XM452 Lecture Notes 2

Erdaifu Luo

15 March 2023

§6 Relatively Prime Integers

§6.1 Relatively Prime

We say that integers a and b are **relatively prime** if $(a, b) = 1$.

Corollary 6.1

If $(a, b) = 1$, there are integers m, n sich that $ma + mb = 1$.

A set of nonzero integers $a_i, \ldots, a_n$ are **pairwise relatively prime** if for all i and j $(i \neq j)$, $(a_i, \ldots, a_j) = 1$.

Theorem 6.2

If $(a, b) = 1$ and $a \mid (bc)$, then $a \mid c$.

Proof. Since $(a, b) = 1$, there are integers m, n such that $ma + nb = 1$. Thus

$$m \cdot ac + n \cdot bc = c.$$

Since $a \mid a$ and $a \mid bc$,

$$a \mid (mab + nbc).$$

Thus.

$$a \mid c.$$

□

§6.2 Relatively Prime Triples

Theorem 6.3

If $(a, b, c) = 1$, then $(a, bc) = (a, b) \cdot (a, c)$. In particular, if $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

Proof. Let d $= (a, bc)$, $d_1 = (a, b)$, and $d_2 = (a, c)$. Show $d = d_1 \cdot d_2$. There are integers r, s, t, u such that

$$d_1 = ar + bs \text{ and } d_2 = at + cu.$$

So,

$$\begin{aligned} d_1 d_2 &= (ar + bs) \cdot (at + cu) \\ &= a(art + rcu + bst) + bc(su). \end{aligned}$$

Now, $d \mid a$ and $d \mid bc$, so $d \mid d_1 d_2$. Thus, $d \leq d_1 d_2$.

Now show that $d_1 d_2 \leq d$. We prove $(d_1, d_2) = 1$. Let $(d_1, d_2) = e \geq 1$. Thus,

$$e \mid d_1 \text{ and } e \mid d_2.$$

So,

$$e \mid a, e \mid b, \text{ and } e \mid c.$$

However, if $e \geq 1$, this contradicts $(a, b, c) = 1$, So, $(d_1, d_2) = 1$.

Since $d_1 \mid a$ and $d_1 \mid b$, $d_1 \mid bc$ and $d_1 \mid d$. Similarily, $d_2 \mid d$.

But $(d_1, d_2) = 1$m so $d_2 \mid \frac{d}{d_1}$.

Thus, $d_1 d_2 \mid d$ and so $d_1 d_2 \leq d \leq d_1 d_2$.

Therefore □

§7 The Fundamental Theorem of Arithmetic

Theorem 7.1

Let n‘1 be an integer. Then one can write

$$n = p_1 \dots p_n,$$

where each p_i is prime. This factorization is unique in the sense that if

$$n = p_1 \dots p_r = q_1 \dots q_s,$$

with $p_j (1 \leq j \leq r)$ and $q_k (1 \leq k \leq s)$ prime, then

$$r = s,$$

and the two factorizations are the same (except for the order of the factors).

Proof. By contradiction, let N be the smallest integer such that the uniqueness claim fails. So the theorem holds for 1, 2, ..., $N - 1$.

The theorem is true for primes, so N must be composite. Let

$$N = p_1 \dots p_r = q_1 \dots q_s.$$

Since ordering is unimportant, assume

$$\begin{aligned} p_r &\geq p_j \quad 1 \leq j \leq r - 1 \\ q_s &\geq q_k \quad 1 \leq k \leq s - 1 \end{aligned}$$

First show $p_r = q_s$. If $p_r \neq q_s$, assume $p_r > q_s$. Then, $p_r \leq q_j$ for $1 \leq j \leq s$. So for all q_j,

$$p_r \nmid q_j.$$

But $(p_r, q_s) = 1$ and $p_r \mid (q_1 \dots q_s)$, so by the previous theorem,

$$p_r \mid (q_1 \dots q_{s-1}).$$

But since $(p_r, q_{s-1}) = 1$,

$$p_r \mid (q_1 \dots q_{s-2}).$$

Continuing, $p_r \mid q_1$, but this contradicts $p_r q_1$. So, $p_r \le q_s$. By a parallel argument, $q_s \le p_r$, so $p_r = q_s$.

Let $M = p_1 \dots p_{r-1} = q_1 \dots q_{s-1}$. Then,

$$M \cdot p_r = N = M \cdot q_s.$$

Since $M < N$, $p_1 \dots q_{r-1}$ and $q_1 \dots q_{s-1}$ are the same factorizations of M. Thus, they re the same factorizations of N, which contradicts our assumption. $\square$

Theorem 7.2

Suppose $(a, b) = 1$, and $a \cdot b = c^n$, $a, b, c > 0$. Then for some integer d, e,

$$a = d^n, b = e^n.$$

Proof. If $a = 1$, let $d = 1$. Then $e = c$. Similarily for $b = 1$, so let's assume $a, b > 1$. Since $(a, b) = 1$, their prime factorizations are distinct. So let

$$a = p_1^{a_1} \dots p_r^{a_r} \text{ and } b = p_{r+1}^{a_{r+1}} \dots p_{r+s}^{a_{r+s}}.$$

Say $c = q_1^{b_1} \dots q_k^{b_k}$ is a prime factorization, then

$$p_1^{a_1} \dots p_{r+s}^{a_{r+s}} = q_1^{b_1} \dots q_k^{b_k}.$$

So $r + s = k$ and the q_j's are the same as the p_j's except for the order. Therefore, their corresponding exponents are the same.

Renumber the q_j's so that $q_j = p_j$ and $1 \le j \le r + s$. Thus,

$$a_j = nb_j.$$

So then,

$$a = p_1^{nb_1} \dots p_r^{nb_r} \text{ and } b = p_{r+1}^{nb_{r+1}} \dots p_{r+s}^{nb_{r+s}}.$$

Let

$$d = p_1^{b_1} \dots p_r^{b_r} \text{ and } e = p_{r+1}^{b_{r+1}} \dots p_{r+s}^{b_{r+s}}.$$

Clearly,

$$a = d^n \text{ and } b = c^n.$$

$\square$

§8 Consequences of Unique Factorization

§8.1 Irrational Numbers

Theorem 8.1

Suppose $a, n > 0$ are integers, and $\sqrt[n]{a}$ is rational. Then $\sqrt[n]{a}$ is an integer.

Proof. Suppose $\sqrt[n]{a} = \frac{r}{s}$ with $r, s > 0$ and $(r, s) = 1$. We want to show that $s = 1$.

If $s \neq 1$, then $s > 1$. So there exists a prime number p such that $p \mid s$. Therefore,

$$p \mid as^m, p \mid r^n.$$

This implies that $p \mid r$. Therefore, we only need to show $p \mid r$. If $p \nmid r$, then $(p, r) = 1$ since p is prime. But we know that

$$\begin{aligned} &p \mid r^n \\ &p \mid r \cdot r^{n-1} \\ &p \mid r^{n-1} \\ &p \mid r \cdot r^{n-2} \end{aligned}$$

Continuing, we know that $p \mid r$, which contradicts our assumption that $(p, r) = 1$, and finishes our theorem. $\square$

This also is very useful as it proves that if an nth root of an integer isn't an integer, it's irrational.

§8.2 Proving Irrationality

Example 8.2

$\sqrt[3]{3}$ is irrational.

Proof. By the previous theorem, if $\sqrt[3]{3}$ were rational, it would be an integer. However, $1^3 = 1$ and $2^3 = 8$. Therefore, since

$$1 < \sqrt[3]{3} < 2,$$

$\sqrt[3]{3}$ is irrational. $\square$

Theorem 8.3

Suppose $(m, n) = 1$, $d > 0$ and $d \mid mn$. Then there are unique, positive intgers d_1 and d_2 such that

$$d = d_1 \cdot d_2, d_1 \mid m, \text{ and } d_2 \mid n.$$

Proof. Let $d_1 = (d, m)$ and $d_2 = (d, n)$. Clearly, $d_2 \mid m$ and $d_2 \mid n$.

Since $d \mid mn$, $(d, mn) = d$. But

$$d = (d, mn) = (d, m) \cdot (d, n) = d_1 d_2.$$

So d_1 and d_2 satisfy the properties.

To prove uniqueness, assume there is another pair d_1, d_2 with $d = d_1 d_2$, $d_1 \mid m$, and $d_2 \mid n$.

$$d_1 = (d, m) \text{ and } d_1 \mid m, d_1 \mid d.$$

Thus, $d_1 \leq d_1$, and $d_2 \leq d_2$. So,

$$d = d_1 d_2 \leq d_1 d_2 = d.$$

$\square$

§9 Examples of Multiplicative Functions

§9.1 Definition of Multiplicative Functions

Let $n > 0$ be an integer. Let $d(n)$ = the number of positive integers that divide n (including 1 and n). Let $\sigma(n)$ = the sum of these positive divisors. $d(n) = 2$ if and only if n is prime.

These formulas satisfy some **multiplicative properties,** e.g.

$$d(2 \cdot 5) = 4 = d(2) \cdot d(5)$$

$$d(3 \cdot 4) = 6 = d(3) \cdot d(4)$$

But the relation don't always hold,

$$d(3 \cdot 6) = 6, d(3) \cdot d(6) = 8$$

The multiplicative property turns out to hold whenever $(a, b) = 1$.

Definition 9.1. A function $f(n)$ is **multiplicative** if for all pairs of relatively prime integers m, n,

$$f(m \cdot n) = f(m) \cdot f(n).$$

If this is true for all positive integers m, n

Example 9.2

$f(n) = n^2$ is completely multiplicative, since

$$f(mn) = (mn)^2 = m^2 n^2 = f(m) \cdot f(n).$$

Claim 9.3 — Let f be a multiplicative function. If we know $f(p^k)$ for all prime p and integers $k \geq 1$, then we know f on all integers.

Proof. Write an integer m in its prime decomposition

$$m = p_1^{k_1} p_2^{k_2} \cdots p_k^{k_k},$$

with

$$p_1 \neq p_j, i \neq j.$$

Note

$$(p_1^{k_1}, p_j^{k_j}) = 1 \text{ for } i \neq j.$$

So

$$f(m) = f(p_1^{k_1}) \cdots f(p_r^{k_r})$$

□

Example 9.4

$$f(12) = f(2^2) \cdot f(3).$$

Claim 9.5 — $d(n)$ is multiplicative; so

$$d(126) = d(2 \cdot 3^2 \cdot 7) = d(2) \cdot d(9) \cdot d(7) = 2 \cdot 3 \cdot 2 = 12,$$

so 126 has exactly 12 divisors.

§9.2 Reduced Residue Systems and Multiplicativity

Given a function $f(n)$, one can define a new function $g(n)$ by

$$g(n) = \sum_{d|n} f(d).$$

Example 9.6

$$g(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12).$$

Theorem 9.7
If $f(n)$ is multiplicative, then so is

$$g(n) = \sum_{d|n} f(d).$$

Claim 9.8 — This theorem implies that $d(n)$ and $\sigma(n)$ are multiplicative.

Claim 9.8. $f(n) = 1$ is completely multiplicative, but

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

Since the right hand side adds 1 for each $d \mid n$, by the above theorem, $d(n)$ is multiplicative, since we're adding up 1 for each $d \mid n$, which is the definiton of $d(n)$.

$f(n) = n$ is completely multiplicative, so by the theorem, so is

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

since we're adding up all d that divides n, which is the definition of $\sigma(n)$. □

§10 Multiplicative Functions and Perfect Numbers

§10.1 Proof of $g(n)$

Formerly, we proved that $d(n) =$ the number of elements in the set $\{d : d \mid n\}$ and

$$\sigma(n) = \sum_{d|n} f(d)$$

are multiplicative using the following result.

Theorem 10.1

If $f(n)$ is multiplicative, then so is

$$g(n) = \sum_{d|n} f(d).$$

Proof. We must show

$$g(m \cdot n) = g(m) \cdot g(n)$$

for all positive relatively prime integers m and n. Now,

$$\begin{aligned} g(m) \cdot g(n) &= \left(\sum_{d_1|m} f(d_1)\right) \cdot \left(\sum_{d_2|n} f(d_2)\right) \\ &= \sum_{d_1|m, d_2|n} f(d_1) \cdot f(d_2) \end{aligned}$$

Say $d_1 \mid m$ and $d_2 \mid n$. Then, since $(m, n) = 1$, $(d_1, d_2) = 2$. But since f is multiplicative, $f(d_1) \cdot f(d_2) = f(d_1 \cdot d_2)$.

So

$$g(m) \cdot g(n) = \sum_{d_1|m, d_2|n} f(d_1 d_2).$$

For each pair, $d_1 \mid m$ and $d_2 \mid n$. So

$$d_1 d_2 \mid m \cdot n.$$

By a previous theorem, any integer d such that $d \mid m \cdot n$ can be written uniquely as

$$d = d_1 \cdot d_2 \text{ where } d_1 \mid m \text{ and } d_2 \mid n.$$

Now,

$$\{d_1 d_2 : d_1 \mid m \& d_2 \mid n \& d_1, d_2 > 0\}$$

equals to the set of positive divisors of $m \cdot n$.

Thus,

$$g(m) \cdot g(n) = \sum_{d_1|m, d_2|n} f(d_1 d_2) = \sum_{d|mn} f(d) = g(mn).$$

Therefore, we have proven that $g(n)$ is multiplicative. □

§10.2 Proof of Formulas for d and σ

Theorem 10.2

If an integer n has its prime factorization

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

where $p_i \neq p_j$ for $i \neq j$, then

$$d(n) = (a_1 + 1) \cdots (a_k + 1)$$

and

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{a_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{a_k})$$

or

$$\sigma(n) = \frac{\left(p_1^{a_1+1} - 1\right)}{(p_1 - 1)} \cdots \frac{\left(p_k^{a_k+1} - 1\right)}{(p_k - 1)}.$$

Proof. This follows from the Multiplicativity of $d(n)$ and $\sigma(n)$ once we know

$$d(p^a) = a + 1$$

for p is a prime, or in other words, the number of divisors of a prime power is that power plus 1. Similarily,

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a.$$

□

Example 10.3

Consider a number

$$240 = 2^4 \cdot 3 \cdot 5,$$

so

$$d(240) = 5 \cdot 2 \cdot 2 = 20$$

and

$$\sigma(240) = (1 + 2 + 2^2 + 2^3 + 2^4) \cdot (1 + 3) \cdot (1 + 5) = 744.$$

§10.3 Perfect Numbers

The ancient greeks studied the function

$$\sigma(n) - n = \sum_{\substack{d|m \\ d<n}} d.$$

The function is essentially adding up all the divisors strictly less than n.

A number n such that $\sigma(n) - n = n$ is called a perfect number.

Example 10.4

6 is perfect since $6 = 2 \cdot 3$, and

$$\sigma(6) - 6 = 3 \cdot 4 - 6 = 12 - 6 = 6.$$

Euler proved that an even perfect number must be of the form

$$n = 2^{p-1}(2^p - 1)$$

where both p and $2^p - 1$ are prime.

§11 Linear Diophantine Equations

§11.1 Diophantine Equations

Definition 11.1. A **Diophantine equation** is an equation or system of equations, where the goal is to find integer solutions.

If the equation are of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n,$$

then they are called linearl.

We'll start with one equation with two unknowns

$$ax + by = c.$$

§11.2 Integral Solutions of a LDE

Theorem 11.2

Suppose $a, b \in \mathbb{Z}$ with $d = (a, b)$.

Then, if $d \nmid c$, then the equation

$$ax + by = c$$

has no integer solutions (for x and y).

If $d \mid c$, then the equation has infinite many integral soltuions.

In fact, if x_0, y_0 is one integral solution, then all integral solutions are given by

$$x = x_0 + t \cdot \frac{b}{d}$$
$$y = y_0 \cdot t \cdot \frac{a}{d}$$

where $t \in \mathbb{Z}$.

Proof. Since $d \mid a$ and $d \mid b$, $d \mid ax + by$ for any choice of integers x and y.

Thus, if $ax + by = c$, then $d \mid c$. If $d \nmid c$, then there can be no integral solutions to the euqation $ax + by = c$.

Suppose $d \mid c$ and $d \cdot e = c$. Since $d = (a, b)$, by the Euclidean algorithm, there are integers r, s such that

$$ar + bs = d.$$

Thus,

$$a(r \cdot e) + b(s \cdot e) = d \cdot e = c.$$

So then we can let $x_0 = re$ and $y_0 = se$, and the equation has an integral equation. So

$$ax_0 + by_0 = c.$$

To verify the theorem, compute

$$a\left(x_0 + t \cdot \frac{b}{d}\right) + b\left(y_0 \cdot t \cdot \frac{a}{d}\right) = ax_0 + by_0 = c$$

for any choice of integer t. Thus, the equation has infinitely many solutions.

Let's show that any solution of $ax + by = c$ is of the form

$$x = x_0 + t \cdot \frac{b}{d}$$
$$y = y_0 \cdot t \cdot \frac{a}{d}$$

for some $t \in \mathbb{Z}$.

So assume $ax + by = c$. We already know $ax_0 + by_0 = c$, dividing,

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0).$$

Therefore,

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0)$$

But

$$(\frac{b}{d}, \frac{a}{d}) = 1.$$

Thus $\frac{b}{d}(x - x_0)$. Therefore there is a $t \in \mathbb{Z}$ such that

$$\frac{b}{d} \cdot t = x - x_0,$$

so

$$x = x_0 + \frac{b}{d} \cdot t.$$

Substituting for $x - x_0$ in our second equation, we get

$$-\frac{a}{d} \cdot t = y - y_0.$$

□

Example 11.3

Find all integral solutions to $17x + 14y = 4$. $a = 17$, $b = 14$, $c = 4$. $d = (17, 14) = 1$.

We must first find a particular solution to

$$17x_0 + 14y_0 = 4$$

and then use the theorem to find all solutions.

If

$$r \cdot 17 + s \cdot 14 = 1 = d,$$

and

$$d \cdot e = c, e = 4,$$

then

$$\begin{aligned} x_0 &= re = 4r \\ y_0 &= se = 4s. \end{aligned}$$

We need to find such r, s such that

$$r \cdot 17 + s \cdot 14 = 1,$$

which can be done using the Euclidean algorithm.