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** \( a = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t} \)
  - where each \( p_1 > p_2 > \ldots > p_t \) are prime numbers and where each \( a_i > 0 \).
  - Examples: \( 91 = 13 \times 7 \), \( 11011 = 13 \times 11^2 \times 7 \).

Basic Number Theory (Cont’d)

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

- Greatest common divisor: \( \gcd(a, b) \)
  - \( \gcd(a, b) = \max \{k \mid k|a \text{ and } k|b\} \)
  - 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 \( q = \lfloor a/n \rfloor \).
  - We write \( r = a \mod n \).
  - 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:
    - \( 7 = 12 \mod 5 \).
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, …, (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.
  – \([(a \mod n) \times (b \mod n)] \mod n = (a \times b) \mod n\)
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
9^{2^{10}} \mod 5 = _____

Properties of Modular Arithmetic

• $\mathbb{Z}_n = \{0, 1, \ldots, (n-1)\}$

• Commutative laws
  – $(w + x) \mod n = (x + w) \mod n$
  – $(w \times x) \mod n = (x \times w) \mod n$

• Associative laws
  – $[((w + x) + y) \mod n] = [(w + (x + y)) \mod n]$
  – $[((w \times x) \times y) \mod n] = [(w \times (x \times y)) \mod n]$

• Distributive law
  – $[w \times (x + y)] \mod n = [(w \times x) + (w \times y)] \mod n$

• Identities
  – $(0 + w) \mod n = w \mod n$
  – $(1 \times w) \mod n = w \mod n$

• 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 $6 \times z = 1 \mod 8$.

<table>
<thead>
<tr>
<th>$Z_8$</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>
</tr>
</thead>
<tbody>
<tr>
<td>$\times 6$</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>18</td>
<td>24</td>
<td>30</td>
<td>36</td>
<td>42</td>
</tr>
<tr>
<td>Residues</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</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)\}.
  – $a \times 2a \times \ldots \times (p-1)a \equiv [(a \mod p) \times (2a \mod p) \times \ldots \times ((p-1)a \mod p)] \mod p$
  – $(p-1)! \times a^{p-1} \equiv (p-1)! \mod p$
  – Thus, $a^{p-1} \equiv 1 \mod p$. 

Totient Function

- Totient function $\phi(n)$: number of integers less than $n$ and relatively prime to $n$
  - If $n$ is prime, $\phi(n)=n-1$
  - If $n=p\times q$, and $p$, $q$ are primes, $\phi(n)=(p-1)(q-1)$
- Examples:
  - $\phi(7) =$
  - $\phi(21) =$

Euler’s Theorem

- For every $a$ and $n$ that are relatively prime, $a^{\phi(n)} \equiv 1 \mod n$.
  - Proof leaves as an exercise.
- Examples
  - $a=3$, $n=10$, $\phi(10) =$, $3^{\phi(10)} \mod 10 =$
  - $a=2$, $n=11$, $\phi(11) =$, $2^{\phi(11)} \mod 11 =$
Modular Exponentiation

- $x^y \mod n = x^{y \mod \phi(n)} \mod n$
- if $y = 1 \mod \phi(n)$ then $x^y \mod n = x \mod n$
- Example:
  - $2^{100} \mod 33 = ____$

Euclid’s Algorithm

- Observation
  - $\gcd(a, b) = \gcd(b, a \mod b)$
- Eulid $(d, f), d > f > 0$. 
  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. \((X_1, X_2, X_3) \leftarrow (1,0,d); \(Y_1, Y_2, Y_3) \leftarrow (0,1,f)\)
  2. If \(Y_3=0\) return \(X_3=gcd\ (d, f)\); no inverse
  3. If \(Y_3=1\) return \(Y_3=gcd\ (d, f); Y_2=d^{-1} \mod f\)
  4. \(Q=[X_3/Y_3]\)
  5. \((T_1, T_2, T_3) \leftarrow (X_1 - QY_1, X_2 - QY_2, X_3 - QY_3)\)
  6. \((X_1, X_2, X_3) \leftarrow (Y_1, Y_2, Y_3)\)
  7. \((Y_1, Y_2, Y_3) \leftarrow (T_1, T_2, T_3)\)
  8. Goto 2

- Observation
  - \(dX_1 + fX_2 = X_3; fY_1 + dY_2 = Y_3\)
  - If \(Y_3 = 1\), then \(fY_1 + dY_2 = 1\)
  - \(Y_2 = d^{-1} \mod f\)

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 \(a \pmod{n}\)
  - The exponent to which \(a\) belongs \(\pmod{n}\)
  - The length of the period generated by \(a\).
Understanding The Order of $a \pmod{n}$

- **Powers of Integers Modulo 19**

<table>
<thead>
<tr>
<th></th>
<th>$a^1$</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>
<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>
<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>16</td>
<td>7</td>
<td>9</td>
<td>17</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td></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>1</td>
<td>1</td>
<td>1</td>
<td></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>
<td></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>
<td></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>
<td></td>
</tr>
</tbody>
</table>

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 \( \phi(n) \).
- Primitive root: If the order of \( a \pmod{n} \) is \( \phi(n) \), then \( a \) is referred to as a primitive root of \( n \).
  - The powers of \( a \): \( a, a^2, \ldots, a^{n-1} \) are distinct \( \pmod{n} \) 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 \( \pmod{p} \).

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 \( a \pmod{p} \), 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</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>
<th>18</th>
</tr>
</thead>
<tbody>
<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 \( xy = a^{\text{ind}_{a,p}(xy)} \mod p \),
  \[ a^{\text{ind}_{a,p}(x)} \mod p = (a^{\text{ind}_{a,p}(x)} \mod p)(a^{\text{ind}_{a,p}(y)} \mod p) \]
  \[ a^{\text{ind}_{a,p}(xy)} \mod p = (a^{\text{ind}_{a,p}(x)+\text{ind}_{a,p}(y)}) \mod p \]
  – By Euler’s theorem: \( a^z \equiv a^q \mod p \) 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.