8 Modular Arithmetic

8.1 Modular Addition and Multiplication

In arithmetic modulo \( n \), when we add, subtract, or multiply two numbers, we take the answer mod \( n \). For example, if we want the product of two numbers modulo \( n \), then we multiply them normally and the answer is the remainder when the normal product is divided by \( n \). The value \( n \) is sometimes called the modulus.

Specifically, let \( \mathbb{Z}_n \) represent the set \{0, 1, \ldots, n - 1\} and define the two operations:

\[
\begin{align*}
    a +_n b &= (a + b) \mod n \\
    a \cdot_n b &= (a \times b) \mod n
\end{align*}
\]

Modular arithmetic obeys the usual rules/laws for the operations addition and multiplication. For example, \( a +_n b = b +_n a \) (commutative law) and \((a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c)\) (associative law).

Now, we can write down tables for modular arithmetic. For example, here are the tables for arithmetic modulo 4 and modulo 5.

<table>
<thead>
<tr>
<th>+4</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\cdot_4</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>\cdot_5</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

The table for addition is rather boring, and it changes in a rather obvious way if we change the modulus.

However, the table for multiplication is a bit more interesting. There is obviously a row with all zeroes. Consider the table for \( \cdot_5 \). Then in each of the other rows, every value is there and
there is no repeated value. This does not always happen; for example, look at the table for modulus 4. Indeed, if both \( x \) and the modulus are a multiple of \( m \), then every value in the row for \( x \) in the multiplication table will be a multiple of \( m \). So the only way it can happen that all values appear in the multiplication table in every nonzero row is that the modulus is a prime. And in that case, yes this happens, as we now prove:

**Theorem 8.1.** If \( p \) is a prime, and \( 1 \leq a \leq p - 1 \), then the values \( 0 \mod p, a \mod p, 2a \mod p, \ldots, (p - 1)a \mod p \) are all distinct.

**Proof.** Proof by contradiction. Suppose \( ia \mod p = ja \mod p \) with \( 0 \leq i < j \leq p - 1 \). Then \((ja - ia) \mod p = ja \mod p - ia \mod p = 0\), and so \( ja - ia = (j - i)a \) is a multiple of \( p \).

However, \( a \) is not a multiple of \( p \); so \( j - i \) is a multiple of \( p \). But that is impossible, because \( j - i > 0 \) and \( j - i < p \). We have a contradiction. \( \Diamond \)

Since there are \( p \) distinct values in the row, but only \( p \) possible values, this means that every value must appear exactly once in the row.

We can also define **modular subtraction** in the same way, provided we say what the mod operation does when the first argument is negative: \( c \mod d \) is the smallest nonnegative number \( r \) such that \( c = qd + r \) for some integer \( q \); for example, \(-1 \mod 4 = 3\).

### 8.2 Modular Inverses

An interesting question is whether one can define division. This is based on the concept of an inverse, which is actually the more important concept. We define:

**The inverse of** \( b \), written \( b^{-1} \), is a number \( y \) in \( \mathbb{Z}_n \) such that \( b \cdot_n y = 1 \).

The question is: does such a \( y \) exist? And if so, how to find it? Well, it certainly does exist in some cases.

**Example 8.1.**

For \( n = 7 \), it holds that \( 4^{-1} = 2 \) and \( 3^{-1} = 5 \).

But \( 0^{-1} \) never exists.

Nevertheless, it turns out that modulo a prime \( p \), all the remaining numbers have inverses. Actually, we already proved this when we showed in Theorem 8.1 that all values appear in a row of the multiplication table. In particular, we know that somewhere in the row for \( b \) there will be a 1; that is, there exists a \( y \) such that \( b \cdot_p y = 1 \).

And what about the case where the modulus is not a prime? For example, \( 7^{-1} = 13 \) when the modulus is 15.
Theorem 8.2 \(b^{-1}\) exists in \(\mathbb{Z}_n\) if and only if \(b\) and \(n\) are relatively prime.

Proof. There are two parts to prove. If \(b\) and \(n\) have a common factor say \(a\), then any multiple of \(b\) is divisible by \(a\) and indeed \(b \cdot y\) is a multiple of \(a\) for all \(y\), so the inverse does not exist.

If \(b\) is relatively prime to \(n\), then consider Euclid’s extended algorithm. Given \(n\) and \(b\), the algorithm behind Theorem 7.2 will produce integers \(x\) and \(y\) such that:

\[
n \times x + b \times y = 1.
\]

And so \(b \cdot y = 1\).  

And, by using the extension of Euclid’s algorithm, one actually has a quick algorithm for finding \(b^{-1}\). One of the exercises is to show that if an inverse exists, then it is unique.

For you to do!  

1. List all the values in \(\mathbb{Z}_{11}\) and their inverses.

8.3 Modular Equations

A related question is trying to solve modular equations. These arise in puzzles where it says that: there was a collection of coconuts and when we divided it into four piles there was one left over, and when we divided it into five piles, etc.

Theorem 8.3 Let \(a \in \mathbb{N}\), and let \(b\) and \(c\) be positive integers that are relatively prime. Then the solution to the equation

\[
c \times x \mod b = a
\]

is all integers of the form \(ib + a \cdot c^{-1}\) where \(i\) is an integer (which can be negative).

Proof. We claim that the solution is all integers \(x\) such that \(x \mod b = a \cdot c^{-1}\), where \(c^{-1}\) is calculated modulo \(b\). The proof of this is just to multiply both sides of the equation by \(c^{-1}\), which we know exists. From there the result follows.  

Example 8.2. Solve the equation \(3x \mod 10 = 4\).

Then \(3^{-1} = 7\) and \(4 \cdot_{10} 7 = 8\). So \(x \mod 10 = 8\).

This is then generalized in the Chinese Remainder Theorem. Here is just a special case:
Theorem 8.4 If $p$ and $q$ are primes, then the solution to the pair of congruences

$$x \equiv_p a \quad \text{and} \quad x \equiv_q b$$

is all integers $x$ such that

$$x \equiv_{pq} qa^{-1} + pb^{-1}$$

where $p^{-1}$ is the inverse of $p$ modulo $q$ and $q^{-1}$ is the inverse of $q$ modulo $p$.

We omit the proof.

Example 8.3. Determine all integers that have remainder 2 when divided by 5 and remainder 4 when divided by 7.

In the notation of the above theorem, $a = 2$, $p = 5$, $b = 4$, and $q = 7$. In $\mathbb{Z}_7$, $5^{-1} = 3$. In $\mathbb{Z}_5$, $7^{-1} = 2^{-1} = 3$. So the set of solutions has remainder $7 \cdot 2 \cdot 3 + 5 \cdot 4 \cdot 3 \equiv_{35} 32$. So the answer is $35x + 32$ for $x$ an integer.

Exercises

8.1. (a) Write out the addition and multiplication tables for $\mathbb{Z}_2$.
    (b) If we define 1 as true and 0 as false, explain which boolean connectives correspond to $+_2$ and $\cdot_2$.

8.2. Give the multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$.

8.3. Calculate $5^{-1}$ and $10^{-1}$ in $\mathbb{Z}_{17}$.

8.4. Prove that if $b$ has an inverse in $\mathbb{Z}_n$, then it is unique.

8.5. How many elements of $\mathbb{Z}_{91}$ have multiplicative inverses in $\mathbb{Z}_{91}$?

8.6. How many rows of the table for $\cdot_{12}$ contain all values?

8.7. Consider $\mathbb{Z}_{10}$.
    (a) List all elements of $\mathbb{Z}_{10}$.
    (b) What is the inverse of 3?
    (c) How many rows of the multiplication table contain every element?

8.8. (a) Consider the primes 5, 7, and 11 for $n$. For each integer from 1 through $n - 1$, calculate its inverse.
(b) A number is **self-inverse** if it is its own inverse. For example, 1 is always self-inverse. Based on the data from (a), state a conjecture about the number of self-inverses when \( n \) is a prime.

(c) Prove your conjecture.

8.9. Given \( a, b \in \mathbb{Z}_n \), we say that \( b \) is a **modular square-root** of \( a \) if \( b \cdot_n b = a \).

(a) List all the elements in \( \mathbb{Z}_{11} \), and for each element, list all their modular square-roots, if they have any.

(b) Prove that if \( n \) is prime then \( a \) has at most two square-roots.

(c) Give an example that shows that it is possible for a number to have more than 2 square-roots.

8.10. (a) Consider the primes 5, 7, and 11 for \( n \). For each \( a \) from 1 through \( n - 1 \), calculate \( a^2 \mod n \) (which is the same as \( a \cdot_n a \)).

(b) A number \( y \) is a **quadratic residue** if there is some \( a \) such that \( y = a^2 \mod n \). For example, 1 is always a quadratic residue (since it is \( 1^2 \mod n \)). Based on the data from (a), state a conjecture about the number of quadratic residues.

(c) Prove your conjecture.

8.11. Describe all solutions to the modular equation \( 7x \mod 8 = 3 \).

8.12. Find the smallest positive solution to the set of modular equations:

\[ x \mod 3 = 2, \quad x \mod 11 = 4, \quad x \mod 8 = 7. \]

---

**Solutions to Practice Exercises**

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