Lecture 1: Basic Concepts in Number Theory

Lecture 1

Objectives

By the end of this lecture you should be able to understand basic concepts of number theory such as:

1. Divisibility and Remainders
2. Divisibility Tests
3. Congruence Relations
4. Modular arithmetic

Outline

Formal Definition

Definition

If $a, b \in \mathbb{Z}$, $b \neq 0$, then a is divisible by b (or b divides a) denoted by $b \mid a$ if there is an integer $k \in \mathbb{Z}$ such that $a = b \times k$

- b is called a factor of a
- a is called a multiple of b
- If b does not divide a, we denote it by $b \nmid a$
- Intuition: assume we have a objects, and we want to split them into groups of size b. This is possible iff $b|a$. The resulting number of groups is k.

Examples

- $a = 20$ is divisible by $b = 4$ since we can pick $k = 5$ such that $a = 15 = 4 \times 5 = b \times k$
- $a = 12$ is divisible by $b = -4$ since we can pick $k = -3$ such that $a = 12 = (-4) \times (-3) = b \times k$
- $a = -24$ is divisible by $b = -6$ since we can pick $k = 4$ such that $a = -24 = (-6) \times 4 = b \times k$
- $a = 15$ is not divisible by $b = 4$ since there is no integer k such that $a = 15 = 4 \times k$

Properties of Division

Theorem

Let $a, b, c \in \mathbb{Z}$

- *If* $c \mid a$ *and* $c \mid b$*, then* $c \mid a \pm b$
- *If* $a \mid b$*, then* $a \mid bc$
- *If* $a \mid b$ *and* $b \mid c$*, then* $a \mid c$
- *If* $a \mid b$ *and* $a \mid c$*, then* $a \mid (mb + nc)$ *for* $m, n \in \mathbb{Z}$

Division with Remainders

Division over integers is not always possible, but we can generalize it.

Theorem

Assume $b \in \mathbb{Z}^+$ is a positive integer. The result of the division of a by b with a remainder is a pair of integers (q, r). q is called the quotient and r is called the remainder such that

$$a = q \times b + r, \quad \text{and} \quad 0 \leq r < b$$

- If $r = 0$, then b divides a.
- Intuition: we would like to split a objects $(a > 0)$ into groups of size b, and we form the groups one by one. There might be some objects left in the end not enough for the new group. The number of the remaining objects is r and the number of groups is q.

Problem

Theorem

Prove that the remainder r satisfies $0 \leq r < b$

Proof.

Take $q = \lfloor a/b \rfloor$ and $r = a - qb$. We need to show that $0 \leq r < d$.

$$a/b - 1 < \lfloor a/b \rfloor \leq a/b$$

$$a - b < \lfloor a/b \rfloor b \leq a$$

$$a - a \leq a - \lfloor a/b \rfloor b < a - (a - b)$$

$$0 \leq r < b$$

□

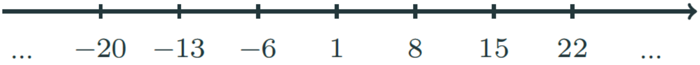
Examples

Let's consider some examples

- $a = 15, b = 4$, then $15 = 3 \times 4 + 3$ and $q = 3, r = 3$
- $a = -13, b = 3$, then $-13 = (-5) \times 3 + 2$ and $q = -5, r = 2$
- $a = 12, b = 4$, then $12 = 3 \times 4 + 0$ and $q = 3, r = 0$, i.e., $4 \mid 12$

Example on Division with Remainder

- How do numbers that give the remainder 1 when divided by 7 look like?
- They have the form $a = q \times 7 + 1$ for $q \in \{..., -3, -2, -1, 0, 1, 2, ...\}$
- for $q = 0$, we have $a = 1$
- for $q > 0$, we have $a = 8, 15, 22, ...$
- for $q < 0$, we have $a = -6, -12, -20, ...$
- Each 7th number on the line has a remainder 1



- All these numbers are equivalent in the sense that they give the same remainder when divided by 7.

General Division with Remainder

- In general, consider the numbers that give remainder r when divided by b
- They have the form $a = q \times b + r$ for $q \in \{..., -3, -2, -1, 0, 1, 2, ...\}$
- for $q = 0$, we have $a = r$
- for $q > 0$, we have $a = r + b, r + 2b, r + 3b, ...$
- for $q < 0$, we have $a = r - b, r - 2b, r - 3b, ...$
- Each bth number on the line has a remainder r

Intuition of Division with Remainders

$a = q \times b + r$, and $0 \leq r < b$

- form groups of a objects one by one until we are left with the amount that is not enough for the new group. The number of groups is q and the number of remaining objects is r
- More formally: subtract b from a recursively until the result is a positive number less than b; the result is the remainder r and the number of subtractions is q
- What if a is negative? Just add b instead of subtracting and stop when the result is a positive number less than b

Connection to Divisibility

Lemma

Integers a_1 and a_2 have the same remainder when divided by b iff $a_1 - a_2$ is divisible by b, i.e., $b \mid (a_1 - a_2)$

Proof.

$\Rightarrow$

- Assume a_1 and a_2 have the same remainder r, i.e.,
  $a_1 = q_1 \times b + r$
  $a_2 = q_2 \times b + r$
- Then $a_1 - a_2 = (q_1 - q_2) \times b$ and $b \mid (a_1 - a_2)$

$\square$

Connection to Divisibility

Lemma

Integers a_1 and a_2 have the same remainder when divided by b iff $a_1 - a_2$ is divisible by b, i.e., $b \mid (a_1 - a_2)$

Proof.

$\Leftarrow$

- Assume $b \mid (a_1 - a_2)$
- Then $a_1 - a_2 = k \times b$
- Assume a_2 has a remainder r when divided by b
- i.e., $a_2 = q_2 \times b + r$
- Then $a_1 = a_2 + k \times b = (q_2 + k) \times b + r$
- Then a_1 has the same remainder r like a_2

$\square$

Division by 4

Problem

Assume a is not divisible by 2 (a is odd). What possible remainders can a have when divided by 4?

- There are four possible remainders when divide by 4: 0, 1, 2, 3
- Clearly, the remainder 0 is impossible: it means that $4 \mid a$, but then a is even
- Assume the remainder is 2, that is $a = 4 \times q + 2$
- But then a is even again, a contradiction
- Two other remainders are possible: $a = 1$, $a = 3$

Four Numbers

Problem

Is it true that for any four integers a, b, c, and d there are two of them whose difference is divisible by 3?

- Let's consider an example: 1, 100, 27, and 5
- $100 - 1 = 99$ is divisible by 3
- In fact it is always true!
- Key idea: there are 3 possible remainders when we divide by 3
- So two of four numbers must have the same remainder
- Their difference is divisible by 3

Division by 101

Problem

How many 3-digit non-negative numbers are there that have remainder 7 when divided by 101? Here we assume that 1-digit and 2-digit numbers are also 3-digit, they just start with 0

- All numbers with remainder 7 when divided by 101 have the form: $a = 7 + q \times 101$ for $q = ..., -2, -1, 0, 1, 2, ...$
- For $q < 0$, a is negative
- For $q = 0$, $a = 7 + 0 \times 101 = 7$
- For $q > 0$, the number a grows
- The last q such that a is still 3-digit is $q = 9$:
  $a = 7 + 9 \times 101 = 7 + 909 = 916$
- So there are 10 numbers: for q from 0 to 9

Divisibility by 10

Problem

What is the remainder and the quotient of 3756 when divided by 10?

- Using the decimal system:
- $3756 = 375 \times 10 + 6$
- So the remainder is 6 and the quotient is 375

Division by 10

In general, we have

Lemma

Suppose we divide a by 10 with a remainder. Then the remainder is the last digit of a and the quotient is the number formed by all digits of a except the last one

In particular, we have the following

Corollary

An integer a is divisible by 10 iff its last digit is 0

Divisibility by 5

Problem

Is 7347 divisible by 5?

- Using the decimal system
- $7347 = 7340 + 7 = 734 \times 10 + 7 = (734 \times 2) \times 5 + 5 + 2$
- So the remainder is 2 and 7347 is not divisible by 5

Divisibility by 5

Lemma

An integer a is divisible by 5 iff its last digit is 0 or 5

- Denote the last digit of a by b
- Then $a - b$ has the last digit 0
- Thus $a - b$ is divisible by 5
- This means a and b have the same reminder when divided by 5
- Out of all possible remainders when dividing by 10 $\{0,1,\ldots,9\}$, b has reminder 0 only if it is 0 or 5

Divisibility by 2

Similarly,

Lemma

An integer a is divisible by 2 iff its last digit is 0, 2, 4, 6 or 8

- Denote the last digit of a by b
- Then $a - b$ has the last digit 0 and is divisible by 2
- This means a and b have the same reminder when divided by 2
- Out of all possible remainders when dividing by 10 $\{0,1,\ldots,9\}$, b has reminder 0 only if it is 0, 2, 4, 6, or 8.

Outline

Modular Congruence

We need an easy way to say that 2 numbers a and b give the same remainder when divided by m.

Definition

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. We say that a is congruent to b modulo m, denoted $a \equiv b \pmod{m}$, if $m \mid (a - b)$.

Corollary

- *Congruence modulo m is an equivalence relation*
- $a \equiv b \pmod{m}$ *iff* $a \bmod m = b \bmod m$, *i.e., same remainder*
- $a \equiv b \pmod{m}$ *iff there exist* $k \in \mathbb{Z}$ *such that* $a = b + km$

Congruence Relations

Theorem

Let $a, b, c, d \in \mathbb{Z}$ *and* $m \in \mathbb{Z}^+$

1. *If* $a \equiv b \pmod{m}$, *then* $(a + c) \equiv (b + c) \pmod{m}$
2. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $(a + c) \equiv (b + d) \pmod{m}$
3. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$

Congruence Relations

Problem

What is the remainder of $14 + 41 + 20 + 13 + 29$ *when divided by 4?*

- We can find a remainder that is congruent to this sum
  $14 + 41 + 20 + 13 + 29 \equiv 2 + 1 + 0 + 1 + 1 \equiv 5 \equiv 1 \pmod 4$
- So, the remainder is 1

Problem

What is the remainder of $17 \times (12 \times 19 + 5) - 23$ *when divided by 3?*

- We can find a remainder that is congruent to this sum
  $2 \times (0 \times 1 + 2) - 2 \equiv 2 \pmod 3$
- For large numbers, we can use the remainders $\{-1, 0, 1\}$
  $-1 \times (0 \times 1 - 1) + 1 \equiv 2 \pmod 3$

Last Digits

Problem

What are the last two digits of the number 99^{99}*?*

- The number consisting of last two digits form a remainder after the division by 100
- So we are interested in the remainder after the division by 100
- Consider 99^{99} modulo 100
- Note that $99 \equiv -1 \pmod{100}$
- So $99^{99} \equiv (-1)^{99} \equiv -1 \equiv 99 \pmod{100}$
- So the remainder is 99

Divisibility by 3

Problem

Is the number 3475 *divisible by* 3

- We can compute the remainder after the division by 3: the number is divisible iff the remainder is 0
- Consider the decimal representation

$$3475 = 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$$

- Note that $10^k \equiv 1 \pmod 3 \ \forall\, k \geq 0$
- Therefore, we can find the remainder after division by 3 as

$$3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5 \equiv 3 + 4 + 7 + 5 \equiv 1 \pmod 3$$

- Therefore, 3475 is not divisible by 3

Divisibility by 3

- We can extend the following intermediate step

$$3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5 \equiv 3 + 4 + 7 + 5 \equiv 1 \pmod 3$$

Lemma

An integer a is congruent modulo 3 to the sum of its digits. In particular, a is divisible by 3 iff the sum of its digits is divisible by 3

Arithmetic Operations on Remainders

- Recall that any number is congruent to its remainder modulo m
- We can represent all numbers by their remainders
- Arithmetic operations preserve congruence
- We can create arithmetic operation tables for remainders

Modular Arithmetic Modulo 2

- Consider division of integers by 2.
- There are two possible remainders: 0 (Even) and 1 (Odd)
- Indeed, a is divisible by 2 iff $-a$ is divisible by 2

$+$	0	1
0	0	1
1	1	0

$-$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

- What is the remainder of $374 \times (419 + 267 \times 38) - 625$ when divided by 2?
- Substitute all numbers by remainders: $0 \times (1 + 1 \times 0) - 1 = 1$

Modular Addition Table Modulo 7

Consider addition modulo 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$10 \% 7 = 3$

Modular Multiplication Table Modulo 7

Consider multiplication modulo 7

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

6 x 4 = 24 % 7 =
21 + 3 = 3 :)

Arithmetic Operation on Remainders

- Using these tables we can perform modular computations: substitute all numbers in an arithmetic expression by their remainders and apply operations according to the tables
- Tables are also convenient to observe properties of operations

Modular Subtraction Modulo 7

- Suppose we have two numbers a and b. Is there x such that $a + x \equiv b \pmod 7$
- Yes, each row contains all possible remainders.
- a is the row and b is the target value; x is a column

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Modular Subtraction

- Given a and b, consider x such that $a + x \equiv b \pmod{7}$
- x exists for any module m
- x plays the role of modular $b - a$
- Existence of x is natural: we can just pick $b - a$ as an integer and consider the corresponding remainder

What about division? Does it always exist? It depends on m!

Modular Division Modulo 7

- Suppose we have a nonzero number a and number b. Is there x such that $a \times x \equiv b \pmod{7}$?
- Each nonzero row contains all possible remainders!
- a is the row and b is the target value; x is a column

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Division Modulo 7

- Given $a \neq 0$ and b consider x such that $a \times x \equiv b \pmod 7$
- We have seen that x exists in this case
- x plays the role of modular division $b/a \pmod 7$

Modular Division Modulo 6

- Consider multiplication modulo 6
- Rows corresponding to 2, 3 and 4 do not contain all remainders
- There is no x such that $3 \times x \equiv 1 \pmod{6}$

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Modular Division

- So what is going on? Why division works modulo 7 and does not work modulo 6?
- It turns out that the modular division requires careful thought
- We will discuss it further in this course

Primes and Composites

Definition

An integer $p > 1$ is prime if the only positive factors of p are 1 and p. Otherwise, p is a composite.

Theorem

If $n \in \mathbb{Z}^+$, then there is a unique increasing sequence $p_1, p_2, \ldots, p_m$ of primes such that $n = p1 \times p2 \times \ldots \times pm$. The sequence $p_1, p_2, \ldots, p_m$ is referred to as the prime factorization of n.

Properties

Theorem

Let $n \in \mathbb{Z}^+$

1. *If* $n = ab$, *then the prime factorization of* n *is the result of merging the prime factorizations of* a *and* b.
2. *If* p *is a prime,* $p \mid n$, *and* $p_1, p_2, \ldots, p_m$ *is the prime factorization of* n, *then* $p = p_i$, *for some* $1 \leq i \leq m$

Finding Prime Factors

Theorem

If n is a composite, then n has a prime factor less than or equal to $\sqrt{n}$

Proof.

Let $n = ab$.

- Assume $a > \sqrt{n}$ and $b > \sqrt{n}$. Hence, $ab > \sqrt{n}\sqrt{n} = n$ which is a contradiction
- Then, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, WLOG assume $a \leq \sqrt{n}$
- If a is prime, we are done.
- Else, a has a prime factor $p < a \leq \sqrt{n}$ which is also a prime factor on n

$\square$

Frame Title

Theorem

There are infinitely many primes.

Proof: Assume not

- Thus, there is some $m \in \mathbb{Z}$ such that primes form an increasing sequence $p_1, p_2, \ldots, p_m$
- Let $n = p_1 \times p_2 \times \ldots p_m + 1$
- Since $n > p_i \; \forall \; 1 \leq i \leq m$, then n is a composite
- Then, there is some p_j $(1 \leq j \leq m)$ such that $p_j | n$
- Since $p_j \,|\, p_1 \times p_2 \times \ldots p_m$, then $p_j \,|\, (n - p_1 \times p_2 \times \ldots p_m)$
- But $n - p_1 \times p_2 \times \ldots p_m = 1$ leading to a contradiction since we assumed $p_j > 1$ becasue they are primes