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
Definition (last week): If $F$ is a finite field (e.g. $F_p = \mathbb{Z}/p\mathbb{Z}$), a primitive root in $F$ is an element $g \in F^\times$ such that $\{1, g, g^2, \ldots, g^{|F^\times| - 1}\}$

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

Example: 2 is a primitive root in $F_{13}$
3 is a primitive root in $F_{31}$
5 is a primitive root in $F_{47}$
6 is a primitive root in $F_{61}$

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

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. 
\[\text{ord}(g) \mid |G|\]
(Previously \( g^{|G|} = e \iff |G| = \text{ord}(g) \) 
then \( g^{|G|} = (\text{ord}(g))^t = e^t = e\) )

**Example:** 
\[G = \mathbb{F}_{11}^\times, \quad |G| = 10 \quad (= 11 - 1)\]

<table>
<thead>
<tr>
<th>( g )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{ord}(g)</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>

**Theorem.** If \( FF \) is a Finite Field with \( |FF| = n \), then
1. \( g \in FF \) is a primitive root \( \iff \text{ord}(g) = n-1 \)
   \( \iff g^d \neq 1 \) for all proper divisors of \( n-1 \).
2. There are \( \phi(n-1) \) primitive roots in \( FF \)

**Example:** \( 2, 6, 7, 9 \) 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 \( \text{ord}(g) = n-1 \), then
  \( n-1 \) things \( \rightarrow \) \( \{ e, g, \ldots, g^{n-2} \} \) are distinct,
  so must be all of \( \mathbb{F}_n^\times \) \( (|\mathbb{F}_n^\times| = n-1) \).
- \( \text{ord}(g) \mid n-1 \) by Lagrange, so
to see \( \text{ord}(g) = n-1 \), just check 
\( g^d \neq 1 \) for all proper divisors \( d \mid n-1 \).

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

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

Know at most \( d \) roots.

See Savin - Proposition 2.6 (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 \( \mathbb{F} \),

\[
\begin{align*}
\mathbb{Z}/(n-1)\mathbb{Z} & \longrightarrow \mathbb{F}^x \\
 k \quad & \quad \mapsto \quad g^k
\end{align*}
\]

is a bijection \(<\) Definition of a primitive root.

The inverse map 
\[
I: \mathbb{F}^x \longrightarrow \mathbb{Z}/(n-1)\mathbb{Z}
\]
\[ x \rightarrow I(x) \quad \text{s.t.} \quad g^{I(x)} = x. \]

is the discrete logarithm for \( \mathbb{F} \) with base \( g \).

\[ I(xy) = I(x) + I(y), \quad I(1) = 0 \]

\[ I(x^k) = k \cdot I(x) \]

Like \[ \mathbb{R}_+^x \xrightarrow{\log} \mathbb{R} \xrightarrow{\exp} \mathbb{R}_+, \quad (\exp(t) = e^t) \]

\[ \log(xy) = \log(x) + \log(y) \]

\[ \log(x^k) = k \cdot \log(x) \]

\[ \log(1) = 0. \]

Can use discrete log in same way!

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