Modular Arithmetic

Vladimir Podolskii

Computer Science Department, Higher School of Economics

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 $3 \times x \equiv 1 \pmod 6$

×	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

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
- We will discuss it further in this course

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