1st basic algebra

2022年4月2日 星期六 下午2:43

division $a = bq + r$ (division algorithm). ①
GCD (greatest common divisor) ②
Euclidean algorithm. ③
Bezout's identity ④
Corollary. ⑤.

Contents.

$\mathbb{Z}$: integers. $\{\dots -3, -2, -1, 0, 1, 2, 3 \dots\}$

addition: $+$ $a+b=c$

subtraction: $-$ $c-a=b$ $\exists b$, s.t. $a+b=c$

multiplication: $\times$ $a \times b = \underbrace{b+b+b\cdots}_{a}$

Definition: a factor of an integer n is a nonzero integer k s.t. $n=kl$ for some integer l.

In this case we say that k divides n, that k is a divisor of n and n is a multiple of k.

we write $k \mid n$. for this relationship.

If n is non-zero, any product formula $n = k l_1 \cdots l_r$ is a factorization of n. $8 = 2\times2\times2 = 8\times1 = -8\times(-1)$ (non-trivial / trivial)

a unit in $\mathbb{Z}$ is a divisor of 1. $n=1$ $\exists k$. s.t. $\exists l$. $kl=1$ $1\times1=1$ $(-1)\times(-1)=1$

hence is either $+1$ or -1.

The factorization $n=kl$ of $n \neq 0$ is called nontrivial if either k nor l is a unit.

An integer $p > 1$ is said to be **prime** if it has no nontrivial factorization $p = kl$.

$7 = 7 \times 1$

$\to x = 1$

proposition: division algorithm: If a and b are integers with $b \neq 0$, then there exist unique integers q and r s.t. $a = bq + r$ and $0 \leq r \leq |b|$.

$0 = b \cdot q + r \Rightarrow q = 0, r = 0.$

proof: Replace q by $-q$ (possible) $\Leftarrow$ we want $b > 0$. $\Leftarrow$ we may assume $b > 0$.

The integers $n = 0, 1, 2, \ldots$ with $bn \leq a$ are bound above by $|a|$.

and there is a largest such integer, say it is q. $bq \leq a$.

Set $r = a - bq \geq 0 \Rightarrow a = bq + r$.

If $r \geq b$, then $r - b \geq 0$ says that:

$$a = b(q+1) + (r-b) \geq b(q+1) \qquad (q+1) \cdot b \leq a$$

contradicts the maximality of q.

we conclude $r < b$. this proves existence.

For uniqueness, when $b > 0$, suppose $a = bq_1 + r_1 = bq_2 + r_2$. (subtraction)

$$bq_1 - bq_2 = r_2 - r_1$$

$$b(q_1 - q_2) = r_2 - r_1 \qquad |r_2 - r_1| < b$$

$$\Rightarrow q_1 - q_2 = 0. \quad q_1 = q_2, \; r_1 = r_2.$$

□

Definition: Let a and b be integers not both 0.

The **greatest common divisor** of a and b is the largest integer $d > 0$ s.t. $d \mid a$, and $d \mid b$.

$a = 21, b = 9$

$d = 3, \; 3 \mid a, \; 3 \mid b.$

existence. $1 \mid a \quad 1 \mid b$.

If b is nonzero then $|d| \leq |b|$ hence d must exist.

we write: $d = GCD(a, b)$.

If b is nonzero then $|a| \leq |b|$ hence d must exist.

we write: $d = GCD(a, b)$.

Euclidean algorithm: Let us suppose that $b \neq 0$.

The Euclidean algorithm consists of iterated application of the division algorithm to a and b until the remainder term r disappears.

$$\Rightarrow a = bq_1 + r_1 \qquad 0 \leq r_1 < b$$
$$b = r_1 q_2 + r_2 \qquad 0 \leq r_2 < r_1 \qquad b > r_1 > r_2 > \cdots \geq 0.$$
$$r_1 = r_2 q_3 + r_3 \qquad 0 \leq r_3 < r_2$$
$$\vdots$$
$$\Rightarrow r_{n-2} = r_{n-1} q_n + \boxed{r_n} \qquad 0 \leq r_n < r_{n-1} \quad (\text{with } r_n \neq 0).$$
$$r_{n-1} = r_n q_{n+1} + r_{n+1} \qquad (r_{n+1} = 0)$$

Example: $a = 13$. $b = 5$.

$13 = 5 \times 2 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + \boxed{1}$

$2 = 1 \times 2$

Proposition: Let a and b be integers with $b \neq 0$ and let $d = GCD(a, b)$. Then.

(a) the number r_n in the Euclidean algorithm is exactly d.

(b). any divisor d' of both a and b necessarily divides d.

Bezout's identity.

(c) there exist integers x and y such that. $ax + by = d$.

Example: $13 = 5 \times 2 + 3$ $\quad 3 = 13 - 5 \times 2$ ←

$5 = 3 \times 1 + 2$ $\quad 2 = 5 - 3 \times 1 = 5 - (13 - 5 \times 2) \times 1 = 5 \times 3 - 13 \times 1$ ←

$5 = 3\times1 + 2$ ⓪ $\quad 2 = 5 - 3\times1 = 5 - (13-5\times2)\times1 = 5\times3 - 13\times1$ ←

$3 = 2\times1 + 1$ ① $\quad 1 = 3 - 2\times1 = 13 - 5\times2 - (5\times3 - 13\times1)\cdot1 -$

$= 13\times2 - 5\times5.$ ←

$1 = 13\cdot x + 5y$ with $x = 2$, and $y = -5$. △

proof: Put $r_0 = b$ $r_{-1} = a$ so that:

$r_{k-2} = r_{k-1}q_k + r_k$ ✱ for $1 \le k \le n$. ⇐

Step 1: show that r_n is a divisor of both a and b.

From $r_{n-1} = r_n \cdot q_{n+1} \Rightarrow r_n \mid r_{n-1}$.

Let $k \le n$. assume r_n divides $r_{k-1}, \cdots r_{n-1}, r_n$ (inductively)

$r_n \mid r_{k-1} \Rightarrow r_{k-2} = r_n \cdot q_{n+1} \cdot q_k + r_n.$

$= r_n(q_{n+1}\cdot q_k + 1), \Rightarrow r_n \mid r_{k-2}.$

induction allows us to conclude that

r_n divides $\underset{a}{r_{-1}}, \underset{b}{r_0}, \cdots r_{n-1}$. r_n divides a and b.

Step 2: we prove that $ax + by = r_n$ for suitable x and y.

by induction on k for $k \le n$ that there exsit integers x and y.

with $ax + by = r_k$.

1) $n = 1$ assume
2) $n = k$ holds $\quad k+1 \Rightarrow$ holds.

$k = -1$ and $k = 0$. trivial ✓

if $k \ge 1$ is give. and the result is known for $k-2$ and $k-1$. ✓

$ax_2 + by_2 = r_{k-2}$

$ax_1 + by_1 = r_{k-1}$ for suitable integers x_2, y_2, x_1, y_1.

multply by q_k

$ax_1q_k + by_1q_k = r_{k-1}q_k.$

✱ $r_k = r_{k-2} - r_{k-1}\cdot q_k. = ax_2 + by_2 - ax_1q_k - by_1q_k$

$\star$ $r_k = r_{k-2} - r_{k-1} \cdot q_k = ax_2 + by_2 - ax_1 q_k - by_1 q_k$

$= a(x_2 - x_1 q_k) + b(y_2 - q_k y_1)$.

the induction is complete. $ax + by = r_n$ for suitable x and y.

Step3: step1 shows r_n divides a and b.

if $d' > 0$ divides both a and b. the $d' \mid r_n$ (step 2)

Thus $d' \leq r_n$. $\Rightarrow r_n$ is the greatest common divisor.

$\Rightarrow$ (a) $\Rightarrow$ (b) (c) from step 2. $\square$.

$r_n = d$

Corollary: within $\mathbb{Z}$. if c is nonzero. integer. that divides a product. mn and if $GCD(c, m) = 1$ then c divides n.

proof: $cx + my = 1$ (Bezout's identity).

$n \cdot cx + my \cdot n = n$. $c \mid mn$.

$c \cdot nx + mn \cdot y = n$

c divides both terms on the left side. $\Rightarrow$ $c \mid n$.

$c = 3$

$m = 7$

$n = 9$

$3 \mid 63$

$GCD(3, 7) = 1$

$\Rightarrow$ 3 divides 9.

$\square$

Corollary: within $\mathbb{Z}$, if a and b are nonzero integers with $GCD(a, b) = 1$, and if both of them divide the integer m, then ab divides m. ✓.

$a = 3b = 7$

$a \mid 42 \Rightarrow a \cdot b \mid 42$

$b \mid 42$ $21 \mid 42$ ✓

$\frac{m}{b}$ $\frac{m}{a}$ are integers

proof: $ax + by = 1$ (Bezout's identity)

$axm + bym = m$.

$ax m + by m = m.$

$a \cdot x \cdot b \cdot \frac{m}{b} + by \cdot a \cdot \frac{m}{a} = m \Rightarrow ab \cdot x \cdot \frac{m}{b} + ab \cdot y \cdot \frac{m}{y} = m$

ab divides each term on the left side. □

$ab \mid m.$