Integers, Prime Factorization, and More on Primes

October 25, 2013

Week 9-10

1 Integers

Definition 1. Let $a, b \in \mathbb{Z}$. We say that a **divides** b (or a is a **factor** of b) if $b = ac$ for some integer c. When a divides b, we write $a \mid b$.

Proposition 2 (Division Algorithm)**.** *Let a be a positive integer. Then for any $b \in \mathbb{Z}$, there exist unique integers q, r such that*

$$b = qa + r, \quad 0 \leq r < a.$$

The integer q is called the **quotient** *and r is the* **remainder***.*

Proof. Consider the rational number $\frac{b}{a}$. Since $\mathbb{R} = \bigcup_{k \in \mathbb{Z}}[k, k+1)$ (disjoint), there exists a unique integer q such that $\frac{b}{a} \in [q, q+1)$, i.e., $q \leq \frac{b}{a} < q+1$. Multiplying through by the positive integer a, we obtain $qa \leq b < (q+1)a$. Let $r = b - qa$. Then we have $b = qa + r$ and $0 \leq r < a$, as required. $\square$

Proposition 3. *Let $a, b, d \in \mathbb{Z}$. If $d \mid a$ and $d \mid b$, then $d \mid (ma + nb)$ for all $m, n \in \mathbb{Z}$.*

Proof. Since $d \mid a$ and $d \mid b$, there exist integers c_1 and c_2 such that $a = c_1 d$ and $b = c_2 a$. Then for any integers $m, n \in \mathbb{Z}$, we have

$$ma + nb = mc_1 d + nc_2 d = (mc_1 + nc_2)d.$$

This means that d divides $ma + nb$. $\square$

2 Euclidean Algorithm

Definition 4. Let $a, b \in \mathbb{Z}$, not all zero. A **common divisor** (or **factor**) of a and b is an integer which divides both a and b. The **greatest common**

divisor of a and b, written $\gcd(a,b)$, is the largest positive integer that divides both a and b.

Proposition 5. *Let $a, b \in \mathbb{Z}$. If $b = qa + r$, then*

$$\gcd(a,b) = \gcd(a,r).$$

Proof. An integer c is a common divisor of a and b if and only if c is a common divisor of a and r. Thus the set of common divisors of a, b are the same as the set of common divisors of a, r. $\square$

Example 1. Find the greatest common divisor of 4346 and 6587.

Euclidean Algorithm: For integers a and b, and assume that a is positive. We write

$$\begin{array}{lcll} b & = & q_1 a + r_1, & 0 \le r_1 < a, \\ a & = & q_2 r_1 + r_2, & 0 \le r_2 < r_1, \\ r_1 & = & q_3 r_2 + r_3, & 0 \le r_3 < r_2, \\ & \vdots & & \\ r_{k-3} & = & q_{k-1} r_{k-2} + r_{k-1}, & 0 \le r_{k-1} < r_{k-2}, \\ r_{k-2} & = & q_k r_{k-1} + r_k, & 0 \le r_k < r_{k-1}, \\ r_{k-1} & = & q_{k+1} r_k + 0. & \end{array}$$

Then by Proposition 5,

$$\gcd(a,b) = \gcd(a,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{k-1},r_k) = r_k.$$

Theorem 6 (Euclidean Theorem)**.** *Let $a, b \in \mathbb{Z}$ and $d = \gcd(a,b)$. Then there exist integers m and n such that*

$$d = ma + nb.$$

Proof. By the Euclidean Algorithm above, we have $d = r_k$ and

$$\begin{array}{lcl} r_k & = & r_{k-2} - q_k r_{k-1}, \\ r_{k-1} & = & r_{k-3} - q_{k-1} r_{k-2}, \\ & \vdots & \\ r_3 & = & r_1 - q_3 r_2, \\ r_2 & = & a - q_2 r_1 \\ r_1 & = & b - q_1 a. \end{array}$$

It follows that r_k is a linear combination of a and b with integer coefficients. $\square$

Proposition 7. *Let $a, b \in \mathbb{Z}$. Then a positive integer d is the greatest common divisor of a and b if and only if*

(1) d divides both a and b;

(2) If c divides both a and b, then c divides d.

Proof. If the above two conditions are satisfied by the integer d, it is clear that d is the largest one among all divisors of a and b.

Let $d = \gcd(a, b)$. The first condition is obviously satisfied. The second condition follows from the Euclidean Algorithm. $\square$

Definition 8. Let $a, b \in \mathbb{Z}$. If $\gcd(a, b) = 1$, we say that a and b are **coprime** each other.

Proposition 9. *Let $a, b, c \in \mathbb{Z}$.*

(1) Let a and b be comprime each other. If $a \mid bc$, then $a \mid c$.

(2) Let p be a prime. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof. (1) By the Euclidean algorithm, there exist integers m, n such that $ma + nb = 1$. Multiplying c to both sides we have $mac + nbc = c$. Since $a \mid bc$, i.e., $bc = qa$ for some integer q, then

$$c = mac + nqa = (mc + nq)a,$$

which means that a is a divisor of c.

(2) If $p \nmid a$, then $\gcd(p, a) = 1$. Thus by (1), we must have $p \mid b$. $\square$

Corollary 10. *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and let p be a prime. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.*

Proof. Let $P(n)$ denote the statement. We prove it by induction on n. For $n = 1$, $P(1)$ says that if "$p \mid a_1$ then $p \mid a_1$," which is trivially true. Suppose it is true for $P(n)$. Consider $P(n+1)$. Let $a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}$. Let $a = a_1 a_2 \cdots a_n$ and $b = a_{n+1}$. Then $p \mid ab$. If $p \mid a$, i.e., $p \mid a_1 a_2 \cdots a_n$, by induction, we have some i $(1 \le i \le n)$ such that $p \mid a_i$. If $p \nmid a$, then by Proposition 9, we have $p \mid b$, i.e., $p \mid a_{n+1}$. Hence $P(n+1)$ is true. $\square$

Definition 11. Let $a, b \in \mathbb{Z}$, not all zero. A **common multiple** of a and b is a nonnegative integer m such that $a|m$ and $b|m$. The very smallest one among all common multiples of a and b is called the **least common multiple**, denoted $\operatorname{lcm}(a, b)$.

Proposition 12. *For $a, b \in \mathbb{Z}$, not all zero, if a, b are nonnegative, then*

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

Proof. Let $d = \gcd(a, b)$, $a = dc_1$ and $b = dc_2$. It is clear that the integer

$$\frac{ab}{d} = dc_1c_2 = ac_2 = bc_1$$

is a common multiple of a and b, $\gcd(c_1, c_2) = 1$. Let m be a common multiple of a and b, i.e., $m = ae_1$ and $b = be_2$. Then $m = ae_1 = dc_1e_1 = dc_2e_2$. It follows that $c_1e_1 = c_2e_2$. Since $\gcd(c_1, c_2) = 1$, we have $c_1 \mid e_2$ and $c_2 \mid e_1$. Write $e_2 = c_1f_1$ and $e_1 = c_2f_2$, then $c_1c_2f_2 = c_2c_1f_1$. Thus $f_1 = f_2$. Therefore

$$m = ae_1 = dc_1e_1 = dc_1c_2f_2 = \frac{ab}{d}f_2,$$

which is a multiple of $\frac{ab}{d} = dc_1c_2$. By definition, $\frac{ab}{d}$ is the least common multiple of a and b. $\square$

3 Prime Factorization

Theorem 13. *(a) Every integer $n \geq 2$ is a product of prime numbers, i.e., there exist primes $p_1, p_2, \ldots, p_k$, where $p_1 \leq p_2 \leq \cdots \leq p_k$, such that*

$$n = p_1p_2 \cdots p_k.$$

(b) The prime factorization in (a) is unique, i.e., if $n = p_1p_2 \cdots p_k = q_1q_2 \cdots q_l$, where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$ are primes, $p_1 \leq p_2 \leq \cdots \leq p_k$, $q_1 \leq q_2 \leq \cdots \leq q_l$, then $k = l$ and

$$p_1 = q_1, \quad p_2 = q_2, \quad \ldots \quad p_k = q_k.$$

Proof. The existence of the prime factorization has been proved before. We only need to prove the uniqueness.

Suppose there is an integer n which has two different prime factorizations, say,

$$n = p_1p_2 \cdots p_k = q_1q_2 \cdots q_l,$$

where $p_1 \leq p_2 \leq \cdots \leq p_k$, $q_1 \leq q_2 \leq \cdots \leq q_l$, and the list of primes $p_1, p_2, \ldots, p_k$ is not the same as the list $q_1, q_2, \ldots, q_l$.

Now in the equation $p_1p_2\cdots p_k = q_1q_2\cdots q_l$, cancel any primes that are common to both sides. Since the two factorizations are different, not all primes will be canceled, and we end up with an equation

$$u_1u_2\cdots u_r = v_1v_2\cdots v_s,$$

where $\{u_1, u_2, \ldots, u_r\}$ is a sub-multiset of the multiset $\{p_1, p_2, \ldots, p_k\}$, $\{v_1, v_2, \ldots, v_s\}$ is a sub-multiset of $\{q_1, q_2, \ldots, q_l\}$, and $\{u_1, u_2, \ldots, u_r\} \cap \{v_1, v_2, \ldots, v_s\} = \emptyset$.

Now we have $u_1 \mid v_1v_2\cdots v_s$ and $v_1 \mid u_1u_2\cdots u_r$. By part (2) of Proposition 9, we see that $u_1 \mid v_j$ for some j and $v_1 \mid u_i$ for some i. It follows that $u_1 = v_j$ for some j and $v_1 = u_i$ for some i. This contradicts to that $\{u_1, u_2, \ldots, u_r\} \cap \{v_1, v_2, \ldots, v_s\} = \emptyset$. □

Corollary 14. *(a) For any integer $n \geq 2$, there is a unique factorization*

$$n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},$$

where $p_1, p_2, \ldots, p_k$ are distinct primes, $p_1 < p_2 < \cdots < p_k$, and $e_1, e_2, \ldots, e_k$ are positive integers.

(b) Let $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, where $p_1 < p_2 < \cdots < p_k$ are primes and all $e_i \geq 0$. If m is positive integer and $m \mid n$, then $m = p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k}$ with $0 \leq d_i \leq e_i$ for all i.

Proof. (a) Collect the same primes and write them into powers.

(b) Since $m \mid n$, then $n = mc$ for a positive integer c. Write m and c into the unique prime factorization forms $m = q_1^{f_1}q_2^{f_2}\cdots q_l^{f_l}$ and $c = u_1^{g_1}u_2^{g_2}\cdots u_r^{g_r}$. Then

$$p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k} = q_1^{f_1}q_2^{f_2}\cdots q_l^{f_l}u_1^{g_1}u_2^{g_2}\cdots u_r^{g_r}$$

By the unique prime factorization, the primes $q_1, q_2, \ldots, q_l$ and $u_1, u_2, \ldots, u_r$ must be some of the primes $p_1, p_2, \ldots, p_k$. Thus

$$m = p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k} \quad \text{and} \quad c = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k},$$

where $d_i \geq 0$ and $a_i \geq 0$ for all i. It follows that $e_i = d_i + a_i$ for all i. Therefore, $0 \leq d_i \leq e_i$ for all i. □

Proposition 15. *Let $a, b \geq 2$ be integers with the prime factorizations*

$$a = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}, \quad b = p_1^{f_1}p_2^{f_2}\cdots p_k^{e_k},$$

where p_i are distinct primes and $e_i, f_i \geq 0$ for all i. Then

(a) $\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}$,

(b) $\operatorname{lcm}(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}$,

(c) $ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$.

4 Some Consequences of the Prime Factorization

Proposition 16. *Let n be a positive integer. Then $\sqrt{n}$ is rational if and only if n is a perfect square, i.e., $n = m^2$ for some integer m.*

Proof. When $n = m^2$ for an integer m, it is clear that m is a rational number and $\sqrt{n} = m$.

Suppose $\sqrt{n} = \frac{a}{b}$ is rational in reduced form, where $a, b \in \mathbb{Z}$. Squaring both sides, we have $nb^2 = a^2$. Let $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then a^2 has the unique prime factorization $a^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$, i.e., each prime in a^2 has an even power. Similarly, every prime in the unique factorization b^2 also has even power. So the prime in the unique factorization of n also has even power. Write $n = q_1^{2d_1} \cdots q^{2d_l}$, we have $n = m^2$ with $m = q_1^{d_1} \cdots q^{d_l}$. $\square$

Proposition 17. *Let a and b be positive integers that are coprime each other.*
(a) If ab is a square, then both a and b are squares.
(b) If ab is an nth power, then both a and b are also nth powers.

Proof. It is trivial if one of a and b is the integer 1. Let $a, b \geq 2$ and be factored into the products

$$a = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}, \quad b = q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k},$$

where $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_l$ are primes, $d_i > 0$ for all i and $e_j > 0$ for all j.

(a) Note that $ab = c^2$ for positive integer c. Let c be factored into the product $c = r_1^{f_1} r_2^{f_2} \cdots r_m^{f_m}$. Then $ab = c^2$ gives the equation

$$p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k} = r_1^{2f_1} r_2^{2f_2} \cdots r_m^{2f_m}.$$

Since a and b are coprime to each other, none of the p_i are equal to any of the q_j. The unique Factorization Theorem implies that $\{p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l\} = \{r_1, r_2, \ldots, r_m\}$ and the corresponding powers are the same. Thus the integers d_i and e_j are even numbers. Write $d_i = 2d_i'$ and $e_j = 2e_j'$. We then have

$$a = \left(p_1^{d_1'} p_2^{d_2'} \cdots p_k^{d_k'}\right)^2, \quad b = \left(q_1^{e_1'} q_2^{e_2'} \cdots q_k^{e_k'}\right)^2.$$

So a and b are squares.

(b) The argument for (b) is the same as for (a). The condition $ab = c^n$ for some integer c gives an equation

$$p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k} = r_1^{nf_1} r_2^{nf_2} \cdots r_m^{nf_m}.$$

The unique Factorization Theorem implies that the integers d_i and e_j are multiples of n. Hence a and b are both nth powers. □

Example 2. Can a nonzero even square exceed a cube by 1? No.

Proof. If there is an even integer $2x$ whose square is equal to a cubic power of an integer y plus 1, then $(2x)^2 = y^3 + 1$. We are to show that the equation

$$4x^2 = y^3 + 1$$

has no integer solution (x, y) such that $x \neq 0$.

Suppose there is an integer solution (x, y) such that $4x^2 = y^3 + 1$. Then $4x^2 - 1 = y^3$. Thus

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

Let $d = \gcd(2x + 1, 2x - 1)$. Since $2x + 1$ and $2x - 1$ are odd numbers, it follows that d is an odd number. Certainly, d divides the difference of $2x + 1$ and $2x - 1$, which is 2. Hence $d = 1$; i.e., $2x + 1$ and $2x - 1$ are coprime. By Proposition 17(b), both $2x + 1$ and $2x - 1$ are cubes. Note that the list of cubes is

$$\ldots, -27, -8, -1, 0, 1, 8, 27, \ldots$$

By inspection, a pair of cubes whose difference is 2 must be the pair $(-1, 1)$. So we must have $x = 0$ and $y = -1$. □

5 More on Prime Numbers

Theorem 18. *There are infinitely many prime numbers.*

Proof. Suppose the result is not true, i.e., there are only finite number of prime numbers, say, $p_1, p_2, \ldots, p_n$. Now consider the positive integer

$$N = p_1 p_2 \cdots p_n + 1.$$

Since $N > p_i$ for all i, the integer N cannot be a prime number. By the Factorization Theorem we have $N = q_1 q_2 \cdots q_k$ for some prime numbers. Since $p_1, p_2, \ldots, p_n$ are the only prime numbers, then $q_1 = p_i$ for some i. Then $p_i \mid N$ by the factorization of N, but $p_i \nmid N$ by definition of N. This is a contradiction. $\square$

Question: *Given a positive integer n, how many of the numbers $1, 2, \ldots, n$ are primes?*

For a positive integer n, let $\pi(n)$ denote the number of primes in $\{1, 2, \ldots, n\}$. For instance, we have

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	$\cdots$
$\pi(n)$	0	1	2	2	3	3	4	4	4	4	5	5	6	6	6	6	7	$\cdots$

Theorem 19 (Prime Number Theorem)**.**

$$\pi(n) \sim \frac{n}{\ln n}, \quad i.e., \quad \lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1.$$

Goldbach Conjecture: Every even positive integer that is greater than 2 is a sum of two primes.

Twin Primes Conjecture: Two prime numbers of the form $p, p+2$ are called **twin primes**. There are infinitely many twin primes.