. prime p always exist. Moreover there are $\varphi(p-1)$ of them.

Note: Corollary is not true for comp~~xxx~~osite m.

Example: $m = 8$ — 1 has order 1; 3, 5, 7 have orders 2; no elements of order $4 = \varphi(8)$

Let b be a primitive root modulo p.

$$b^d \equiv b^{d'} \pmod p \iff d \equiv d' \pmod{p-1}$$

In other words $\{b^1, b^2, \dots, b^{p-1}\}$ is a reduced set of residues mod p.

$\Rightarrow$ For any $a \not\equiv 0 \pmod p$ there is a unique value $d \in \{0, 1, \dots, p-1\}$ such that $b^d \equiv a \pmod p$.

Definition. Let p be prime, b be a primitive root mod p. Then the <u>discrete logarithm of a</u> $\log_{b,p}(a)$ is the value $d \in \{0, 1, \dots, p-1\}$ such that

$$b^d \equiv a \pmod{p}.$$