3rd basic algebra

2022年4月16日 星期六 下午1:09

Euler φ function
$GCD(a_1, \cdots, a_t)$
polynomials

① ② ③ Contents

If n is a positive integer.

we define $\varphi(n)$ to be the numbers of k with $0 \le k < n$ s.t. k and n are relatively prime.

φ: Euler φ function.

$n=5$ $1,2,3,4$ $\varphi(5)=4$ ①

$n=6$ $1,5$ $\varphi(6)=2$. ②

$GCD(0,5)=1,5$. $GCD(0,5)=5\neq 1$

$0=1*0$ $0=5*0$

$5=1*5$ $5=5*1$

Corollary: Let $N>1$ be an integer. $N=p_1^{k_1}\cdots p_r^{k_r}$ be a prime. factorization of N.

$$\varphi(N)=\prod_{j=1}^{r} p_j^{k_j-1}(p_j-1)$$

$N=1$ if we interpret the right side of the formula to be the empty product.

$5=5^1$ $\varphi(5)=5^{1-1}\cdot(5-1)=1\times 4=4$ ①

$P_1=5$ $k_1=1$

$6=2^1 3^1$ $\varphi(6)=2^{1-1}(2-1)\cdot 3^{1-1}(2)=2$ ②

$P_1=2$ $k_1=1$

$P_2=3$ $k_2=1$

Proof: For positive integers a and b. we check.

$\varphi(6)=\varphi(2)\cdot\varphi(3)$ $1\neq 2$ $\triangleright$ $\varphi(ab)=\varphi(a)\varphi(b)$ if $GCD(a,b)=1$. ⊛

$=$ $GCD(n,ab)=1$ $GCD(r,a)=1$ $GCD(s,b)=1$. $ax+by=1$

$\varphi(b)$ = GCD(n, ab)=1 From corollary (CRT). GCD(r, a)=1 GCD(s, b)=1. $ax+by=1$

We want to check:

mapping $(r, s) \to n$ has property

$3 \mid 7-r$ $5 \mid 7-s$. $r, s \to 7$ (7, 15)

$\forall$ GCD(r, a) = GCD(s, b) = 1 if and only if GCD(n, ab)=1

$\Leftarrow$

suppose n satisfies $0 \le n < ab$ and GCD(n, ab) > 1. $\Leftarrow$

Choose a prime p dividing both n and ab. $\Rightarrow$ p divides a or p divides b (corollary)

$p=1$

Assume. p divides a, (symmetry).

If (r, s) is the corresponding pair of n (CRT)

$a \mid n-r \xrightarrow[p \mid a]{} p \mid n-r \xrightarrow[p \mid n]{} p \mid r \Rightarrow GCD(r, a) > 1.$ $\Downarrow$

$\Rightarrow$

Conversely suppose that (r, s) s.t. GCD(r, a) = GCD(s, b) = 1. is false.

$0 \le r < a$, $0 \le s < b$

(symmetry): GCD(r, a) > 1. choose a prime p, $p \mid r$, $p \mid a$.

if n is the integer $0 \le n < ab$. corresponding to (r, s).

$a \mid n-r \xrightarrow[p \mid a]{} p \mid n-r \xrightarrow[p \mid r]{} p \mid n \Rightarrow GCD(n, ab) > 1.$???

$\to$

For a power p^k of a prime p with $k > 0$, the integers n with $0 \le n < p^k$ s.t. GCD(n, p^k) > 1. are the multiples of p $(0, p, 2p, \cdots p^{k-1}-p)$ p^{k-1}.

GCD(n, p^k) = 1 $\Rightarrow$ $p^k - p^{k-1} = p^{k-1}(p-1)$.

Δ $\varphi(p^k) = p^{k-1} \cdot (p-1)$ p is prime and $k \ge 1$

we induct on r.

$r=1$ $N = p_1^{k_1}$ $\varphi(N) = \varphi(p_1^{k_1}) = p_1^{k_1-1}(p_1-1)$ ✓

$\varphi(ab) = \varphi(a)\varphi(b)$

n-1 ✓.

$r-1$ ✓

r: $N = p_1^{k_1} \cdots p_r^{k_r}$ $\varphi(ab) = \varphi(a)\varphi(b)$

$$\varphi(N) = \varphi(p_1^{k_1} \cdots p_r^{k_{r-1}}) \cdot \varphi(p_r^{k_r}),$$

$$= \prod_{j=1}^{r-1} p_j^{k_j-1}(p_j-1) \cdot \varphi(p_r^{k_r})$$

$$= \prod_{j=1}^{r} p_j^{k_j-1}(p_j-1) \qquad \square$$

GCD (a, b)

GCD $(a_1, a_2 \cdots a_t) = d$. If $a_1, a_2, \cdots a_t$ are integers not all 0.

the greatest common divisor is the largest integer $d > 0$ that divides all $a_1 \cdots a_t$.

Corollary: Let $a_1, \cdots a_t$ be positive integers. Let d be their greatest common divisor. Then.

1). if for each j with $1 \le j \le t$. $a_j = p_1^{k_{1,j}} \cdots p_r^{k_{r,j}}$ is an expansion of a_j as a product of r distinct primes. $p_1 \cdots p_r$, it follows that

$$d = p_1^{\min_{1 \le j \le t} \{k_{1,j}\}} \cdots p_r^{\min_{1 \le j \le t} \{k_{r,j}\}}.$$

2) any divisor d' of all of $a_1, \cdots a_t$ necessarily divides d.

3). $d = \text{GCD}(\text{GCD}(a_1 \cdots a_{t-1}), a_t)$ if $t > 1$

4) there exist integers $x_1 \cdots x_t$. s.t. $a_1 x_1 + \cdots + a_t x_t = d$.

proof. 1). same way. apply r times rather than twice.

2) $d' = p_1^{m_1} \cdots p_r^{m_r}$.

$m_1 \le k_{1,j} \cdot \forall j$

$m_r \le k_{r,j} \ \forall j$

$\Rightarrow d' \mid d$.

d

$(3, 5) 7$ $\quad (d, 7) \to x_1 x_2 x_3$

$3x + 5y = 1$

$m_r \equiv k_r \; \forall j$

3). use 1).

4). use 3). and Bezout's identity.

$3x+5y=1$ $\quad x_1 x_2 x_3$

$3x_1+5x_2+7x_3=1.$

$(3x+5y)\times 8 + 7x - 1 = 1$ □

$24x+40y-7=1$

Polynomials.

$\mathbb{Q}$ rational numbers $\quad \mathbb{R}$ real numbers $\quad \mathbb{C}$ complex numbers

$f(x)$ continues.
$f(x_0) < 0$
$f(x_1) > 0$
$\exists x \in (x_0, x_1)$ s.t. $f(x) = 0.$

$\mathbb{F}$ denote any $\mathbb{Q}$. $\mathbb{R}$. $\mathbb{C}$ the members of $\mathbb{F}$ are called scalars

ordinary polynomials with coeffients in $\mathbb{F}$.

$P(x) = a_n x^n + \cdots a_1 x + a_0$ with $a_n \cdots a_1 \in \mathbb{F}$.

x: independent variable.

sequence. $(a_0, a_1, \cdots a_n, 0, 0, 0\cdots)$ of coefficients.

A polynomial in one indeterminate with coefficients in $\mathbb{F}$ is an infinite sequence of members of $\mathbb{F}$ s.t. all terms of the sequence are 0 from some point on. $\quad (a_0 + a_1 x + \cdots + a_n x^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \cdots)$.

indexing of the sequence is to begin with 0

Addition. $(a_0, \cdots a_n, 0, 0.) + (b_0, \cdots b_n, 0, 0.) = (a_0+b_0, \cdots a_n+b_n, 0, 0\cdots)$

subtraction $(a_0 \cdots) - (\cdots) = (a_0-b_0 \cdots a_n-b_n, 0, 0\cdots)$

scalar multiplication. $c(a_0, \cdots a_n, 0, 0\cdots) = (ca_0 \; ca_1 \cdots ca_n, 0, 0\cdots)$

coordinate-by-coordinate

multiplication: $(a_0, a_1 \cdots 0, 0, \cdots)(b_0, b_1, \cdots 0 0 \cdots) = (c_0, c_1, \cdots 0, 0).$

$$c_N = \sum_{k=0}^{N} a_k b_{N-k}.$$

$c_0 = a_0 b_0 \quad c_1 = a_0 b_1 + a_1 b_0 \quad c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$c_N = \sum_{k=0} a_k b_{N-k}$.

$c_1 = a_0 b_1 + a_1 b_0$ $\quad c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

associative law.
commutative law
distributive law.
are valid.

set of all polynomials in the indeterminate X.
is denoted by $F(X)$.

zero polynomial : the polynomial with all entries 0. is denoted by 0.

For all non-zero polynomials, the degree of P. is the largest index n s.t. $a_n \neq 0$.

$P = (a_0 \cdots a_n, 0 0 \cdots)$ $\quad \deg P$

constant polynomials $\rightarrow$ zero polynomial
$\searrow$ $\deg P = 0$.

$P \cdot Q$. nonzero polynomials.

$P = X$, $Q = -X$ $\quad P + Q = 0$.

$P + Q = 0$ or $\rightarrow \deg(P+Q) \leq \max(\deg P, \deg Q)$ $\Leftarrow$ equality holds. if $\deg P \neq \deg Q$.

$\deg(cP) = \deg P$.

$\deg(PQ) = \deg P + \deg Q$.

example: $\deg(x^8) = 8 = \deg(x^5) + \deg(x^3) = 5+3$.

$\rightarrow$ $PQ \neq 0$ unless $P = 0$ or $Q = 0$.

cancellation law.

$PR = QR$. with $R \neq 0 \Rightarrow P = Q$.

$PR - QR = 0 \Rightarrow (P-Q)R = 0$.

$R \neq 0$. $\quad P - Q = 0$