

Math 300 Spring 2008 - Note 3

Zhigang Han, Umass at Amherst

1 Basic Number Theory

1.1 The Division Algorithm

Def 1: Let $a, b \in \mathbb{Z}$. We say a **divides** b (write $a|b$), if there exists $q \in \mathbb{Z}$ such that $b = aq$.

Rmk: If no such $q \in \mathbb{Z}$ exists, we say a does not divide b , and write $a \nmid b$.

Rmk: If a divides b , we also say a is a factor of b , or b is a multiple of a .

Eg 1: $3|6$; $-5|20$; $4|0$; $0|0$; but $0 \nmid 3$.

Eg 2: TRUE or FALSE:

- (i) $\forall b \in \mathbb{Z}, \exists a \in \mathbb{Z}, a|b$.
- (ii) $\exists b \in \mathbb{Z}, \forall a \in \mathbb{Z}, a|b$.
- (iii) $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, a|b$.
- (iv) $\exists a \in \mathbb{Z}, \forall b \in \mathbb{Z}, a|b$.

Prop 1: Let $a, b, c \in \mathbb{Z}$.

- (i) If $a|b$ and $b|c$, then $a|c$.
- (ii) If $a|b$ and $a|c$, then $a|bx + cy$ for all $x, y \in \mathbb{Z}$.
- (iii) If $a|b$ and $b|a$, then $a = \pm b$.
- (iv) If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

Division Algorithm: Let $a, b \in \mathbb{Z}$ and $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r, \text{ where } 0 \leq r < |b|.$$

Rmk: q is called the **quotient**, and r is called the **remainder**. The remainder r is always nonnegative.

Rmk: We often use the notation $\exists!$ for “there exist unique”. The Division Algorithm can be written as

$$\forall(a, b \in \mathbb{Z}) \wedge (b \neq 0), \exists! q, r \in \mathbb{Z}, (a = qb + r) \wedge (0 \leq r < |b|).$$

Rmk: We used in our proof the **well-ordering principle** which states that any nonempty subset of \mathbb{N} always contains a smallest element.

Eg 3: (i) If $a = -40$, $b = 12$, then $-40 = (-4) \cdot 12 + 8$ with $q = -4$, $r = 8$.
(ii) If $a = -75$, $b = -11$, then $-75 = 7 \cdot (-11) + 2$ with $q = 7$, $r = 2$.

1.2 The Euclidean Algorithm

Def 2: Let $a, b \in \mathbb{Z}$, not both zero. The **greatest common divisor** of a and b is the largest positive integer that divides both a and b . It is denoted by $\gcd(a, b)$, or simply (a, b) if there is no confusion.

Rmk: We define $\gcd(0, 0) = 0$. Thus $\gcd(a, 0) = |a|$ for all $a \in \mathbb{Z}$.

Prop 2: If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Euclidean Algorithm: Let a and b be two nonzero integers, and $|a| \geq |b|$. If $b \nmid a$, then $\gcd(a, b)$ is the last nonzero remainder r_n in the following list of equations obtained from the Division Algorithm. If $b|a$, then $\gcd(a, b) = |b|$.

$$\begin{aligned}a &= q_1b + r_1, \quad \text{where } 0 < r_1 < |b| \\b &= q_2r_1 + r_2, \quad \text{where } 0 < r_2 < r_1 \\r_1 &= q_3r_2 + r_3, \quad \text{where } 0 < r_3 < r_2 \\&\vdots \\r_{n-2} &= q_nr_{n-1} + r_n, \quad \text{where } 0 < r_n < r_{n-1} \\r_{n-1} &= q_{n+1}r_n + 0.\end{aligned}$$

Rmk: If $a = 0$, then $\gcd(0, b) = |b|$.

Eg 4: Find $\gcd(408, 187)$.

GCD Characterization Theorem: Let d be a nonnegative common divisor of a and b . Then $d = \gcd(a, b)$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$.

Corollary: (i) $\gcd(a, b) = 1$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

(ii) If $d = \gcd(a, b) \neq 0$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Prop 3: Let $a, b, c \in \mathbb{Z}$. If $c|ab$ and $\gcd(c, a) = 1$, then $c|b$.

Extended Euclidean Algorithm: Set the first two rows as $(1, 0, a)$ and $(0, 1, b)$. Think of a as r_1 and b as r_2 . For $i \geq 3$,

$$\text{Row } i = \text{Row } (i - 2) - q_i \cdot \text{Row } (i - 1).$$

Here q_i is the quotient when r_{i-2} is divided by r_{i-1} . The algorithm stops when $r_{n+1} = 0$.

$$\begin{array}{lcl} \text{Equation :} & ax + by & = r \\ \text{Row 1 :} & 1 & 0 \quad a \\ \text{Row 2 :} & 0 & 1 \quad b \\ \text{Row 3 :} & x_3 & y_3 \quad r_3 \\ \text{Row 4 :} & x_4 & y_4 \quad r_4 \\ & \vdots & \vdots \quad \vdots \\ \text{Row } n : & x_n & y_n \quad r_n \\ \text{Row } n + 1 : & x_{n+1} & y_{n+1} \quad 0 \end{array}$$

Conclusions:

- (i) $\gcd(a, b) = r_n$.
- (ii) Each row is a triple (x, y, r) satisfying the equation $ax + by = r$.
- (iii) One integer solution to $ax + by = \gcd(a, b)$ is $x = x_n, y = y_n$.

Eg 5: Use the extended Euclidean Algorithm to find $\gcd(408, 187)$, and to find $x, y \in \mathbb{Z}$ such that $408x + 187y = \gcd(408, 187)$.

1.3 Prime Numbers

Def 3: An integer $p > 1$ is called a **prime** if its only positive factors are 1 and p ; otherwise it's called **composite**.

Rmk: 1 is neither prime nor composite.

Prop 4: If p is prime and $p|ab$, then $p|a$ or $p|b$.

Unique Factorization Theorem: Every integer larger than 1 can be expressed as a product of primes, and the expression is unique up to the order of the factors.

Rmk: This theorem is often referred to as the **Fundamental Theorem of Arithmetic**.

Rmk: One can use strong mathematical induction or the method of contradiction to prove the existence.

Euclid's Theorem: There are infinitely many primes.

Eg 6: Construct 100 consecutive composite numbers.

Prop 5: If $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of a , then the positive divisors of a are those integers of form

$$d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}, \quad \text{where } 0 \leq d_i \leq a_i \text{ for } i = 1, 2, \dots, k.$$

Corollary: The number of positive divisors of $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is $N = (1 + a_1)(1 + a_2) \cdots (1 + a_k)$.

Theorem 1: If $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ are prime factorizations of a and b , where some exponents may be zero, then

$$\gcd(a, b) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k},$$

where $d_i = \min(a_i, b_i)$ for $i = 1, 2, \dots, k$.

Corollary: The number of positive common divisors of $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ is $N = (1 + d_1)(1 + d_2) \cdots (1 + d_k)$, where $d_i = \min(a_i, b_i)$ for $i = 1, 2, \dots, k$ as above.

Rmk: Here and in the previous corollary, we have used **Multiplication Counting Principle**.

Eg 5: How many positive divisors do 1000 and 420 have, respectively? How many positive common divisors do 1000 and 420 have?

Def 4: The least common multiple of two positive integers a and b is the smallest positive integer that is divisible by both a and b . It is denoted by $\text{lcm}(a, b)$.

Theorem 2: If $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ are prime factorizations of a and b , where some exponents may be zero, then

$$\text{lcm}(a, b) = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $e_i = \max(a_i, b_i)$ for $i = 1, 2, \dots, k$.

Theorem 3: For any positive integers a and b , we have

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

Eg 7: $a = 36 = 2^2 \times 3^2$ and $b = 24 = 2^3 \times 3^1$. Then $\text{gcd}(a, b) = 2^2 \times 3^1 = 12$ and $\text{lcm}(a, b) = 2^3 \times 3^2 = 72$, so $\text{gcd}(a, b) \cdot \text{lcm}(a, b) = 12 \times 72 = 864$ and $ab = 36 \times 24 = 864$.