**Congruences**

**Definition:** \( n \) is a positive integer, \( a, b \in \mathbb{Z} \)

\[ a \equiv b \pmod{n} \] means \( a = b + ny \) for some \( y \in \mathbb{Z} \)

Equivalently, \( n \mid (a - b) \)

**Fact:** for fixed \( n \), the binary relation “\( \cdot \equiv \cdot \pmod{n} \)” is an equivalence relation on the set \( \mathbb{Z} \)

**Fact:** Let \( a, a', b, b', n \in \mathbb{Z} \) with \( n > 0 \). If

then

\[ a \equiv a' \pmod{n} \quad \text{and} \quad b \equiv b' \pmod{n} \]

\[ a + b \equiv a' + b' \pmod{n} \quad \text{and} \quad a \cdot b \equiv a' \cdot b' \pmod{n} \]

**Proof:** Suppose \( a = a' + nx, b = b' + ny \)

\[ a + b = a' + b' + n(x + y) \]

\[ ab = (a' + nx)(b' + ny) = a'b' + n(a'y + b'x + nxy) \]
**Example:** Divisibility-by-3 rule

\[ x = 25614 \]

Add the digits: \[ 2 + 5 + 6 + 1 + 4 = 18 \] is divisible by 3

\[ \therefore x \text{ is divisible by 3} \]

Why does this work?

Suppose \( x = (a_{k-1} \cdots a_0)_{10} \), so \( x = \sum_{i=0}^{k-1} a_i 10^i \)

**Key observation:** \( 10 \equiv 1 \pmod{3} \)

So \( 10^i \equiv 1^i \equiv 1 \pmod{3} \)

So \( x \equiv \sum_i 10^ia_i \equiv \sum_i a_i \pmod{3} \)
Fact: Let \( a, n \in \mathbb{Z} \) with \( n > 0 \). Then there exists a unique integer \( z \) such that \( z \equiv a \pmod{n} \) and \( x \in \{0, \ldots, n-1\} \)

Proof: Follows from division: \( a = nq + z \), where \( 0 \leq z < n \)

Example: Find integer solutions to \( 3z + 4 \equiv 6 \pmod{7} \)

Subtract 4 from both sides: \( 3z \equiv 2 \pmod{7} \)

Since \( 5 \cdot 3 \equiv 15 \equiv 1 \pmod{7} \), we can multiply both sides by 5: \( z \equiv 3 \pmod{7} \)

\[ \therefore \text{z is a solution to } 3z + 4 \equiv 6 \pmod{7} \iff z \equiv 3 \pmod{7} \]

\[ \therefore \text{the set of solutions is } \{7y + 3 : y \in \mathbb{Z}\}: \]

\[ \ldots, -18, -11, -4, 3, 10, 17, 24, \ldots \]
Solving Linear Congruences

**Theorem:** Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$

(i) $az \equiv b \pmod{n}$ has a solution $z \in \mathbb{Z}$ $\iff$ $d \mid b$

\[
az \equiv b \pmod{n} \quad \text{for some } z \in \mathbb{Z}
\]
\[
\iff az = b + ny \quad \text{for some } z, y \in \mathbb{Z} \quad \text{(by def'n of congruence)}
\]
\[
\iff az - ny = b \quad \text{for some } z, y \in \mathbb{Z}
\]
\[
\iff d \mid b \quad \text{(by GCD theorem)}
\]

(ii) $az \equiv 0 \pmod{n}$ $\iff$ $z \equiv 0 \pmod{n/d}$

\[
n \mid az \iff n/d \mid (a/d)z
\]
\[
\iff n/d \mid z \quad \text{(because } \gcd(a/d, n/d) = 1)\]

(iii) $az \equiv az' \pmod{n}$ $\iff$ $z \equiv z' \pmod{n/d}$

\[
az \equiv az' \pmod{n} \iff a(z - z') \equiv 0 \pmod{n}
\]
\[
\iff z - z' \equiv 0 \pmod{n/d} \quad \text{(by part (ii))}
\]
**Example:** $n = 15$ and $a = 1, 2, 3, 4, 5, 6$

<table>
<thead>
<tr>
<th>$z$</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>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2z$</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>14</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>$3z$</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>$4z$</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>3</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>$5z$</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>$6z$</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>9</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>9</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>
A cancellation law: if \( \gcd(a, n) = 1 \) and \( az \equiv az' \pmod{n} \), then \( z \equiv z' \pmod{n} \).

Modular inverses: the congruence \( az \equiv 1 \pmod{n} \) has a sol’n \( z \iff \gcd(a, n) = 1 \)

if it has a sol’n a unique sol’n \( z \in \{0, \ldots, n - 1\} \)

Notation: \( z = a^{-1} \pmod{n} \)

Terminology: “multiplicative inverse of \( a \) modulo \( n \)”

Computing modular inverses:

- Assume \( 0 \leq a < n \) (replace \( a \) by \( a \mod n \) if not)
- \((d, s, t) \leftarrow \text{ExtEuclid}(n, a)\)
- \( d = \gcd(n, a) \) and \( ns + at = d \)
- \( d \neq 1 \Rightarrow \) no inverse
- \( d = 1 \Rightarrow \) inverse is \( t \mod n \)
Residue Classes

We know: for any fixed positive integer $n$, the binary relation “$\cdot \equiv \cdot \pmod{n}$” is an equivalence relation on the set $\mathbb{Z}$.

This relation partitions the set $\mathbb{Z}$ into equivalence classes — called residue classes mod $n$.

We denote the equivalence class containing the integer $a$ by $[a]_n$ — or $[a]$ when $n$ is clear from context.

$$z \in [a] \iff z \equiv a \pmod{n}$$

$$\iff z = a + ny \text{ for some } y \in \mathbb{Z}$$

and hence

$$[a] = a + n\mathbb{Z} := \{a + ny : y \in \mathbb{Z}\}$$
**Notation:** $\mathbb{Z}_n$ is the set of residue classes mod $n$

**Fact:** $\mathbb{Z}_n$ consists of the $n$ distinct residue classes $[0], [1], \ldots, [n - 1]$

We can “equip” $\mathbb{Z}_n$ with $+$ and $\cdot$ operators:

$[a] + [b] := [a + b]$

$[a] \cdot [b] := [a \cdot b]$

**Note:** def’n is unambiguous: if $[a] = [a']$ and $[b] = [b']$, then $[a + b] = [a' + b']$ and $[a \cdot b] = [a' \cdot b']$

**Note:**

$[a] + [b] = [c] \iff a + b \equiv c \pmod{n}$,

and

$[a] \cdot [b] = [c] \iff a \cdot b \equiv c \pmod{n}$,
Example: residue classes mod $n = 6$

\[
\begin{align*}
[0] &= \{\ldots, -12, -6, 0, 6, 12, \ldots \} \\
[1] &= \{\ldots, -11, -5, 1, 7, 13, \ldots \} \\
[2] &= \{\ldots, -10, -4, 2, 8, 14, \ldots \} \\
[3] &= \{\ldots, -9, -3, 3, 9, 15, \ldots \} \\
[4] &= \{\ldots, -8, -2, 4, 10, 16, \ldots \} \\
\end{align*}
\]

<table>
<thead>
<tr>
<th>$+$</th>
<th>[0]</th>
<th>[1]</th>
<th>[2]</th>
<th>[3]</th>
<th>[4]</th>
<th>[5]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
<tr>
<td>[3]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
</tr>
<tr>
<td>[4]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
</tr>
<tr>
<td>[5]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\cdot$</th>
<th>[0]</th>
<th>[1]</th>
<th>[2]</th>
<th>[3]</th>
<th>[4]</th>
<th>[5]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[0]</td>
<td>[2]</td>
<td>[4]</td>
<td>[0]</td>
<td>[2]</td>
</tr>
<tr>
<td>[3]</td>
<td>[3]</td>
<td>[0]</td>
<td>[3]</td>
<td>[0]</td>
<td>[3]</td>
<td>[0]</td>
</tr>
<tr>
<td>[4]</td>
<td>[4]</td>
<td>[0]</td>
<td>[4]</td>
<td>[2]</td>
<td>[0]</td>
<td>[4]</td>
</tr>
<tr>
<td>[5]</td>
<td>[5]</td>
<td>[0]</td>
<td>[5]</td>
<td>[4]</td>
<td>[3]</td>
<td>[2]</td>
</tr>
</tbody>
</table>

9
Algebraic properties of $\mathbb{Z}_n$

Addition and multiplication are commutative and associative.

Multiplication distributes over addition:
\[ \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma \text{ for all } \alpha, \beta, \gamma \in \mathbb{Z}_n \]

[0] is the additive identity.

[1] is the multiplicative identity.

For $\alpha \in \mathbb{Z}_n$, we call $\beta \in \mathbb{Z}_n$ a multiplicative inverse of $\alpha$ if $\alpha\beta = [1]$.

$\mathbb{Z}_n^*$ := the set of residue classes that have a multiplicative inverses.

**Facts:**
- $\mathbb{Z}_n^*$ closed under multiplication
- $\alpha = [a] \in \mathbb{Z}_n^* \iff \gcd(a, n) = 1$
- If $p$ is prime, then $\mathbb{Z}_p^* = \{\alpha \in \mathbb{Z}_p : \alpha \neq [0]\}$
Example: $n = 15$

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha^{-1}$</td>
<td>[1]</td>
<td>[8]</td>
<td>[4]</td>
<td>[13]</td>
<td>[2]</td>
<td>[11]</td>
<td>[7]</td>
<td>[14]</td>
</tr>
</tbody>
</table>

**Alternative approach to defining** $\mathbb{Z}_n$

Define it as the set of $n$ “symbols” $[0], [1], \ldots, [n−1]$

Addition and multiplication defined directly:

\[
[a] + [b] := [(a + b) \mod n]
\]
\[
[a] \cdot [b] := [(a \cdot b) \mod n]
\]
Fermat’s Little Theorem

Let $\alpha \in \mathbb{Z}_n^*$

Consider the sequence of powers of $\alpha$:

$$1 = \alpha^0, \alpha^1, \alpha^2, \ldots$$

Sequence must repeat: let $k$ be the smallest positive integer such that $\alpha^k = \alpha_i$ for some $i < k$

Claim: $\alpha^k = 1$

- If $\alpha^k = \alpha^i$ for $i > 0$, cancel $\alpha$, obtaining $\alpha^{k-1} = \alpha^{i-1}$, contradicting minimality of $k$

This value $k$ is called the (multiplicative) order of $\alpha$
Facts:

- Order of $\alpha \in \mathbb{Z}_n^*$ is the smallest positive integer $k$ such that $\alpha^k = 1$
- The elements $\alpha^0, \ldots, \alpha^{k-1}$ are distinct
- The sequence $\alpha^0, \alpha^1, \alpha^2, \ldots$ just repeats this pattern of $k$ distinct elements over and over

Example: $n = 7$

<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>order</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1^i \mod 7$</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>$2^i \mod 7$</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>$3^i \mod 7$</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>$4^i \mod 7$</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>$5^i \mod 7$</td>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>$6^i \mod 7$</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Fermat’s Little Theorem: Let \( p \) be a prime and let \( \alpha \in \mathbb{Z}_p^* \). Then \( \alpha^{p-1} = 1 \). In particular, the order of \( \alpha \) divides \( p - 1 \)

Proof: Consider the “multiplication by \( \alpha \)” map:

\[
\tau_\alpha : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^* \\
\beta \mapsto \alpha \beta.
\]

Easy to see that \( \tau_\alpha \) is a bijection

So, as \( \beta \) ranges over the set \( \mathbb{Z}_p^* \), so does \( \alpha \beta \)

Therefore

\[
\prod_{\beta \in \mathbb{Z}_p^*} \beta = \prod_{\beta \in \mathbb{Z}_p^*} (\alpha \beta) = \alpha^{p-1} \left( \prod_{\beta \in \mathbb{Z}_p^*} \beta \right)
\]

Now cancel \( \prod_{\beta \in \mathbb{Z}_p^*} \beta \) from both sides: \( 1 = \alpha^{p-1} \)
Equivalent formulations of the theorem

If $p$ is prime, then

$$\alpha^p = \alpha \text{ for all } \alpha \in \mathbb{Z}_p$$

If $p$ is prime, then

$$\alpha^p \equiv a \pmod{p} \text{ for all } \alpha \in \mathbb{Z}$$

Application: primality testing

To test if $n$ is prime, check if $\alpha^{n-1} = 1$ for several non-zero values $\alpha \in \mathbb{Z}_n$

If some check fails, then $n$ is definitely not prime

If all checks succeed, test is inconclusive

This test is not “fool proof”, but it can be strengthened a bit to make it so
Computing large powers in $\mathbb{Z}_n$

Given $\alpha \in \mathbb{Z}_n$ and $e \geq 0$, compute $\beta := \alpha^e \in \mathbb{Z}_n$

Naive algorithm:

\[
\beta \leftarrow [1]_n \in \mathbb{Z}_n \\
\text{repeat } e \text{ times} \\
\quad \beta \leftarrow \beta \cdot \alpha
\]

Takes $e$ multiplications in $\mathbb{Z}_n$

Repeated squaring: $O(\log e)$ multiplications in $\mathbb{Z}_n$

Warmup: suppose $e = 2^k$

\[
\beta \leftarrow \alpha \\
\text{repeat } k \text{ times} \\
\quad \beta \leftarrow \beta^2
\]
Repeated Squaring algorithm

Binary representation: $e = (b_1 \cdots b_k)_2$

Computation:

$$\beta \leftarrow [1]_n \in \mathbb{Z}_n$$

for $i$ in $[1 .. k]$ do

$$\beta \leftarrow \beta^2$$

if $b_i = 1$ then $\beta \leftarrow \beta \cdot \alpha$

Claim: after the $i$th loop iteration, we have $\beta = \alpha^{e_i}$, where $e_i = (b_1 \cdots b_i)_2$

Observe that $e_i = 2e_{i-1} + b_i$, and therefore,

$$\alpha^{e_i} = \alpha^{2e_{i-1} + b_i} = (\alpha^{e_{i-1}})^2 \cdot \alpha^{b_i}.$$
**Example:** $e = 37 = (100101)_2$

\[
\begin{align*}
\beta &\leftarrow [1] \quad \text{\# 0} \\
\beta &\leftarrow \beta^2, \beta \leftarrow \beta \cdot \alpha \quad \text{\# 1} \\
\beta &\leftarrow \beta^2 \quad \text{\# 10} \\
\beta &\leftarrow \beta^2 \quad \text{\# 100} \\
\beta &\leftarrow \beta^2, \beta \leftarrow \beta \cdot \alpha \quad \text{\# 1001} \\
\beta &\leftarrow \beta^2 \quad \text{\# 10010} \\
\beta &\leftarrow \beta^2, \beta \leftarrow \beta \cdot \alpha \quad \text{\# 100101}
\end{align*}
\]
Primitive roots

**Example:** \( n = 7 \)

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

**Fact:** for every prime \( p \), there exists an element in \( \mathbb{Z}^*_p \) of order \( p - 1 \)

- **Proof:** later

Such an element is called a **primitive root mod \( p \)**

- Example: \([3]\) and \([5]\) are primitive roots mod 7

If \( \alpha \in \mathbb{Z}^*_p \) is a primitive root, then every \( \beta \in \mathbb{Z}^*_p \) can be expressed as a power of \( \alpha \)