Basic Number Theory -- Foundation of Public Key Cryptography (II)
Review

- GCD
- Relatively Prime
- (Extended) Euclid's Algorithm
- Modular Operations/Laws
- Multiplicative Inverse
- Fermat's Little Theorem
\( \mathbb{Z}_n \) vs \( \mathbb{Z}_n^* \)

- \( \mathbb{Z}_n \) is the set \{0, 2, ..., \( n-1 \}\}, the space induced by the \((\text{mod } n)\) operator.

- \( \mathbb{Z}_n^* \) is the set with all positive integers less than \( n \) and relatively prime to \( n \).
  - a subset of \( \mathbb{Z}_n \)

- Q: \( \mathbb{Z}_n^*=? \) when \( n=5 \).

- Q: Can we say the following are equivalent:
  - a and \( n \) is relatively prime
  - a is in \( \mathbb{Z}_n^* \)
The Totient Function

- $\phi(n) = |\mathbb{Z}_n^*|$: the number of elements in $\mathbb{Z}_n^*$.
  - $\mathbb{Z}_n^*$ is the set of integers less than $n$ and relatively prime to $n$.

Examples

- $\phi(4)$ = ?
  - $GCD(1, 4) = ?$
  - $GCD(2, 4) = ?$
  - $GCD(3, 4) = ?$

- $\phi(6)$ = ?
  - $GCD(1, 6) = ?$
  - $GCD(2, 6) = ?$
  - $GCD(3, 6) = ?$
  - $GCD(4, 6) = ?$
  - $GCD(5, 6) = ?$
Properties of Totient Function

a) if \( n \) is prime, then \( \phi(n) = n - 1 \)

Example: \( \phi(7) = 6 \)

b) if \( n = p^\alpha \), where \( p \) is prime and \( \alpha > 0 \), then
\[
\phi(n) = (p-1)p^{\alpha-1}
\]

Example: \( \phi(25) = \phi(5^2) = 4*5^1 = 20 \)

c) if \( n=p*q \), and \( p, q \) are relatively prime, then
\[
\phi(n) = \phi(p)*\phi(q)
\]

Example: \( \phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8 \)
Exercise 1

• $\phi(13)=?$
• $\phi(19)=?$
Exercise II

- $\phi(20) = ?$
- $\phi(21) = ?$

Tip:

If $n = p \times q$, and $p$, $q$ are relatively prime, then

$\phi(n) = \phi(p) \times \phi(q)$
Exercise III

- $\phi(500) = ?$

$\phi(500) = \phi(125) \times \phi(4) = \phi(5^3) \times 2 = (5-1) \times 5^2 \times 2 = 4 \times 25 \times 2 = 200$
Computing Totient Function

• If $n$ is very large, it is generally hard to find the value of $\phi(n)$.
  - Finding $\phi(n)$ requires factoring $n$ first
  - Suppose that $n$ is some number on the order of $2^{1024}$, it is computationally difficult to factoring $n$.
  - There is no simple/efficient method!

Key: factoring a large number is computationally hard!
Euler’s Theorem

• For every $a$ and $n$ that are relatively prime, $a^{\phi(n)} \equiv 1 \mod n$

Example: $3 \phi(10) \equiv 1 \mod 10$ (a = 3, n = 10, which are relatively prime)

Verify: $\phi(10) = \phi(2*5) = \phi(2) * \phi(5) = 1*4 = 4$
$3 \phi(10) = 3^4 = 81 \equiv 1 \mod 10$

Example: $2 \phi(11) \equiv 1 \mod 11$ (a = 2, n = 11, which are relatively prime)

Verify: $\phi(11) = 11-1 = 10$
$2 \phi(11) = 2^{10} = 1024 \equiv 1 \mod 11$
More Euler...

- **Variant**: for all $n$, all $a$ in $\mathbb{Z}_n^*$, and all non-negative $k$, $a^{k\phi(n)+1} \equiv a \mod n$

Example: for $n = 20$, $a = 7$, $\phi(n) = 8$, and $k = 3$:

$$7^{3 \cdot 8 + 1} \equiv 7 \mod 20$$

- **Generalized Euler’s Theorem**: for $n = pq$ ($p$ and $q$ distinct primes) and for all $a$ in $\mathbb{Z}_n$, and all non-negative $k$, $a^{k\phi(n)+1} \equiv a \mod n$

Example: for $n = 15$, $a = 6$, $\phi(n) = 8$, and $k = 3$:

$$6^{3 \cdot 8 + 1} \equiv 6 \mod 15$$
Euler’s vs Fermat Little Theorems

• For every $a$ and $n$ that are relatively prime,
  $a^\varphi(n) \equiv 1 \pmod{n}$

• If $n$ is prime,
  $a^{n-1} \equiv 1 \pmod{n}$

Fermat Little Theorem is a special case for Euler’s Theorem!
Modular Exponentiation

- \( a^x \mod n = a^x \mod \phi(n) \mod n \)
  
  - \( a \) and \( n \) are relatively prime

Example: \( 5^7 \mod 6 = 5^7 \mod \phi(6) \mod 6 \)

\[ = 5^7 \mod 2 \mod 6 = 5 \]

Example: \( 2^{101} \mod 33 = 2^{101} \mod \phi(33) \mod 33 \)

\[ = 2^{101} \mod 20 \mod 33 \]

\[ = 2 \mod 33 \]

\[ = 2 \]
Exercise

• $2^{10000} \mod 33 = ?$

  $= 2^{10000} \mod \phi(33) \mod 33$

  $= 2^{10000} \mod 20 \mod 33 = 2^0 \mod 33 = 1$

Using: $a^x \mod n = a^{x \mod \phi(n)} \mod n$
The Powers of An Integer, Modulo $n$

- Given $a$, consider equation: $a^m \equiv 1 \mod n$
  - $m$ can be 1, 2, 3, 4, ...
  - Is it possible to find a value of $m$ to satisfy the equation?

- Yes. If $a$ and $n$ are relatively prime, there is at least one integer $m$!

Example: for $a = 3$ and $n = 7$, what is $m$?

<table>
<thead>
<tr>
<th>$m$</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>
</tr>
</thead>
<tbody>
<tr>
<td>$3^m \mod 7$</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>
The Power (Cont’d)

- The **smallest** positive exponent \( m \) for which the equation

\[
a^m \equiv 1 \mod n
\]

holds is referred to as...

- the **order of a** \((\mod n)\), or
- the **length of the period** generated by \( a \)

<table>
<thead>
<tr>
<th></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>
</tr>
</thead>
<tbody>
<tr>
<td>(m)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(3^m \mod 7)</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>
Understanding Order of $a \pmod{n}$

- If we fix $n$, and change $a$ in $a^m \pmod{n}$ for $m = 1, 2, 3, 4, ...$
- Example: $n=19$

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2$</th>
<th>$a^3$</th>
<th>$a^4$</th>
<th>$a^5$</th>
<th>$a^6$</th>
<th>$a^7$</th>
<th>$a^8$</th>
<th>$a^9$</th>
<th>$a^{10}$</th>
<th>$a^{11}$</th>
<th>$a^{12}$</th>
<th>$a^{13}$</th>
<th>$a^{14}$</th>
<th>$a^{15}$</th>
<th>$a^{16}$</th>
<th>$a^{17}$</th>
<th>$a^{18}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>13</td>
<td>7</td>
<td>14</td>
<td>9</td>
<td>18</td>
<td>17</td>
<td>15</td>
<td>11</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>5</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>7</td>
<td>9</td>
<td>17</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>16</td>
<td>7</td>
<td>9</td>
<td>17</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>11</td>
<td>4</td>
<td>17</td>
<td>1</td>
<td>9</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>11</td>
<td>4</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
</tr>
</tbody>
</table>

Order: 1, 18, 9, 3, 6, 9, 2
Observations on The Previous Table

• $n = 19$, then $\phi(n) = 18$, and $\mathbb{Z}_n^*=?$

• Some of the sequences are of length 18
  - e.g., the base $a=2$ generates (via powers) all members of $\mathbb{Z}_n^*$
  - The base is called the primitive root (mod $n$)
  - The base is also called the generator when $n$ is prime
    • $a, a^2, \ldots, a^{n-1}$ are all distinct numbers mod $n$ in $\mathbb{Z}_n^*$

• Key: No simple general formula to compute primitive roots modulo $n$
Discrete Logarithms
Square Roots

• x is a non-trivial square root of 1 mod n if it satisfies the equation $x^2 \equiv 1 \mod n$, but x is neither 1 nor n-1.
  - Why n-1 is always a square root of 1 mod n?

Ex: 6 is a square root of 1 mod 35 since $6^2 \equiv 1 \mod 35$

• Theorem: if there exists a non-trivial square root of 1 mod n, then n is not prime
  - i.e., prime numbers will not have non-trivial square roots
Roots (Cont’d)

If $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where $p_1 \ldots p_k$ are distinct primes > 2, then the number of square roots (including trivial square roots) are:

- $2^k$ if $\alpha_0 \leq 1$

Example: for $n = 70 = 2^1 * 5^1 * 7^1$, $\alpha_0 = 1$, $k = 2$, and
the number of square roots = $2^2 = 4$ (1,29,41,69)

- $2^{k+1}$ if $\alpha_0 = 2$

Example: for $n = 60 = 2^2 * 3^1 * 5^1$, $k = 2$,
the number of square roots = $2^3 = 8$ (1,11,19,29,31,41,49,59)

- $2^{k+2}$ if $\alpha_0 > 2$

Example: for $n = 24 = 2^3 * 3^1$, $k = 1$,
the number of square roots = $2^3 = 8$ (1,5,7,11,13,17,19,23)
Discrete Logarithms

• For a primitive root $a$ of a number $p$, where $a^i \equiv b \mod p$, for some $0 \leq i \leq p-1$
  
  - the exponent $i$ is referred to as the *index of $b$ for the base $a$ (mod $p$)*, denoted as $\text{ind}_{a,p}(b)$
    - sometime also denoted as $d\log_{a,p}(b)$

  - $i$ is also referred to as the *discrete logarithm of $b$ to the base $a$, mod $p$*
Logarithms (Cont’d)

- Example: \( a=2 \) is a primitive root of \( p=19 \). It is straightforward to get \( b = a^i \mod p \)

<table>
<thead>
<tr>
<th>( i )</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>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>( b )</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>13</td>
<td>7</td>
<td>14</td>
<td>9</td>
<td>18</td>
<td>17</td>
<td>15</td>
<td>11</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

- How to get the discrete logarithm \( i \) from \( b \); e.g., \( \text{ind}_{2,19}(9) \)

<table>
<thead>
<tr>
<th>( b )</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>
</tr>
</thead>
<tbody>
<tr>
<td>( i = \text{ind}_{2,19}(b) ) = ( \log(b) \mod 2 \mod 19 )</td>
<td>0</td>
<td>1</td>
<td>13</td>
<td>2</td>
<td>16</td>
<td>14</td>
<td>6</td>
<td>3</td>
<td>8</td>
</tr>
</tbody>
</table>

| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |
Computing Discrete Logarithms

- However, given $a$, $b$, and $p$, computing $i = \text{ind}_{a,p}(b)$ is computationally difficult
  - Used as the basis of some public key cryptosystems
Some properties of discrete logarithms

- \( \text{ind}_{a,p}(1) = 0 \) because \( a^0 \mod p = 1 \)
- \( \text{ind}_{a,p}(a) = 1 \) because \( a^1 \mod p = a \)
- \( \text{ind}_{a,p}(yz) = (\text{ind}_{a,p}(y) + \text{ind}_{a,p}(z)) \mod \phi(p) \)

Example: \( \text{ind}_{2,19}(5*3) = (\text{ind}_{2,19}(5) + \text{ind}_{2,19}(3)) \mod 18 = 11 \)

- \( \text{ind}_{a,p}(y^r) = (r \text{ ind}_{a,p}(y)) \mod \phi(p) \)

Example: \( \text{ind}_{2,19}(3^3) = (3*\text{ind}_{2,19}(3)) \mod 18 = 3 \)
More on Discrete Logarithms

- $a^{\text{ind}_{a,p}(x)} \equiv x \mod p,$

- $(a^{\text{ind}_{a,p}(x)} \mod p)(a^{\text{ind}_{a,p}(y)} \mod p) 
  \equiv (a^{\text{ind}_{a,p}(x)+\text{ind}_{a,p}(y)}) \mod p 
  \equiv a^{\text{ind}_{a,p}(xy)} \mod p$

Ex: $2^{13} \mod 19 = 3$
Difficulties in Modular Arithmetic

- Factoring large numbers
- Computing Totient function
  - Need factoring first
- Obtaining primitive roots
- Discrete logarithm

- Public key cryptography design should leverages all these difficulties!