分圆多项式、算术函数

李 辉

Table of Contents

欧拉函数的计算

Euler's totient function

If the number m is prime, then

$$\phi(m) = m - 1.$$

Example

$$0 \quad 1 \quad 2 \quad 3 \quad 4$$

$$\phi(5) = 4.$$

If p is prime and $k \geq 1$ then

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

$$= p^k\left(1 - \frac{1}{p}\right).$$

Proof.

The multiples of p that are less than to p^k are $0, p, 2p, \cdots, (p^{k-1} - 1)p$, and there are p^{k-1} of them.

Therefore, the other $p^k - p^{k-1}$ numbers are all relatively prime to p^k.

Example

$$\begin{matrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{matrix}$$

$$9 - 3 = 6$$

$$\phi(3^2) = 3^2 - 3^1 = 6.$$

If two numbers m and n are coprime, then $\phi(mn) = \phi(m)\phi(n)$.

Example

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ 10 & 11 & 12 & 13 & 14 \end{matrix}$$

$$5 \times 3 - 3 - 5 + 1 = (5 - 1)(3 - 1) = 8.$$

$$\phi(3 \times 5) = \phi(3)\phi(5) = 2 \times 4 = 8.$$

The fundamental theorem of arithmetic states that if $n > 1$ there is a unique expression for n,

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < p_2 < \cdots < p_r$ are prime numbers and each $k_i \geq 1$.

Then

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

$$\begin{aligned}
\phi(n) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) \\
&= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

Example

$$\phi(225) = \phi(3^2 5^2)$$
$$= 225\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 225 \cdot \frac{2}{3} \cdot \frac{4}{5}$$
$$= 90.$$

Excise012

What is the last two digits of $27^{987654321}$?

Property established by Gauss.

$$\sum_{d|n} \phi\,(d) = n,$$

where the sum is over all positive divisors d of n.

Example

$$\phi(20) + \phi(10) + \phi(5) + \phi(4) + \phi(2) + \phi(1) = 20$$
$$8 + 4 + 4 + 2 + 1 + 1 = 20$$

$$\frac{1}{20}, \frac{2}{20}, \frac{3}{20}, \frac{4}{20}, \frac{5}{20}, \frac{6}{20}, \frac{7}{20}, \frac{8}{20}, \frac{9}{20}, \frac{10}{20},$$
$$\frac{11}{20}, \frac{12}{20}, \frac{13}{20}, \frac{14}{20}, \frac{15}{20}, \frac{16}{20}, \frac{17}{20}, \frac{18}{20}, \frac{19}{20}, \frac{20}{20}$$

Put them into lowest terms:

$$\frac{1}{20}, \frac{1}{10}, \frac{3}{20}, \frac{1}{5}, \frac{1}{4}, \frac{3}{10}, \frac{7}{20}, \frac{2}{5}, \frac{9}{20}, \frac{1}{2},$$
$$\frac{11}{20}, \frac{3}{5}, \frac{13}{20}, \frac{7}{10}, \frac{3}{4}, \frac{4}{5}, \frac{17}{20}, \frac{9}{10}, \frac{19}{20}, \frac{1}{1}$$

$$\phi(20) \rightarrow \left(\frac{1}{20}, \frac{3}{20}, \frac{7}{20}, \frac{9}{20}, \frac{11}{20}, \frac{13}{20}, \frac{17}{20}, \frac{19}{20}\right)$$

$$\phi(10) \rightarrow \left(\frac{1}{10}, \frac{3}{10}, \frac{7}{10}, \frac{9}{10}\right)$$

$$\phi(5) \rightarrow \left(\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}\right),\ \phi(4) \rightarrow \left(\frac{1}{4}, \frac{3}{4}\right)$$

$$\phi(2) \rightarrow \left(\frac{1}{2}\right),\ \phi(1) \rightarrow \left(\frac{1}{1}\right)$$

分圆多项式

Definition

The n-th **Cyclotomic Polynomials**, for any positive integer n, is the monic polynomial which is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any $k < n$.

Its roots are the n-th primitive roots of unity

$$e^{2i\pi\frac{k}{n}},$$

where k runs over the integers lower than n and coprime to n.

In other words, n-th **Cyclotomic Polynomials** is equal to

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - e^{2i\pi\frac{k}{n}}\right)$$

Example

Start with $x^6 - 1 = (x^3 - 1)(x^3 + 1)$.

Throw out $(x^3 - 1)$ due to $3|6$.

Then $x^3 + 1 = (x + 1)(x^2 - x + 1)$.

Throw out $(x + 1)$ due to $x + 1|x^2 - 1$ and $2|6$.

So, $\Phi_6(x) = x^2 - x + 1$.

Example

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_8(x) = x^4 + 1$$

Excise013

$$\Phi_9(x) = ?$$

Theorem

$$x^n - 1 = \prod_{d|n} \Phi_d\,(x),$$

which means that each n-th root of unity is a primitive d-th root of unity for a unique d dividing n.

Example

$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$$

Proof.

$$x^n - 1 = \prod_{1 \le k \le n} \left(x - e^{2i\pi\frac{k}{n}}\right)$$

If $gcd(\ ,n) = d$ then

$$x - e^{2i\pi\frac{k}{n}} = x - e^{2i\pi\frac{k'}{n'}},$$

where $k' = k/d, n' = n/d$, and $gcd(k', n') = 1$.

$x - e^{2i\pi\frac{k'}{n'}}$ is one of the factors of $\Phi_{n'}(x)$, for every n' dividing n, exactly once. So,

$$x^n - 1 = \prod_{n'|n} \Phi_{n'}(x)$$

Theorem

The degree of $\Phi_n(x)$, or in other words the number of n-th primitive roots of unity, is $\phi(n)$, where ϕ is Euler's totient function.

Theorem

$\Phi_n(x)$ has integer coefficients.

Proof. (By PMI) $\Phi_1(x) = x - 1$. Suppose the claim is true for $k < m$. Then

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

$$= \left(\prod_{\substack{d|m \\ d<m}} \Phi_d(x) \right) \cdot \Phi_m(x),$$

The first part is monic with integer coefficients. So, $\Phi_m(x)$ also has integer coefficients.

Theorem

For $n \geq 2$, $\Phi_n(x)$ is reciprocal. Namely,

$$\Phi_n\left(\frac{1}{x}\right) \cdot x^{\phi(n)} = \Phi_n(x).$$

Example

$$\Phi_6(x) = x^2 - x + 1$$

$$\left[\left(\frac{1}{x}\right)^2 - \left(\frac{1}{x}\right) + 1\right] \cdot x^2 = x^2 - x + 1$$

Proof.(By BMI) It is true for $n = 2$ because $\Phi_2(x) = x + 1$ and

$$\Phi_2\left(\frac{1}{x}\right) \cdot x^1 = \Phi_2(x).$$

Suppose it is true for $n < m$.

$$\left(\frac{1}{x}\right)^m - 1 = \prod_{d|m} \Phi_d\left(\frac{1}{x}\right)$$

$$= \left(\prod_{\substack{d|m \\ 1<d<m}} \Phi_d\left(\frac{1}{x}\right)\right) \cdot \Phi_m\left(\frac{1}{x}\right) \cdot \left(\frac{1}{x} - 1\right)$$

Multiply by $x^m = x^{\sum_{d|m}\phi(d)} = \prod_{d|m} x^{\phi(d)}$ on both sides.

$$1 - x^m = \left(\prod_{\substack{d|m \\ 1<d<m}} \Phi_d\left(\frac{1}{x}\right) x^{\phi(d)}\right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\phi(m)} \cdot \left(\frac{1}{x} - 1\right) x^1$$

$$= \left(\prod_{\substack{d|m \\ 1<d<m}} \Phi_d(x)\right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\phi(m)} (-\Phi_1(x))$$

$$\prod_{d|m} \Phi_d(x) = \Phi_1(x)\left(\prod_{\substack{d|m \\ 1<d<m}} \Phi_d(x)\right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\phi(m)}$$

Cancelling the common facts, we obtain:

$$\Phi_m(x) = \Phi_m\left(\frac{1}{x}\right) x^{\phi(m)}.$$

Example

If n is a prime number then

$$x^n - 1 = (x-1)(x^{n-1} + \cdots + x^2 + x + 1).$$

$$\Phi_n(x) = 1 + x + x^2 + \cdots + x^{n-1}.$$

If $n = 2p$ where p is an odd prime number then

$$x^{2p} - 1 = (x^{2p} - 1)(x+1) \cdot (x^{p-1} - \cdots + x^2 - x + 1).$$

$$\Phi_{2p}(x) = x^{p-1} - \cdots + x^2 - x + 1.$$

Excise014

$$\Phi_{24}(x) = ?$$

Lemma. Let $p \nmid n$ (p is a prime) and $m|n$ be a proper divisor of n ($m \neq n$). Then $\Phi_n(x)$ and $x^m - 1$ cannot have a common root mod p.

Proof. (By contradiction) Suppose a is a common root mod p. Then $a^m \equiv 1 \, mod \, p$ forces $gcd(a, p) = 1$. Next,

$$x^n - 1 = \Phi_n(x)\left(\prod_{\substack{d|n \\ d<n}} \Phi_d\,(x)\right)$$

$x^m - 1 = \prod_{d|m} \Phi_d\,(x)$ has all factors in the last product.

So $x^n - 1$ should have a double root at a, one for $\Phi_n(x)$, the other for $x^m - 1$ or $x^m - 1 = \prod_{d|m} \Phi_d\,(x)$.

Thus

$$x^n - 1 \equiv (x - a)^2 f(x) \, mod \, p$$

for some $f(x)$.

Then $na^{n-1} \equiv 0 \, mod \, p$.

However, $p \nmid n$ and $p \nmid a$, make a contradiction.

Theorem Let n be a positive integer. There are infinitely many primes congruent to 1 mod n.

Proof. (By contradiction) Suppose not, let $\{p_1, p_2, \cdots, p_N\}$ be all the primes congruent to 1 mod n.

Choose some large number l and let $M = \Phi_n(lnp_1 \cdots p_N)$. Since $\Phi_n(x)$ is monic, if l is large enough, M will be > 1 and so divisible by some prime p.

First, p cannot equal p_i for any i , since $\Phi_n(x)$ has constant term 1, and so p_i divides every term except the last of $\Phi_n(lnp_1 \cdots p_n) \Rightarrow$ it doesn't divide M.

For the same reason, $p \nmid n$. In fact, $gcd(p, a) = 1$ where $a = lnp_1 \cdots p_N$.

Now $\Phi_n(a) \equiv 0 \, mod \, p$ by definition, which means $a^n \equiv 1 \, mod \, p$.

By the lemma, we cannot have $a^m \equiv 1 \, mod \, p$ for any $m|n, m < n$.

So the order of $a \, (mod \, p)$ is exactly n, which means that $n|p-1$,

$$\Rightarrow p \equiv 1 \, mod \, n.$$

So, p is another prime $\equiv 1 \, mod \, n$.
Contradiction. ■

算术函数

Definition An **arithmetic function** is a function f: $\mathcal{N} \to \mathcal{C}$

Examples

Define $v_{p_i}(n)$ as the exponent of the highest power of the prime p_i that divides n.

That is to say, $a_i = v_{p_i}(n)$, otherwise it is zero. Then

$$n = \prod_i^k p_i^{a_i} = \prod_i^k p_i^{v_{p_i}(n)}.$$

In terms of the above definition, functions ω and Ω are defined by

$$\omega(n) = k,$$
$$\Omega(n) = a_1 + a_2 + \cdots + a_k.$$

Definition

An arithmetic function f is

additive: if $f(mn) = f(m) + f(n$ for all coprime natural numbers m and n

multiplicative: if $f(mn) = f(m)f(n$ for all coprime natural numbers m and n

not coprime ⇔ completely ⋯

Multiplicative functions

Definition

$\sigma_k(n)$ is the sum of the k-th powers of the positive divisors of n, including 1 and n, where k is a complex number. $\sigma_1(n)$, the sum of the (positive) divisors of n, is usually denoted by $\sigma(n)$.

Since a positive number to the zero power is one, $\sigma_0(n)$ is therefore the number of (positive) divisors of n, denoted by $d(n)$.

Definition **Möbius function**

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} = (-1)^{\Omega(n)} & \text{if } \omega(n) = \Omega(n) \\ 0 & \text{if } \omega(n) \neq \Omega(n). \end{cases}$$

This implies that $\mu(1) = 1$. (Because $\Omega(1) = \omega(1) = 0$.)

Definition

$$f(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } otherwise. \end{cases}$$

is completely multiplicative. It's sometimes called $\mathcal{I}$.

Example

- $f(n) = n^k$ for some fixed $k \in N$ is also completely multiplicative.
- $\phi(n)$ is multiplicative.

Additive functions

$\Omega(n)$, $\omega(n)$, and $\nu_p(n)$.

Example

$2^{\omega(n)}$ is multiplicative

Neither multiplicative nor additive

Definition

$\pi(n)$, the prime counting function, is the number of primes not exceeding n.

Definition **Perfect Number** A perfect number n is one for which $\sigma(n) = 2n$.

Example

6, 28, 496

An open conjecture: Every perfect number is even ?

Excise015

Please write a program to find a perfect number other than 6, 28, 496.

卷积***

$$c(n) = \sum_{ij=n} a\,(i)b(j) = \sum_{i|n} a\,(i)b\left(\frac{n}{i}\right),$$

This function $c(n)$ is called the Dirichlet **convolution** of a and b, and is denoted by $a * b$. Similar to:

$$(f * g)(t) \overset{\text{def}}{=} \int_{-\infty}^{\infty} f\,(\tau)\, g(t-\tau)\, d\tau$$
$$= \int_{-\infty}^{\infty} f\,(t-\tau)\, g(\tau)\, d\tau.$$

Example: $f * \mathcal{I} = \mathcal{I} * f = f$ for every f.

Theorem If f and g are multiplicative then $f * g$ is multiplicative.

Proof. Suppose m and n are coprime. Then any divisor of mn is of the form d_1, d_2 , where $d_1|m$ and $d_2|n$, uniquely. So we have

$$(f * g)(mn) = \sum_{d|mn} f\,(d) g(\frac{mn}{d})$$
$$= \sum_{d_1|m} \sum_{d_2|n} f\,(d_1 d_2) g\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right)$$

$$= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right)$$

$$= \left(\sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right)\right)$$

$$= (f * g)(m)(f * g)(n) \quad \blacksquare$$

Definition

Let $U(n) = 1$ for all n.

Then for any arithmetic function f, we have

$$(f * U)(n) = \sum_{d|n} f(d) U\left(\frac{n}{d}\right) = \sum_{d|n} f(d)$$

This is called $F(n)$.

Proof of "$\sigma_k(n)$ is multiplitive".

For the function $r_k(n) = n^k$, we have

$$(r_k * U)(n) = \sum_{d|n} d^k = \sigma_k(n),$$

which is therefore multiplicative. ■

Other important properties

convolution is **commutative**

$$f * g = g * f$$

convolution is **associative**

$$f * (g * h) = (f * g) * h$$

The proof is not provided.