Math 208: Discrete Mathematics
Lesson 11: Lecture Video Notes

Topics

20. The integers
    (a) integer operations
    (b) order properties
21. The *divides* relation and primes
    (a) properties of *divides*
    (b) prime numbers
    (c) division algorithm for integers

Readings: Chapters 20-21

§20. The integers

The integers, denoted $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, have a surprising amount of structure and properties which serve as a basis for an area of mathematics called *number theory*. One central topic in number theory is the study of divisibility and factorization into primes. This leads to careful examination of the *divides* relation and powerful results such as the Fundamental Theorem of Arithmetic.

Let's begin with an overview of properties of $\mathbb{Z}$.

20a. Integer operations

From a first glance, the integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ are merely a set of a numbers. Things get more interesting by noticing that addition and multiplication are two binary operations on $\mathbb{Z}$ with many nice properties.

Defn. A *binary operation* $*$ on a set S is a function $* : S \times S \to S$. Typically, the value or *product under* $*$ is written as $a * b$ where $a, b \in S$ (instead of $*(a, b)$).

Examples of binary operations.

- Addition $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. E.g. $2 + (-9) = -7$
- Multiplication $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. E.g. $2 \cdot (-9) = -18$
- Define $*$ on $\mathbb{Z}$ by $a * b = 2a - b$. E.g. $2 * (-9) = 2(2) - (-9) = 13$
- Let $S = \mathcal{P}(\{a, b, c\})$. Then intersection and union are binary operations on S.

Properties of addition and multiplication on $\mathbb{Z}$

1. **Closure of addition and multiplication**:

   $$\forall a, b \in \mathbb{Z},\ a + b \in \mathbb{Z} \text{ and } a \cdot b \in \mathbb{Z}$$

   When two integers are added or multiplied, the result is another integer. Note the integers are not closed under division. E.g. $1 \div 2 = \frac{1}{2} \notin \mathbb{Z}$.

2. **Addition and multiplication are commutative**:

   $$\forall a, b \in \mathbb{Z},\ a + b = b + a \text{ and } a \cdot b = b \cdot a$$

   The order two integers are added or multiplied does not affect the final value.

3. **Addition and multiplication are associative**:

   $$\forall a, b, c \in \mathbb{Z},\ (a + b) + c = a + (b + c) \text{ and } (ab)c = a(bc)$$

   When three integers are added or multiplied, we get the same result by performing the operation on the first two and then the third as when performing the operation of the last two and then the first.

4. **Additive identity**:
$$\forall a \in \mathbb{Z},\ 0 + a = a = a + 0$$
There is an integer 0 called the additive identity which added to any integer a results in the integer a again.

5. **Addition inverse**:
$$\forall a \in \mathbb{Z},\ \exists b \in \mathbb{Z} \text{ such that } a + b = 0 = b + a$$
Given an integer a, there exists an integer b such that $a + b = 0$. Usually, we write $-a$ for b and say $-a$ is the *additive inverse* of a.

6. **Multiplicative identity**:
$$\forall a \in \mathbb{Z},\ 1 \cdot a = a = a \cdot 1$$
There is an integer 1 called the multiplicative identity which multiplied to any integer a results in the integer a again.

7. **Multiplication distributes over addition**:
$$\forall a, b, c \in \mathbb{Z},\ a(b + c) = ab + ac$$

From these basic properties, many other familiar results can be derived.

Integer cancellation law. For integers a, b, c, if $a + c = b + c$, then $a = b$.

Proof.

Theorem. For any integer a, we have $0a = 0$.

Proof.

Remark. Abstract algebra studies algebraic structures which generalize properties of the integers. A set with a binary operation which is closed, associative, has an identity, and contains inverses is called a *group*. For example, bijective functions on the set S are a group under the binary operation of function composition. A set with two binary operations with properties such as $\mathbb{Z}$ is called a *commutative ring with (multiplicative) identity*.

20b. Order properties
The integers $\mathbb{Z}$ also admit an order relation where aRb iff $a \leq b$. This relation on $\mathbb{Z}$ is:

- reflexive
- antisymmetric
- transitive

Notation The expression $b \geq a$ means the same as $a \leq b$. Also, $a < b$ and $b > a$ are shorthand ways to say $a \leq b$ and $a \neq b$.

Trichotomy Law. For each $a \in \mathbb{Z}$, exactly one of the following holds:

- $a > 0$
- $a = 0$
- $a < 0$

Thm. The following properties hold for the relation $\leq$ on $\mathbb{Z}$:

(i) If $a < b$, then $a + c < b + c$ for all $c \in \mathbb{Z}$.

(ii) If $a < b$ and $c > 0$, then $ac < bc$.

(iii) If $a < b$ and $c < 0$, then $ac > bc$.

Ex. Prove that if $a > 0$ and $b > 0$, then $ab > 0$.

Well Ordering Principle for $\mathbb{Z}$: Every nonempty subset of positive integers has a least element.

Remark. The Well Ordering Principle for $\mathbb{Z}$ is often referred to by saying the set of positive integers is *well-ordered*. The well ordering property of $\mathbb{Z}$ is critical for justifying the logic behind proofs by induction.

§21. The *divides* relation and primes

Defn. Let a and b be integers. We say that a *divides* b and write $a|b$ if there exists an integer c such that $b = ac$.

Ex. True or False:

(a) $5|(-15)$

(b) $2|5$

Note. Think of the *divides* relation as a true/false statement. So, either $a|b$ or $a \not|ertb$. Statements such as $(-3)|18 = -6$ are nonsense!

Remarks. The following are equivalent sayings:

- a divides b
- a is a divisor of b
- a is a factor of b
- b is a multiple of a

21a. Properties of *divides*

We list several basic facts about the *divides* relation for $\mathbb{Z}$.

Thm. For $a, b, c \in \mathbb{Z}$, we have

(1) $a|0$

(2) $\pm 1|a$

(3) If $a|b$, then $-a|b$

(4) If $a|b$ and $b|c$, then $a|c$. Thus *divides* is a transitive relation on $\mathbb{Z}$.

(5) $a|(-a)$

(6) If $a|b$ and $b \neq 0$, then $0 < |a| \leq |b|$

(7) If $a|1$, then $a = \pm 1$

(8) If $a|b$ and $b|a$, then $a = \pm b$

(9) If $a|b$ and $a|c$, then $a|(mb + nc)$ for all $m, n \in \mathbb{Z}$.

(10) If $a|b$, then $a|bc$ for all $c \in \mathbb{Z}$

Proof of (1). We show that $a|0$ for all $a \in \mathbb{Z}$.

Proof of (3). We show that if $a|b$ then $(-a)|b$.

Defn. Let $b, c \in \mathbb{Z}$. We say the expression $mb + nc$ for some $m, n \in \mathbb{Z}$ is a *linear combination* of b and c.

Proof of (9). Prove that if $a|b$ and $a|c$, then $a|(mb + nc)$ for all $m, n \in \mathbb{Z}$.

21b. Prime numbers

Intuitively a prime number is an integer which cannot be factored in a meaningful way. Let's make this notion more precise.

Defn. A positive integer $n > 1$ is *prime* if its only positive divisors are 1 and n. If $n > 1$ is not prime, then it is said to be *composite*.

Caution. The number 1 is not prime since by definition requires a prime number p to satisfy $p > 1$ by definition.

Ex. Prime or composite:

(i) 19

(ii) 21

Prime numbers and factorization play key roles in an area of mathematics called number theory. In cryptography (a sub-area of number theory), it is useful to have methods to classify large positive integers as prime or composites. This is known as *prime testing*.

Let n be a large positive integer.

Prime testing: attempt 1. Trial divide n by $2, 3, 4, \ldots, n-1$. If we find a divisor, then n is composite. If not, n is prime.

Ex. Let $n = 29$. Then trial divide 29 by $2, 3, 4, 5, \ldots, 28$. None are divisors, so $n = 29$ is prime.

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

Pf. Let $n > 1$ be given. Consider the set $D = \{a \in \mathbb{Z} \mid a > 1 \text{ and } a|n\}$, so D is the set of all integers greater than 1 that divide n. Let m be the smallest element of D. (Why does m exist?)

We claim m is a prime.

Prime testing: attempt 2. Trial divide n by all primes p with $p < n$.

Ex. Let $n = 29$. The trial divide 29 by $2, 3, 5, 7, 11, 13, 17, 19, 23$. None are divisors, so $n = 29$ is prime.

The next result improves the prime testing procedure further.

Thm. Every composite number n has a divisor a with

$$2 \leq a \leq \sqrt{n}.$$

Pf.

Upshot. If we haven't found a divisor for n by the time we reach $\sqrt{n}$ on our list, then n must be a prime.

Prime testing: attempt 3. Trial divide n by all primes p with $p < \sqrt{n}$.

Ex. Let $n = 29$. Then $\sqrt{29} \approx 5.39$ The trial divide 29 by $2, 3,$ and 5. None are divisors, so $n = 29$ is prime.

The Sieve of Eratosthenes. A procedure to make a list of all primes.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Remark. The Sieve of Eratosthenes was developed by Greek mathematicians.

One more important property of prime numbers is:

Thm. The set of prime integers is infinite.

Pf. (Euclid)

21c. The division algorithm for integers

The Division Algorithm for Integers. If $a, d \in \mathbb{Z}$ with $d > 0$, then there exists unique integers q and r with $a = qd + r$ and $0 \leq r < d$. The integers q and r are called the *quotient* and *remainder* respectively.

Ex. Find the quotient and remainder for the following (if possible):

(i) 26 divided by 7

(ii) -26 divided by 7

(iii) 0 divided by 7

(iv) 26 divided by 0

Note. The *divisor* d in the division algorithm is positive. The *dividend* a can be any integer.

Pf. Consider the set $S = \{a - nd \mid n \in \mathbb{Z}, \text{ and } a - nd \geq 0\}$.