The Group of Units in the Integers mod n

- \( U_n \) consists of the elements of \( \mathbb{Z}_n \) which are relatively prime to \( n \); it is a group under multiplication mod \( n \).

- **Fermat’s Theorem** states that if \( a \) and \( p \) are integers, \( p \) is prime, and \( p \nmid a \), then

\[
a^{p-1} = 1 \pmod{p}.
\]

---

The group \( \mathbb{Z}_n \) consists of the elements \{0, 1, 2, \ldots, \( n-1 \)\} with addition mod \( n \) as the operation. You can also *multiply* elements of \( \mathbb{Z}_n \), but you do not obtain a group: The element 0 does not have a multiplicative inverse, for instance.

However, if you confine your attention to the units in \( \mathbb{Z}_n \) — the elements which have multiplicative inverses — you *do* get a group under multiplication mod \( n \). It is denoted \( U_n \), and is called the **group of units** in \( \mathbb{Z}_n \).

**Proposition.** Let \( U_n \) be the set of units in \( \mathbb{Z}_n \), \( n \geq 1 \). Then \( U_n \) is a group under multiplication mod \( n \).

**Proof.** To show that multiplication mod \( n \) is a binary operation on \( U_n \), I must show that the product of units is a unit.

Suppose \( a, b \in U_n \). Then \( a \) has a multiplicative inverse \( a^{-1} \) and \( b \) has a multiplicative inverse \( b^{-1} \). Now

\[
(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = b^{-1}b = 1,
\]

\[
(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1.
\]

Hence, \( b^{-1}a^{-1} \) is the multiplicative inverse of \( ab \), and \( ab \) is a unit. Therefore, multiplication mod \( n \) is a binary operation on \( U_n \).

(By the way, you may have seen the result \( (ab)^{-1} = b^{-1}a^{-1} \) when you studied linear algebra; it’s a standard identity for invertible matrices.)

I’ll take it for granted that multiplication mod \( n \) is associative.

The identity element for multiplication mod \( n \) is 1, and 1 is a unit in \( \mathbb{Z}_n \) (with multiplicative inverse 1).

Finally, every element of \( U_n \) has a multiplicative inverse, by definition.

Therefore, \( U_n \) is a group under multiplication mod \( n \). \( \square \)

Before I give some examples, recall that \( m \) is a unit in \( \mathbb{Z}_n \) if and only if \( m \) is relatively prime to \( n \).

---

**Example.** (The groups of units in \( \mathbb{Z}_{14} \)) \( U_{14} \) consists of the elements of \( \mathbb{Z}_{14} \) which are relatively prime to 14. Thus,

\[
U_{14} = \{1, 3, 5, 9, 11, 13\}.
\]

You multiply elements of \( U_{14} \) by multiplying as if they were integers, then reducing mod 14. For example,

\[
11 \cdot 13 = 143 = 3 \pmod{14}, \quad \text{so} \quad 11 \cdot 13 = 3 \pmod{\mathbb{Z}_{14}}.
\]
Here’s the multiplication table for $U_{14}$:

<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>11</th>
<th>13</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>11</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>9</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>3</td>
<td>7</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>4</td>
<td>3</td>
<td>8</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>6</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>9</td>
<td>4</td>
<td>10</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>3</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>9</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>6</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Notice that the table is symmetric about the main diagonal. Multiplication mod 14 is commutative, and $U_{14}$ is an abelian group.

Be sure to keep the operations straight: The operation in $\mathbb{Z}_{14}$ is addition mod 14, while the operation in $U_{14}$ is multiplication mod 14.

**Example. (The groups of units in $\mathbb{Z}_p$)** If $p$ is prime, then all the positive integers smaller than $p$ are relatively prime to $p$. Thus,

$$U_p = \{1, 2, 3, \ldots, p - 1\}.$$

For example, in $\mathbb{Z}_{11}$, the group of units is

$$U_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

The operation in $U_{11}$ is multiplication mod 11. For example, $8 \cdot 6 = 4$ in $U_{11}$. Here’s the multiplication table for $U_{11}$:

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

**Example. (The subgroup generated by an element)** The elements in $\{0, 1, 2, \ldots, 17\}$ which are relatively prime to 18 are the elements of $U_{18}$:

$$U_{18} = \{1, 5, 7, 11, 13, 17\}.$$

The operation is multiplication mod 18.
Since the operation is multiplication, the cyclic subgroup generated by 7 consists of all powers of 7:

\[ 7^0 = 1, \quad 7^1 = 7, \quad 7^2 = 13. \]

I can stop here, because \( 7^3 = 343 = 1 \mod 18 \). So

\[ \langle 7 \rangle = \{1, 7, 13\}. \]

On the other hand, consider \( \mathbb{Z}_{20} \), the cyclic group of order 20. In this group, the operation is addition \( \mod 20 \). Since the operation is addition, the subgroup generated by an element — say 8 — consists of all multiples of 8:

\[ 0 \cdot 8 = 0, \quad 1 \cdot 8 = 8, \quad 2 \cdot 8 = 16, \quad 3 \cdot 8 = 4, \quad 4 \cdot 8 = 12. \]

I can stop here, because \( 5 \cdot 8 = 0 \mod 20 \). So

\[ \langle 8 \rangle = \{0, 8, 16, 4, 12\}. \]

For the next result, I’ll need a special case of Lagrange’s theorem: The order of an element in a finite group divides the order of the group. I’ll prove Lagrange’s theorem when I discuss cosets.

As an example, in a group of order 10, an element may have order 1, 2, 5, or 10, but it may not have order 8.

**Corollary. (Fermat’s Theorem)** If \( a \) and \( p \) are integers, \( p \) is prime, and \( p \not| a \), then

\[ a^{p-1} = 1 \pmod{p}. \]

**Proof.** The elements

\[ 1, 2, 3, \ldots, p - 1 \]

of \( \mathbb{Z}_p \) are relatively prime to \( p \), so

\[ U_p = \{1, 2, 3, \ldots, p-1\}. \]

In particular, \( |U_p| = p - 1 \).

Now if \( p \not| a \), then

\[ a = b \pmod{p}, \quad \text{where} \quad b \in \{1, 2, 3, \ldots, p-1\}. \]

Lagrange’s theorem implies that the order of an element divides the order of the group. As a result, \( b^{p-1} = 1 \) in \( U_p \). Hence,

\[ a^{p-1} = b^{p-1} = 1 \pmod{p}. \]

**Example. (Using Fermat’s Theorem to reduce a power)** Compute \( 77^{2401} \pmod{97} \).

The idea is to use Fermat’s theorem to reduce the power to smaller numbers where you can do the computations directly.

97 is prime, and \( 97 \not| 77 \). By Fermat’s theorem,

\[ 77^{96} = 1 \pmod{97}. \]

So

\[ 77^{2401} = 77^{2400} \cdot 77 = (77^{96})^{25} \cdot 77 = 1 \cdot 77 = 77 \pmod{97}. \]