Lecture 8

Alex Hassett
Applied Analysis

June 4, 2025

Definition 8.1. If n and d are integers, then n is divisible by d if and only if n equals d times some integer and $d \neq 0$. The notation "$d \mid n$" is read "d divides n." Formally, let $n, d \in \mathbb{Z}$. Then

$$d \mid n \iff \exists k \in \mathbb{Z} \text{ such that } n = dk \text{ and } d \neq 0.$$

Note that the notation $d \nmid n$ is read "d does not divide n".

Theorem 8.2. If a positive integer a divides a positive integer b, then a is less than or equal to b. Formally,

$$\forall a, b \in \mathbb{Z}^+ (a \mid b \implies a \leq b).$$

Proof. By Definition 8.1, there exists a positive integer $k \in \mathbb{Z}^+$ such that $b = ak$. Since $k \in \mathbb{Z}^+$, we know that $k \geq 1$. Thus, we have

$$b = a \cdot k \geq a \cdot 1 = a$$

Therefore, $b \geq a$ or equivalently $a \leq b$. □

Theorem 8.3. The only divisors of 1 in $\mathbb{Z}$ are 1 and -1.

Proof. In the ring $\mathbb{Z}$ (see Theorem 8.31), an element $u \in \mathbb{Z}$ is called a *unit* if there exists $v \in \mathbb{Z}$ such that $u \cdot v = 1$. In other words, u is a unit if and only if u divides 1. Thus, the divisors of 1 in $\mathbb{Z}$ are precisely the units of $\mathbb{Z}$. It is a standard fact that the only units in $\mathbb{Z}$ are 1 and -1, since:

$$1 \cdot 1 = 1 \quad \text{and} \quad (-1) \cdot (-1) = 1,$$

while for any integer $|u| \geq 2$, the equation $u \cdot v = 1$ has no integer solution v. Therefore, the only divisors of 1 in $\mathbb{Z}$ are 1 and -1. □

Definition 8.4. An integer n is even if and only if n equals two times some integer k. Symbolically,

$$\forall n \in \mathbb{Z} (n \text{ is even} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k).$$

In other words, an integer n is even if and only if $2 \mid n$.

Definition 8.5. An integer n is odd if and only if n equals two times some integer k plus one. Symbolically,

$$\forall n \in \mathbb{Z} (n \text{ is odd} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k + 1).$$

Definition 8.6. An integer n is prime if and only if $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. Symbolically,

$$\forall n \in \mathbb{Z} (n \text{ is prime} \iff n > 1 \text{ and } \forall r, s \in \mathbb{Z}^+ (n = rs \implies \text{either } (r = 1 \text{ and } s = n) \text{ or } (r = n \text{ and } s = 1))).$$

In other words, n is prime if and only if it is only divisible by 1 and itself. Formally, a positive integer $p > 1$ is called *prime* if its only positive divisors are 1 and p; that is, if for any $d \in \mathbb{Z}^+$, $d \mid p$ implies $d = 1$ or $d = p$.

Definition 8.7. An integer n is composite if and only if $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$. Symbolically,

$$\forall n \in \mathbb{Z}(n \text{ is composite } \iff n > 1 \text{ and } \exists r, s \in \mathbb{Z}^+ \text{ such that } n = rs \text{ with } 1 < r < n \text{ and } 1 < s < n).$$

In other words, an integer n that is greater than 1 is composite if and only if it is not prime. Formally, a positive integer $n > 1$ is called *composite* if it is not prime; equivalently, if there exists an integer d such that $1 < d < n$ and $d \mid n$.

Definition 8.8. A real number r is rational if and only if it can be expressed as a quotient of two integers with a non-zero denominator. Symbolically,

$$\forall r \in \mathbb{R}(r \in \mathbb{Q} \iff \exists p, q \in \mathbb{Z} \text{ such that } r = \frac{p}{q} \text{ and } q \neq 0).$$

Note that $\mathbb{Q}$ is the set of the rational numbers.

Theorem 8.9. Divisibility is transitive; that is, for all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$. Then there exist integers $k, m \in \mathbb{Z}$ such that

$$b = a \cdot k, \quad c = b \cdot m.$$

Substituting $b = a \cdot k$ into the second equation, we have

$$c = (a \cdot k) \cdot m = a \cdot (km).$$

Since $k, m \in \mathbb{Z}$, it follows that $a \mid c$. □

Theorem 8.10. The Principle of Strong Induction is as follows: let $P(n)$ be a property defined for integers $n \geq n_0$. Suppose that

(i) $P(n_0)$ is true (base case), and

(ii) For all $k \geq n_0$, if $P(n_0), P(n_0 + 1), \ldots, P(k)$ are all true, then $P(k + 1)$ is true (induction step).

Then $P(n)$ is true for all $n \geq n_0$.

Proof. Define the set

$$S = \{n \geq n_0 \mid P(n) \text{ is true}\}.$$

We will prove that $S = \{n \in \mathbb{Z} \mid n \geq n_0\}$.

Base case. By assumption, $P(n_0)$ is true, so $n_0 \in S$.

Induction step. Suppose $n \geq n_0$ and assume that $n_0, n_0 + 1, \ldots, n$ are all in S (that is, $P(n_0), \ldots, P(n)$ are true). Then by assumption (ii), $P(n + 1)$ is true, so $n + 1 \in S$.

Thus, by the theorem of induction (Theorem 4.24) on $n - n_0$, it follows that S contains all integers $n \geq n_0$. Therefore, $P(n)$ is true for all $n \geq n_0$. □

Definition 8.11. The *sign function* $\text{sign}(n)$ is defined for $n \in \mathbb{Z} \setminus \{0\}$ by

$$\text{sign}(n) = \begin{cases} 1, & n > 0, \\ -1, & n < 0. \end{cases}$$

Theorem 8.12. The Quotient-Remainder Theorem is stated as follows: let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

The integer q is called the *quotient*, and r is called the *remainder*. Note that the Quotient-Remainder Theorem (also called the Division Algorithm) implies that if an integer n is divisible by an integer d the possible remainders are $0, 1, 2, \ldots, (d - 1)$. Thus, n can be written in one of the following forms:

$$dq, \quad dq + 1, \quad dq + 2, \quad \ldots, \quad dq + (d - 1)$$

for some integer q.

Proof. To prove existence, consider the set

$$S = \{a - bq \in \mathbb{Z} \mid q \in \mathbb{Z},\ a - bq \geq 0\}.$$

Since $b \neq 0$, the set S is nonempty (for large enough q, $a - bq$ will be negative, and for small enough q, it will be positive). Thus S contains some non-negative integers. By the well-ordering theorem (Theorem 7.22), S has a least element; we call it r. Then there exists some $q \in \mathbb{Z}$ such that

$$r = a - bq, \quad \text{with } r \geq 0.$$

Thus, we have

$$a = bq + r.$$

We now show that $r < |b|$. Suppose, for contradiction, that $r \geq |b|$. Then

$$r - |b| \geq 0.$$

Now consider

$$r - b \cdot \text{sign}(b) = (a - bq) - b \cdot \text{sign}(b) = a - b(q + \text{sign}(b)).$$

This quantity belongs to S, and it is smaller than r — contradicting the minimality of r. Hence,

$$0 \leq r < |b|.$$

To prove uniqueness, suppose that

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|,$$

and

$$a = bq_2 + r_2, \quad 0 \leq r_2 < |b|.$$

Then subtracting both equations, we have

$$b(q_1 - q_2) = r_2 - r_1.$$

Thus

$$|r_2 - r_1| < |b|.$$

But $b(q_1 - q_2)$ is a multiple of b, so the right-hand side must be 0. Thus $r_1 = r_2$, and consequently $q_1 = q_2$. Therefore, the integers q and r are unique. □

Definition 8.13. Let $a, b \in \mathbb{Z}$, not both zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest positive integer d such that

$$d \mid a \quad \text{and} \quad d \mid b.$$

Theorem 8.14. Bezout's Identity is stated as follows: let $a, b \in \mathbb{Z}$, not both zero. Then there exist integers $x, y \in \mathbb{Z}$ such that

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

Proof. Consider the set

$$S = \{am + bn \in \mathbb{Z} \mid m, n \in \mathbb{Z},\ am + bn > 0\}.$$

Since S is a nonempty subset of the positive integers, by the well-ordering principle (Theorem 7.22), S has a least element; we call it d. Thus, $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$. We claim that $d = \gcd(a, b)$. First, we show that d divides both a and b. By Theorem 8.12, we write

$$a = qd + r, \quad 0 \leq r < d.$$

Then, we have

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

If $r > 0$, then $r \in S$ and $r < d$, which would contradict the fact that d is the smallest positive element of S. Hence $r = 0$, so $d \mid a$. Similarly, applying the same argument to b, we find $d \mid b$. Therefore d is a common divisor of a and b. Now let c be any common divisor of a and b. Then $c \mid a$ and $c \mid b$, so we have

$$c \mid (ax_0 + by_0) = d.$$

Thus, by Theorem 8.2, d is the greatest common divisor of a and b, and we have expressed it as

$$\gcd(a, b) = ax_0 + by_0.$$

□

Lemma 8.15. Euclid's Lemma is stated as follows: let p be a prime number, and let $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Since p is prime, the only positive divisors of p are 1 and p. Thus, $\gcd(p, a)$ is either p or 1.

Case 1. If $\gcd(p, a) = p$, then $p \mid a$, and we are done.

Case 2. If $\gcd(p, a) = 1$, then by Bezout's identity (Theorem 8.14), there exist integers x, y such that

$$px + ay = 1.$$

Multiplying both sides by b, we have

$$pbx + aby = b.$$

Since $p \mid pbx$ and $p \mid ab$ (by assumption), it follows that p divides the left-hand side of this equation. Thus, $p \mid b$. Therefore, in either case, $p \mid a$ or $p \mid b$. □

Remark 8.16. Here we provide a less number-theoretic proof of Euclid's Lemma.

Proof. We proceed by strong induction on b.

Base case. $b = 1$. Then $ab = a \cdot 1 = a$. Thus, $p \mid ab$ implies $p \mid a$, so the lemma holds.

Induction step. Suppose the lemma holds for all positive integers less than b, where $b > 1$. Then applying Theorem 8.12, we have

$$b = pq + r, \quad 0 \leq r < p.$$

Multiplying a and b, we have

$$ab = a(pq + r) = p(aq) + ar.$$

Since $p \mid ab$ and $p \mid p(aq)$, it follows that $p \mid ar$.

Case 1. If $r = 0$, then $b = pq$, so $p \mid b$ and we are done.

Case 2. If $r > 0$, then $r < p \leq b$, so by the induction hypothesis (since $r < b$), we conclude that $p \mid a$ or $p \mid r$. If $p \mid r$, then $p \mid b$ since $b = pq + r$. Thus, in all cases, $p \mid a$ or $p \mid b$.

Therefore, by strong induction (Theorem 8.10), the lemma holds for all $b \in \mathbb{Z}^+$. □

Theorem 8.17. Every integer is either even or odd, and no integer is both.

Proof. By Theorem 8.12, we have that for any $n \in \mathbb{Z}$, there exist unique integers q, r such that

$$n = 2q + r, \quad \text{where } r = 0 \text{ or } r = 1.$$

If $r = 0$, then $n = 2q$, so n is even. If $r = 1$, then $n = 2q + 1$, so n is odd. Since Theorem 8.12 guarantees that this representation is unique, no integer can be both even and odd. Therefore, every integer is either even or odd, and no integer is both. □

Theorem 8.18. The Fundamental Theorem of Arithmetic is stated as follows: every integer $n > 1$ can be written as a product of prime numbers, and this factorization is unique up to the order of the factors.

Proof. We prove the theorem in two parts: *existence* and *uniqueness*. To prove existence we use strong induction on $n > 1$.

Base case. $n = 2$. Since 2 is prime, the statement holds.

Induction step. Suppose that every integer k with $2 \leq k \leq n$ can be factored into primes. Then consider $n + 1$. If $n + 1$ is prime, it is its own prime factorization. If $n + 1$ is composite, then $n + 1 = ab$ with $2 \leq a, b \leq n$. By the induction hypothesis, both a and b have prime factorizations. Thus, $n + 1$ is the product of those primes.

Therefore, by strong induction, every $n > 1$ has a prime factorization. We now prove that the prime factorization of n is unique up to order. Suppose

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m, \tag{1}$$

where each p_i and q_j is prime. We proceed by induction on n.

Base case: $n = 2$. Then $n = 2$ is prime, so the factorization is unique.

Induction step. Suppose that uniqueness holds for all integers $2 \leq k < n$. Since $p_1 \mid q_1 q_2 \ldots q_m$, by Euclid's Lemma (Theorem 8.15), we have $p_1 \mid q_j$ for some j. But since q_j is prime, it follows that $p_1 = q_j$. Cancelling p_1 and q_j from both sides of equation (1), we have

$$\frac{n}{p_1} = \prod_{i \neq 1} p_i = \prod_{t \neq j} q_t.$$

By the induction hypothesis, the remaining products of primes are equal up to order. Therefore, by Theorem 4.24, the prime factorization of n is unique up to order. □

Definition 8.19. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. The *integer quotient* of a divided by b, denoted $\operatorname{div}(a, b)$, is the unique integer q such that

$$a = bq + r, \quad 0 \leq r < |b|,$$

where r is the remainder from Theorem 8.12.

Definition 8.20. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then the *remainder* of a modulo b, denoted $\operatorname{mod}(a, b)$ or $a \bmod b$, is the unique integer r such that

$$a = bq + r, \quad 0 \leq r < |b|,$$

where $q = \operatorname{div}(a, b)$ is the integer quotient from Theorem 8.12.

Theorem 8.21. Every integer $n > 1$ is divisible by a prime.

Proof. We use strong induction on n.

Base case. $n = 2$. Since 2 is prime, 2 is divisible by itself.

Induction step. Suppose that every integer k with $2 \leq k \leq n$ is divisible by a prime. Then consider $n+1$. If $n + 1$ is prime, then it is divisible by itself. If $n + 1$ is composite, then, by Definition 8.7, there exists an integer d such that $1 < d < n + 1$ and $d \mid (n + 1)$. By the induction hypothesis, d is divisible by a prime p. Then $p \mid d$ and $d \mid (n + 1)$, so by transitivity of divisibility (Theorem 8.9), we have $p \mid (n + 1)$.

Therefore, by strong induction (Theorem 8.10), every integer $n > 1$ is divisible by a prime. □

Definition 8.22. A real number $x \in \mathbb{R}$ is called *irrational* if it is not a rational number; that is, if there do not exist integers $p, q \in \mathbb{Z}$ with $q \neq 0$ such that

$$x = \frac{p}{q}.$$

Theorem 8.23. The sum of any irrational number and any rational number is irrational.

Proof. Let $x \in \mathbb{R}$ be irrational, and let $r \in \mathbb{Q}$ be rational. Suppose, for contradiction, that $x + r$ is rational. Then there exist integers p, q with $q \neq 0$ such that

$$x + r = \frac{p}{q}.$$

Rearranging, we have

$$x = \frac{p}{q} - r.$$

Since $\frac{p}{q} \in \mathbb{Q}$ and $r \in \mathbb{Q}$, their difference is rational. Thus, x would be rational — contradicting the assumption that x is irrational. Therefore, $x + r$ must be irrational. □

Definition 8.24. Let $A \subseteq \mathbb{R}$ and suppose $A \neq \emptyset$. An element $M \in A$ is called the *maximum* of A if

$$\forall x \in A, \quad x \leq M.$$

If such an element exists, it is denoted by $\max A$.

Definition 8.25. Let $A \subseteq \mathbb{R}$ and suppose $A \neq \emptyset$. An element $m \in A$ is called the *minimum* of A if

$$\forall x \in A, \quad m \leq x.$$

If such an element exists, it is denoted by $\min A$.

Definition 8.26. The *floor function* (operator) assigns to each real number $x \in \mathbb{R}$ the greatest integer less than or equal to x. It is denoted by $\lfloor x \rfloor$, and is defined by

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

Definition 8.27. The *ceiling function* (operator) assigns to each real number $x \in \mathbb{R}$ the smallest integer greater than or equal to x. It is denoted by $\lceil x \rceil$, and is defined by

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid n \geq x\}.$$

Remark 8.28. The following definitions/theorems are provided simply for completeness as rings were used in the proof of Theorem 8.3.

Definition 8.29. A *semigroup* is a set S equipped with a binary operation $\cdot : S \times S \to S$ such that

(i) (Associativity) For all $a, b, c \in S$,
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Definition 8.30. A *ring* is a set R equipped with two binary operations, called *addition* $(+)$ and *multiplication* $(\cdot)$, such that the following properties hold:

(i) $(R, +)$ is an abelian group.
   (a) (Associativity) For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$.
   (b) (Identity element) There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
   (c) (Inverses) For all $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.
   (d) (Commutativity) For all $a, b \in R$, $a + b = b + a$.

(ii) $(R, \cdot)$ is a semigroup.
   (a) (Associativity) For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii) (Distributive laws) Multiplication distributes over addition.
   (a) For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

(b) For all $a, b, c \in R$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

If, in addition, there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$, then R is called a *ring with unity*, and 1 is called the *multiplicative identity* of R. If the multiplication is also commutative, that is, $a \cdot b = b \cdot a$ for all $a, b \in R$, then R is called a *commutative ring*.

Theorem 8.31. The set of integers $\mathbb{Z}$, equipped with the usual operations of addition and multiplication, forms a ring.

Proof. We verify the ring axioms one by one.

(i) $(\mathbb{Z}, +)$ is an abelian group.

(a) (Associativity of addition) For all $a, b, c \in \mathbb{Z}$,

$$(a + b) + c = a + (b + c).$$

This holds because addition of integers is associative.

(b) (Identity element for addition) The integer $0 \in \mathbb{Z}$ satisfies

$$a + 0 = a = 0 + a, \quad \text{for all } a \in \mathbb{Z}.$$

(c) (Additive inverses) For each $a \in \mathbb{Z}$, the integer $-a \in \mathbb{Z}$ satisfies

$$a + (-a) = 0.$$

(d) (Commutativity of addition) For all $a, b \in \mathbb{Z}$,

$$a + b = b + a.$$

(ii) $(\mathbb{Z}, \cdot)$ is a semigroup.

(a) (Associativity of multiplication) For all $a, b, c \in \mathbb{Z}$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

This holds because multiplication of integers is associative.

(iii) Distributive laws.

(a) For all $a, b, c \in \mathbb{Z}$,

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

(b) For all $a, b, c \in \mathbb{Z}$,

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

All of the above properties hold because they follow directly from the standard arithmetic properties of addition and multiplication of integers, which are proven in the construction of $\mathbb{Z}$ (see Definition 6.13). Therefore, $\mathbb{Z}$ satisfies all the axioms of a ring. □