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

Agro Rachmatullah

2019-07-08

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 $\{10, 12, 14, \dots\}$ 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 $d \mid a_1$, $d \mid a_2$, $\dots$ $d \mid a_n$, then $d \mid (c_1a_1 + c_2a_2 + \cdots + c_na_n)$ for any integers $c_1, c_2, \dots, c_n$

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,

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

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 $(b, r) = d$. □

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,

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

□

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

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

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. □

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 $d \mid b$. □

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. □

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 $ab \mid m$. □

2 Unique Factorization

Definition 2.1. A **prime** is an integer that is greater than 1 and has no positive divisors other than 1 and itself.

Examples 2, 3, 5, 7 and 11 are primes.

Definition 2.2. An integer that is greater than 1 but is not prime is called **composite**.

Examples 4 is a composite because it is divisible by 2. 10 is a composite because it has 2 and 5 as its divisor.

Definition 2.3. 1 is neither a prime nor composite. We will call 1 a **unit**.

Lemma 2.1. Every integer n, $n > 1$, is divisible by a prime.

Proof. Consider the set of all divisors of n larger than 1 and smaller than n itself. If it is empty, then n is a prime which means that it is divisible by a prime (namely itself).

If it is nonempty, then by the least integer principle it has a smallest divisor, say p. If p is not a prime, then it has divisor $q > 1$ but smaller than itself. However q must divide n which is a contradiction because p is supposed to be the smallest in the set. Therefore p is a prime, and n has a prime divisor which is p. □

Proof. (By induction) The lemma is true by inspection for $n = 2$. Suppose it is true for $n \leqslant k$. Then either $k + 1$ is prime, in which case we are done, or it is divisible by some number k_1 with $k_1 \leqslant k$. But from the induction assumption, k_1 is divisible by a prime, and this prime also divides $k + 1$. Again, we are done. □

Lemma 2.2. Every integer n, $n > 1$, can be written as a product of primes.

Proof. From Lemma 1, we know that there is a prime p_1 such that $p_1 \mid n$. That is, $n = p_1 n_1$, where $1 \leqslant n_1 < n$. If $n_1 = 1$, then we are done: $n = p_1$ is an expression of n as a products of primes. If $n_1 > 1$, then from Lemma 1 again, there is a prime that divides n_1. That is, $n_1 = p_2 n_2$, where p_2 is a prime and

$1 \leqslant n_2 < n_1$. If $n_2 = 1$, again we are done: $n = p_1 p_2$ is written as a product of primes. But if $n_2 > 1$, then Lemma 1 once again says that $n_2 = p_3 n_3$, with p_3 a prime and $1 \leqslant n_3 < n_2$. If $n_3 = 1$, we are done. If not we continue. We will sooner or later come to one of the n_i equal to 1, because $n > n_1 > n_2 > \ldots$ and each n, is positive; such a sequence cannot continue forever. For some k, we will have $n_k = 1$, in which case $n = p_1 p_2 \cdots p_k$ is the desired expression of n as a product of primes. Note that the same prime may occur several times in the product. $\square$

Theorem 2.1 (Euclid)**.** There are infinitely many primes.

Proof. Suppose not. Then there are only finitely many primes. Denote them by $p_1, p_2, \ldots, p_r$. Consider the integer

$$n = p_1 p_2 \cdots p_r + 1 \tag{1}$$

From Lemma 1, we see that n is divisible by a prime, and since there are only finitely many primes, it must be one of $p_1, p_2, \ldots, p_r$. Suppose that it is p_k. Then since

$$p_k \mid n \text{ and } p_k \mid p_1 p_2 \cdots p_r \ ,$$

it divides two of the terms in (1). Consequently it divides the other term in (1); thus $p_k \mid 1$. This is nonsense: no primes divide 1 because all are greater than 1. This contradiction shows that we started with an incorrect assumption. Since there cannot be only finitely many primes, there are infinitely many. $\square$

Lemma 2.3. If n is composite, then it has divisor d such that $1 < d \leqslant n^{\frac{1}{2}}$.

Proof. Since n is composite, there are integers d_1 and d_2 such that $d_1 d_2 = n$ and $1 < d_1 < n$, $1 < d_2 < n$. If d_1 and d_2 are both larger than $n^{\frac{1}{2}}$, then

$$n = d_1 d_2 > n^{\frac{1}{2}} n^{\frac{1}{2}} = n$$

$\square$

which is impossible. Thus, one of d_1 and d_2 must be less than or equal to $n^{\frac{1}{2}}$.

Lemma 2.4. If n is composite, then it has a prime divisor less than or equal to $n^{\frac{1}{2}}$.

Proof. We know from Lemma 2.3 that n has a divisor—call it d—such that $1 < d \leqslant n^{\frac{1}{2}}$. From Lemma 2.1, we know that d has a prime divisor p. Since $p \leqslant d \leqslant n^{\frac{1}{2}}$, the lemma is proved. $\square$

Lemma 2.5. If p is a prime and $p \mid ab$, then $p \mid a$ or $b \mid b$.

Examples $2 \mid 4 \cdot 3$, so 2 must either divide 4 or 3. Indeed, $2 \mid 4$.

The same couldn't be said if the divisor is not a prime. For example, even though $4 \mid 2 \cdot 6$, 4 doesn't divide either 2 nor 6.

Proof. Since p is prime, its only positive divisors are 1 and p. Thus $(p, a) = p$ or $(p, a) = 1$. In the first case, $p \mid \boldsymbol{a}$, and we are done. In the second case, Corollary 1.4.1 tells us that $p \mid \boldsymbol{b}$, and again we are done. $\square$

Lemma 2.6. If p is a prime and $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some i, $i = 1, 2, \ldots, k$.

Proof. Lemma 2.6 is true by inspection if $k = 1$, and Lemma 2.5 shows that it is true if $k = 2$. We will proceed by induction. Suppose that Lemma 2.6 is true for $k = r$. Suppose that $p \mid a_1 a_2 \cdots a_{r+1}$. The $p \mid a_1 a_2 \cdots a_r$ or $p \mid a_{r+1}$. In the first case, the induction assumption tells us that $p \mid a_i$ for some i, $i = 1, 2, \ldots, r$. In the second case, $p \mid a_i$ for $i = r + 1$. In either case, $p \mid a_i$ for some i, $i = 1, 2, \ldots, r + 1$. Thus, if the lemma is true for $k = r$, it is true for $k = r + 1$, and since it is true for $k = 1$ and $k = 2$, it is true for any positive integer k. $\square$

Lemma 2.7. If $p, q_1, q_2, \ldots, q_n$ are primes, and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k.

Proof. From Lemma 2.6 we know that $p \mid q_k$ for some k. Since p and q_k are primes, $p = q_k$. (The only positive divisors of q_k are 1 and q_k, and p is not 1.) $\square$

Theorem 2.2 (The Unique Factorization Theorem)**.** Any positive integer can be written as a product of primes in one and only one way.

Proof. Recall that we agreed to consider as identical all factorizations that differ only in the order of the factors.

We know already from Lemma 2.2 that any integer n, $n > 1$ can be written as a product of primes. Thus to complete the proof of the theorem, we need to show that n cannot have two such representations. That is, if

$$n = p_1 p_2 \cdots p_m \text{ and } n = q_1 q_2 \cdots q_r \tag{2}$$

then we must show that the same primes appear in each product, and the same number of times, though their order may be different. That is, we must show that the integer $p_1, p_2, \ldots, p_m$ are just a rearrangement of the integers $q_1 q_2, \ldots, q_r$. From (2) we see that since $p_1 \mid n$,

$$p_1 \mid q_1 q_2 \cdots q_r$$

From Lemma 2.7, it follows that $p_1 = q_i$ for some i. If we divide

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_r$$

by the common factor, we have

$$p_2p_3\cdots p_m = q_1q_2\cdots q_{i-1}q_{i+1}\cdots q_r \ . \tag{3}$$

Because p_2 divides the left-hand side of this equation, it also divides the right-hand side. Applying Lemma 2.7 again, it follows that $p_2 = q_j$ for some j ($j = 1, 2, \ldots, i-1, i+1, \cdots n$). Cancel this factor from both sides of (3), and continue the process. Eventually we will find that each p is a q. We cannot run out of q's before all the p's are gone, because we would then have a product of primes equal to 1, which is impossible. If we repeat the argument with the p's and q's interchanged, we see that each q is a p. Thus the numbers $p_1, p_2, \ldots, p_m$ are rearrangement of $q_1, q_2, \ldots q_r$ and the two factorizations differ only in the order of the factors. □

Proof. (Induction) The theorem is true, by inspection, for $n = 2$. Suppose that it is true for $n \leqslant k$. Suppose that $k+1$ has two representations:

$$k + 1 = p_1p_2\cdots p_m = q_1q_2\cdots q_r \ .$$

As in the last proof, $p_1 = q_i$ for some i, so

$$p_2p_3\cdots p_m = q_1q_2\cdots q_{i-1}q_{i+1}\cdots q_r \ .$$

But this number is less than or equal to k, and by the induction assumption, its prime decomposition is unique. Hence the integers $q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots, q_r$ are a rearrangement of $p_2, p_3, \ldots, p_m$, and since $p_1 = q_i$ the proof is complete. □

Definition 2.4. From the unique factorization theorem it follows that each positive integer can be written in exactly one way in the form

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

where $e_i \geqslant 1, i = 1, 2, \ldots, k$, each p_i is a prime, and $p_i \neq p_j$ for $i \neq j$. We call this representation the **prime-power decomposition** of n,

Theorem 2.3. If $e_1 \geqslant 0$, $f_1 \geqslant 0$, $(i = 1, 2, \ldots k)$,

$$m = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k} \ \text{ and } \ n = p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k} \ ,$$

then

$$(m, n) = p_1^{g_1}p_2^{g_2}\cdots p_k^{g_k}$$

where $g = \min(e_i, f_i)$, $i = 1, 2, \ldots k$

3 Linear Diophantine Equations

Definition 3.1. Equations in which we look for solutions in a restricted class of numbers—be they positive integers, negative integers, rational numbers, or whatever—are called **diophantine equations**.

Example $x^2 + y^2 = z^2$ where we look for solutions in integers. One such solution is $x = 3$, $y = 4$, $z = 5$.

Lemma 3.1. If x_0, y_0 is a solutions of $ax + by = c$, then so is

$$x_0 + bt, y_0 - at$$

for any integer t.

Example $x + 2y = 4$ has $x = 0, y = 2$ as one of its solution. If we set $t = 2$, then

$$\begin{aligned} x &= 0 + 2 \cdot 2 = 4 \\ y &= 2 - 1 \cdot 2 = 0 \end{aligned}$$

is also a solution for the diophantine equation.

Proof. We are given that $ax_0 + by_0 = c$. Thus

$$\begin{aligned} a(x_0 + bt) + b(y_0 - at) &= ax_0 + abt + by_0 - bat \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

so $x_0 + bt, y_0 - at$ satisfies the equation too. □

Lemma 3.2. If $(a, b) \nmid c$. then $ax + by = c$ has no solutions, and if $(a, b) \mid c$, then $ax + by = c$ has a solution.

Example The equation $2x + 4y = 5$ has no solution because $(2, 4) = 2 \nmid 5$.

Proof. Suppose that there are integers x_0, y_0 such that $ax_0 + by_0 = c$, Since $(a, b) \mid ax_0$ and $(a, b) \mid by_0$, it follows that $(a, b) \mid c$. Conversely, suppose that $(a, b) \mid c$. Then $c = m(a, b)$ for some m. From Theorem 1.4, we know that there are integers r and s such that

$$ar + bs = (a, b)$$

Then

$$a(rm) + b(sm) = m(a, b) = c$$

and $x = rm, y = sm$ is a solution. □

Lemma 3.3. Suppose that $(a,b) = 1$ and x_0, y_0 is a solution of $ax + by = c$. Then all solutions of $ax + by = c$ are given by

$$\begin{aligned} x &= x_0 + bt \\ y &= y_0 - at \end{aligned}$$

where t is an integer.

Proof. We see from Lemma 2 that the equation does have a solution, because $(a,b) = 1$ and $1 \mid c$ for all c. Then, let r, s be *any* solution of $ax + by = c$. We want to show that $r = x_0 + bt$ and $s = y_0 - at$ for some integer t. From $ax_0 + by_0 = c$ follows

$$c - c = (ax_0 + by_0) - (ar + bs)$$

or

$$a(x_0 - r) + b(y_0 - s) = 0 \tag{1}$$

Because $a \mid a(x_0 - r)$ and $a \mid 0$, we have $a \mid b(y_0 - s)$. But we have supposed that a and b are relatively prime. It follows from Corollary 1.1 that $a \mid y_0 - s$. That is, there is an integer t such that

$$at = y_0 - s \tag{2}$$

Substituting in (1), this gives

$$a(x_0 - r) + bat = 0$$

Because $a \neq 0$, we may cancel it to get

$$x_0 - r + bt = 0 \tag{3}$$

But (2) and (3) say that

$$\begin{aligned} s &= y_0 - at \\ r &= x_0 + bt \end{aligned}$$

Since r, s was *any* solution, the lemma is proved. □

Theorem 3.1. The linear diophantine equation $ax + by = c$ has no solutions if $(a,b) \nmid c$. If $(a,b) \mid c$, there are infinitely many solutions

$$x = r + \frac{b}{(a,b)}t, \quad y = s - \frac{a}{(a,b)}t$$

where r, s is any solution and t is an integer.