Summary for "Greatest Common Divisor"

Xiang Sun[*†]

October 31, 2010

1 Divisibility

Definition 1.1. *Let m, n be integers, we say m* **divides** *n if there exists an integer q, such that $n = mq$. Notation: $m \mid n$. If $m \mid n$, then we say that m is divisor.*

Proposition 1.2 (Theorem 11.2)**.** *Let a, b, c be integers with $a \neq 0$*

1. *If $a \mid b$, then $a \mid (bc)$;*
2. *If $a \mid b$ and $b \mid c$, where $b \neq 0$, then $a \mid c$.*
3. *If $a \mid b$ and $b \mid c$, then $a \mid (bx + cy)$ for all integers x, y.*

Proof. Please refer to Theorem 11.2 in the textbook. □

Proposition 1.3 (Theorem 11.3)**.** *Let a, b be nonzero integers.*

1. *If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.*
2. *If $a \mid b$, then $|a| \leq |b|$.*

Proof. Please refer to Theorem 11.3 in the textbook. □

Theorem 1.4 (The Division Algorithm)**.**
- *(Theorem 11.4) Original case: For all positive integers a and b, there exist unique integers q and r, such that*
$$b = aq + r, \text{ where } 0 \leq r < a.$$
- *(Corollary 11.5) Generalization: For all integers a and b, there exist unique integers q and r, such that*
$$b = aq + r, \text{ where } 0 \leq r < |a|.$$
Here allow a and b to be negative.

Proof. Please refer to Theorem 11.4 and Corollary 11.5 in the textbook. □

2 Greatest Common Divisor

Definition 2.1. *Let a, b be integers, and d a nonzero integer. We say d is* **a common divisor of** *a* **and** *b if $d \mid a$ and $d \mid b$. We use $\mathrm{cd}(a, b)$ to denote the set of all common divisors of a and b.*

Remark 1.
- *For any integers a and b, 0 can not be a common divisor of a and b.*
- *The notation $\mathrm{cd}(a, b)$ is not defined in the textbook, if you want to use it, you had better give the precise definition.*

Definition 2.2. *Let a, b be integers, not both zero. The largest integer that divides both a and b is called* **the greatest common divisor of** *a* **and** *b. Notation: $\gcd(a, b)$.*

Remark 2.
- $\gcd(a, b) = \max \mathrm{cd}(a, b)$. *(very useful)*
- $\gcd(0, 0)$ *is not defined.*

Definition 2.3 (Working definition)**.** *Let a, b be integers, not both zero, and $d \in \mathbb{N}$.*
$$d = \gcd(a, b) \Leftrightarrow \begin{cases} d \mid a \text{ and } d \mid b; \\ \text{for all } k \in \mathbb{N}, \text{ if } k \mid a, k \mid b, \text{ then } k \leq d. \end{cases}$$

[*]Email: xiangsun@nus.edu.sg
[†]Corrections are always welcome.

3 Theorems and Propositions

Proposition 3.1. *Let a be a nonzero integer. Then*

1. $\gcd(a, 0) = |a|$;
2. $\gcd(a, a) = |a|$;
3. $\gcd(a, an) = |a|$ *for all* $n \in \mathbb{Z}$.

Proof. 1. If a is positive, then a is a common divisor of a and 0. For any other common divisor k, we have $k \mid a$, and hence $k \leq a$ by Proposition 1.3. Thus, by working definition (Definition 2.3), a is the greatest common divisor of a and 0.

If a is negative, then $-a > 0$ is a common divisor of a and 0. For any other common divisor k, we have $k \mid a$, and hence $k \mid (-a)$ by Proposition 1.3. Thus $k \leq -a$. Therefore, by working definition (Definition 2.3), $-a$ is the greatest common divisor of a and 0.

Combining the two cases above, we have $\gcd(a, 0) = |a|$.

2. If a is positive, then a is a common divisor of a and a. For any other common divisor k, we have $k \mid a$, and hence $k \leq a$ by Proposition 1.3. Thus, by working definition (Definition 2.3), a is the greatest common divisor of a and a.

If a is negative, then $-a > 0$ is a common divisor of a and a. For any other common divisor k, we have $k \mid a$, and hence $k \mid (-a)$. Thus $k \leq -a$ by Proposition 1.3. Therefore, by working definition (Definition 2.3), $-a$ is the greatest common divisor of a and a.

Combining the two cases above, we have $\gcd(a, a) = |a|$.

3. For any divisor d of a, d is also a divisor of an for all $n \in \mathbb{Z}$. Hence $\mathrm{cd}(a, an)$ is the set of all divisors of a, in which $|a|$ is the largest element. Therefore $\gcd(a, an) = |a|$.

□

Proposition 3.2. *Let a, b be integers, not both zero. Then* $\gcd(a, b) > 0$.

Proof. We apply proof by cases:

- If $a = 0$, then $b \neq 0$, and hence $\gcd(a, b) = |b| > 0$ by Proposition 3.1.
- If $b = 0$, then $a \neq 0$, and hence $\gcd(a, b) = |a| > 0$ by Proposition 3.1.
- If $a \neq 0$ and $b \neq 0$, then it is trivial that 1 is a common divisor of a and b. Hence $\gcd(a, b) \geq 1 > 0$.

Combining the three cases above, we have $\gcd(a, b) > 0$. □

Proposition 3.3. *Let a, b be integers, not both zero. Then*

1. $\gcd(a, b) = \gcd(b, a)$.
2. $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.
3. $\gcd(a, b) = \gcd(a, b + an)$ *for all* $n \in \mathbb{Z}$.

Proof. 1. It is trivial that $\mathrm{cd}(a, b) = \mathrm{cd}(b, a)$. Hence, $\gcd(a, b) = \max \mathrm{cd}(a, b) = \max \mathrm{cd}(b, a) = \gcd(b, a)$.

2. It is trivial that $\mathrm{cd}(a, b) = \mathrm{cd}(a, -b) = \mathrm{cd}(-a, b) = \mathrm{cd}(-a, -b)$. Hence $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.

3. It suffices to show $\mathrm{cd}(a, b) = \mathrm{cd}(a, b + an)$ for all $n \in \mathbb{N}$:

For any $d \in \mathrm{cd}(a, b)$, then $d \mid a$ and $d \mid b$. By Definition 1.1, we have $a = dp$ and $b = dq$ for some integers p and q. Then $b + an = d(q + pn)$, and hence $d \mid (b + an)$. Therefore $d \in \mathrm{cd}(a, b + an)$.

For any $k \in \mathrm{cd}(a, b+an)$, then $d \mid a$ and $d \mid (b+an)$. By Definition 1.1, we have $a = dp$ and $b+an = dq$ for some integers p and q. Then $b = (b + an) - an = dq - dpn = d(q - pn)$, where $q - pn$ is an integer. Also by Definition 1.1, we have $d \mid b$. Therefore, $d \in \mathrm{cd}(a, b)$.

□

Proposition 3.4. *Let a be an integer, and p a prime number. Then*

$$\gcd(p,a)=\begin{cases} p, & \text{if } p \mid a; \\ 1, & \text{if } p \nmid a. \end{cases}$$

Proof. If $p \mid a$, then $a = pn$ for some integer n. By Proposition 3.1, we have $\gcd(p,a) = \gcd(p,pn) = |p| = p$ since $p > 0$.

If $p \nmid a$. Since p is a prime number, p has only 4 divisors: 1, -1, p and $-p$. Since $p \nmid a$, the common divisors of p and a are 1 and -1, and hence $\gcd(p,a) = \max\{1,-1\} = 1$. □

Proposition 3.5. *Let a, b be integers, not both zero, c a positive integer. If $c \mid \gcd(a,b)$, then*

$$\gcd\left(\frac{a}{c},\frac{b}{c}\right)=\frac{\gcd(a,b)}{c}.$$

Specially, we have

$$\gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1.$$

Proof. Let $D = \gcd(a,b)$.

Since $c \mid D$, we have $c \mid a$ and $c \mid b$. Then $\frac{a}{c}$, $\frac{b}{c}$ and $\frac{D}{c}$ are integers. Since $D \mid a$ and $D \mid b$, we have $\frac{D}{c} \mid \frac{a}{c}$ and $\frac{D}{c} \mid \frac{b}{c}$. Hence $\frac{D}{c} > 0$ is a common divisor of $\frac{a}{c}$ and $\frac{b}{c}$.

Let d be a common divisor of $\frac{a}{c}$ and $\frac{b}{c}$, then we have $(cd) \mid a$ and $(cd) \mid b$, and hence cd is a common divisor of a and b. Hence $cd \le \gcd(a,b) = D$, and $d \le \frac{D}{c}$.

By working definition (Definition 2.3), $\frac{D}{c} = \gcd(\frac{a}{c},\frac{b}{c})$, i.e.

$$\gcd\left(\frac{a}{c},\frac{b}{c}\right)=\frac{\gcd(a,b)}{c}.$$

Let $c = \gcd(a,b)$, then we have

$$\gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1.$$

□

Corollary 3.6. *Let a, b be integers, c a positive integer. Then $\gcd(ca,cb) = c\gcd(a,b)$.*

Proof.

$$\frac{\gcd(ca,cb)}{c}=\gcd\left(\frac{ca}{c},\frac{cb}{c}\right)=\gcd(a,b).$$

□

Theorem 3.7 (Theorem 11.7)**.** *Let a, b be integers, not both 0, then $\gcd(a,b)$ is the smallest positive linear combination of a and b. That is,*

$$\gcd(a,b)=ax+by$$

for some integers x and y.

Proof. Please refer to Theorem 11.7 in the textbook. □

Corollary 3.8. *If $c \mid a$ and $c \mid b$, then $c \mid \gcd(a,b)$.*

Proof. By Theorem 3.7, we have

$$\gcd(a,b)=ax+by$$

for some integers x, y. Since $c \mid a$ and $c \mid b$, by Proposition 1.2, we have $c \mid (ax+by)$. Therefore, $c \mid \gcd(a,b)$. □

Theorem 3.9 (Theorem 11.8)**.** *Let a, b be integers, not both 0, and $d \in \mathbb{N}$.*

$$d=\gcd(a,b) \Leftrightarrow \begin{cases} d \mid a \text{ and } d \mid b; \\ \text{for all } k \in \mathbb{N}, \ \text{if } k \mid a, k \mid b, \ \text{then } k \mid d. \end{cases}$$

Proof. Please refer to Theorem 11.8 in the textbook. □

Theorem 3.10. *1. If* $\gcd(a,b) = 1$*, then* $\gcd(ac,b) = \gcd(c,b)$*.*

2. If $\gcd(a,b) = 1$ *and* $a \mid (bc)$*, then* $a \mid c$*. (Theorem 11.13)*

3. Euclid's Lemma:

- *Let* a, b *be integers and* p *a prime number. If* $p \mid (ab)$*, then* $p \mid a$ *or* $p \mid b$*. (Corollary 11.14)*
- *Let* $a_1, a_2, \ldots, a_n$ *an be integers and* p *be a prime number. If* $p \mid a_1 a_2 \cdots a_n$*, then* $p \mid a_k$ *for some* k $(1 \le k \le n)$*. (Corollary 11.15)*

Proof. Please refer to Theorem 11.13, Corollary 11.14, and Corollary 11.15 in the textbook. Here I will give an alternative proof:

1. Let $m = \gcd(ac,b)$ and $n = \gcd(c,b)$. We shall show $m \le n$ and $n \le m$.

   Now $n = \gcd(c,b)$ implies $n \mid c$ and $n \mid b$. So $n \mid ac$. Hence n is a common divisor of ac and b. So $n \le m$, which is the greatest common divisor of ac and b.

   On the other hand, $m = \gcd(ac,b)$. So $m \mid ac$ and $m \mid b$. That is,

   $$ac = mp, \quad b = mq \tag{1}$$

   for some integers p, q. Since $\gcd(a,b) = 1$, we have

   $$ax + by = 1 \tag{2}$$

   for some integers x, y.

   Multiplying c to the Equation (2), we have $acx+bcy = c$. By the Equation (1), we have $(mp)x+(mq)cy = c$ which gives $m(px + qcy) = c$. Hence $m \mid c$, and m is a common divisor of c and b. So $m \le n$, which is the greatest common divisor of c and b.

2. By Part 1, we have $a = \gcd(bc,a) = \gcd(c,a)$. Hence $a \mid c$.

3. Given $p \mid (ab)$.

   - If $p \mid a$, we have done.
   - If $p \nmid a$. Then $\gcd(p,a) = 1$. By Part 2, we have $p \mid b$.

□

Proposition 3.11. *1. If* $\gcd(a,b) = 1$ *and* $\gcd(a,c) = 1$*, then* $\gcd(a,bc) = 1$*.*

2. If $\gcd(a,b) = 1$*,* $a \mid c$*,* $b \mid c$*, then* $(ab) \mid c$*. (Theorem 11.16)*

Proof. 1. If $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, there exist integers p, q, x, y such that

$$ap + bq = 1, \quad ax + cy = 1.$$

   From this, we see that

$$\begin{aligned} 1 &= (ap + bq)(ax + cy) \\ &= apax + apcy + bqax + bqcy \\ &= a(pax + pcy + bqx) + bc(qy) \end{aligned}$$

   We see that 1 is a linear combination of a and bc and hence $\gcd(a,bc) = 1$.

2. Since $\gcd(a,b) = 1$, we have

   $$ax + by = 1$$

   for some integers x, y. Multiplying c to the Equation, we will obtain

   $$axc + byc = c.$$

   Since $a \mid c$ and $b \mid c$, we have $c = ap$ and $c = bq$ for some integers p, q. Hence, the Equation becomes

   $$ab(xq + yp) = axbq + byap = c.$$

   Therefore $(ab) \mid c$.

□