

Modular Arithmetic

Cunsheng Ding

HKUST, Hong Kong

February 14, 2017

Contents

- 1 The Floor and Ceiling Function
- 2 Greatest Common Divisor
- 3 Euclidean Algorithm
- 4 Modulo n Arithmetic
- 5 The multiplicative inverse modulo n

The Floor and Ceiling Function

Definition 1

The floor function $\lfloor x \rfloor$: The largest integer $\leq x$.

Example 2

$$\lfloor 3.99 \rfloor = 3. \quad \lfloor 5/2 \rfloor = 2. \quad \lfloor 3 \rfloor = 3.$$

Definition 3

The ceiling function $\lceil x \rceil$: The smallest integer $\geq x$.

Example 4

$$\lceil 3.99 \rceil = 4. \quad \lceil 5/2 \rceil = 3. \quad \lceil 3 \rceil = 3.$$

Quotient and Remainder

Theorem 5 (Division Algorithm)

Let $b \neq 0$ be an integer and let a be any integer. Then there are two unique integers q and $0 \leq r < |b|$ such that $a = qb + r$.

Proof.

The proof is constructive. Define $\varepsilon_b = 1$ if $b > 0$ and $\varepsilon_b = -1$ if $b < 0$. Let $q = \lfloor a/b\varepsilon_b \rfloor$ and $r = a - q\varepsilon_b b$. It is easily checked that $0 \leq r < |b|$ and $a = bq + r$. The proof of the uniqueness of q and r with $0 \leq r < |b|$ is left as an exercise. □

Definition 6

The q and r in the proof above are the **quotient** and **remainder** when a is divided by b . We write $r = a \bmod b$.

If $a \bmod b = 0$, b is called a **divisor** or **factor** of a . In this case, we say that a is divisible by b or b divides a .

Quotient and Remainder

Example 7

$73 \bmod 7 = 3$ and $-11 \bmod 7 = 3$.

Definition 8

A **prime** is a positive integer $n > 1$ with only two positive divisors 1 and n .

Definition 9

A **common divisor** of two integers a and b is a divisor of both a and b .

Example 10

60 and 24 have the positive common divisors 1, 2, 3, 4, 6, 12.

The Greatest Common Divisor

Definition 11

The greatest common divisor (GCD) of two integers a and b , denoted by $\gcd(a, b)$, is the largest among all the common divisors of a and b .

Example 12

$\gcd(60, 24) = 12$, as all the positive common divisors of 60 and 24 are 1, 2, 3, 4, 6, 12.

Proposition 13

$$\gcd(b, a) = \gcd(-b, a) = \gcd(b, -a) = \gcd(-b, -a) = \gcd(a, b).$$

Because of this proposition, we will consider only the case that $a \geq 0$ and $b \geq 0$ in the sequel.

The Greatest Common Divisor

Proposition 14

Let a and b be two integers such that $(a, b) \neq (0, 0)$. Then $\gcd(b, a)$ must exist.

Proof.

The total number of positive common divisors of a and b is at most $\max\{|a|, |b|\}$. □

Question 1

Is there any efficient algorithm for computing $\gcd(a, b)$ for any two positive integers a and b ?

Answer

Yes, the Euclidean algorithm.

Computing $\gcd(a, b)$ Recursively

Lemma 15

Let $b \neq 0$. Then $\gcd(a, b) = \gcd(b, a \bmod b)$.

Proof.

Note that $a = qb + r$, where $r = a \bmod b$ is the remainder.

By this equation, any common divisor of a and b must be a common divisor of b and r . Conversely, any any common divisor of b and r must be a common divisor of a and b . Hence a and b have the same set of common divisors as b and r . Hence, the two sets of integers have the same GCD. $\square$

Remark

A recursive application of this lemma gives an efficient algorithm for computing the $\gcd(a, b)$, which is called the **Euclidean algorithm**.

Euclidean Algorithm

Example: Find $\gcd(66, 35)$.

Algorithm: It works as follows and stops when the remainder becomes 0:

$$\begin{array}{lll} 66 & = & 1 \times 35 + 31 & \gcd(35, 31) \\ 35 & = & 1 \times 31 + 4 & \gcd(31, 4) \\ 31 & = & 7 \times 4 + 3 & \gcd(4, 3) \\ 4 & = & 1 \times 3 + 1 & \gcd(3, 1) \\ 3 & = & 3 \times 1 + 0 & \gcd(1, 0) \end{array}$$

Hence by the lemma in the previous page

$$\gcd(66, 35) = \gcd(35, 31) = \gcd(31, 4) = \gcd(4, 3) = \gcd(3, 1) = \gcd(1, 0) = 1.$$

Euclidean Algorithm

Pseudo code

- 1 $x \leftarrow a; y \leftarrow b$
- 2 If $y = 0$ return $\gcd(a, b) = x$
- 3 $r \leftarrow x \bmod y.$
- 4 $x \leftarrow y$
- 5 $y \leftarrow r$
- 6 goto step 2

Remarks

- No need to read and explain this code. The example in the previous slide is clear enough.
- The time complexity is $O(\log |b| \times [\log |b| + \log |a|]^2)$

The Least Common Multiple

Definition 16

The **least common multiple** of two integers a and b , denoted by $\text{lcm}(a, b)$, is the smallest positive integer that is divisible by both a and b .

Example 17

Let $a = 24 = 3 \times 2^3$ and $b = 15 = 3 \times 5$. Then $\text{lcm}(a, b) = 3 \times 5 \times 2^3 = 120$.

Question 2

*How do we compute the least common multiple $\text{lcm}(a, b)$ **efficiently**?*

Computing the Least Common Multiple

Lemma 18

Let a and b be integers. Then

$$\text{lcm}(a, b) = \frac{|ab|}{\text{gcd}(a, b)}.$$

An approach

Use the lemma above. As long as we have an efficient algorithm for computing $\text{gcd}(a, b)$, we have an efficient one for computing the $\text{lcm}(a, b)$.

Useful Results Regarding $\gcd(A, B)$

Proposition 19

Let a , m and n be positive integers. Then

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1.$$

Proposition 20

Let a , m and n be positive integers. Define $d = \gcd(m, n)$. Then

$$\gcd(a^m + 1, a^n - 1) = \begin{cases} 1, & \text{if } n/d \text{ is odd and } a \text{ is even,} \\ 2, & \text{if } n/d \text{ is odd and } a \text{ is odd,} \\ a^d + 1, & \text{if } n/d \text{ is even.} \end{cases}$$

The proofs of these two propositions are left as exercises for those who look for challenging problems.

Modulo n Arithmetic

Definition 21

Let $n > 1$ be an integer. We define

$$x \oplus_n y = (x + y) \bmod n, \quad [12 \oplus_5 7 = (12 + 7) \bmod 5 = 4]$$

$$x \ominus_n y = (x - y) \bmod n, \quad [12 \ominus_5 7 = (12 - 7) \bmod 5 = 0]$$

$$x \otimes_n y = (x \times y) \bmod n, \quad [12 \otimes_5 7 = (12 \times 7) \bmod 5 = 4]$$

where $+$, $-$ and $\times$ are the integer operations. The operations $\oplus_n$, $\ominus_n$ and $\otimes_n$ are called the modulo- n addition, modulo- n subtraction, and modulo- n multiplication. The integer n is called the **modulus**.

Properties of Modulo n Operations

Proposition 22

Let $n > 1$ be the modulus, $\mathbb{Z}_n = \{0, 1, \dots, (n-1)\}$.

- *Commutative laws:*

$$x \oplus_n y = y \oplus_n x, \quad x \otimes_n y = y \otimes_n x.$$

- *Associative laws:*

$$(x \oplus_n y) \oplus_n z = x \oplus_n (y \oplus_n z)$$

$$(x \otimes_n y) \otimes_n z = x \otimes_n (y \otimes_n z).$$

- *Distribution law:*

$$z \otimes_n (x \oplus_n y) = (z \otimes_n x) \oplus_n (z \otimes_n y).$$

Properties of Modulo n Operations

Proof of Proposition 22

- Commutative laws: $x \oplus_n y = y \oplus_n x$, $x \otimes_n y = y \otimes_n x$.

Proof: By definition and the commutative laws of integer addition and multiplication.

- Associative laws:

$$(x \oplus_n y) \oplus_n z = x \oplus_n (y \oplus_n z)$$

$$(x \otimes_n y) \otimes_n z = x \otimes_n (y \otimes_n z).$$

Proof: By definition and the associative laws of integer addition and multiplication.

- Distribution law: $z \otimes_n (x \oplus_n y) = (z \otimes_n x) \oplus_n (z \otimes_n y)$.

Proof: By definition and the distribution law of integer addition and multiplication.

The Multiplicative Inverse

Definition 23

Let $x \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$. If there is an integer $y \in \mathbb{Z}_n$ such that

$$x \otimes_n y =: (x \times y) \bmod n = 1.$$

The integer y is called a *multiplicative inverse* of x , usually denoted x^{-1} (it is unique if it exists).

Example 24

Let $n = 15$. Then 2 has the multiplicative inverse 8. But 3 does not have one.

Question 3

- Which elements of $\mathbb{Z}_n$ have a multiplicative inverse?
- If x has a multiplicative inverse, is it unique?
- If x has a multiplicative inverse, is there any efficient algorithm for computing the inverse?

$\gcd(a, b)$ as a Linear Combination of a and b

Lemma 25

There are two integers u and v such that $\gcd(a, b) = ua + vb$.

Proof.

Set $a_0 = a$ and $a_1 = b$. By the EA, we have

$$\begin{aligned}a_0 &= q_1 \times a_1 + a_2 \\a_1 &= q_2 \times a_2 + a_3 \\&\vdots \\a_{t-2} &= q_{t-1} \times a_{t-1} + a_t \\a_{t-1} &= q_t \times a_t + 0\end{aligned}$$

where $a_i \neq 0$ for $i \leq t$. Hence $\gcd(a, b) = a_t$. Reversing back, we can express a_t as a linear combination of a_0 and a_1 . □

$\gcd(a, b)$ as a Linear Combination of a and b

Example 26

Find integers u and v such that $\gcd(66, 35) = u66 + v35$.

Solution 27

The extended Euclidean algorithm works as follows:

$$\begin{array}{ll} 66 &= 1 \times 35 + 31 & 1 &= -9 \times 66 + 17 \times 35 \\ 35 &= 1 \times 31 + 4 & 1 &= 8 \times 35 - 9 \times 31 \\ 31 &= 7 \times 4 + 3 & 1 &= -1 \times 31 + 8 \times 4 \\ 4 &= 1 \times 3 + 1 & 1 &= 4 - 1 \times 3 \\ 3 &= 3 \times 1 + 0 \end{array}$$

Hence $u = -9$ and $v = 17$.

The Multiplicative Inverse

Proposition 28

If $a \in \mathbb{Z}_n$ has a multiplicative inverse, then it is unique.

Proof.

Let $b \in \mathbb{Z}_n$ and $c \in \mathbb{Z}_n$ be two multiplicative inverses of a . Then $a \otimes_n b = 1$ and $a \otimes_n c = 1$. By definition

$$a \otimes_n b \otimes_n c = (a \otimes_n b) \otimes_n c = 1 \otimes_n c = c.$$

On the other hand, by the associativity and commutativity,

$$a \otimes_n b \otimes_n c = b \otimes_n (a \otimes_n c) = b \otimes_n 1 = b.$$

Hence $b = c$. □

The Multiplicative Inverse

Theorem 29

Let $n > 1$ be an integer. Then any $a \in \mathbb{Z}_n$ has the multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.

Proof.

Suppose that $\gcd(a, n) = e \neq 1$. Then $n = en_1$ for some $n_1 < n$. Then $n_1 \otimes_n a = 0$. If there were an element $b \in \mathbb{Z}_n$ such that $a \otimes_n b = 1$, then we would have

$$n_1 \otimes_n (a \otimes_n b) = n_1 \otimes 1 = n_1 \bmod n = n_1$$

and

$$n_1 \otimes_n (a \otimes_n b) = (n_1 \otimes_n a) \otimes_n b = 0.$$

Hence, $n_1 = 0$, a contradiction.

By Lemma 25, there are two integers u and v such that $1 = ua + vn$. Hence $au \bmod n = 1$. Define $a' = u \bmod n$. Then $aa' \bmod n = 1$. □

Computing the Multiplicative Inverse

The algorithm

Let $a \in \mathbb{Z}_n$ with $\gcd(a, n) = 1$. Apply the Extended Euclidean Algorithm to a and n to compute the two integers u and v such that $1 = ua + vn$. Then $u \bmod n$ is the inverse of a modulo n .

Example 30

Compute the inverse $35^{-1} \bmod 66$.

Solution 31

In Solution 27, we got

$$1 = -9 \times 66 + 17 \times 35.$$

Hence, $35^{-1} \bmod 66 = (17) \bmod 66 = 17$.

Finite Fields $\mathbb{Z}_p$

Theorem 32

Let p be a prime. Then every nonzero element in $\mathbb{Z}_p$ has the multiplicative inverse modulo p .

Definition 33

Let p be a prime. Then the triple $(\mathbb{Z}_p, \oplus_p, \otimes_p)$ is called a *finite field* with p elements.

Remarks

We will introduce finite fields in genera later.