Summary for “Elementary Number Theory: Second Edition by Underwood Dudley”

Agro Rachmatullah

2018-12-10

1 Integers

Definition 1.1 (Least-integer principle)**.** A nonempty set of integers that is bounded below contains a smallest element.

Example The set $\{4, 5, 6\}$ has 4 as the smallest element. The set $\{10, 12, 14, ...\}$ has 10 as the smallest element.

Definition 1.2 (Greatest-integer principle)**.** A nonempty set of integers that is bounded above contains a largest element.

Example The set $\{4, 5, 6\}$ has 6 as the largest element. The set $\{1\}$ has 1 as the largest element.

Definition 1.3. a divides b (written $a \mid b$) if and only if there is an integer d such that $ad = b$.

Examples $3 \mid 6$, $15 \mid 60$, $9 \mid 9$, $-4 \mid 16$, and $2 \mid -100$.

Definition 1.4. If a does not divide b, we write $a \nmid b$.

Examples $10 \nmid 5$ and $3 \nmid 7$.

Lemma 1.1. If $d \mid a$ and $d \mid b$, then $d \mid (a + b)$.

Example $2 \mid 4$ and $2 \mid 10$, so $2 \mid 14$.

Lemma 1.2. If $d \mid a_1$, $d \mid a_2$, ... $d \mid a_n$, then $d \mid (c_1a_1 + c_2a_2 + ... + c_na_n)$ for any integers $c_1, c_2, ..., c_n$

Example $2 \cdot 6 + 4 \cdot 9 = 12 + 36 = 48$. Because $3 \mid 6$ and $3 \mid 9$, we conclude that $3 \mid 48$.

Definition 1.5. d is the greatest common divisor of a and b (written $d = (a, b)$) if and only if

(i) $d \mid a$ and $d \mid b$, and

(ii) if $c \mid a$ and $c \mid b$, then $c \leqslant d$

Examples $(2, 6) = 2$ and $(5, 7) = 1$.

Theorem 1.1. If $(a, b) = d$, then $(a/d, b/d) = 1$.

Examples
$(16, 20) = 4$, so $(16/4, 20/4) = (4, 5) = 1$
$(12, 6) = 3$, so $(12/3, 6/3) = (4, 2) = 2$

Proof. Suppose that $c = (a/d, b/d)$. If follows that $c \mid (a/d)$ and $c \mid (b/d)$. Therefore there are integers q and r such that $cq = a/d$ and $cr = b/d$. That is,

$$(cd)q = a \text{ and } (cd)r = b$$

which means cd is a divisor of both a and b. Because $(a, b) = d$, it must be the case that $cd \leqslant d$. d is positive so $c \leqslant 1$.

Because $c = (a/d, b/d)$, it follows that $c \geqslant 1$. Therefore $c = 1$. □

Definition 1.6. If $(a, b) = 1$, then we will say that a and b are **relatively prime**.

Examples $(4, 5) = 1$, so 4 and 5 are relatively prime. 10 and 7 are also relatively prime.

Theorem 1.2 (The Division Algorithm)**.** Given positive integers a and b, $b \neq 0$, there exist unique integers q and r, with $0 \leqslant r < b$ such that

$$a = bq + r$$

Example With $a = 17$ and $b = 5$, we have $17 = 5 \cdot 3 + 2$

Proof. Consider the set of integers $\{a, a - b, a - 2b, a - 3b, \ldots, a - qb\}$ bounded below by 0. It contains members that are nonnegative and nonempty (because at least a is a member). From the least-integer principle, it contains a smallest element $a - qb$.

The smallest element must be less than b, because if not the smallest element in the set would have to be $a - (q + 1)b$.

Ler $r = a - qb$. It follows that $a = bq + r$ and we only have to show that q and r are unique.

Suppose that we have found q, r and q_1, r_1 such that $a = bq + r = bq_1 + r_1$ with $0 \leqslant r < b$ and $0 \leqslant r_1 < b$. Subtracting, we get

$$\begin{aligned} 0 &= b(q - q_1) + (r - r_1) \\ b(q_1 - q) &= r - r_1 \end{aligned}$$

Since b divides the left side of the equation, it follows that $b \mid r - r_1$.

Because $0 \leqslant r_1 < b$, we have $-b < -r_1 \leqslant 0$. We also have $0 \leqslant r < b$, so it follows that

$$-b < r - r_1 < b$$

Since the only number in that range divisible by b is 0, $r - r_1 = 0$ which implies $q - q_1 = 0$. Hence the numbers q and r in the theorem is unique. □

Lemma 1.3. If $a = bq + r$, then $(a, b) = (b, r)$.

Proof. Let $d = (a, b)$. Because $d \mid a$ and $d \mid b$, we know from $a = bq + r$ that $d \mid r$. Therefore, d is a common divisor of b and r. It remains to show that d is not just any common divisor but in fact the greatest common divisor.

Now let us assume that c is a common divisor of b and r, so $c \mid b$ and $c \mid r$. From the equation $a = bq + r$, we know that $c \mid a$. So c is common divisor of both a and b. Because $(a, b) = d$, it must be the case that $c \leqslant d$.

Since d is a common divisor of b and r, and for any common divisor c we have $c \leqslant d$, we have proven that $(b, r) = d$. $\square$

Theorem 1.3 (The Eucledian Algorithm)**.** If a and b are positive integers, $b \neq 0$, and

$$\begin{aligned}
a &= bq + r, & 0 &\leqslant r < b, \\
b &= rq_1 + r_1, & 0 &\leqslant r_1 < r, \\
r &= r_1 q_2 + r_2, & 0 &\leqslant r_2 < r_1 \\
&. & &. \\
&. & &. \\
&. & &. \\
r_k &= r_{k+1} q_{k+2} + r_{k+2}, & 0 &\leqslant r_{k+2} < r_{k+1}
\end{aligned}$$

then for k large enough, say $k = t - 1$, we have

$$r_{t-1} = r_t q_{t+1}$$

and $(a, b) = r_t$.

Proof. The sequence

$$b > r > r_1 > r_2 > \dots$$

is decreasing, and we know that they are nonnegative, so we will eventually reach 0. Suppose $r_{t+1} = 0$. Then we have $r_{t-1} = r_t q_{t+1}$. If we apply Lemma 3 over and over,

$$(a, b) = (b, r) = (r, r_1) = (r_1, r_2) = \cdots = (r_{t-1}, r_t) = r_t$$

$\square$

Theorem 1.4. If $(a, b) = d$, then there are integers x and y such that

$$ax + by = d$$

Proof. Let us assume that a and b are positive integers with $a \geqslant b$ and $b \neq 0$. We can always switch the order of a and b, and if $b = 0$ then the proof is trivial.

If $(a, b) = b$, then $a \cdot 0 + b \cdot 1 = b$ so the equation is true with $x = 0$ and $y = 1$.

For $d < b$, then d will be one of the remainders in the set of equations from Theorem 3. If we call the remainders $r_0, r_1, \ldots$ then we can rewrite the equations as

$$\begin{aligned} r_0 &= a - bq \\ r_1 &= b - r_0 q_1 \\ r_2 &= r_0 - r_1 q_2 \\ &\cdots \\ r_n &= r_{n-2} - r_{n-1} q_n \end{aligned}$$

For the base case of r_0 and r_1, it is easy to confirm that they can be written as $ax + by$.

Now, assuming that $r_{n-2} = ax + by$ and $r_{n-1} = ax' + by'$, then

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1} q_n \\ &= ax + by - q_n(ax' + by') \\ &= a(x - q_n x') + b(y - q_n y') \end{aligned}$$

Because the base case and inductive case is proven, it is proved for all r_n.

If one or both of a and b are negative, we can use the property $(a, b) = (-a, b) = (a, -b) = (-a, -b)$. We can also switch the order such that $a \geqslant b$ as required by the beginning of the proof. $\square$

Corollary 1.4.1. If $d \mid ab$ and $(d, a) = 1$, then $d \mid b$.

Proof. Because d and a is relatively prime, we have

$$\begin{aligned} dx + ay &= 1 \\ d(bx) + (ab)y &= b \end{aligned}$$

Because the left side is divisible by d, we conclude that $d \mid b$. $\square$

Corollary 1.4.2. Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$. Then $c \mid d$.

Examples $(18, 12) = 6$, and 3 is a common divisor of both 18 and 12. Thus by the corollary $3 \mid 6$.

Proof. We know that there are integers x and y such that

$$ax + by = d$$

Because $c \mid ax$ and $c \mid by$, c divides the right hand side too. $\square$

Corollary 1.4.3. If $a \mid m$, $b \mid m$, and $(a, b) = 1$, then $ab \mid m$.

Examples $3 \mid 30$, $5 \mid 30$, and $(3, 5) = 1$. Thus $3 \cdot 5 = 15 \mid 30$.

Proof. $b \mid m$ means there is an integer q such that $m = bq$. Since $a \mid m$, we have $a \mid bq$.

However since $(a, b) = 1$, from Corollary 1 we know that $a \mid q$. Therefore there is an integer r such that $q = ar$, so $m = bar = (ab)r$. Thus $ab \mid m$. $\square$