Numbers

- We are used to numbers and use them constantly

Numbers

- We are used to numbers and use them constantly
- But why do we have our numbers?

Numbers

- We are used to numbers and use them constantly
- But why do we have our numbers?
- It all starts with counting: 1, 2, 3, ...

pexels.com

Numbers

- We are used to numbers and use them constantly
- But why do we have our numbers?
- It all starts with counting: 1, 2, 3, ...
- Addition and multiplication are possible

pexels.com

Inverse operations

- But are inverse operations possible?

Inverse operations

- But are inverse operations possible?
- Subtraction is an inverse to addition:
  suppose we add 4 to 5: $5 + 4 = 9$
  we need to subtract 4 to get 5 from the result:
  $9 - 4 = 5$

Inverse operations

- But are inverse operations possible?
- Subtraction is an inverse to addition:
  suppose we add 4 to 5: $5 + 4 = 9$
  we need to subtract 4 to get 5 from the result:
  $9 - 4 = 5$
- Division is an inverse to multiplication:
  suppose we multiply 3 by 4: $3 \times 4 = 12$
  we need to divide the result by 4 to get 3 again:
  $12/4 = 3$

Inverse operations

- But are inverse operations possible?
- Subtraction is an inverse to addition:
  suppose we add 4 to 5: $5 + 4 = 9$
  we need to subtract 4 to get 5 from the result:
  $9 - 4 = 5$
- Division is an inverse to multiplication:
  suppose we multiply 3 by 4: $3 \times 4 = 12$
  we need to divide the result by 4 to get 3 again:
  $12/4 = 3$
- So, are these operations always applicable to numbers $1, 2, 3, \ldots$?

Integer Numbers

- Subtraction is not always possible
  cannot subtract 3 from 2: $2 - 3 = ?$

Integer Numbers

- Subtraction is not always possible
  cannot subtract 3 from 2: $2 - 3 = ?$
- Solution: negative numbers and zero

Integer Numbers

- Subtraction is not always possible
  cannot subtract 3 from 2: $2 - 3 = ?$
- Solution: negative numbers and zero
- Now we have integer numbers: $\ldots, -2, -1, 0, 1, 2, \ldots$

Integer Numbers

- Subtraction is not always possible
  cannot subtract 3 from 2: $2 - 3 = ?$
- Solution: negative numbers and zero
- Now we have integer numbers: $\ldots, -2, -1, 0, 1, 2, \ldots$
- Now subtraction is always possible:
  $2 - 3 = -1, -2 - 3 = -5, 3 - (-2) = 5$

Integer Numbers

- Subtraction is not always possible
  cannot subtract 3 from 2: $2 - 3 = ?$
- Solution: negative numbers and zero
- Now we have integer numbers: $\ldots, -2, -1, 0, 1, 2, \ldots$
- Now subtraction is always possible:
  $2 - 3 = -1, -2 - 3 = -5, 3 - (-2) = 5$
- Addition and multiplication can be extended to
  negative numbers:
  $-2 + 3 = 1, -2 + (-3) = -5, 2 + (-3) = -1$

Integer Numbers

- Now addition, subtraction and multiplication are possible

Integer Numbers

- Now addition, subtraction and multiplication are possible
- But division is not always possible: $3/2 = ?$

Integer Numbers

- Now addition, subtraction and multiplication are possible
- But division is not always possible: $3/2 = ?$
- Solution: rational numbers

Integer Numbers

- Now addition, subtraction and multiplication are possible
- But division is not always possible: $3/2 = ?$
- Solution: rational numbers
- But often it is important to have an integer answer

William Blake, The Judgment of Solomon

Number Theory

- Number theory: studies integers and operations on them

Number Theory

- Number theory: studies integers and operations on them
- Basics of number theory have natural applications

Number Theory

- Number theory: studies integers and operations on them
- Basics of number theory have natural applications
- Advanced number theory had not

Number Theory

- Number theory: studies integers and operations on them
- Basics of number theory have natural applications
- Advanced number theory had not
- This was stated explicitly (and praised) by top number theorists (Godfrey Hardy, Leonard Dickson)

Number Theory and Applications

- So number theory is useless?

Number Theory and Applications

- So number theory is useless?
- Not anymore!

Number Theory and Applications

- So number theory is useless?
- Not anymore!
- Donald Knuth: "...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations"

Number Theory and Applications

- So number theory is useless?
- Not anymore!
- Donald Knuth: "...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations"
- Even more, number theory is vital for the modern cryptography

Number Theory and Applications

- So number theory is useless?
- Not anymore!
- Donald Knuth: "...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations"
- Even more, number theory is vital for the modern cryptography
- Through cryptography it dramatically affects our life: email, messengers, online transactions, Internet as a whole, etc.

Divisibility

- What does it mean that $\frac{a}{b}$ is integer?

Divisibility

- What does it mean that $\frac{a}{b}$ is integer?
- It means that the denominator cancels out

Divisibility

- What does it mean that $\frac{a}{b}$ is integer?
- It means that the denominator cancels out
- That is, a can be represented as a product of two integers, b and some other integer k: $a = b \times k$; and then we have $\frac{a}{b} = \frac{b \times k}{b} = k$

Divisibility

- What does it mean that $\frac{a}{b}$ is integer?
- It means that the denominator cancels out
- That is, a can be represented as a product of two integers, b and some other integer k: $a = b \times k$; and then we have $\frac{a}{b} = \frac{b \times k}{b} = k$
- And this reformulation only use simple notions

Divisibility

- What does it mean that $\frac{a}{b}$ is integer?
- It means that the denominator cancels out
- That is, a can be represented as a product of two integers, b and some other integer k: $a = b \times k$; and then we have $\frac{a}{b} = \frac{b \times k}{b} = k$
- And this reformulation only use simple notions
- So, this is our formal definition of divisibility:

Divisibility

a is divisible by b (or b divides a) denoted by $b \mid a$ if there is an integer k such that $a = b \times k$

Divisibility

- What does it mean that $\frac{a}{b}$ is integer?
- It means that the denominator cancels out
- That is, a can be represented as a product of two integers, b and some other integer k: $a = b \times k$; and then we have $\frac{a}{b} = \frac{b \times k}{b} = k$
- And this reformulation only use simple notions
- So, this is our formal definition of divisibility:

Divisibility

a is divisible by b (or b divides a) denoted by $b \mid a$ if there is an integer k such that $a = b \times k$

- If b does not divide a we denote it by $b \nmid a$

Properties

- Why do we care about formal definitions if everything is trivial with specific numbers?

Properties

- Why do we care about formal definitions if everything is trivial with specific numbers?
- Formal definitions allow to prove general properties

Lemma

If c divides a and c divides b, then c divides $a \pm b$

Properties

- Why do we care about formal definitions if everything is trivial with specific numbers?
- Formal definitions allow to prove general properties

Lemma

If c divides a and c divides b, then c divides $a \pm b$

- Why is this true?

Properties

- Why do we care about formal definitions if everything is trivial with specific numbers?
- Formal definitions allow to prove general properties

Lemma

If c divides a and c divides b, then c divides $a \pm b$

- Why is this true?
- Since c divides a and b, then $a = c \times k_1$ and $b = c \times k_2$ for some k_1 and k_2

Properties

- Why do we care about formal definitions if everything is trivial with specific numbers?
- Formal definitions allow to prove general properties

Lemma

If c divides a and c divides b, then c divides $a \pm b$

- Why is this true?
- Since c divides a and b, then $a = c \times k_1$ and $b = c \times k_2$ for some k_1 and k_2
- Then $a \pm b = c \times k_1 \pm c \times k_2 = c \times (k_1 \pm k_2)$

Properties

- Why do we care about formal definitions if everything is trivial with specific numbers?
- Formal definitions allow to prove general properties

Lemma

If c divides a and c divides b, then c divides $a \pm b$

- Why is this true?
- Since c divides a and b, then $a = c \times k_1$ and $b = c \times k_2$ for some k_1 and k_2
- Then $a \pm b = c \times k_1 \pm c \times k_2 = c \times (k_1 \pm k_2)$
- So $a \pm b$ is divisible by c

Properties

Problem

Suppose $b \mid a$. Is it true that $b \mid 3a$?

Properties

Problem

Suppose $b \mid a$. Is it true that $b \mid 3a$?

- Yes, this is true

Properties

Problem

Suppose $b \mid a$. Is it true that $b \mid 3a$?

- Yes, this is true
- Indeed, since $b \mid a$ we have that $a = b \times k$ for some k

Properties

Problem

Suppose $b \mid a$. Is it true that $b \mid 3a$?

- Yes, this is true
- Indeed, since $b \mid a$ we have that $a = b \times k$ for some k
- So we have $3a = b \times (3k)$

Properties

Problem

Suppose $b \mid a$. Is it true that $b \mid 3a$?

- Yes, this is true
- Indeed, since $b \mid a$ we have that $a = b \times k$ for some k
- So we have $3a = b \times (3k)$
- So by definition $b \mid 3a$

Properties

More generally, we have

Lemma

If $b \mid a$, then for any integer c we have $b \mid (a \times c)$

Properties

More generally, we have

Lemma

If $b \mid a$, then for any integer c we have $b \mid (a \times c)$

- The proof is basically the same

Properties

More generally, we have

Lemma

If $b \mid a$, then for any integer c we have $b \mid (a \times c)$

- The proof is basically the same
- Indeed, since $b \mid a$ we have that $a = b \times k$ for some k

Properties

More generally, we have

Lemma

If $b \mid a$, then for any integer c we have $b \mid (a \times c)$

- The proof is basically the same
- Indeed, since $b \mid a$ we have that $a = b \times k$ for some k
- So we have $c \times a = b \times (c \times k)$

Properties

More generally, we have

Lemma

If $b \mid a$, then for any integer c we have $b \mid (a \times c)$

- The proof is basically the same
- Indeed, since $b \mid a$ we have that $a = b \times k$ for some k
- So we have $c \times a = b \times (c \times k)$
- So by definition $b \mid c \times a$

Division with Remainders

- So, division over integers is not always possible

Division with Remainders

- So, division over integers is not always possible
- But we can generalize it

Division with remainder

Suppose b is a positive integer. The result of the division of a by b with a remainder is a pair of integers, q called quotient and r called a remainder such that

$$a = q \times b + r$$

and $0 \leq r < b$

Division with Remainders

- So, division over integers is not always possible
- But we can generalize it

Division with remainder

Suppose b is a positive integer. The result of the division of a by b with a remainder is a pair of integers, q called quotient and r called a remainder such that

$$a = q \times b + r$$

and $0 \leq r < b$

If $r = 0$, then b divides a

Examples

Let's consider several examples

- $a = 15, b = 4$. Then $15 = 3 \times 4 + 3$ and $q = 3, r = 3$

Examples

Let's consider several 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 $q = -5, r = 2$

Examples

Let's consider several 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 $q = 3, r = 0$

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

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

- Indeed, suppose a_1 and a_2 have the same remainder r:
  $a_1 = q_1 \times b + r$
  $a_2 = q_2 \times b + r$

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

- Indeed, suppose a_1 and a_2 have the same remainder r:
  $a_1 = q_1 \times b + r$
  $a_2 = q_2 \times b + r$
- Then $a_1 - a_2 = q_1 \times b - q_2 \times b = (q_1 - q_2) \times b$ and $b \mid (a_1 - a_2)$

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

- In the other direction, suppose $b \mid (a_1 - a_2)$

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

- In the other direction, suppose $b \mid (a_1 - a_2)$
- Then $a_1 - a_2 = k \times b$

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

- In the other direction, suppose $b \mid (a_1 - a_2)$
- Then $a_1 - a_2 = k \times b$
- a_2 has some remainder when divided by b: $a_2 = q_1 \times b + r$, for $0 \leq r < b$

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

- In the other direction, suppose $b \mid (a_1 - a_2)$
- Then $a_1 - a_2 = k \times b$
- a_2 has some remainder when divided by b: $a_2 = q_1 \times b + r$, for $0 \leq r < b$
- Then $a_1 = a_2 + k \times b = (q_1 + k) \times b + r$ and a_1 has the same remainder

Summary

- Number theory studies integer numbers

Summary

- Number theory studies integer numbers
- Important for fast numerical computations

Summary

- Number theory studies integer numbers
- Important for fast numerical computations
- Vital for cryptography

Summary

- Number theory studies integer numbers
- Important for fast numerical computations
- Vital for cryptography
- We discussed basic notions: divisibility and remainders

Summary

- Number theory studies integer numbers
- Important for fast numerical computations
- Vital for cryptography
- We discussed basic notions: divisibility and remainders
- We will use them to build more advanced theory

Outline

Modular Arithmetic

Applications

Modular Subtraction and Division

Remainders

Problem

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

Remainders

Problem

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

- Do we need to compute the number to answer the question?

Remainders

Problem

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

- Do we need to compute the number to answer the question?
- Is there a better way?

Remainders

Problem

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

- Do we need to compute the number to answer the question?
- Is there a better way?
- It is helpful to study remainders more

Congruence Relations

Definition

We say that two numbers a and b are congruent modulo m if they have the same remainder when divided by m. We write

$a \equiv b \pmod{m}$

Congruence Relations

Definition

We say that two numbers a and b are congruent modulo m if they have the same remainder when divided by m. We write

$a \equiv b \pmod{m}$

- As we discussed, equivalently, $a \equiv b \pmod{m}$ iff $a - b$ is divisible by m

Congruence Relations

Definition

We say that two numbers a and b are congruent modulo m if they have the same remainder when divided by m. We write

$a \equiv b \pmod{m}$

- As we discussed, equivalently, $a \equiv b \pmod{m}$ iff $a - b$ is divisible by m
- Every number a is congruent modulo m to all numbers $a + k \times m$ for all integer k

Congruence Relations

Definition

We say that two numbers a and b are congruent modulo m if they have the same remainder when divided by m. We write

$a \equiv b \pmod{m}$

- As we discussed, equivalently, $a \equiv b \pmod{m}$ iff $a - b$ is divisible by m
- Every number a is congruent modulo m to all numbers $a + k \times m$ for all integer k
- In particular, if r is a remainder of a when divided by m, then $a \equiv r \pmod{m}$

Congruence Relations

Congruence relations has nice and convenient properties

Addition of constant

If $a \equiv b \pmod{m}$ then $a + c \equiv b + c \pmod{m}$ for any c

Congruence Relations

Congruence relations has nice and convenient properties

Addition of constant

If $a \equiv b \pmod{m}$ then $a + c \equiv b + c \pmod{m}$ for any c

- That is, if we add the same number to two congruent numbers, the results will also be congruent

Congruence Relations

Congruence relations has nice and convenient properties

Addition of constant

If $a \equiv b \pmod{m}$ then $a + c \equiv b + c \pmod{m}$ for any c

- That is, if we add the same number to two congruent numbers, the results will also be congruent
- Indeed, congruence of a and b modulo m means that $m \mid (a - b)$

Congruence Relations

Congruence relations has nice and convenient properties

Addition of constant

If $a \equiv b \pmod{m}$ then $a + c \equiv b + c \pmod{m}$ for any c

- That is, if we add the same number to two congruent numbers, the results will also be congruent
- Indeed, congruence of a and b modulo m means that $m \mid (a - b)$
- Note that $(a + c) - (b + c) = a - b$, so it is also divisible by m

Congruence Relations

The previous rule can be extended

Addition

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$a + c \equiv b + d \pmod{m}$

Congruence Relations

The previous rule can be extended

Addition

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$a + c \equiv b + d \pmod{m}$

- That is, congruence is preserved under addition

Congruence Relations

The previous rule can be extended

Addition

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$a + c \equiv b + d \pmod{m}$

- That is, congruence is preserved under addition
- The proof is simple now:
  $a + c \equiv a + d \equiv b + d \pmod{m}$

Congruence Relations

The previous rule can be extended

Addition

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$a + c \equiv b + d \pmod{m}$

- That is, congruence is preserved under addition
- The proof is simple now:
  $a + c \equiv a + d \equiv b + d \pmod{m}$
- Note that we just use the previous property twice:
  $a + c \equiv a + d \pmod{m}$,
  $a + d \equiv b + d \pmod{m}$
  are just additions of constants to congruent numbers

Congruence Relations

Problem

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

Congruence Relations

Problem

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

- We can apply our results

Congruence Relations

Problem

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

- We can apply our results
- We can find a remainder that is congruent to this sum:
  $14 + 41 + 20 + 13 + 29 \equiv 2 + 1 + 0 + 1 + 1$
  $\equiv 5 \equiv 1 \pmod 4$

Congruence Relations

Problem

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

- We can apply our results
- 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

Congruence Relations

Multiplication by a constant

If $a \equiv b \pmod{m}$ then $a \times c \equiv b \times c \pmod{m}$ for any c

Congruence Relations

Multiplication by a constant

If $a \equiv b \pmod{m}$ then $a \times c \equiv b \times c \pmod{m}$ for any c

- That is, if we multiply two congruent numbers by the same number, the results will also be congruent

Congruence Relations

Multiplication by a constant

If $a \equiv b \pmod{m}$ then $a \times c \equiv b \times c \pmod{m}$ for any c

- That is, if we multiply two congruent numbers by the same number, the results will also be congruent
- Indeed, congruence of a and b modulo m means that $m \mid (a - b)$

Congruence Relations

Multiplication by a constant

If $a \equiv b \pmod{m}$ then $a \times c \equiv b \times c \pmod{m}$ for any c

- That is, if we multiply two congruent numbers by the same number, the results will also be congruent
- Indeed, congruence of a and b modulo m means that $m \mid (a - b)$
- But then $m \mid c \times (a - b)$

Congruence Relations

The previous rule can be extended

Multiplication

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$a \times c \equiv b \times d \pmod{m}$

Congruence Relations

The previous rule can be extended

Multiplication

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$a \times c \equiv b \times d \pmod{m}$

- That is, congruence is preserved under multiplication

Congruence Relations

The previous rule can be extended

Multiplication

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$a \times c \equiv b \times d \pmod{m}$

- That is, congruence is preserved under multiplication
- The proof is just like for addition:
  $a \times c \equiv a \times d \equiv b \times d \pmod{m}$

Congruence Relations

The previous rule can be extended

Multiplication

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$a \times c \equiv b \times d \pmod{m}$

- That is, congruence is preserved under multiplication
- The proof is just like for addition:
  $a \times c \equiv a \times d \equiv b \times d \pmod{m}$
- Note that we just use the previous property twice:
  $a \times c \equiv a \times d \pmod{m}$,
  $a \times d \equiv b \times d \pmod{m}$
  are just multiplication of congruent numbers by constants

Remainders

Now we are ready to solve the problem from the beginning

Problem

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

- We can just look at this number modulo 3

Remainders

Now we are ready to solve the problem from the beginning

Problem

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

- We can just look at this number modulo 3
- Can substitute all numbers by their remainders $0, 1, 2$ and the remainder will remain the same:
  $2 \times (0 \times 1 + 2) - 2$

Remainders

Now we are ready to solve the problem from the beginning

Problem

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

- We can just look at this number modulo 3
- Can substitute all numbers by their remainders $0, 1, 2$ and the remainder will remain the same:
  $2 \times (0 \times 1 + 2) - 2$
- Additional idea: we can substitute numbers by $0, 1, -1$:
  $-1 \times (0 \times 1 - 1) + 1 \equiv 2 \pmod 3$

Outline

Modular Arithmetic

Applications

Modular Subtraction and Division

Last Digits

Problem

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

Last Digits

Problem

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

- The number itself is huge; it would be nice not to compute it

Last Digits

Problem

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

- The number itself is huge; it would be nice not to compute it
- We can use remainders

Last Digits

Problem

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

- The number itself is huge; it would be nice not to compute it
- We can use remainders
- The number consisting of last two digits form a remainder after the division by 100

Last Digits

Problem

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

- The number itself is huge; it would be nice not to compute it
- We can use remainders
- 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

Last Digits

Problem

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

- Consider 99^{99} modulo 100

Last Digits

Problem

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

- Consider 99^{99} modulo 100
- Note that $99 \equiv -1 \pmod{100}$

Last Digits

Problem

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

- Consider 99^{99} modulo 100
- Note that $99 \equiv -1 \pmod{100}$
- So $99^{99} \equiv (-1)^{99} \equiv -1 \equiv 99 \pmod{100}$

Last Digits

Problem

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

- 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?

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

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
- But how to compute the remainder?

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
- But how to compute the remainder?
- $3475 = 3000 + 400 + 70 + 5$
  $= 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$

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
- But how to compute the remainder?
- $3475 = 3000 + 400 + 70 + 5$
  $= 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$
- Now we can use modular arithmetic!

Divisibility by 3

Problem

Is the number 3475 divisible by 3?

- Note that $10 \equiv 1 \pmod{3}$

Divisibility by 3

Problem

Is the number 3475 divisible by 3?

- Note that $10 \equiv 1 \pmod{3}$
- Thus $10^k \equiv 1^k \equiv 1 \pmod{3}$

Divisibility by 3

Problem

Is the number 3475 divisible by 3?

- Note that $10 \equiv 1 \pmod 3$
- Thus $10^k \equiv 1^k \equiv 1 \pmod 3$
- So we have $3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$
  $\equiv 3 + 4 + 7 + 5 \pmod 3$

Divisibility by 3

Problem

Is the number 3475 divisible by 3?

- Note that $10 \equiv 1 \pmod 3$
- Thus $10^k \equiv 1^k \equiv 1 \pmod 3$
- So we have $3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5 \equiv 3 + 4 + 7 + 5 \pmod 3$
- Now $3 + 4 + 7 + 5 \equiv 19 \equiv 1 \pmod 3$

Divisibility by 3

Problem

Is the number 3475 divisible by 3?

- Note that $10 \equiv 1 \pmod 3$
- Thus $10^k \equiv 1^k \equiv 1 \pmod 3$
- So we have $3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5 \equiv 3 + 4 + 7 + 5 \pmod 3$
- Now $3 + 4 + 7 + 5 \equiv 19 \equiv 1 \pmod 3$
- So 3475 is not divisible by 3

Divisibility by 3

- Observe the following intermediate step in our solution:
  $3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$
  $\equiv 3 + 4 + 7 + 5 \pmod 3$

Divisibility by 3

- Observe the following intermediate step in our solution:
  $3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$
  $\equiv 3 + 4 + 7 + 5 \pmod 3$
- We have that $10^k \equiv 1 \pmod 3$ for all k

Divisibility by 3

- Observe the following intermediate step in our solution:
  $3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$
  $\equiv 3 + 4 + 7 + 5 \pmod 3$
- We have that $10^k \equiv 1 \pmod 3$ for all k
- So this step works for all numbers!

Divisibility by 3

- Observe the following intermediate step in our solution:
  $3475 \equiv 3 \times 10^3 + 4 \times 10^2 + 7 \times 10 + 5$
  $\equiv 3 + 4 + 7 + 5 \pmod 3$
- We have that $10^k \equiv 1 \pmod 3$ for all k
- So this step works for all numbers!

Divisibility by 3

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

Outline

Modular Arithmetic

Applications

Modular Subtraction and Division

Operations on Remainders

- Recall that any number is congruent to its remainder modulo m

Operations on Remainders

- Recall that any number is congruent to its remainder modulo m
- We can represent all numbers by their remainders

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

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 Addition Table

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

Modular Multiplication Table

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

Operations 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

Operations 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

- Suppose we have two numbers a and b. Is there x such that $a + x \equiv b \pmod 7$?

$+$	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

Modular Subtraction

- 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!

$+$	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

- 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 $a + x \equiv b \pmod{7}$

Modular Subtraction

- Given a and b consider x such that $a + x \equiv b \pmod{7}$
- x exists for any module m

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 $b - a$

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

Modular Division

- Suppose we have a nonzero number a and number b. Is there x such that $a \times x \equiv b \pmod 7$?

$\times$	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

Modular Division

- 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!

$\times$	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

- 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

- Given $a \neq 0$ and b consider x such that $a \times x \equiv b \pmod{7}$

Modular Division

- Given $a \neq 0$ and b consider x such that $a \times x \equiv b \pmod 7$
- We have seen that x exists

Modular Division

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

Modular Division

- Given $a \neq 0$ and b consider x such that $a \times x \equiv b \pmod 7$
- We have seen that x exists
- x plays the role of modular division b/a
- So everything is finally good and the construction of modular arithmetic is complete?

Modular Division

- Consider multiplication modulo 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

- Consider multiplication modulo 6
- Rows corresponding to $2, 3$ and 4 does not contain all remainders

$\times$	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

- Consider multiplication modulo 6
- Rows corresponding to $2, 3$ and 4 does 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?

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 is more complicated

Conclusion

- We have started with the simple notions: divisibility, remainders

Conclusion

- We have started with the simple notions: divisibility, remainders
- We then developed the basics of modular arithmetic

Conclusion

- We have started with the simple notions: divisibility, remainders
- We then developed the basics of modular arithmetic
- But things are complicated, we do not understand it completely yet

Conclusion

- We have started with the simple notions: divisibility, remainders
- We then developed the basics of modular arithmetic
- But things are complicated, we do not understand it completely yet
- Is it “bad” that things are complicated?

Conclusion

- We have started with the simple notions: divisibility, remainders
- We then developed the basics of modular arithmetic
- But things are complicated, we do not understand it completely yet
- Is it “bad” that things are complicated?
- In some sense, yes; we would like things to be simple to compute them

Conclusion

- We have started with the simple notions: divisibility, remainders
- We then developed the basics of modular arithmetic
- But things are complicated, we do not understand it completely yet
- Is it “bad” that things are complicated?
- In some sense, yes; we would like things to be simple to compute them
- But in come sense complicated is “good”

Conclusion

- We have started with the simple notions: divisibility, remainders
- We then developed the basics of modular arithmetic
- But things are complicated, we do not understand it completely yet
- Is it “bad” that things are complicated?
- In some sense, yes; we would like things to be simple to compute them
- But in come sense complicated is “good”
- Complicated things are crucial for cryptography