2nd basic algebra

2022年4月9日 星期六 下午1:23

Fundamental theorem of arithmetic ①
Chinese remainder theorem ②
Euler φ function. ✗ next class. ③

Contents.

Lemma. Within $\mathbb{Z}$, if p is a prime and p divides a product ab.
Euclid's lemma then p divides a or p divides b.

proof: suppose p does not divide a, since p is prime.

$$GCD(a,p)=1$$

Taking $m=a$, $n=b$ and $c=p$, from previous corollary.
p divides b. □

FToA. Each positive integer n can be written as a product of primes, $n=p_1p_2\cdots p_r$. with the integer 1 being written as an empty product. $15=3\times5$ (1) existense

This factorization is unique in the following sense:
$15=5\times3$
if $n=q_1q_2\cdots q_s$ is another such factorization, then $r=s$, and after some reordering of the factors. $q_j=p_j$ for $1\le j\le r$
(2) uniqueness.

proof: (1) induct on n. $n=1$ ✓

$k=1 \Rightarrow k=n-1$. ① n is prime $n=n$ ✓
② n is not prime $n=ab$. $a>1$. $b>1$.
$a\le n-1$
$b\le n-1$
→ a,b have factorizations into primes.

→ a, b have factorizations into primes.

$a \cdot b$

Putting them together yields a factorization into primes for $n = ab$.

(2). suppose $n = p_1 p_2 \cdots p_r = q_1 \cdots q_s$ with all factors prime. $r \le s$.

By induction. $r=0$ trivial.

$r=1$ following from the definition of prime. $n = p_1 = q_1$

$r-1$ ✓

Inductively from Euclid's lemma, we have $p_r \mid q_k$ for some k.

since q_k is prime. $p_r = q_k$.

Thus we cancel and obtain $p_1 \cdots p_{r-1} = q_1 q_2 \cdots \hat{q_k} \cdots q_s$.

omited factor.

By induction, the factors on the two sides here are the same, except for order.

$p_1 \cdots p_r = q_1 \cdots q_s$. □

prime factorization of n.

$n = p_1 p_2 \cdots p_r = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ with primes p_j distinct.

$\forall\, k_j \ge 0$.

we dropped $p_j^{k_j}$ if $k_j = 0$. this kind of decomposition is unique up to order.

Corollary: If $n = p_1^{k_1} \cdots p_r^{k_r}$ is a prime factorization of a positive integer n then the positive divisors d of are exactly all products $d = p_1^{l_1} \cdots p_r^{l_r}$ with $0 \le l_j \le k_j$. $\forall j$.

for all.

$24 = 2 \times 2 \times 2 \times 3 = 2^3 3^1$ $k_1 = 3$ $k_2 = 1$

$3 = 3^1 = 2^0 3^1$ → $p_1 = 2$ $p_2 = 3$ ⇒ $0 \le l_j \le k_j$. $\forall j$

$8 = 2 \times 2 \times 2 = 2^3 3^0$ $l_1 = 0$, $l_2 = 1$

$l_1 = 3$ $l_2 = 0$

4

6

proof: Certainly all such product divides n. $p_1^{k_1-l_1} p_2^{k_2-l_2} \cdots p_r^{k_r-l_r}$

If d divides n, $n = dx$ for some positive integer x.

$d = d_1 \cdots d_r$

$x = q_1 \cdots q_s$

$n = d_1 \cdots d_r q_1 \cdots q_s$ ⊛ $= p_1^{k_1} \cdots p_r^{k_r}$.

unique. only prime can occur in ⊛ are $p_1 \cdots p_r$.

the sum of the exponents. of p_j in ⊛ is k_j.

therefore. $d = p_1^{l_1} \cdots p_r^{l_r}$. $0 \le l_j \le k_j$ □

$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{h_1} \cdots q_s^{h_s} x_1^{z_1} \cdots x_t^{z_t}$

$n = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} x_1^{y_1} \cdots x_t^{y_t} g_1 \cdots$

GCD(m, n)

$p_1^{\min(d_1, k_1)} p_2^{\min(k_2, d_2)} \cdots p_r^{\min(k_r, d_r)}$

$x_1^{\min(0, y_1) = 0} = 1$

$24 = 2^3 \cdot 3^1$

$30 = 3 \cdot 2 \cdot 5 = 2^1 \cdot 3^1 \cdot 5^0$ ✓

$2^1 3^1 = 6 = GCD(24, 30)$

Corollary, If two positive integers a and b have expansions as products of power of r distinct prime given by

$a = p_1^{k_1} \cdots p_r^{k_r}$ and $b = p_1^{l_1} \cdots p_r^{l_r}$ then

$GCD(a, b) = p_1^{\min(k_1, l_1)} \cdots p_r^{\min(k_r, l_r)}$

proof: Let $d' = p_1^{\min(k_1, l_1)} \cdots p_r^{\min(k_r, l_r)}$ ⇐

d' is positive ✓

d' divides a and b. ✓

From previous corollary: the GCD of a and b is a number d of the form $p_1^{m_1} \cdots p_r^{m_r}$ with the property that $m_j \le k_j$ and

of the form $p_1^{m_1} \cdots p_r^{m_r}$ with the property that $m_j \le k_j$ and $m_j \le l_j$ for all j. $\Rightarrow$ $m_j \le \min(k_j, l_j)$ $\forall j$. $d \le d'$

m_j: d ; $\min(k_j, l_j)$: d'

since any positive divisor of a and b is $\le d$. $d' \le d$.

GCD

$d = d'$ □

Two nonzero integers a and b are said to be relatively prime if $GCD(a,b) = 1$.

a and b are relatively prime if and only if there is no prime p that divides both a and b.

Corollary: Let a and b be positive relatively prime integers.

Chinese Remainder Theorem. To each pair (r,s) of integers with $0 \le r < a$, $0 \le s < b$ corresponds a unique integer n, such that $0 \le n < ab$, a divides $n-r$, b divides $n-s$.

Moreover, every integer n with $0 \le n < ab$ arises from some such pair (r,s)

$a = 3$
$b = 5$

(r,s). $0 \le r < 3$, $0 \le s < 5$.

$(2,4)$

$3 \mid n-2$
$5 \mid n-4$
$n = 14$.

$0 \le n < 15$

$(1,2)$

$3 \mid n-1$
$5 \mid n-2$
$n = 7$

△

Remark.

If $GCD(a,b) = 1$, then the congruences $n \equiv r \bmod a$ and $n \equiv s \bmod b$ have one and only one simultaneous solution n with $0 \le n < ab$.

Proof. ① n. exists.

a, b are relatively prime. $\Rightarrow ax' - by' = 1$ x', y' integers.

multiplying $s-r$. $(ax'-by')(s-r) = s-r$

$$ax's - by's - ax'r + by'r = s-r$$

$$a(x's - x'r) - b(y's - y't) = s-r$$

$$ax - by = s-r \quad \text{for suitable integers } x, y.$$

put. $t = ax + r = by + s$

division algorithm : $t = abq + n$ $(0 \le n < ab)$ for suitable q.

$(t, ab) \Rightarrow (a, b)$

$n - r \overset{\circledast}{=} t - abq - r \overset{\triangle}{=} ax - abq = a(x - bq)$. is divisible by a.

similiarly $n-s$ is divisible by b.

② suppose n and n' both have the asserted properties.

a divides $n - n' = (n-r) - (n'-r)$.

b divides $n - n' = (n-s) - (n'-s)$

a, b are relatively prime.

From corollary 1.4. ab divides $n-n'$. $|n-n'| < ab$.

and the only integer $|N|$ with $|N| < ab$ that is divisible by ab is $N = 0$

$n - n' = 0 \Rightarrow n = n'$.

(r, s) $0 \le r < a$, $0 \le s < b$ $\Rightarrow$ ab pairs. $\xrightarrow[\text{one to one function.}]{}$ $0 \le n < ab$

□

23. April.

4 pm.

4 pm.