Basic Number Theory

• We are talking about integers!
• Divisor
  – We say that $b \neq 0$ divides $a$ if $a = mb$ for some $m$, denoted $b | a$. $b$ is a divisor of $a$.
  – If $a | 1$, then $a = 1$ or $-1$.
  – If $a | b$ and $b | a$, then $a = b$ or $-b$.
  – Any $b \neq 0$ divides $0$.
  – If $b | g$ and $b | h$, then $b | (mg + nh)$ for arbitrary integers $m$ and $n$. 
Basic Number Theory (Cont’d)

• Prime numbers
  – An integer $p > 1$ is a prime number if its only divisors are 1, $-1$, $p$, and $-p$.
  – Examples: 2, 3, 5, 7, 11, 13, 17, 19, 31,…

• Any integer $a > 1$ can be factored in a unique way as $a = p_1^{a_1}p_2^{a_2}...p_t^{a_t}$
  – where each $p_1 > p_2 > ... > p_t$ are prime numbers and where each $a_i > 0$.
  – Examples: $91 = 13 \cdot 7$, $11011 = 13 \cdot 827$.

Basic Number Theory (Cont’d)

• Another view of $a|b$:
  – Let $P$ be the set of all prime numbers
  – Represent $a$ as $a = \prod_{p \in P} p^{a_p}$, where $a_p \geq 0$.
  – Represent $b$ as $b = \prod_{p \in P} p^{b_p}$, where $b_p \geq 0$.
  – $a|b$ means that $a_i \mid b_i$. 
Basic Number Theory (Cont’d)

- Greatest common divisor: gcd\((a, b)\)
  - gcd\((a, b) = \max\{k \mid k \mid a \text{ and } k \mid b\}\)
  - Examples
    - gcd\((6, 15) = 3\).
    - gcd\((60, 24) = \gcd(60, -24) = 12\).
    - gcd\((a, 0) = a\).
  - gcd\((a, b)\) can be easily derived if we can factor \(a\) and \(b\).

- Relatively Prime Numbers
  - Integers \(a\) and \(b\) are relatively prime if gcd\((a, b) = 1\).
  - Example: 8 and 15 are relatively prime.

Modulo Operator

- Given any positive integer \(n\) and any integer \(a\), we have \(a = qn + r\), where \(0 \leq r < n\) and \(q = \lceil a / n \rceil\)
  - We write \(a = r \mod n\).
  - The remainder \(r\) is often referred to as a residue.
  - Example:
    - \(2 = 12 \mod 5\).

- Two integer \(a\) and \(b\) are said to be congruent modulo \(n\) if \(a \mod n = b \mod n\).
  - We write \(a \equiv b \mod n\)
  - Example:
    - \(7 \equiv 12 \mod 5\).
Modulo Operator (Cont’d)

- Properties of modulo operator
  - \( a \equiv b \mod n \) if \( n | (a - b) \)
  - \( (a \mod n) = (b \mod n) \) implies \( a \equiv b \mod n \).
  - \( a \equiv b \mod n \) implies \( b \equiv a \mod n \).
  - \( a \equiv b \mod n \) and \( b \equiv c \mod n \) imply \( a \equiv c \mod n \).

Modular Arithmetic

- Observation:
  - The \((\mod n)\) operator maps all integers into the set of integers \(\{0, 1, 2, \ldots, (n-1)\}\).
- Modular addition.
  - \( [(a \mod n) + (b \mod n)] \mod n = (a+b) \mod n \)
- Modular subtraction.
  - \( [(a \mod n) - (b \mod n)] \mod n = (a - b) \mod n \)
- Modular multiplication.
  - \( [(a \mod n) \cdot (b \mod n)] \mod n = (a \cdot b) \mod n \)
An Exercise (n=5)

- **Addition**
  
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</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>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Multiplication**
  
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</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>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Exponentiation**
  
  9² mod 5 = ____

Properties of Modular Arithmetic

- $\mathbb{Z}_n = \{0, 1, \ldots, (n-1)\}$
- Commutative laws
  - $(w + x) \mod n = (x + w) \mod n$
  - $(w \cdot x) \mod n = (x \cdot w) \mod n$
- Associative laws
  - $[(w + x) + y] \mod n = [w + (x + y)] \mod n$
  - $[(w \cdot x) \cdot y] \mod n = [w \cdot (x \cdot y)] \mod n$
- Distributive law
  - $[w \cdot (x + y)] \mod n = [(w \cdot x) + (w \cdot y)] \mod n$
- Identities
  - $(0 + w) \mod n = w \mod n$
  - $(1 \cdot w) \mod n = w \mod n$
- Additive inverse ($-w$)
  - For each $w \in \mathbb{Z}_n$, there exists a $z$ such that $w + z = 0 \mod n$. 
About Multiplicative Inverse

• Not always exist
  – Example: There doesn’t exist a $z$ such that $6 \equiv z \equiv 1 \mod 8$.

$$
\begin{array}{cccccc}
  Z_8 & 0 & 1 & 2 & 3 & 4 \\
  6 & 0 & 12 & 24 & 36 & 42 \\
\end{array}
$$

<table>
<thead>
<tr>
<th>Residues</th>
<th>0</th>
<th>6</th>
<th>2</th>
<th>0</th>
<th>6</th>
<th>4</th>
<th>2</th>
</tr>
</thead>
</table>

• An integer $a \in \mathbb{Z}_n$ has a multiplicative inverse if $\gcd(a, n) = 1$.
• In particular, if $n$ is a prime number, then all elements in $\mathbb{Z}_n$ have multiplicative inverse.

Fermat’s Theorem

• If $p$ is prime and $a$ is a positive integer not divisible by $p$, then $a^{p-1} \equiv 1 \mod p$.
  – Observation: \{a \mod p, 2a \mod p, \ldots, (p-1)a \mod p\} = \{1, 2, \ldots, (p-1)\}.
  – $a \equiv (p-1)a \equiv [(a \mod p) \equiv (2a \mod p) \equiv \ldots \equiv ((p-1)a \mod p)] \mod p$
  – $(p-1)! \equiv a^{p-1} \equiv (p-1)! \mod p$
  – Thus, $a^{p-1} \equiv 1 \mod p$. 

Totient Function

- Totient function \( \varphi(n) \): number of numbers less than \( n \) relatively prime to \( n \)
  - If \( n \) is prime, \( \varphi(n) = n - 1 \)
  - If \( n = p \cdot q \), and \( p, q \) are primes, \( \varphi(n) = (p-1)(q-1) \)

- Examples:
  - \( \varphi(7) = \)____
  - \( \varphi(21) = \)____

Euler’s Theorem

- For every \( a \) and \( n \) that are relatively prime, \( a^{\varphi(n)} \equiv 1 \mod n \).
  - Proof leaves as an exercise.

- Examples
  - \( a=3, n=10, \varphi(10)=\)____, \( 3^{\varphi(10)} \mod 10 = \)____
  - \( a=2, n=11, \varphi(11)=\)____, \( 2^{\varphi(11)} \mod 11 = \)____.
Modular Exponentiation

\[ x^y \mod n = x^{y \mod \varphi(n)} \mod n \]

• if \( y = 1 \mod \varphi(n) \) then \( x^y \mod n = x \mod n \)

• Example:
  \[ 2^{100} \mod 33 = \_\_\_\_ \]

Euclid’s Algorithm

• Observation
  \[ \gcd(a, b) = \gcd(b, a \mod b) \]

• Euclid \((d, f), d > f > 0\).
  1. \( X \leftarrow d; Y \leftarrow f \)
  2. If \( Y = 0 \) return \( X = \gcd(d, f) \)
  3. \( R = X \mod Y \)
  4. \( X \leftarrow Y \)
  5. \( Y \leftarrow R \)
  6. Goto 2
Extended Euclid Algorithm

- **Extended Euclid (d, f)**
  1. \((X1, X2, X3) \equiv (1,0,f); (Y1, Y2, Y3) \equiv (0,1,d)\)
  2. If \(Y3=0\) return \(X3=\text{gcd}(d, f)\); no inverse
  3. If \(Y3=1\) return \(Y3=\text{gcd}(d, f)\); \(Y2=d^{-1} \mod f\)
  4. \(Q=\lceil X3/Y3 \rceil\)
  5. \((T1, T2, T3) \equiv (X1 - QY1, X2 - QY2, X3 - QY3)\)
  6. \((X1, X2, X3) \equiv (Y1, Y2, Y3)\)
  7. \((Y1, Y2, Y3) \equiv (T1, T2, T3)\)
  8. Goto 2

- **Observation**
  - \(fX1 + dX2 = X3; fY1 + dY2 = Y3\)
  - If \(Y3 = 1\), then \(fY1 + dY2 = 1\)
  - \(Y2 = d^{-1} \mod f\)

---

The Power of An Integer Modulo \(n\)

- Consider the following expression
- \(a^m \equiv 1 \mod n\)
- If \(a\) and \(n\) are relatively prime, then there is at least one integer \(m\) that satisfies the above equation.
  - That is, the Euler’s totient function \(\phi(n)\).
- The least positive exponent \(m\) for which the above equation holds is referred to as:
  - The order of \(a \mod n\)
  - The exponent to which \(a\) belongs \(\mod n\)
  - The length of the period generated by \(a\).
Understanding The Order of $a$ (mod $n$)

- **Powers of Integers Modulo 19**

| $a$  | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ | $a^{12}$ | $a^{13}$ | $a^{14}$ | $a^{15}$ | $a^{16}$ | $a^{17}$ | $a^{18}$ |
|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| 1    | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1       | 1       | 1       | 1       | 1       | 1       | 1       | 1       | 1       | 1       |
| 2    | 4     | 8     | 16    | 13    | 7     | 14    | 9     | 18    | 17    | 15      | 11      | 3       | 6       | 12      | 5       | 10      | 1       |
| 4    | 16    | 7     | 9     | 17    | 11    | 6     | 5     | 1     | 4     | 16      | 7       | 9       | 17      | 11      | 6       | 5       | 1       |
| 7    | 11    | 1     | 7     | 11    | 1     | 7     | 11    | 1     | 7     | 11      | 1       | 7       | 11      | 1       |
| 8    | 7     | 18    | 11    | 12    | 1     | 8     | 7     | 18    | 11    | 12      | 1       | 8       | 7       | 18      | 11      | 12      | 1       |
| 9    | 5     | 7     | 6     | 16    | 11    | 4     | 17    | 1     | 9     | 5       | 7       | 6       | 16      | 11      | 4       | 17      | 1       |
| 18   | 1     | 18    | 1     | 18    | 1     | 18    | 1     | 18    | 1     | 18      | 1       | 18      | 1       | 18      | 1       | 18      | 1       |

Observations in The Previous Table

- All sequences end in 1.
- The length of a sequence divides $\phi(19) = 18$.
  - Lengths: 1, 2, 3, 6, 9, 18.
- Some of the sequences are of length 18.
  - The base integer $a$ generates (via powers) all nonzero integers modulo 19.
**Primitive Root**

- The highest possible order of $a \pmod{n}$ is $\varphi(n)$.
- Primitive root: If the order of $a \pmod{n}$ is $\varphi(n)$, then $a$ is referred to as a primitive root of $n$.
  - The powers of $a$: $a, a^2, \ldots, a^{p-1}$ are distinct (mod $n$) and are all relatively prime to $n$.
- For a prime number $p$, if $a$ is a primitive root of $p$, then $a, a^2, \ldots, a^{p-1}$ are all the distinct numbers mod $p$.

**Discrete Logarithm**

- Given a primitive root $a$ for a prime number $p$:
  - The expression $b \equiv a^i \pmod{p}$, $0 \leq i \leq (p-1)$, produces the integers from 1 to $(p-1)$.
  - The exponent $i$ is referred to as the index of $b$ for the base $a$ (mod $p$), denoted as $\text{ind}_{a,p}(b)$.
  - $\text{ind}_{a,p}(1)=0$, because $a^0 \pmod{p} = 1$.
  - $\text{ind}_{a,p}(a)=1$, because $a^1 \pmod{p} = a$.

- Example:
  - Integer 2 is a primitive root of prime number 19

<table>
<thead>
<tr>
<th>Number</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>Index</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>
<tr>
<td>Number</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>Index</td>
<td>17</td>
<td>12</td>
<td>15</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>4</td>
<td>10</td>
<td>9</td>
</tr>
</tbody>
</table>
Discrete Logarithm (Cont’d)

- Consider $x = a^\text{ind}_{a,p}(x) \mod p$, $y = a^\text{ind}_{a,p}(y) \mod p$, and $xy = a^\text{ind}_{a,p}(xy) \mod p$.
  - $a^\text{ind}_{a,p}(xy) \mod p = (a^\text{ind}_{a,p}(x) \mod p)(a^\text{ind}_{a,p}(y) \mod p)$
  - $a^\text{ind}_{a,p}(xy) \mod p = (a^\text{ind}_{a,p}(x)+\text{ind}_{a,p}(y)) \mod p$
  - By Euler’s theorem: $a^z \equiv a^q \mod n$ iff $z \equiv q \mod \phi(p)$.
  - $\text{ind}_{a,p}(xy) = \text{ind}_{a,p}(x) + \text{ind}_{a,p}(y) \mod \phi(p)$.
  - $\text{ind}_{a,p}(y^r) = [r \cdot \text{ind}_{a,p}(y)] \mod \phi(p)$.

- Discrete logarithm mod $p$: index mod $p$.

- Computing a discrete logarithm mod a large prime number $p$ is in general difficult
  - Used as the basis of some public key cryptosystems.