Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 25, 2023

What we have seen last lecture

- Infinitude of primes
- Prime number theorem
- Gaps between primes

Today's topics

- Divisor set
- Multiplicative functions
- Euclid-Euler theorem

Mersenne Primes & even perfect numbers

Divisor set

Divisor set i

We will use $\mathscr{D}(n)$ to denote the set of divisors of n. The size of the set $\mathscr{D}(n)$ is denoted by $\sigma_0(n)$.

Theorem 7.1

positive

Let m, n be two integers. The multiplication gives a map

$$\Phi\colon\ \mathscr{D}(m) \times \mathscr{D}(n) \longrightarrow \mathscr{D}(mn).$$

Moreover, if m, n are coprime, Φ is bijective.

Proof. First, the multiplication does give a map Φ: if $a \in \mathscr{D}(m)$ and $b \in \mathscr{D}(n)$, then there are integers u, v such that $m = ua$ and $n = vb$. Hence, $mn = uvab$. Namely, $ab \in \mathscr{D}(mn)$.

Divisor set ii

Now, let's prove Φ is ***surjective***. Suppose $c \in \mathscr{D}(mn)$. Let

$$a = \gcd(m, c) \qquad \text{and} \qquad b = \gcd(n, c).$$

Clearly, $a \in \mathscr{D}(m), b \in \mathscr{D}(n)$. It remains to show $ab = c$.

Since m, n are coprime, for all prime p, at least one of $v_p(m), v_p(n)$ is 0. Let's say $v_p(m) = 0$. Then we have $v_p(c) \leqslant v_p(m) + v_p(n) = v_p(n)$. Therefore,

$$v_p(a) = \min\{v_p(m), v_p(c)\} = 0,$$
$$v_p(b) = \min\{v_p(n), v_p(c)\} = v_p(c).$$

In particular, $v_p(a) + v_p(b) = v_p(c)$. Similar for the case $v_p(n) = 0$. Hence, we have $v_p(a) + v_p(b) = v_p(c)$ for all prime p. This means $ab = c$.

Divisor set iii

$\Phi(a,b) = c \Rightarrow (a,b)$ is unique

wts: construct a, b from $c = ab$

Now, let's prove Φ is ***injective***. Indeed, we only need to show that for all $a \in \mathscr{D}(m), b \in \mathscr{D}(n)$, we have

$$a = \gcd(m, ab) \qquad \text{and} \qquad b = \gcd(n, ab).$$

Since m, n are coprime, for all prime p, at least one of $v_p(m), v_p(n)$ is 0. Let's say $v_p(m) = 0$. Then we have $v_p(a) \leqslant v_p(m) = 0$. Therefore, $a \mid m$

$$\min\{v_p(m), v_p(ab)\} = 0 = v_p(a),$$
$$\min\{v_p(n), v_p(ab)\} = \min\{v_p(n), v_p(b)\} = v_p(b).$$

$b \mid n$

Similar for the case $v_p(n) = 0$. Hence, $\min\{v_p(m), v_p(ab)\} = v_p(a)$, $\min\{v_p(n), v_p(ab)\} = v_p(b)$ for all prime p. This means $a = \gcd(m, ab)$ and $b = \gcd(n, ab)$. □

Multiplicative functions

Multiplicative functions

Definition 7.2

An ***arithmetic function*** is a complex-valued function defined on $\mathbb{Z}_+$. An arithmetic function $f(\cdot)$ is ***multiplicative***[5] if for every pair of coprime positive integers (a, b),

$$f(ab) = f(a)f(b).$$

Example 7.3

As a consequence of theorem 7.1, the function $\sigma_0(\cdot)$ is multiplicative.

$\sigma_0(m) \cdot \sigma_0(n) = \sigma_0(mn)$ (m,n) coprime

[5] if we remove the coprime requirement, the property is called ***completely multiplicative***

Formula of $\sigma_0(\cdot)$

$$\sigma_0(n) = \prod_{p \text{ is prime}} \sigma_0(p^{v_p(n)})$$

Corollary 7.4

Let n be a positive integer. We have

$$\sigma_0(n) = \prod_{p \text{ is prime}} (v_p(n) + 1).$$

Note that only for finitely many primes p, we have $v_p(n) > 0$. Hence the product is essentailly a finite product (since multiply with 1 does nothing).

Formula of $\sigma_0(\cdot)$

Corollary 7.4

Let n be a positive integer. We have

$$\sigma_0(n) = \prod_{p \text{ is prime}} (v_p(n) + 1).$$

Proof. By the multiplicativity of $\sigma_0(\cdot)$, we only need to prove for all prime p and natural number e that $\sigma_0(p^e) = e + 1$.

Indeed, from the unique prime factorization, it is easy to see that $\mathscr{D}(p^e) = \{1, p, \cdots, p^e\}$. Hence, its size is $e + 1$. □

General sigma functions

We generalize $\sigma_0(\cdot)$ to the following functions ($k \in \mathbb{Z}$):

$$\sigma_k(n) := \sum_{d \in \mathcal{D}(n)} d^k.$$

$\sigma_0(n) = \sum_{d \in \mathcal{D}(n)} 1 = \#\mathcal{D}(n)$

Theorem 7.5

Each $\sigma_k(\cdot)$ is a multiplicative function.

$\sigma_k(mn) = \sigma_k(m)\sigma_k(n)$ when m, n coprime.

Proof of the theorem

Proof. Let m, n be two coprime integers. Then we have

$$\sigma_k(mn) = \sum_{c \in \mathcal{D}(mn)} c^k \overset{\text{substitution}}{=} \sum_{(a,b) \in \mathcal{D}(m) \times \mathcal{D}(n)} (ab)^k = a^k b^k$$

$$= \left(\sum_{a \in \mathcal{D}(m)} a^k \right) \cdot \left(\sum_{b \in \mathcal{D}(n)} b^k \right) \quad \text{distributive law}$$

sum of prod = prod of sum

$$= \sigma_k(m)\sigma_k(n)$$

□

Proof of the theorem

Proof. Let m, n be two coprime integers. Then we have

$$\begin{aligned}\sigma_k(mn) &= \sum_{c \in \mathcal{D}(mn)} c^k \overset{\spadesuit}{=} \sum_{(a,b) \in \mathcal{D}(m) \times \mathcal{D}(n)} (ab)^k \\ &= \left(\sum_{a \in \mathcal{D}(m)} a^k \right) \cdot \left(\sum_{b \in \mathcal{D}(n)} b^k \right) \\ &= \sigma_k(m)\sigma_k(n)\end{aligned}$$

Let me explain what happened at ♠: we have changed the expression from the previous one using the ***bijection***

$$\Phi \colon \mathcal{D}(m) \times \mathcal{D}(n) \to \mathcal{D}(mn) \colon (a, b) \mapsto ab.$$

$c = ab$

We still obtain an equality since through such a bijection, the values of $(ab)^k$ and $\Phi(a, b)^k$ are the same. □

Formula of $\sigma_k(\cdot)$

$$\sigma_k(n) = \prod_{p \text{ prime}} \sigma_k(p^{v_p(n)})$$

Let's generalize corollary 7.4 to $\sigma_k(\cdot)$.

Theorem 7.6

Let n be a positive integer and $k \in \mathbb{Z}$. We have

$$\sigma_k(n) = \prod_{p \text{ is prime}} \frac{p^{k(v_p(n)+1)} - 1}{p^k - 1}.$$

Clearly, it suffices to show for all prime p and natural number e that

$$\sigma_k(p^e) = \frac{p^{k(e+1)} - 1}{p^k - 1}.$$

Proof

We first introduce a lemma.

Lemma 7.7

If x is a real number other than 1 and e is a natural number, then

$$\sum_{i=0}^{e} x^i := 1 + x + x^2 + \cdots + x^e = \frac{x^{e+1} - 1}{x - 1}.$$

Proof. Let $S = 1 + x + x^2 + \cdots + x^e$,

then $xS = x + x^2 + \cdots + x^e + x^{e+1}$.

Hence, $(x - 1)S = x^{e+1} - 1$.

Since $x \neq 1$, we can divide both sides by $x - 1$. □

Proof

Now we can prove the theorem 7.6.

Proof. Let p be a prime and e a natural number. Then since $\mathscr{D}(p^e) = \{1, p, \cdots, p^e\}$, we have

$$\sigma_k(p^e) = \sum_{i=0}^{e} (p^i)^k = \sum_{i=0}^{e} \underbrace{(p^k)}_{x}{}^i = \frac{p^{k(e+1)} - 1}{p^k - 1}.$$

Here, in the last step, we applied lemma 7.7 to $x = p^k$. □

Examples

Example 7.8

Compute $\sigma_3(12)$.

First note that $12 = 2^2 \cdot 3$. Hence, $\sigma_3(12) = \sigma_3(2^2)\sigma_3(3)$.

By theorem 7.6, we have

$$\sigma_3(2^2) = \frac{2^{3\cdot(2+1)} - 1}{2^3 - 1} = \frac{2^9 - 1}{2^3 - 1} = 73$$

$$\sigma_3(3) = \frac{3^{3\cdot(1+1)} - 1}{3^3 - 1} = \frac{3^6 - 1}{3^3 - 1} = 28$$

Hence, $\sigma_3(12) = 73 \cdot 28 = 2044$.

Examples

Example 7.9

Suppose $f(\cdot)$ is a multiplicative function. If we know

$$f(2) = 4, f(3) = 11, f(4) = 3.$$

Do we know enough to compute $f(6)$? $f(24)$?

$24 = 2^3 \cdot 3$

$f(6) = f(2) \cdot f(3) = 4 \cdot 11 = 44$

$f(24) = f(8) \cdot f(3)$ $\not=$ $f(4) f(6) = 3 \cdot 44$

unknown !

Not true !!

Not coprime

Euclid-Euler theorem

Mersenne primes

Recall that a ***Mersenne prime*** is a prime of the form $2^n - 1$.

Lemma 7.10

If $2^n - 1$ is a prime, then so is n.

Proof. Suppose, for the sake of contradiction, $n = ab$. Then

$$2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)(1 + 2^a + \cdots + (2^a)^{b-1}).$$

$x^b - 1 = (x-1)(1 + x + \cdots + x^{b-1})$

Here the last equality follows by applying lemma 7.7 to $x = 2^a$. □

Note that the converse is not true. For example, $2^{11} - 1 = 2047 = 23 \cdot 89$.

We will use M_p to denote the candidate of Mersenne prime $2^p - 1$.

Euclid-Euler theorem i

We are going to prove the following theorem.

Theorem 7.11 (Euclid-Euler)

An even natural number N is perfect if and only if it has the form $N_p := 2^{p-1}M_p$, where M_p is a Mersenne prime.

sum of all divisors

First, recall that a positive number N is ***perfect*** iff $\sigma_1(N) = 2N$.

Proof. ($\Longleftarrow$) Suppose M_p is a Mersenne prime. Then we have

$$\begin{aligned}
\sigma_1(N_p) &= \sigma_1(2^{p-1})\sigma_1(M_p) && \text{by the multiplicativity of } \sigma_1(\cdot) \\
&= \frac{2^p - 1}{2 - 1}(1 + M_p) && \text{by theorem 7.6} \\
&= (2^p - 1) \cdot 2^p && M_p := 2^p - 1 \\
&= M_p \cdot 2^{p-1} \cdot 2 = 2N_p.
\end{aligned}$$

↓ bec M_p is a prime

Euclid-Euler theorem ii

($\Longrightarrow$) Suppose N is an even perfect number. Let $p = v_2(N) + 1$. Note that $p \geqslant 2$ and hence $M_p \geqslant 3$. Let $q = \frac{N}{2^{p-1}}$. By the prime factorization of N, it is coprime to 2^{p-1}. Hence, ↑ odd factor of N

$$\sigma_1(N) = \sigma_1(2^{p-1})\sigma_1(q) = (2^p - 1)\sigma_1(q) = M_p\sigma_1(q).$$

On the other hand, by perfectness of N, we have

$$\sigma_1(N) = 2N = 2^p q = (1 + M_p)q.$$

Combine above equalities, we obtain

$$\sigma_1(q) = q + \frac{q}{M_p}.$$

Euclid-Euler theorem iii

Note that, since $M_p \geqslant 3$, $\frac{q}{M_p}$ is a proper divisor of q. If $q \neq M_p$, then we have at least three distinct divisors of q: 1, $\frac{q}{M_p}$, and q. By the definition of $\sigma_1(\cdot)$, we must have

$$\sigma_1(q) \gneqq 1 + \frac{q}{M_p} + q,$$

which causes a contradiction. Therefore, we must have $q = M_p$, and it has to be a prime since it has only two distinct divisors. □

After Class Work

Substitution in indexed sum and product i

In the lecture, we used the substitution

$$\sum_{(a,b)\in\mathscr{D}(m)\times\mathscr{D}(n)} (ab)^k = \sum_{c\in\mathscr{D}(mn)} c^k.$$

Let me explain further how substitution works in general.

In general, suppose you have an indexed sum $\sum_{a\in S} f(a)$ and you want to substitute in, say $a = g(b)$ $(b \in T)$. What you actually doing is:

1. change the expression from $\sum_{a\in S} f(a)$ to $\sum_{b\in T} f(g(b))$;
2. the new expression gives the same value as the old one since: 1, since $g : T \to S$ is bijective, the summations have the same number of terms; 2, for each pair of terms $(f(a), f(g(b)))$ corresponding through $a = g(b)$, we know that they give the same value.

Substitution in indexed sum and product ii

This should be fairly clear. However, how the substitution works may not be obvious in practice. One situation is that we may want to keep the index simple and save the use of letters.

Usually a letter appears both in the expression and the rule of a set's presentation $\{\text{expression} \mid \text{rule}\}$ is a ***local notation***, namely it will be released and free to serve in other usage outside this context. The same rule applies to indexed sum and product.

Substitution in indexed sum and product iii

Example 7.12

In the following equalities, the letter a in the left and right sides are NOT the same variable:

$$\sum_{a\in\mathscr{D}(n)} f(a) = \sum_{a\in\mathscr{D}(n)} f(\frac{n}{a}),$$

$$\sum_{a|n} f(a) = \sum_{a|n} f(\frac{n}{a}).$$

Exercise 7.1

Give a bijection from $\mathscr{D}(n)$ to itself and use this bijection to justify the equalities in above example.

Substitution in indexed sum and product iv

Another situation is when the index set consists of tuples and therefore the function $f(\cdot)$ is multi-variable. This usually comes with the previous issue.

Exercise 7.2

Give bijections between the sets $\left\{(a,b) \in \mathbb{Z}_+^2 \,\middle|\, a \mid n, b \mid a\right\}$, $\left\{(a,b) \in \mathbb{Z}_+^2 \,\middle|\, a \mid n, b \mid \frac{n}{a}\right\}$, and $\left\{(a,b,c) \in \mathbb{Z}_+^3 \,\middle|\, abc = n\right\}$. Then use them to justify the substitutions:

$$\sum_{a|n,b|a} f(b, \frac{a}{b}, \frac{n}{a}) = \sum_{abc=n} f(a,b,c) = \sum_{a|n,b|\frac{n}{a}} f(a,b,\frac{n}{ab}).$$