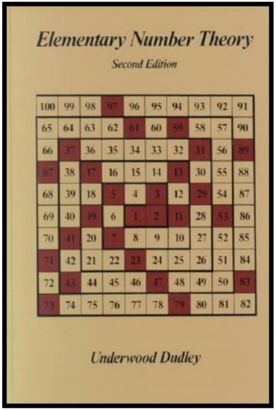
Elementary Number Theory

Section 1. Integers—Proofs of Theorems



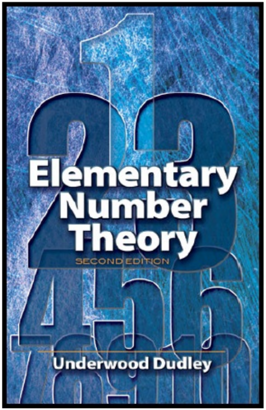


Table of contents

Lemma 1.1

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

Proof. By the definition of divisibility, $d \mid a$ implies that there is integer q such that $dq = a$, and $d \mid b$ implies that there is integer r such that $dr = b$. So (by the distributive property)

$$a + b = dq + db = d(q + b),$$

where $q + b$ is an integer. Hence, by the definition of divisibility again, $d \mid (a+b)$, as claimed. □

Lemma 1.1

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

Proof. By the definition of divisibility, $d \mid a$ implies that there is integer q such that $dq = a$, and $d \mid b$ implies that there is integer r such that $dr = b$. So (by the distributive property)

$$a + b = dq + db = d(q + b),$$

where $q + b$ is an integer. Hence, by the definition of divisibility again, $d \mid (a+b)$, as claimed. $\square$

Lemma 1.2

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

Proof. By the definition of divisiblity, there are integers $q_1, q_2, \ldots, q_n$ such that $a_1 = dq_1$, $a_2 = dq_2$, ...,$a_n = dq_n$. So (by the distributive property)

$$c_1 a_1 + c_2 a_2 + \cdots + c_n a_n = c_1 dq_1 + c_2 dq_2 + \cdots c_n dq_n$$

$$= d(c_1 q_1 + c_2 q_2 + \cdots + c_n q_n),$$

where $c_1 q_1 + c_2 q_2 + \cdots + c_n q_n$ is an integer. Hence, by the definition of divisibility again, $d \mid (c_1 a_1 + c_2 a_2 + \cdots + c_n a_n)$, as claimed. □

Lemma 1.2

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

Proof. By the definition of divisiblity, there are integers $q_1, q_2, \ldots, q_n$ such that $a_1 = dq_1$, $a_2 = dq_2$, ...,$a_n = dq_n$. So (by the distributive property)

$$c_1a_1 + c_2a_2 + \cdots + c_na_n = c_1dq_1 + c_2dq_2 + \cdots c_ndq_n$$

$$= d(c_1q_1 + c_2q_2 + \cdots + c_nq_n),$$

where $c_1q_1 + c_2q_2 + \cdots + c_nq_n$ is an integer. Hence, by the definition of divisibility again, $d \mid (c_1a_1 + c_2a_2 + \cdots + c_na_n)$, as claimed. □

Theorem 1.1

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

Proof. Since $(a, b) = d$ then d divides a and so a/d is an integer. Similarly, since $(a, b) = d$ then d divides b and so b/d is an integer. Let c denote the greatest common divisor $c = (a/d, b/d)$. We want to show that $c = 1$.

Theorem 1.1

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

Proof. Since $(a, b) = d$ then d divides a and so a/d is an integer. Similarly, since $(a, b) = d$ then d divides b and so b/d is an integer. Let c denote the greatest common divisor $c = (a/d, b/d)$. We want to show that $c = 1$.

Since 1 is a divisor of every integer, then every greatest common divisor is at least 1; that is, $c \geq 1$. Since $c \mid (a/d)$ and $c \mid (b/d)$ then there are integers q and r such that $a/d = cq$ and $b/d = cr$. This is equivalent to the equations $(cd)q = a$ and $(cd)r = b$. So, by the definition of divisibility, cd is a divisor of both a and b. Therefore cd is less than or equal to the greatest common divisor of a and b, $d = (a, b)$. This $cd \leq d$. Since d is positive (being a greatest common divisor), this gives $c \leq 1$. Hence $c = (a/d, b/d) = 1$, as claimed. □

Theorem 1.1

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

Proof. Since $(a, b) = d$ then d divides a and so a/d is an integer. Similarly, since $(a, b) = d$ then d divides b and so b/d is an integer. Let c denote the greatest common divisor $c = (a/d, b/d)$. We want to show that $c = 1$.

Since 1 is a divisor of every integer, then every greatest common divisor is at least 1; that is, $c \geq 1$. Since $c \mid (a/d)$ and $c \mid (b/d)$ then there are integers q and r such that $a/d = cq$ and $b/d = cr$. This is equivalent to the equations $(cd)q = a$ and $(cd)r = b$. So, by the definition of divisibility, cd is a divisor of both a and b. Therefore cd is less than or equal to the greatest common divisor of a and b, $d = (a, b)$. This $cd \leq d$. Since d is positive (being a greatest common divisor), this gives $c \leq 1$. Hence $c = (a/d, b/d) = 1$, as claimed. $\square$

Theorem 1.2

Theorem 1.2. The Division Algorithm.
Given positive integers a and b, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

Proof. Consider the set of integers $A = \{a, a-b, a-2b, a-3b, \ldots\}$. Set A contains a subset of nonnegative integers which is nonempty (since a is positive by hypothesis) and bounded below by 0. By the Least-Integer Principle, A contains a least element, say $a - qb$ where q is an integer. Now $a - qb$ is nonnegative and it less than b (or else $a - (q+1)b$ would be a lesser nonnegative element of A, contradicting the minimality of $a - qb$). Let $r = a - bq$. The $0 \leq r < b$ and $a = bq + r$, as required. We now need to show that such q and r are unique.

Theorem 1.2

Theorem 1.2. The Division Algorithm.
Given positive integers a and b, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

Proof. Consider the set of integers $A = \{a, a-b, a-2b, a-3b, \ldots\}$. Set A contains a subset of nonnegative integers which is nonempty (since a is positive by hypothesis) and bounded below by 0. By the Least-Integer Principle, A contains a least element, say $a - qb$ where q is an integer. Now $a - qb$ is nonnegative and it less than b (or else $a - (q+1)b$ would be a lesser nonnegative element of A, contradicting the minimality of $a - qb$). Let $r = a - bq$. The $0 \leq r < b$ and $a = bq + r$, as required. We now need to show that such q and r are unique.

Suppose that q, r, q_1, and r_1 satisfy $a = bq + r = bq_1 + r_1$ with $0 \leq r < b$ and $0 \leq r_1 < b_1$. Then we have

$$0 = a - a = (bq + r) - (bq_1 + r_1) = b(q - q_1) + (r - r_1). \qquad (1)$$

Theorem 1.2

Theorem 1.2. The Division Algorithm.
Given positive integers a and b, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

Proof. Consider the set of integers $A = \{a, a - b, a - 2b, a - 3b, \ldots\}$. Set A contains a subset of nonnegative integers which is nonempty (since a is positive by hypothesis) and bounded below by 0. By the Least-Integer Principle, A contains a least element, say $a - qb$ where q is an integer. Now $a - qb$ is nonnegative and it less than b (or else $a - (q + 1)b$ would be a lesser nonnegative element of A, contradicting the minimality of $a - qb$). Let $r = a - bq$. The $0 \leq r < b$ and $a = bq + r$, as required. We now need to show that such q and r are unique.

Suppose that q, r, q_1, and r_1 satisfy $a = bq + r = bq_1 + r_1$ with $0 \leq r < b$ and $0 \leq r_1 < b_1$. Then we have

$$0 = a - a = (bq + r) - (bq_1 + r_1) = b(q - q_1) + (r - r_1). \qquad (1)$$

Theorem 1.2 (continued)

Theorem 1.2. The Division Algorithm.
Given positive integers a and b, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

Proof (continued). Then we have

$$0 = a - a = (bq + r) - (bq_1 + r_1) = b(q - q_1) + (r - r_1). \qquad (1)$$

Hence $r_1 - r = b(q - q_1)$, so that (by the definition of divisibility) $b \mid (r_1 - r)$. But since $0 \leq r < b$ (or, equivalently, $-b < r \leq 0$) and $0 \leq r_1 < b$ then we have

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

But the only multiple of b strictly between $-b$ and b is 0. Hence $r_1 - r = 0$ or $r = r_1$ and from (1) we have $q - q_1 = 0$ or $q = q_1$. Hence the numbers q and r are unique, as claimed. $\square$

Lemma 1.3

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

Proof. Let d be the greatest common divisor of a and b, $d = (a, b)$. Then d is a divisor of a and d is a divisor of b (that is, $d \mid a$ and $d \mid b$), so by Lemma 1.3 d is a divisor of $a - bq = r$ (that is, $d \mid r$). So d is a common divisor of b and r.

Lemma 1.3

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

Proof. Let d be the greatest common divisor of a and b, $d = (a, b)$. Then d is a divisor of a and d is a divisor of b (that is, $d \mid a$ and $d \mid b$), so by Lemma 1.3 d is a divisor of $a - bq = r$ (that is, $d \mid r$). So d is *a* common divisor of b and r.

Suppose that c is any common divisor of b and r, so that $c \mid b$ (and so $c \mid bq$) and $c \mid r$. Then, by Lemma 1.1, $c \mid bq + r$ or $c \mid a$. Hence c is a common divisor of a and b. Since d is the *greatest* common divisor of a and b, then $c \leq d$.

Lemma 1.3

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

Proof. Let d be the greatest common divisor of a and b, $d = (a, b)$. Then d is a divisor of a and d is a divisor of b (that is, $d \mid a$ and $d \mid b$), so by Lemma 1.3 d is a divisor of $a - bq = r$ (that is, $d \mid r$). So d is *a* common divisor of b and r.

Suppose that c is any common divisor of b and r, so that $c \mid b$ (and so $c \mid bq$) and $c \mid r$. Then, by Lemma 1.1, $c \mid bq + r$ or $c \mid a$. Hence c is a common divisor of a and b. Since d is the *greatest* common divisor of a and b, then $c \leq d$.

So d is (1) a common divisor of b and r, and (2) if c is a common divisor of b and r then $c \leq d$. Therefore (by definition) d is the greatest common divisor of b and r (that is, $d = (b, r)$), as claimed. □

Lemma 1.3

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

Proof. Let d be the greatest common divisor of a and b, $d = (a, b)$. Then d is a divisor of a and d is a divisor of b (that is, $d \mid a$ and $d \mid b$), so by Lemma 1.3 d is a divisor of $a - bq = r$ (that is, $d \mid r$). So d is *a* common divisor of b and r.

Suppose that c is any common divisor of b and r, so that $c \mid b$ (and so $c \mid bq$) and $c \mid r$. Then, by Lemma 1.1, $c \mid bq + r$ or $c \mid a$. Hence c is a common divisor of a and b. Since d is the *greatest* common divisor of a and b, then $c \leq d$.

So d is (1) a common divisor of b and r, and (2) if c is a common divisor of b and r then $c \leq d$. Therefore (by definition) d is the greatest common divisor of b and r (that is, $d = (b, r)$), as claimed. □

Theorem 1.3

Theorem 1.3. The Euclidean Algorithm.
If a and b are positive integers, $b \neq 0$, and

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

the for k large enough, say $k = t$, we have $r_{t-1} = r_t q_{t+1}$, and $(a, b) = r_t$.

Proof. Since the sequence of nonnegative integers $b > r > r_1 > r_2 > \cdots$ is bounded below, then it must contain a least element by the Least-Integer Principle. Since r_{i+1} is strictly less than r_i (and by The Division Algorithm [Theorem 1.2], if $r_i \neq 0$ then we can produce r_{i+1}) then the sequence must have a least element, say $r_{t+1} = 0$.

Theorem 1.3

Theorem 1.3. The Euclidean Algorithm.
If a and b are positive integers, $b \neq 0$, and

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

the for k large enough, say $k = t$, we have $r_{t-1} = r_t q_{t+1}$, and $(a, b) = r_t$.

Proof. Since the sequence of nonnegative integers $b > r > r_1 > r_2 > \cdots$ is bounded below, then it must contain a least element by the Least-Integer Principle. Since r_{i+1} is strictly less than r_i (and by The Division Algorithm [Theorem 1.2], if $r_i \neq 0$ then we can produce r_{i+1}) then the sequence must have a least element, say $r_{t+1} = 0$.

Theorem 1.3 (continued)

Theorem 1.3. The Euclidean Algorithm.
If a and b are positive integers, $b \neq 0$, and

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

the for k large enough, say $k = t$, we have $r_{t-1} = r_t q_{t+1}$, and $(a, b) = r_t$.

Proof (continued). Then we must have

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

and so $r_t \mid r_{t-1}$ or $(r_{t-1}, r_t) = r_t$. Applying Lemma 1.3 repeatedly we have

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

as claimed. □

Corollary 1.1

Corollary 1.1. If $d \mid ab$ and $(d, a) = 1$, then $d \mid b$.

Proof. Since d and a are relatively prime, then by Theorem 1.4 there are integers x and y such that $dx + ay = 1$. Therefore $b(dx + ay) = b$ or $d(bx) + (ab)y = b$. Since $d \mid d(bx)$ and $d \mid ab$ (by hypothesis; so we also have $d \mid (ab)y$) then by Lemma 1.1 $d \mid (d(bx) + (ab)y)$. That is, $d \mid b$, as claimed. □

Corollary 1.1

Corollary 1.1. If $d \mid ab$ and $(d, a) = 1$, then $d \mid b$.

Proof. Since d and a are relatively prime, then by Theorem 1.4 there are integers x and y such that $dx + ay = 1$. Therefore $b(dx + ay) = b$ or $d(bx) + (ab)y = b$. Since $d \mid d(bx)$ and $d \mid ab$ (by hypothesis; so we also have $d \mid (ab)y$) then by Lemma 1.1 $d \mid (d(bx) + (ab)y)$. That is, $d \mid b$, as claimed. □

Corollary 1.2

Corollary 1.2. Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$. Then $c \mid d$. That is, every common divisor of integers a and b is a divisor of the greatest common divisor of a and b.

Proof. By Theorem 1.4, there are integers x and y such that $ax + by = d$. Since $c \mid a$ and $c \mid b$ then $c \mid (ax)$ and $c \mid (by)$; hence, by Lemma 1.1 $c \mid (ax + by)$. Since $d = ax + by = d$, then $c \mid d$, as claimed. □

Corollary 1.2

Corollary 1.2. Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$. Then $c \mid d$. That is, every common divisor of integers a and b is a divisor of the greatest common divisor of a and b.

Proof. By Theorem 1.4, there are integers x and y such that $ax + by = d$. Since $c \mid a$ and $c \mid b$ then $c \mid (ax)$ and $c \mid (by)$; hence, by Lemma 1.1 $c \mid (ax + by)$. Since $d = ax + by = d$, then $c \mid d$, as claimed. □

Corollary 1.3

Corollary 1.3. If $a \mid m$, $b \mid m$, and $(a, b) = 1$, then $ab \mid m$.

Proof. Since $b \mid m$ then by the definition of divisibility, there is integer q such that $m = bq$. Now $a \mid m$, so $a \mid bq$. Next, $(a, b) = 1$ so by Corollary 1.1, $a \mid q$. Hence there is integer r such that $q = ar$, so that $m = bq = bar$. By the definition of divisibility, this implies that $ab \mid m$, as claimed. □

Corollary 1.3

Corollary 1.3. If $a \mid m$, $b \mid m$, and $(a, b) = 1$, then $ab \mid m$.

Proof. Since $b \mid m$ then by the definition of divisibility, there is integer q such that $m = bq$. Now $a \mid m$, so $a \mid bq$. Next, $(a, b) = 1$ so by Corollary 1.1, $a \mid q$. Hence there is integer r such that $q = ar$, so that $m = bq = bar$. By the definition of divisibility, this implies that $ab \mid m$, as claimed. □