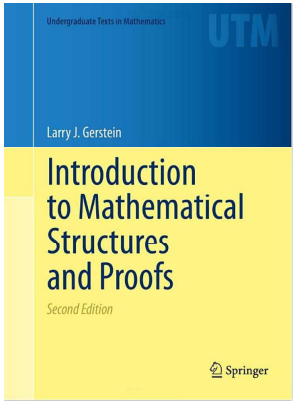
# Mathematical Reasoning

**Chapter 6. Number Theory**

6.3. Divisibility: The Fundamental Theorem of Arithmetic—Proofs of Theorems








## Theorem 6.15(a)

**Theorem 6.15.** Let $a, b, c \in \mathbb{Z}$. Then

(a) If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.

**Proof.** If $a \mid b$ and $b \neq 0$, then $b = ac$ for some $c \in \mathbb{Z}$ by Definition 6.13; notice that $c \neq 0$. Since $\in \mathbb{Z}$ and $c \neq 0$, then $|n| \geq 1$ and so by Theorem 6.2.A(c),

$$|b| = |ac| = |a|\,|c| \geq |a|,$$

as claimed. □





## Theorem 6.16 (Euclid)

**Theorem 6.16.** (Euclid, circa 300 BCE) There are infinitely many prime numbers.

**Proof.** We use the Principle of Induction and show that for every natural number $n$ there are at least $n$ prime numbers. For $n = 1$, we have that 2 is prime and the basis step is established. For the induction hypothesis, suppose $p_1, p_2, \ldots, p_k$ are $k \geq 1$ distinct primes. We need to show the existence of prime $p_{k+1}$ for the induction step. Consider the number $M = (p_1 p_2 \cdots p_k) + 1$. By Theorem 2.71, $M$ has a prime divisor $p$ so that $M = pq$ for some natural number $q$. ASSUME $p \in \{p_1, p_2, \ldots, p_k\}$, say $p = p_1$. But then $1 = M - p_1 p_2 \cdots p_k = p_1(q - p_2 p_3 \cdots p_k)$. But this implies that $p_1 \mid 1$, which is a CONTRADICTION to the fact that $p_1 > 1$. So the assumption that $p \in \{p_1, p_2, \ldots, p_k\}$ is false, and hence $\{p_1, p_2, \ldots, p_k, p_{k+1}\}$, where $p_{k+1} = p$, is a set of $k + 1$ prime numbers and the induction step holds. Therefore, by the Principle of Mathematical Induction, for each $n \in \mathbb{N}$ there is a prime number and (since the primes are distinct) there are infinitely many primes. □





## Theorem 6.17. Division Algorithm

**Theorem 6.17. Division Algorithm.**
Let $a, b \in \mathbb{Z}$, with $b > 0$. Then there are integers $q$ and $r$ such that $a = bq + r$ and $0 \leq r < b$. Moreover, $q$ and $r$ are uniquely determined by these conditions. Here, $q$ is the *quotient* and $r$ is the *remainder*.

**Proof.** Let $bq$ be the largest multiple of $b$ not exceeding $a$. Then we have $bq \leq a < b(q + 1)$. Define $r = a - bq$, so that $0 \leq r = a - bq < b(q + 1) - bq = b$, as claimed.

To show that $r$ is unique, suppose that $a = bq + r$ and $a = bq_1 + r_1$, with $0 \leq r < b$ and $0 \leq r_1 < b$. This implies $b(q - q_1) = r_1 - r$, and we see that $b \mid (r_1 - r)$. Since $0 \leq r < b$ and $0 \leq r_1 < b$, then the farthest $r$ and $_1$ can be is $b - 1$; that is, $|r - r_1| \leq b - 1 < b$. But $b \mid (r_1 - r)$ and $r_1 - r \neq 0$ implies $|b| \leq |r_1 - r|$ by Theorem 6.15(a), so we cannot have $r_1 - r \neq 0$. That is, $r_1 = r$ and we now have that the remainder is unique, as claimed. □

## Theorem 6.20

**Theorem 6.20.** If $a$ and $b$ are integers, not both 0, then $a$ and $b$ have a unique greatest common divisor.

**Proof.** Consider the set $L = \{xa + yb \mid x, y \in \mathbb{Z}\}$. Set $L$ contains, for example, all integer multiples of $a$ and $b$ so that $L$ contains some positive integers. Let $d$ be the least positive integer in $L$; say $d = x_1a + y_1b$, with $x_1, y_1 \in \mathbb{Z}$. ASSUME $d \nmid a$. Then by the Division Algorithm (Theorem 6.17) there are integers $q$ and $r$ such that $a = dq + r$ where $0 < r < d$. But then

$$r = a - dq = a - (x_1a + y_1b)q = (1 - x_1q)a + (-y_1q)b \in L,$$

a CONTRADICTION since $r < d$ and $d$ is the smallest positive integer in $L$. So the assumption that $d \nmid a$ is false and hence $d \mid a$. The same argument applies to $b$ to deduce that $d \mid b$ so that $d$ is a common divisor of $a$ and $b$.





## Theorem 6.20 (continued)

**Theorem 6.20.** If $a$ and $b$ are integers, not both 0, then $a$ and $b$ have a unique greatest common divisor.

**Proof (continued).** Now suppose $d'$ is any common divisor of $a$ and $b$; say $a = d'a_1$ and $b = d'b_1$. Then

$$d = x_1a + y_1b = x_1d'a_1 + y_1d'b_1 = d'(x_1a_1 + y_1b_1)$$

and so $d' \mid d$. Thus $d$ is a *greatest* common divisor of $a$ and $b$.

For uniqueness, suppose $d$ and $d_1$ are both greatest common divisors for $a$ and $b$. Then $d_1 \mid d$ (since $d$ is a greatest common divisor) and $d \mid d_1$ (since $d_1$ si a greatest common divisor). By Theorem 6.15(a), we have $|d| = |d_1|$. But by definition (Definition 6.18), both $d$ and $d_1$ are positive so that $d = d_1$. Therefore the greatest common divisor of $a$ and $b$ is unique. □





## Lemma 6.22

**Lemma 6.22.** If $a = bq + r$ then $(a, b) = (b, r)$.

**Proof.** Let $d = (a, b)$. A divisor of $a$ and $b$ is also a divisor of $bq$ and so, by Theorem 6.15(b), is a divisor of $r = a - bq$. Since $d = (a, b)$ divides both $a$ and $b$, then $d \mid r$ and hence $d \mid (b, r)$ (by Definition 6.18 of common divisor). That is, $(a, b) \mid (b, r)$.

Let $d' = (b, r)$. A divisor of $b$ and $r$ is also a divisor of $bq$ and so, by Theorem 6.15(b), is a divisor of $a = bq + r$. Since $d' = (b, r)$ divides both $b$ and $r$, then $d' \mid a$ and hence $d' \mid (a, b)$. That is, $(b, r) \mid (a, b)$. Combining these two results, we have $(a, b) = (b, r)$, as claimed. □





## Theorem 6.26

**Theorem 6.26.** Let $p$ be a prime number and let $a$ and $b$ be integers. Then the following implication holds: If $p \mid ab$ then either $p \mid a$ or $p \mid b$.

**Proof.** Suppose that $p \mid ab$. If $p \mid a$ and $p \mid b$ then the result holds, so we can assume without loss of generality that $p \nmid a$ or $p \nmid b$; say $p \nmid a$.

For $p \nmid a$ we must have $(p, a) = 1$ since the only positive divisors of prime $p$ are 1 and $p$. By Corollary 6.21 there are integers $x$ and $y$ such that $xp + ya = 1$. So $b = b \cdot 1 = b(xp + ya) = p(xb) + (ab)y$ and since $p \mid ab$ then $p \mid (p(xb) + (ab)y$ (by Theorem 6.15(b)); that is, $p \mid b$.

We have shown that if $p \nmid a$ then $p \mid b$. So we can conclude that either $p \mid a$ or $p \mid b$, as claimed. □

## Corollary 6.28

**Corollary 6.28.** Let $m$ be an integer greater than 1. Then $m$ is prime if and only if the following implication holds for all $a, b \in \mathbb{Z}$: If $m \mid ab$ then either $m \mid a$ or $m \mid b$.

**Proof.** With the hypothesis that $m$ is prime, the claim holds by Theorem 6.26.

We consider the contrapositive of the converse and and suppose that $m$ is *not* prime. Then there are integers $a$ and $b$ with $1 < a < m$ and $1 < b < m$ such that $m = ab$. So $m \mid ab$ (D'uh!) but $m \nmid a$ and $m \nmid b$ (that is, neither $m \mid a$ nor $m \mid b$), as claimed. □





## Theorem 6.29. The Fundamental Theorem of Arithmetic

**Theorem 6.29. The Fundamental Theorem of Arithmetic.** Let $n$ be an integer greater than 1. Then there are prime numbers $p_1, p_2, \ldots, p_r$ such that $n = p_1 p_2 \cdots p_r$. Moreover, this factorization of $n$ is unique in the following sense: If $n = q_1 q_2 \cdots q_s$ also, with the $q$'s prime, then the $q$'s are just a rearrangement of the $p$'s. That is, $r = s$ and, if we label the primes so that $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $p_i = q_i$ for $1 \leq i \leq r$.

**Proof.** The fact that such a prime factorization exists is addressed in Theorem 2.71 in Section 2.10. Mathematical Induction and Recursion So we only need to show uniqueness.

We give an inductive proof on positive integer $n$ itself. Suppose $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ with the $p$'s and $q$'s prime and $p_1 \leq p_2 \leq \cdots \leq p_r$. If $n = 2$ then $n = p_1 = q_1 = 2$, establishing the basis case. For the induction hypothesis, assume that $n > 2$ and that the theorem holds for all integers $t$ satisfying $2 \leq t \leq n - 1$.





## Theorem 6.29. Fundamental Theorem of Arithmetic (cont)

**Theorem 6.29. The Fundamental Theorem of Arithmetic.** Let $n$ be an integer greater than 1. Then there are prime numbers $p_1, p_2, \ldots, p_r$ such that $n = p_1 p_2 \cdots p_r$. Moreover, this factorization of $n$ is unique in the following sense: If $n = q_1 q_2 \cdots q_s$ also, with the $q$'s prime, then the $q$'s are just a rearrangement of the $p$'s.

**Proof (continued).** Since $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, we have $p \mid q_1 q_2 \ldots q_s$ so that by Corollary 6.27 $p_1 \mid q_i$ for some $i$. By a change of subscripts on the $q$'s (if necessary), we can suppose that $p_1 \mid q_1$. But $q_1$ is prime and $p_1 \neq 1$, so we have $p_1 = q_1$. So by the Cancellation Law (Theorem 6.9(c)) we have $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$. Now $p_2 p_3 \cdots p_r < n$, so by the induction hypothesis we have that $r - 1 = s - 1$ (and so $r = s$) and (assuming without loss of generality that $q_2 \leq q_3 \leq \cdots \leq q_r$), we have $p_i = q_i$ for $2 \leq i \leq r$. That is, $r = s$ and $p_i = q_i$ for $1 \leq i \leq r$; so the induction step holds. Therefore, by the Principle of Mathematical Induction, the result holds for all $n > 1$, as claimed. □





## Corollary 6.30

**Corollary 6.30.** Let $n \in \mathbb{Z}$ with $|n| \geq 2$. Then $n$ has a unique factorization of the form $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ where $t \geq 1$, the $p_i$ are distinct primes satisfying $p_1 \leq p_2 \leq \cdots \leq p_t$, and $\alpha_i \geq 1$ for $1 \leq i \leq t$.

**Proof.** Notice that $|n| > 1$. So by the Fundamental Theorem of Arithmetic (Theorem 6.29), there is a unique factorization of $|n|$ into a product of primes of the form $|n| = q_1 q_2 \cdots q_s$ where $q_1 \leq q_2 \leq \cdots \leq q_s$ (unique in the sense stated in Theorem 6.29). Denote the least of $q_1, q_2, \ldots, q_s$ as $p_1$ and let $\alpha_1$ be the number of times $p_1$ appears in the list $q_1, q_2, \ldots, q_s$. Let $p_2$ be the second least of $q_1, q_2, \ldots, q_s$ and let $\alpha_2$ be the number of times $p_2$ appears in the list. Similarly, let $p_i$ be the $i$th least of $q_1, q_2, \ldots, q_s$ and let $\alpha_i$ be the number of times $p_i$ appears in the list. Since the list is finite, then this process ends at some $p_t$ (the greatest of $q_1, q_2, \ldots, q_s$). We then have that $|n| = q_1 q_2 \cdots q_s = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$. So if $n > 1$ then $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, and if $n < -1$ then $n = -p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, as claimed. □

## Theorem 6.31

**Theorem 6.31.** The real number $\sqrt{2}$ is irrational.

**Proof.** ASSUME that $\sqrt{2}$ is rational, so that $\sqrt{2} = a/b$for some positive integers $a$ and $b$. Notice that by factoring $a$ and $b$ into primes using the Fundamental Theorem of Arithmetic (Theorem 6.29) and removing any common prime factors, we can assume that the greatest common divisor $(a, b) = 1$. We have $\sqrt{2}b = a$ so that, squaring both sides, $2b^2 = a^2$. Therefore $2 \mid a^2$. By Theorem 6.26, this implies $2 \mid a$ so that $a = 2m$ for some $m \in \mathbb{Z}$. But then $2b^2 = 4m^2$ or $b^2 = 2m^2$. Therefore $2 \mid b$. But then 2 is a common divisor $a$ and $b$, CONTRADICTING the fact that $(a, b) = 1$. So the assumption that $\sqrt{2}$ is rational is false, and hence $\sqrt{2}$ is irrational, as claimed. □





## Exercise 6.33

**Exercise 6.33.** Suppose $a$ and $b$ are integers such that for distinct primes $p_1, p_2, \ldots, p_t$, and integers $\alpha_i \geq 0$ and $\beta_i \geq 0$ for $1 \leq i \leq t$ we have $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$. Then

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_i^{\min\{\alpha_i, \beta_i\}} \cdots p_t^{\min\{\alpha_t, \beta_t\}}.$$

**Proof.** With $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$, we see that

$$p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_i^{\min\{\alpha_i, \beta_i\}} \cdots p_t^{\min\{\alpha_t, \beta_t\}}$$

is $a$ common divisor of $a$ and $b$ (since $p_i^k$ divides $p_i^\ell$ for any $k \leq \ell$). ASSUME there is a common divisor of $a$ and $b$ that is greater than this common divisor. Then its prime decomposition (given by the Fundamental Theorem of Arithmetic, Theorem 6.29) includes some additional prime factor $q$.





## Exercise 6.33 (continued)

**Exercise 6.33.** Suppose $a$ and $b$ are integers such that for distinct primes $p_1, p_2, \ldots, p_t$, and integers $\alpha_i \geq 0$ and $\beta_i \geq 0$ for $1 \leq i \leq t$ we have $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$. Then

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_i^{\min\{\alpha_i, \beta_i\}} \cdots p_t^{\min\{\alpha_t, \beta_t\}}.$$

**Proof (continued).** If $q$ is one of $p_1, p_2, \ldots, p_t$, then (when $q = p_i$) we have that $p_i^{\min\{\alpha_i, \beta_i\}+1}$ is a factor of both $a$ and $b$. But this is not a factor of $a$ when $\alpha_i = \min\{\alpha_i, \beta_i\}$ and this is not a factor of $b$ when $\beta_i = \min\{\alpha_i, \beta_i\}$; that is, $p_i^{\min\{\alpha_i, \beta_i\}+1}$ is not a common factor of $a$ and $b$, a CONTRADICTION. Next, if $q$ is some prime other than one of $p_1, p_2, \ldots, p_t$, then by Corollary 6.27 we have $q \mid p_i$ for some $1 \leq i \leq t$, a CONTRADICTION. So the assumption that there is a common divisor $a$ and $b$ greater than the common divisor

$$p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_i^{\min\{\alpha_i, \beta_i\}} \cdots p_t^{\min\{\alpha_t, \beta_t\}}$$

is false, and hence this is $(a, b)$, as claimed. □





## Theorem 6.35

**Theorem 6.35.** If $a$ and $b$ are nonzero integers, then $[a, b] = |ab|/(a, b)$.

**Proof.** By Corollary 6.30, we have for distinct primes $p_1, p_2, \ldots, p_t$ that $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$ for integers $\alpha_i \geq 0$ and $\beta_i \geq 0$, for $1 \leq i \leq t$ (for prime divisors of $a$ that are not divisors of $b$ make the corresponding exponents 0 in the representation of $b$, and vice versa for the prime divisors of $b$ that are not divisors of $a$). By Exercise 6.33,

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_i^{\min\{\alpha_i, \beta_i\}} \cdots p_t^{\min\{\alpha_t, \beta_t\}}.$$

By Note 6.3.A,

$$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_i^{\max\{\alpha_i, \beta_i\}} \cdots p_t^{\max\{\alpha_t, \beta_t\}}.$$

In the quotient $|ab|/(a, b)$, notice that the exponents $\alpha_i + \beta_i - \min\{\alpha_i, \beta_i\} = \max\{\alpha_i, \beta_i\}$ for $1 \leq i \leq t$. Therefore, this quotient equals $[a, b]$, as claimed. □