Modular Arithmetic

IT3122 Computer Security

2025.09.01

Intended Learning Outcomes

- Understand the concept of divisibility and the division algorithm.
- Understand how to use the Euclidean algorithm to find the greatest common divisor.
- Present an overview of the concepts of modular arithmetic.
- Explain the operation of the extended Euclidean algorithm.

Modulo Operation

Let $a, r, m \in \mathbb{Z}$ (where $\mathbb{Z}$ is a set of all integers) and $m > 0$. We write

$$a \equiv r \bmod m$$

if m divides $a - r$.

m is called the **modulus** and r is called the **remainder**.

Computation of the Remainder

It is always possible to write $a \in \mathbb{Z}$, such that

$$a = q \cdot m + r \text{ for } 0 \leq r < m$$

Since $a - r = q \cdot m$, i.e., m divides $a - r$, we can now write:
$a \equiv r \bmod m$. Note that $r \in \{0, 1, 2, \ldots, m-1\}$.

Example 1

Let $a = 42$ and $m = 9$. Then

$$42 = 4 \cdot 9 + 6$$

and therefore $42 \equiv 6 \bmod 9$.

The Remainder is Not Unique

- For every given modulus m and number a, there are (infinitely) many valid remainders.
- E.g.,
  - $12 \equiv 3 \bmod 9$, 3 is a valid remainder since $9|(12-3)$
  - $12 \equiv 21 \bmod 9$, 21 is a valid remainder since $9|(12-21)$
  - $12 \equiv -6 \bmod 9$, -6 is a valid remainder since $9|(12-(-6))$

Equivalence Class

The set of numbers:

$$\{\ldots, -24, -15, -6, 3, 12, 21, 30, \ldots\}$$

form an **equivalence class** for the modulus 9.

There is a total of nine equivalence classes for the modulus 9:

$$\{\ldots, -27, -18, -9, 0, 9, 18, 27, \ldots\}$$
$$\{\ldots, -26, -17, -8, 1, 10, 19, 28, \ldots\}$$
$$\vdots$$
$$\{\ldots, -19, -10, -1, 8, 17, 26, 35, \ldots\}$$

All Members of an Equivalence Class Behave Equivalently

1. $3^8 = 6561 \equiv 2 \bmod 7$
2. $3^8 = 3^4 \cdot 3^4 = 81 \cdot 81 \equiv 4 \cdot 4 = 16 \equiv 2 \bmod 7$

Which Remainder Do We Choose?

By agreement, we usually choose r such that:

$$0 \leq \mathrm{r} \leq \mathrm{m} - 1$$

However, mathematically it does not matter which member of an equivalent class we use.

Integer Rings

The **integer ring** $\mathbb{Z}_m$ consists of:

1. The set $\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$
2. Two operations "$+$" and "$\cdot$" for all $a,b \in \mathbb{Z}_m$ such that:
   1. $a + b \equiv c \bmod m \qquad (c \in \mathbb{Z}_m)$
   2. $a \cdot b \equiv d \bmod m \qquad (d \in \mathbb{Z}_m)$

Example 2

Let $m = 9$.

1. $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

2.

1. $6 + 8 = 14 \equiv 5 \bmod 9$
2. $6 \cdot 8 = 48 \equiv 3 \bmod 9$

Properties of Rings

- We can add and multiply any two numbers from the set and the result is always in the ring. A ring is said to be **closed**.
- Addition and multiplication are **associative**, i.e., $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for all $a, b, c \in \mathbb{Z}_m$.
- Addition is **commutative**, i.e., $a + b = b + a$, for all $a, b \in \mathbb{Z}_m$.
- There is the **neutral element 0 with respect to addition**, i.e., for every element $\mathrm{a} \in \mathbb{Z}_\mathrm{m}$ it holds that $a + 0 \equiv a \bmod m$.

Properties of Rings

- For any element a in the ring, there is always the negative element $-a$ such that $a + (-a) \equiv 0 \bmod m$, i.e., the **additive inverse** always exists.
- There is the **neutral element 1 with respect to multiplication**, i.e., for every element $\mathrm{a} \in \mathbb{Z}_{\mathrm{m}}$ it holds that $a \cdot 1 \equiv a \bmod m$.

Properties of Rings

- The **multiplicative inverse** exists only for some, but not for all, elements. Let $a \in \mathbb{Z}$. The inverse a^{-1} is defined such that
$$a \cdot a^{-1} \equiv 1 \bmod m$$
If an inverse exists for a, we can divide by this element since $b/a \equiv b \cdot a^{-1} \bmod m$.
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in \mathbb{Z}_m$, i.e., the **distributive law** holds.

Multiplicative Inverse

- An element $a \in \mathbb{Z}$ has a multiplicative inverse a^{-1} if and only if $\gcd(a, m) = 1$, where $\gcd$ is the **greatest common divisor**, i.e., the largest integer that divides both numbers a and m.
- If $\gcd(a, m) = 1$, then a and m are said to be **relatively prime** or **coprime**.

Euclidean Algorithm

Input: positive integers r_0 and r_1 with $r_0 > r_1$

Output: $\gcd(r_0, r_1)$

Initialization: $i = 1$

Algorithm:

```
1     DO
1.1       i = i + 1
1.2       r_i = r_{i-2} mod r_{i-1}
      WHILE r_i ≠ 0
2     RETURN
          gcd(r_0, r_1) = r_{i-1}
```

Example 3

Let $r_0 = 973$ and $r_1 = 301$. The $\gcd$ is then computed as

$973 = 3 \cdot 301 + 70$	$\gcd(973, 301) = \gcd(301, 70)$
$301 = 4 \cdot 70 + 21$	$\gcd(301, 70) = \gcd(70, 21)$
$70 = 3 \cdot 21 + 7$	$\gcd(70, 21) = \gcd(21, 7)$
$21 = 3 \cdot 7 + 0$	$\gcd(21, 7) = \gcd(7, 0) = 7$

Extended Euclidean Algorithm

In addition to computing the $\gcd$, the **extended Euclidean algorithm** (EEA) computes a linear combination of the form:

$$\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$$

where s and t are integer coefficients.

This equation is often referred to as a **Diophantine equation**.

Extended Euclidean Algorithm

Input: positive integers r_0 and r_1 with $r_0 > r_1$

Output: $\gcd(r_0, r_1)$,
as well as s and t such that $\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$.

Initialization:

$s_0 = 1 \qquad t_0 = 0$

$s_1 = 0 \qquad t_1 = 1$

$i = 1$

Algorithm:

1 DO

1.1 $i = i + 1$

1.2 $r_i = r_{i-2} \bmod r_{i-1}$

1.3 $q_{i-1} = (r_{i-2} - r_i)/r_{i-1}$

1.4 $s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$

1.5 $t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$

WHILE $r_i \neq 0$

2 RETURN

$\gcd(r_0, r_1) = r_{i-1}$

$s = s_{i-1}$

$t = t_{i-1}$

Example 4

Consider the extended Euclidean algorithm with $r_0 = 973$ and $r_1 = 301$.

i	$r_{i-2} = q_{i-1} \cdot r_{i-1} + r_i$	$r_i \;= [s_i]\; r_0 + [t_i]\; r_1$
2	$973 \;= 3 \cdot 301 + 70$	$70 = [1]\; r_0 + [-3]\; r_1$
3	$301 \;= 4 \cdot 70 + 21$	$21 = 301 - 4 \cdot 70$ $= r_1 - 4(1r_0 - 3\, r_1)$ $= [-4]\; r_0 + [13]\; r_1$
4	$70 \;= 3 \cdot 21 + 7$	$7 \;= 70 - 3 \cdot 21$ $= (1r_0 - 3r_1) - 3(-4r_0 + 13r_1)$ $= [13]\; r_0 + [-42]\; r_1$
	$21 \;= 3 \cdot 7 + 0$	

$\gcd(973,301) = 7$, $s = 13$ and $t = -42$.

Multiplicative Inverse

The inverse only exists if $\gcd(r_0, r_1) = 1$.

$$s \cdot r_0 + t \cdot r_1 = 1 = \gcd(r_0, r_1)$$
$$s \cdot 0 + t \cdot r_1 \equiv 1 \bmod r_0$$
$$r_1 \cdot t \equiv 1 \bmod r_0$$
$$t \equiv r_1^{-1} \bmod r_0$$

Example 5

Compute $12^{-1} \bmod 67$.

i	q_{i-1}	r_i	s_i	t_i
2	5	7	1	-5
3	1	5	-1	6
4	1	2	2	-11
5	2	1	-5	**28**

$$12^{-1} \equiv 28 \bmod 67$$

Reference

- C. Paar, J. Pelzl, and Tim Güneysu, "Modular Arithmetic and More Historical Ciphers," in *Understanding Cryptography*, Springer, 2nd Edition, 2024, pp. 15–22.