Introduction to Information Security

Lecture 5: Number Theory

2007. 6.

Prof. Byoungcheon Lee
sultan (at) joongbu . ac . kr

Information and Communications University
Contents

1. Number Theory
   - Divisibility
   - Prime numbers and factorization
   - gcd and lcm
   - Euclidean algorithm, Extended Euclidean algorithm
   - Congruence and modular arithmetic
   - Chinese remainder theorem
   - Fermat’s theorem and Euler’s theorem
   - Legendre symbol and Jacobi symbol

2. Finite Fields
   - Group, Ring
   - Field, Finite field
   - Cyclic group
Divisibility

- Let $\mathbb{Z}$ denote the set of all integers. $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Division Theorem ($a, b \in \mathbb{Z}$)
  - For nonzero $b$, $\exists q, r \in \mathbb{Z}$ s.t. $a = qb + r$, $0 \leq r < b$
  - $q$: quotient, $r$: remainder
- Divide
  - $b$ divides $a$, or $b|a$ iff $\exists c \in \mathbb{Z}$ s.t. $a = bc$ (i.e. $r = 0$)
  - If $a|b$, then $a|bc$
  - If $a|b$ and $a|c$, then $a|(bx + cy)$
  - If $a|b$ and $b|a$ then $a = \pm b$ (antisymmetry)
  - If $a|b$ and $b|c$, then $a|c$ (transitivity)
Prime Numbers

- Prime
  - An integer $p$ is called prime if its divisors are $\pm 1$ and $\pm p$
  - A number that is divisible only by 1 and itself
  - $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$
  - If a prime $p$ divides $ab$, then $p|a$ or $p|b$

- Composite number
  - Any number that is not prime
Prime Number Theorem

- There are infinitely many prime numbers

- Prime number theorem

\[ \pi(x) \approx \frac{x}{\ln x} : \text{number of primes less than } x \]

\[ \lim_{n \to \infty} \frac{\pi(x) \ln(x)}{x} = 1 \]

- Example: Estimate the number of 100-digit primes

\[ \pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9 \times 10^{97} \]
Sieve of Eratosthenes

- **Sieve of Eratosthenes**: Determine all primes smaller than $N$
  
  S1. Create an initial set of all numbers $N_N = \{2, 3, 4, ..., N-1\}$
  
  S2. For all integers $n < \sqrt{N}$, remove all multiples of $n$ from the above $N_N$
  
  S3. The final reduced set $N_N$ contains all primes smaller than $N$

- **Exercise 1**: Obtain all primes less than 200
Factorization

- Factorization
  - Any positive integer can be uniquely factored into the product of primes
    \[ n = \prod_{p \in P} p^{e_p} \]
  - \( 504 = 2^3 3^2 7 \), \( 1125 = 3^2 5^3 \)
lcm and gcd

- \( \text{lcm}(a,b) \) - least common multiple
  - \( \text{lcm} \) of \( a \) and \( b \) is the smallest integer which is divisible by both \( a \) and \( b \)

- \( \text{gcd}(a,b) \) - greatest common divisor
  - \( \text{gcd} \) of \( a \) and \( b \) is the largest integer which divides both \( a \) and \( b \)
  - Example: \( \text{gcd}(24,60)=12 \), \( \text{gcd}(5,7)=1 \)
  - \( a \) and \( b \) are relatively prime if \( \text{gcd}(a,b)=1 \)

Finding \( \text{gcd}(a,b) \)

- Using the factorization of \( a \) and \( b \)
  - \( 576=2^63^2 \), \( 135=3^35 \), \( \text{gcd}(576,135)=3^2 \)
- Using the Euclidean algorithm
Euclidean Algorithm - find gcd using division and remainder

- Find $gcd(a,b)$
  - Initialize $r_0=a$, $r_1=b$
  - Computes the following sequence of equations
    
    \[
    r_0 = q_1r_1 + r_2 \\
    r_1 = q_2r_2 + r_3 \\
    r_2 = q_3r_3 + r_4 \\
    \ldots \ \\
    r_{n-2} = q_{n-1}r_{n-1} + r_n \quad \text{where } r_n = 0
    \]

- Then $gcd(a,b) = r_{n-1}$
  
  \[
  r_0 = a = (??) \times r_{n-1} \\
  r_1 = b = (??) \times r_{n-1}
  \]
Euclidean Algorithm - find gcd using division and remainder

Example: \( \gcd(3465, 882) = 63 \)

\[
\begin{align*}
3465 &= 3 \times 882 + 819 \\
882 &= 1 \times 819 + 63 \\
819 &= 13 \times 63 + 0
\end{align*}
\]

\[
\begin{array}{c|ccc|}
& 3 & 3465 & 882 & 1 \\
\hline
13 & 819 & 63 & 0
\end{array}
\]
Extended Euclidean Algorithm

- Extended Euclidean Algorithm
  - Let \( d = \gcd(a, b) \). Then there exist integers \( x, y \) such that \( ax + by = d \).
  - If \( a \) and \( b \) are relatively prime, then there exist \( x, y \) such that \( ax + by = 1 \)

\[
\begin{align*}
a &= q_1b + r_2 & r_2 &= a - q_1b \\
b &= q_2r_2 + r_3 & r_3 &= b - q_2r_2 = -q_2a + (1 + q_1q_2)b \\
r_2 &= q_3r_3 + r_4 & r_4 &= r_2 - q_3r_3 = (?)a + (?)b \\
\cdots & \cdots \\
r_{n-2} &= q_{n-1}r_{n-1} & r_{n-1} &= (?)a + (?)b & \rightarrow & ax + by = d
\end{align*}
\]

Example

\[
\begin{align*}
\gcd(10, 7) &= 1 & 1 &= (-2)(10) + (3)(7) \\
\gcd(367, 221) &= 1 & 1 &= (-56)(367) + (93)(221)
\end{align*}
\]
Extended Euclidean Algorithm

- Easier calculation algorithm by hand
  - \(\text{http://marauder.millersville.edu/~bikenaga/absalg/exteuc/exteucex.html}\)

- Example: for \(\gcd(187,102) = 17\)

\[
\begin{align*}
(\text{next } x) &= (\text{next-to-last } x) - q \ (\text{last } x) \\
(\text{next } y) &= (\text{next-to-last } y) - q \ (\text{last } y)
\end{align*}
\]

\[17 = (187,102) = (-1)(187) + (2)(102).\]
Extended Euclidean Algorithm

Exercise 2: For the following pair of numbers
1. Find gcd using Euclidean algorithm
2. Solve $ax+by=d$ using Extended Euclidean algorithm

1. $gcd(55, 123)$
2. $gcd(41, 789)$
3. $gcd(352, 124)$
4. $gcd(1124, 368)$
5. $gcd(2733, 725)$
Congruence

- **Definition** Congruence
  \[ a \equiv b \mod n \iff n|(a-b) \]
  \[ a = b + kn \] for some integer \( k \)
  \[ a \% n = b \% n \]
  \( a \) is congruent to \( b \) modulo \( n \)

- \( a \equiv a \)
- \( a \equiv b \) iff \( b \equiv a \)
- If \( a \equiv b \) and \( b \equiv c \) then \( a \equiv c \)

- **Residue Class Group**: \( \mathbb{Z}_n = \{ x \in \mathbb{Z} | 0 \leq x < n \} \)
  - Addition: \( a + b = (a + b) \mod n \)
  - Multiplication: \( ab = (ab) \mod n \)
  - Closed under addition, subtraction, and multiplication
  - Closed under division if \( n \) is prime

- \( 32 \equiv 2 \mod 5 \)
- \( -12 \equiv 37 \mod 7 \)
Modular Arithmetic

- Modular addition
- Modular subtraction
- Modular multiplication
  - Fill out the table

Modular multiplication in mod 11
Compute \( axb \mod 11 \)

<table>
<thead>
<tr>
<th>x</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>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
Modular Arithmetic

- Modular exponentiation
- Fill out the table

<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>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Modular exponentiation in mod 11
Compute $a^b \mod 11$
Modular Arithmetic

Modular exponentiation in mod 13
Compute \( a^b \mod 13 \)

<table>
<thead>
<tr>
<th>a (^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>
<th>10</th>
<th>11</th>
<th>12</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>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>10</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>12</td>
<td>3</td>
<td>12</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>12</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>10</td>
<td>8</td>
<td>9</td>
<td>2</td>
<td>12</td>
<td>7</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>10</td>
<td>5</td>
<td>9</td>
<td>11</td>
<td>12</td>
<td>6</td>
<td>3</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>12</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>12</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>12</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>9</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>10</td>
<td>9</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>7</td>
<td>12</td>
<td>2</td>
<td>9</td>
<td>8</td>
<td>10</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
</tr>
</tbody>
</table>
Modular Arithmetic

- Modular division
  - Solve: $2x + 7 = 3 \pmod{17} \rightarrow 2x = -4 \pmod{17} \rightarrow x = -2 \pmod{17} = 15$

- You can divide by $a$ mod $n$ only when $\gcd(a, n) = 1$
  - Find the multiplicative inverse of $a$ mod $n = a^{-1}$ and then multiply $a^{-1}$
  - $b / a \pmod{n} = b * a^{-1} \pmod{n}$
  - If $ac = 1 \pmod{n}$, then $c = a^{-1} \pmod{n}$
  - Compute $a^{-1} \pmod{n}$ using the extended Euclidean algorithm
  - For $\gcd(n, a) = 1$, solve $ax + ny = 1$, then $x = a^{-1} \pmod{n}$
Efficient Modular Exponentiation

- How to compute $a^x \ (mod \ n)$ efficiently?
  - Multiply $a$ $x$ times? No good

$2^{1234} \ mod \ 789 = 2^{1024+128+64+16+2} \ mod \ 789$

$= 2^{1024} * 2^{128} * 2^{64} * 2^{16} * 2^2 \ mod \ 789$

$= 286 * 559 * 367 * 49 * 4 \ mod \ 789$

$= 481 \ mod \ 789$
Square and Multiply Algorithm

- How to compute \( y = a^x \mod n \) efficiently?
  1. binary representation of \( x = x_r x_{r-1} \ldots x_1 x_0 \)
  2. Let \( y = a \)
  3. For \( i \) from \( r-1 \) to 0
      - \( y = y^2 \mod n \)
      - If \( x_i = 1 \), then \( y = ya \mod n \)
  4. Output \( y \)

Compute \( 7^{21} \mod 11 \), \( 21 = 10101_2 \), \( r = 4 \)

<table>
<thead>
<tr>
<th>i</th>
<th>bit</th>
<th>( y^2 )</th>
<th>( y \cdot a )</th>
<th>( y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>7^2=5</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>7^2=5</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>5^2=3</td>
<td>3*7=10</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>10^2=1</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1^2=1</td>
<td>1*7=7</td>
<td>7</td>
</tr>
</tbody>
</table>

Output 7 as the result
Chinese Remainder Theorem (CRT)

- **Chinese Remainder Theorem**

  Suppose $\gcd(m, n) = 1$. Given integers $a$ and $b$, there exists exactly one solution $x \pmod{mn}$ to the simultaneous congruences
  
  $x = a \pmod{m}, \ x = b \pmod{n}$

**proof**

- there exists $s, t$ such that $ms + nt = 1$
- $ms = 1 \pmod{n}, \ nt = 1 \pmod{m}$
- Let $x = ant + bms$, then
  
  - $x = ant \pmod{m} = a \pmod{m}$
  - $x = bms \pmod{n} = b \pmod{n}$
Chinese Remainder Theorem (CRT)

Find a number $x$ which satisfies

$$x = b_1 \mod m_1$$

......

$$x = b_n \mod m_n$$

- Efficient algorithm to compute $x$
  1. $m = m_1 m_2 \ldots m_n = 5*7*11 = 385$
  2. $M_1 = m/m_1 = 385/5 = 7*11 = 77$
     $M_2 = m/m_2 = 385/7 = 5*11 = 55$
     $M_3 = m/m_3 = 385/11 = 5*7 = 35$
  3. $N_1 = M_1^{-1} \mod m_1 = 77^{-1} \mod 5 = 3$
     $N_2 = M_2^{-1} \mod m_2 = 55^{-1} \mod 7 = 6$
     $N_3 = M_3^{-1} \mod m_3 = 35^{-1} \mod 11 = 6$
  4. $T = b_1 M_1 N_1 + b_2 M_2 N_2 + b_3 M_3 N_3 \mod m$
     $= 4*77*3 + 3*55*6 + 6*35*6 \mod 385 = 94$

Example: Find $x$ such that

$$x = 4 \mod 5$$
$$x = 3 \mod 7$$
$$x = 6 \mod 11$$

Use extended Euclidean algorithm
Chinese Remainder Theorem (CRT)

Exercise 3: find a number which satisfies

1. \( x = 3 \equiv 6 \equiv 8 \mod 11 \mod 7 \mod 13 \)

2. \( x = 5 \equiv 6 \equiv 8 \mod 31 \mod 17 \mod 29 \)
Euler phi function: $\phi(n)$

- Euler phi function (or Euler totient function): $\phi(n)$
  - The number of integers in $[1, n]$, which are relatively prime to $n$
  - If $p$ is prime, $\phi(p) = p-1$
  - $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ for prime $p > 2$
  - If $\gcd(n, m) = 1$, $\phi(nm) = \phi(n) \cdot \phi(m)$ (multiplicative property)
  - So, for primes $p$ & $q$, $\phi(pq) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$
Fermat’s Theorem and Euler’s Theorem

- **Fermat’s Theorem**
  - Let $p$ be a prime
  - If $\gcd(x, p) = 1$, then $x^{p-1} = 1 \mod p$
  - If $a = b \mod p-1$, then $x^a = x^b \mod p$ for all integers $x$
  - $x^p = x \mod p$ for all integers $x$

- **Euler’s Theorem**
  - Let $n$ be an integer
  - If $\gcd(x, n) = 1$, then $x^{\phi(n)} = 1 \mod n$
  - If $n$ is a product of distinct primes and $a = b \mod \phi(n)$, then $x^a = x^b \mod n$ for all integers $x$
  - $x^n = x \mod n$ for all integers $x$
Legendre Symbol

- Quadratic congruence for a prime modulus p
  \[ x^2 = a \pmod{p} \] where p is a prime

It will have
1. one solution if \( a \equiv 0 \pmod{p} \)
2. two solutions if \( a \) is a quadratic residue modulo p
3. no solution if \( a \) is a quadratic non-residue modulo p

- Legendre symbol is defined as

\[
\left( \frac{a}{p} \right) = \begin{cases} 
0 & \text{If } a = 0 \\
1 & \text{If } a \text{ is a QR} \\
-1 & \text{If } a \text{ is a QNR}
\end{cases}
\]

It is computed by
\[
\left( \frac{a}{p} \right) = a^{\frac{1}{2}(p-1)} \pmod{p}
\]
Quadratic Residue

- **Example in Z_{13}^\ast**

\[
\begin{align*}
1^2 &\equiv 1 \pmod{13} & 7^2 &\equiv 10 \pmod{13} \\
2^2 &\equiv 4 \pmod{13} & 8^2 &\equiv 12 \pmod{13} \\
3^2 &\equiv 9 \pmod{13} & 9^2 &\equiv 3 \pmod{13} \\
4^2 &\equiv 3 \pmod{13} & 10^2 &\equiv 9 \pmod{13} \\
5^2 &\equiv 12 \pmod{13} & 11^2 &\equiv 4 \pmod{13} \\
6^2 &\equiv 10 \pmod{13} & 12^2 &\equiv 1 \pmod{13}
\end{align*}
\]

- **QR = \{1, 3, 4, 9, 10, 12\}**

\[
\frac{3}{13} = 3^{\frac{1}{2}(13-1)} \pmod{13} = 3^6 \pmod{13} = 1
\]

- **QNR = \{2, 5, 6, 7, 8, 11\}**

\[
\frac{2}{13} = 2^{\frac{1}{2}(13-1)} \pmod{13} = 2^6 \pmod{13} = -1
\]
Jacobi Symbol

- Generalization of Legendre symbol
- Quadratic congruence for an arbitrary modulus n
  \[ x^2 = a \pmod{n} \quad \text{where} \quad n = p_1 \cdots p_r \]

It is computed by

\[
\left( \frac{a}{n} \right) = \prod_{i=1}^{r} \left( \frac{a}{p_i} \right)
\]
Definition) A group \((G,*)\) consists of a set \(G\) with a binary operation \(*\) on \(G\) satisfying the following three axioms.

1. \(a*(b*c)=(a*b)*c\) for all \(a,b,c \in G\) : associative
2. There is an element \(1 \in G\) called the identity element s.t. \(a*1=1*a=a\)
3. For each \(a \in G\) there exists an element \(a^{-1}\) (inverse) s.t. \(a*a^{-1}=a^{-1}*a=1\)

A group \(G\) is abelian (or commutative) if, furthermore,
4. \(a*b=b*a\) for all \(a,b \in G\)
Ring

Definition) A ring \((R, +, \times)\) consists of a set \(R\) with two binary operations arbitrarily denoted \(+\) (addition) and \(\times\) (multiplication) on \(R\) satisfying the following axioms.

1. \((R, +)\) is an abelian group with identity denoted 0.
2. The operation \(\times\) is associative. That is \(a(x(b+c)) = (axb)xc\) for all \(a, b, c \in R\).
3. There is a multiplicative identity denoted 1, s.t. \(1xa = ax1 = a\) for all \(a \in R\).
4. The operation \(\times\) is distributive over \(+\). \(ax(b+c) = (axb)+(xbc)\) for all \(a, b, c \in R\).

The ring \(R\) is a commutative ring if \(ab = ba\) for all \(a, b \in R\).
Field and Finite Field

Definition) A field is a commutative ring in which all non-zero elements have multiplicative inverses.

Definition) A finite field (Galois Field) is a field F which contains a finite number of elements.

Galois Field GF(p)=\(\mathbb{Z}_p\) with prime p
- addition, subtraction, multiplication, and division by non-zero elements are all well-defined.
- arithmetic modulo p.

Galois Field GF(q^n) with prime q and degree n
- arithmetic modulo irreducible polynomials of degree n whose coefficients are integers modulo q.
Order of Group

- Order of group in modular arithmetic
  - $x = y \mod n : x$ is congruent to $y$ modulo $n$; $n$ divides $(x-y)$
  - $Z_n = \{0, 1, 2, \ldots, n-1\}$
  - $Z_n^* = \{ x \in Z_n \mid \gcd(x, n) = 1 \}$: multiplicative group of $Z_n$
  - Order of $Z_n^*$ = the number of elements in $Z_n^*$ = $|Z_n^*| = \phi(n)$
  - Order of $x \in Z_n^*$ = smallest integer $r$ such that $x^r = 1 \mod n$
  - $\text{Ord}(x)$ for any $x \in Z_n^*$ = a divisor of $\phi(n)$
Cyclic Group

- Let p be a prime
  - \( \mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\} \)
  - \( \mathbb{Z}_p^* = \{ x \in \mathbb{Z}_p \mid \gcd(x, p) = 1\} = \{1, 2, \ldots, p-1\} = \mathbb{Z}_p - \{0\} \)
  - Order of \( \mathbb{Z}_p \) = \( | \mathbb{Z}_p^* | = \phi(p) = p-1 \)
  - Order of an element \( \alpha \in \mathbb{Z}_p^* = \text{Ord}(\alpha) = \) a divisor of \( p-1 \)
    - \( \alpha \) is a generator / primitive element of \( \mathbb{Z}_p^* \) if \( \text{Ord}(\alpha) = \phi(p) = p-1 \)
      - Then \( \mathbb{Z}_p^* = \{\alpha^i \mid i = 0, 1, \ldots, p-2\} : \) cyclic group
      - For any \( y \in \mathbb{Z}_p^* \), there exists an integer \( x \in [0, p-2] \) such that \( y = \alpha^x \mod p \)

- Let p be a prime and q be a prime divisor of p-1, i.e., p-1 = kq
  - Let g be an element of order q, i.e., \( g \neq 1 \) and \( g^q = 1 \mod p \)
  - \( <g> = \{g^i \mid i = 0, 1, \ldots, q-1\} \subset \mathbb{Z}_p^* \) : a multiplicative subgroup of \( \mathbb{Z}_p^* \)
  - That is, for any \( y \in <g> \), there exists an integer \( x \in [0, q-1] \) such that \( y = g^x \mod p \)
Cyclic Group

- Example: $p = 13$
  - $Z_{13} = \{0, 1, 2, \ldots, 12\}$
  - $Z_{13}^* = \{1, 2, \ldots, 12\}; \mid Z_p^* \mid = 12$

- $\alpha = 6$ : a generator of $Z_{13}^*$

<table>
<thead>
<tr>
<th>i</th>
<th>0</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>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha^i \mod 13$</td>
<td>1</td>
<td>6</td>
<td>10</td>
<td>8</td>
<td>9</td>
<td>2</td>
<td>12</td>
<td>7</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>11</td>
</tr>
</tbody>
</table>

- Order of $x \in Z_{13}^*$ : a divisor of 12 = 2.2.3

<table>
<thead>
<tr>
<th>x</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>
</tr>
</thead>
<tbody>
<tr>
<td>Ord(x)</td>
<td>1</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td>4</td>
<td>12</td>
<td>12</td>
<td>4</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>2</td>
</tr>
</tbody>
</table>

- Exercise 4. Find the order of $x \in Z_{31}^*$
\( \mathbb{Z}_{13}^* \)

<table>
<thead>
<tr>
<th>( a^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>
<th>10</th>
<th>11</th>
<th>12</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>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>10</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>9</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>12</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>12</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>12</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>10</td>
<td>8</td>
<td>9</td>
<td>2</td>
<td>12</td>
<td>7</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>10</td>
<td>5</td>
<td>9</td>
<td>11</td>
<td>12</td>
<td>6</td>
<td>3</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>12</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>12</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>12</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>9</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>10</td>
<td>9</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>7</td>
<td>12</td>
<td>2</td>
<td>9</td>
<td>8</td>
<td>10</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
<td>12</td>
<td>1</td>
</tr>
</tbody>
</table>

\( \text{Ord}(a) \)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>12</th>
<th>3</th>
<th>6</th>
<th>4</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>12</td>
<td>1</td>
<td>4</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>1</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>1</td>
<td>4</td>
<td>12</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>4</td>
<td>12</td>
<td>1</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

\( a \) and \( b \) are elements of the multiplicative group \( \mathbb{Z}_{13}^* \).

The table shows the powers of \( a \) and the entries \( b \).

The \( \text{Ord}(a) \) denotes the order of each element in the group, which is the smallest positive integer \( n \) such that \( a^n = 1 \).
Homework #5

Solve the exercises appeared in this lecture.

1. Exercise 1 on finding prime numbers
2. Exercise 2 on Euclidean / Extended Euclidean algorithm
3. Exercise 3 on Chinese Remainder Theorem
4. Exercise 4 on Order in cyclic group