Elementary Group Theory

- $G =$ multiplicative group of finite elements. $n = \text{order}(G) = |G|$
- e.g. $G = \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}, |G| = p-1$.
- Let $g \in G$, $\text{order}(g) = \min\{m > 0 | g^m = 1\}$
- Theorem 5.4. $\text{order}(g) | \text{order}(G)$.
  - page 170, due to Lagrange.
  - e.g. $b \in \mathbb{Z}_p^*$ then $b^{p-1} = 1 \mod p$. 

Some Simple Number Theory

- Fermat’s Little Theorem: (page 171)
  - For a prime $p$, $b \neq 0$.
  - $b^{p-1} = 1 \mod p$.
- Euler’s Theorem: (page 170)
  - For any $n$ and $\gcd(b,n) = 1$.
  - $b^{\phi(n)} = 1 \mod n$.
  - $\phi(n)$: number of integers between 1 and $n$ that are relative prime to $n$.

Euler’s Theorem

- For any $n$ and $\gcd(y,n) = 1$,
  - $y^{\phi(n)} = 1 \mod n$.
  - $\phi(n)$: number of integers between 1 and $n$ that are relative prime to $n$.
- E.g. $n=20$,
  - $\phi(n) = 8 = \#S, S = \{y | \gcd(y,20)=1\}$
  - $13^8 = 1 \mod 20$.
  - $13^{-1} = 13^7 = 17 \mod 20$. 

Euler totient function $\varphi(n)$
- $\varphi(n)$: number of integers between 1 and n that are relative prime to n.
- Computation of $\varphi(n)$:
  1. $\varphi(p^e) = p^{e-1}(p-1)$
  2. $\varphi(p^e q^f) = \varphi(p^e) \varphi(q^f)$ if $\gcd(p,q)=1$.
- E.g.
  - $\varphi(20) = \#\{1, 3, 7, 9, 11, 13, 17, 19\} = 8$
  - $\varphi(5) = \#\{1, 2, 3, 4\} = 4$
  - $\varphi(4) = \#\{1, 3\} = 2$

Cyclic Group
- G is a cyclic group if there exists an element $g \in G$ such that $\text{order}(g) = \text{order}(G)$. Such a g is called a “generator” or “primitive element”.
- Theorem 5.7 (page 171) $\mathbb{Z}_p^* = \{1,2,\ldots,p-1\}$ is a cyclic group, if p is a prime number.

Example: $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

<table>
<thead>
<tr>
<th>g</th>
<th>g^2</th>
<th>g^3</th>
<th>g^4</th>
<th>g^5</th>
<th>g^6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

$\mathbb{Z}_7^*$ is a cyclic group, 3 and 5 are primitive roots.
More example of group: \( F_{23}^* \)

- \( F_{23}^* = \{1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\} \) is also a cyclic group of 7 elements under irreducible \( f(x) = x^4+x+1 \).
- \( x \) is a primitive element (generator).
- It is easy to see \( (3)^{\ast}\ast = (x^3)^{x^3} = x^6 = (0) \).
- How about \( (3)^{\ast}\ast \) ? \( = x^4 = (1) \).

<table>
<thead>
<tr>
<th>( i )</th>
<th>( x^i \mod f(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( x )</td>
</tr>
<tr>
<td>2</td>
<td>( x^2 )</td>
</tr>
<tr>
<td>3</td>
<td>( x+1 )</td>
</tr>
<tr>
<td>4</td>
<td>( x^2+x )</td>
</tr>
<tr>
<td>5</td>
<td>( x^2+x+1 )</td>
</tr>
<tr>
<td>6</td>
<td>( x^2+1 )</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

More about \( Z_p^* \)

- \( Z_p^* = Z_p \setminus \{0\} \). When \( p \) is a prime, \( Z_p^* \) is a cyclic group.
- Let \( \alpha \in Z_p^* \) be a primitive root. Then \( \alpha \) can generate all elements in \( Z_p^* \):
  - \( \{\alpha^i : 0 \leq i \leq p-1\} = Z_p^* \)
  - Order of \( \beta = \alpha^i \mod p \) is \( (p-1)/\gcd(p-1,i) \).
  - If \( \gcd(p-1,i) = 1 \), then \( \beta = \alpha^i \mod p \) is also a primitive root. (why?)
  - How many? \( \varphi(p-1) \). (why?)

Example: \( Z_7^* = \{1, 2, 3, 4, 5, 6\} \)

- \( g=3 \) and \( 5 \) are two primitive roots.
  - \( \varphi(7) = \varphi(2) \varphi(3) = (2-1)(3-1) = 2 \).
  - \( \{i: \gcd(i,6)=1\} = \{1,5\} \)
  - \( g=3, \{g^1, g^5\} = \{3, 5\} \)
  - \( g=5, \{g^1, g^3\} = \{5, 3\} \)

<table>
<thead>
<tr>
<th>( g )</th>
<th>( g^2 )</th>
<th>( g^3 )</th>
<th>( g^4 )</th>
<th>( g^5 )</th>
<th>( g^6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

\( Z_7^* \) is a cyclic group, 3 and 5 are primitive roots.
Example 5.4. $\mathbb{Z}_{13}^*$

- How many primitive roots? $\phi(13-1)=4$.
- 2 is a primitive root.
- (shown on the right)
- List of all primitive roots: $\{2, 6, 11, 7\}$.
- Q: how to verify primitive root when $p$ is large? e.g. $p=131$.

<table>
<thead>
<tr>
<th>i</th>
<th>2^i mod 13</th>
<th>\phi(i)/2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Theorem 5.8 (page 172)

- $\alpha \in \mathbb{Z}_p^*$ is a primitive root if and only if $\alpha^{(p-1)/q} \neq 1 \mod p$ for any prime $q|(p-1)$.
- e.g. $p=13$. $p-1=12=2^2 \times 3$. Need to check $(p-1)/q$, for $q=2$ and $q=3$.
  - $12/2=6$, $12/3=4$.
  - $2^6 \neq 1 \mod 13$, and $2^4 \neq 1 \mod 13$.
  - Hence, 2 is a primitive root.

Theorem 5.8 (page 172)

- $\alpha \in \mathbb{Z}_p^*$ is a primitive root if and only if $\alpha^{(p-1)/q} \neq 1 \mod p$ for any prime $q|(p-1)$.
- e.g. $p=131$. $p-1=130=2^*5^*13$.
  - $130/2=65$, $130/5=26$, $130/13=10$.
  - Find $g$ such that $g^{65} \neq 1 \mod 131$, $g^{26} \neq 1 \mod 131$, and $g^{26} \neq 1 \mod 131$.
  - Show $g=2$ is a primitive root.
RSA Parameter Generation

- Rivest-Shamir-Adelman (RSA) (1977)
- Algorithm 5.4 (page 175)
  - \( n = p \cdot q \), where \( p \) and \( q \) are large primes.
  - \( \phi(n) = (p-1)(q-1) \) (why?)
  - Choose a random \( e \) with \( \gcd(e, \phi(n)) = 1 \).
  - Find \( d = e^{-1} \mod \phi(n) \).
- Use public key \((n, e)\) to encrypt: \( C = P^e \mod n \)
- Use private key \( d \) to decrypt: \( P = C^d \mod n \)

Attack and analysis of RSA

We can break the RSA, if

- we can factor \( n \) which is known to be a hard problem when \( n \) is large.
  - current technology: \( n = O(2^{12}) = O(10^{154}) \).
  - hence, it is safe to choose \( p, q = O(2^{12}) \).
- Problem with large \( n = pq = O(2^{1024}) \):
  - need multi-precision arithmetic software
  - need to compute \( x^e \mod n \) fast

Big-O bounds for large integer operations

- \( x, y \) be two large integers with length \( k \) and \( l \):
  - \( k = \lceil \log_2 x \rceil + 1 \),
  - \( l = \lceil \log_2 y \rceil + 1 \).
  - \( k \geq l \).
- Assume “standard” techniques used.

<table>
<thead>
<tr>
<th>Operations</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x+y ), ( x-y )</td>
<td>( O(k) )</td>
</tr>
<tr>
<td>( x \cdot y )</td>
<td>( O(kl) )</td>
</tr>
<tr>
<td>( \lfloor x/y \rfloor )</td>
<td>( O((k-l)) )</td>
</tr>
<tr>
<td>( \gcd(x, y) )</td>
<td>( O(k^3) )</td>
</tr>
</tbody>
</table>
Big-O bound for $Z_n$ operations

- $x, y$ be two elements in $Z_n$:
  - $k = \lceil \log_2 n \rceil + 1$,
  - Assume “standard” techniques used.
  - $x^c \mod n$: Modular exponentiation is used frequently.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x+y, x-y$</td>
<td>$O(k)$</td>
</tr>
<tr>
<td>$x \cdot y$</td>
<td>$O(k^2)$</td>
</tr>
<tr>
<td>$x^{-1}$</td>
<td>$O(k^3)$</td>
</tr>
<tr>
<td>$x^c$</td>
<td>$O(\log_2 c \ k^2)$</td>
</tr>
</tbody>
</table>

Modular Exponentiation (Recursive)

- $x^c \mod n =$
  - $[x^{c/2} \mod n]^2 \mod n$, if $c$ is even
  - $[x^{c/2} \mod n]^2 \cdot x \mod n$, if $c$ is odd
  - (stopping condition) $x^0 \mod n = 1$.

- e.g. show $2^{26} = 53 \mod 131$
- e.g. show $2^{124} = 216 \mod 1000$

$2^{124} \mod 1000 = 216$

```
<table>
<thead>
<tr>
<th>c</th>
<th>c/2</th>
<th>c/2 mod 1000</th>
<th>216*c/2 mod 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>124</td>
<td>62</td>
<td>36</td>
<td>1520</td>
</tr>
<tr>
<td>62</td>
<td>31</td>
<td>17</td>
<td>149</td>
</tr>
<tr>
<td>31</td>
<td>15</td>
<td>10</td>
<td>650</td>
</tr>
<tr>
<td>15</td>
<td>7</td>
<td>6</td>
<td>850</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>4</td>
<td>720</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>126</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
```
Modular Exponentiation (Iterative)

- Algorithm 5.5 (page 177) Square-and-multiply algorithm. Find $x^c \mod n$.
- Find binary representation of $c = \sum c_i 2^i$.
- $z \leftarrow 1$;
- for $c_i$ from MSD to LSD (least sig. digit)
  - $z \leftarrow z^{2^i} \mod n$
  - if ($c_i=1$) then $z \leftarrow z \times x \mod n$ [or $z \leftarrow z^{x \cdot c_i}$]
- return ($z$).

Compute $9726^{3533} \mod 11413$

Euler’s Theorem

- For any $n$ and $\gcd(y,n)=1$, $y^{\phi(n)} \equiv 1 \pmod{n}$.
  - $\phi(n)$: number of integers between 1 and $n$ that are relative prime to $n$.
- E.g. $n=20$,
  - $\phi(20) = 8 = \#S$, $S = \{ y \mid \gcd(y,20) = 1 \}$
  - $13^8 = 1 \pmod{20}$.
  - $13^{-1} = 13^7 = 17 \pmod{20}$. 
Euler totient function $\varphi(n)$

- $\varphi(n)$: number of integers between 1 and $n$ that are relative prime to $n$.
- Computation of $\varphi(n)$:
  - $\varphi(p^e) = p^{e-1}(p-1)$
  - $\varphi(\text{P Q}) = \varphi(\text{P}) \varphi(\text{Q})$, if $\gcd(\text{P}, \text{Q}) = 1$.
- E.g.
  - $\varphi(20) = \{1, 3, 7, 9, 11, 13, 17, 19\} = 8$
  - $\varphi(5) = \{1, 2, 3, 4\} = 4$
  - $\varphi(4) = \{1, 3\} = 2$

RSA Encryption: Main Idea

- $n = \text{p x q}$, where $\text{p}$ and $\text{q}$ are huge numbers (so $?$)
- Given $\text{d}$ and $\text{e}$ with $\text{d x e} = 1 \mod (p-1)(q-1)$
- Note $\varphi(n) = \varphi(p) \varphi(q) = (p-1)(q-1)$
- $\text{C} = P^\text{e} \mod n$; $\text{P} = C^\text{d} \mod n$
- Key point: for any $Y < n$, we have $Y^{de} = Y \mod n$.

Why $Y^{de} = Y \mod n$?

- Case 1: $\gcd(Y, n) = \gcd(Y, \text{p q}) = 1$.
  - Follows easily from Euler’s Theorem and $\text{d x e} = 1 \mod (p-1)(q-1)$
  - How?
    - $\text{d x e} = 1 + k(p-1)(q-1) = 1 + k \varphi(n)$.
    - $Y^{\varphi(n)} = 1 \mod n$. [Euler’s Theorem]
    - $Y^{de} = Y \times Y^{\varphi(n)k} = Y \mod n$. \

Why \( Y^{de} = Y \mod n \) ?

[where \( d \times e = 1 + k \varphi(n) \)]

Case 2: \( \gcd(Y,n) = \gcd(Y,p) > 1 \).
- Either \( p \mid Y \) or \( q \mid Y \) but not both.
- \( Y = w \times p \) [similar proof for \( q \mid Y \)]
- \( Y^{q-1} = 1 \mod q \). [Fermat’s Little Theorem]
- Hence, \( Y^{(q-1)(p-1)} = Y^{k \varphi(n)} = 1 \mod q \).
  - \( Y^k \varphi(n) = 1 + mq \)
  - \( Y^{Y^k \varphi(n)} = Y^{(1 + mq)} = Y^w \times p \times m \times q \)
  - \( Y^{de} = Y^{k \varphi(n)+1} = Y \mod pq \)

Comparing Secret Key and Public Key Encryption

- Number of keys
- Ease of Key distribution
- Speed of encryption/decryption:
  - Symmetric key: fast
  - Asymmetric key: slow, 1,000+ times slower.
- Best Uses
  - Symmetric key: cryptographic workhorse.
  - Asymmetric key: key exchange, authentication.

Summary

- Some mathematical tools discussed:
  - Basic Group Theory
  - Fermat Little Theorem
  - Euler Theorem
  - Primitive element mod n and its properties
  - Integer factorization.
- Attack and analysis of RSA
- Fast Modulus Exponentiation.
HW5

- (written assignment)
  - 5.3, 5.5, 5.6, 5.7, 5.33
- (program assignment)
  - 5.12.

Multi-precision arithmetic software packages

- Modular arithmetic operations are provided to compute residues, perform exponentiation, and compute multiplicative inverses:
  - BigInteger class in Java:
    - [http://java.sun.com/j2se/1.4.2/docs/api/java/math/BigInteger.html](http://java.sun.com/j2se/1.4.2/docs/api/java/math/BigInteger.html)
  - MAPLE or MATHEMATICA.