Math 4400
Week 7 - Tuesday
Primitive roots + Discrete logarithm

Last week: Cryptography

- Diffie-Hellman
- RSA

These used:

- Primitive roots
- big primes

It depended on the difficulty of:

- Discrete logarithm

• Factoring

Definition (last week): If $\mathbb{F}$ is a finite field (e.g. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$), a <u>primitive root in $\mathbb{F}$</u> is an element $g \in \mathbb{F}^\times$ such that

$$\mathbb{F}^\times = \{\underbrace{1}_{\text{"}g^0\text{"}}, g, g^2, \dots, g^{|\mathbb{F}^\times|-1}\}$$

i.e. every element of $\mathbb{F}^\times$ can be written uniquely as g^k, $0 \le k < |\mathbb{F}^\times|$.

Example: 2 is a primitive root in $\mathbb{F}_{13}$
3 is a primitive root in $\mathbb{F}_{31}$
5 is a primitive root in $\mathbb{F}_{47}$
6 is a primitive root in $\mathbb{F}_{41}$

Definition: If G is a group, the <u>order</u> of $g \in G$ is the smallest positive integer k such that $g^k = e$. We write $\mathrm{ord}(g)$.

Lagrange's Theorem (revisited): If G is a finite group and $g \in G$, the order of g divides the size of G, i.e.

$$\operatorname{ord}(g) \mid |G|$$

(Previously $g^{|G|} = e \iff |G| = q \operatorname{ord}(g)$, then $g^{|G|} = (g^{\operatorname{ord}(g)})^q = e^q = e$)

Example: $G = \mathbb{F}_{11}^{\times}$ $\quad |G| = 10 \; (= 11 - 1)$.

g	1	2	3	4	5	6	7	8	9	10
$\operatorname{ord}(g)$	1	10	5	5	5	10	10	10	5	2

Theorem. If $\mathbb{F}$ is a finite field with $|\mathbb{F}| = n$, then

① $g \in \mathbb{F}$ is a primitive root $\iff \operatorname{ord}(g) = n-1$
$\iff g^d \neq 1$ for all proper divisors of $n-1$.

② There are $\phi(n-1)$ primitive roots in $\mathbb{F}$

Example: 2, 6, 7, 8 are the primitive roots in $\mathbb{F}_{11}$.

$$\phi(11-1) = \phi(10) = \phi(5)\phi(2) = 4 \cdot 1 = 4$$

Proof: Part ①

- if $\operatorname{ord}(g) = n-1$, then
  $n-1$ things $\rightarrow \{e, g, \dots, g^{n-2}\}$ are distinct,
  so must be all of $\mathbb{F}^{\times}$ $(|\mathbb{F}^{\times}| = n-1)$.
- $\operatorname{ord}(g) \mid n-1$ by Lagrange, so

to see $\operatorname{ord}(g) = n-1$, just check $g^d \neq 1$ for all proper divisors $d \mid n-1$.

Part ② - There are $\phi(n-1)$ primitive roots.

$x^4 - 1$
$\equiv$
at most 4 roots.

Idea: $g^d = 1 \iff g$ is a root of $x^d - 1$ in $\mathbb{F}$.

Know at most d roots.

See Savin - Proposition 20 (p. 73) for full proof.

Uses $\sum_{d \mid n} \phi(d) = n$ (See worksheet, exercise 4)

Discrete Logarithm: If $\mathbb{F}$ is a finite field, $|\mathbb{F}| = n$, and g is a primitive root of $\mathbb{F}$

$$\mathbb{Z}/(n-1)\mathbb{Z} \longrightarrow \mathbb{F}^\times$$
$$k \longmapsto g^k$$

is a <u>bijection</u>. ⟵ Definition of a primitive root.

The inverse map

$$I : \mathbb{F}^\times \longrightarrow \mathbb{Z}/(n-1)\mathbb{Z}$$

$$x \longmapsto I(x) \text{ s.t. } g^{I(x)} = x.$$

is the <u>discrete logarithm</u> for $\mathbb{F}$ with base g.

$$I(xy) = I(x) + I(y).$$

$$I(1) = 0$$

$$I(x^k) = k\, I(x)$$

Like $\qquad \mathbb{R}^{\times}_{>0} \underset{\exp}{\overset{\log}{\rightleftarrows}} \mathbb{R}, + \quad (\exp(t) = e^t).$

$$\log(xy) = \log(x) + \log(y)$$

$$\log(x^k) = k \log(x)$$

$$\log(1) = 0.$$

Can use discrete log in same way!

(e.g. solve equations by replacing multiplication with addition).