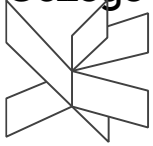


Gør tanke til handling

**VIA University
College**




Modular arithmetic

Intro to modular arithmetic

We'll start with an example:

Remember that we can e.g. write the remainder of 10 after division by 3 as $\text{rem}(10,3) = 1$. Let's consider what happens when we take the remainder of increasing numbers after division by 3:



$\text{rem}(0,3) = 0$	The number we are taking the remainder with respect to is called the modulus
$\text{rem}(1,3) = 1$	
$\text{rem}(2,3) = 2$	
$\text{rem}(3,3) = 0$	
$\text{rem}(4,3) = 1$	
$\text{rem}(5,3) = 2$	
$\text{rem}(6,3) = 0$	
\vdots	

Notice that only 3 different numbers occur (0, 1, and 2), and that there is a clear pattern: as the number on the left increases by 1 in each line, the remainders run through 0, 1, 2, 0, 1, 2 and so on.

Intro to modular arithmetic

In modular arithmetic, we **only** care about the remainder of numbers after division by some number, called the **modulus**. When the modulus is 3 (as in the last slide), any two numbers which have the same remainder after division by 3 are called **congruent** to each other. For example, 1 and 10 are congruent when the modulo is 3 because

$$\text{rem}(10,3) = \text{rem}(1,3).$$

We use a special version of the equality sign for showing that two numbers are congruent (i.e. have the same remainder) modulo some number:

$$10 \equiv 1 \pmod{3}$$

Example

How many different numbers are there modulo 5?

To figure this out, we can try to take the remainder of increasing numbers modulo 5, and see when the numbers start to repeat:

$$\text{rem}(0,5) = 0$$

$$\text{rem}(1,5) = 1$$

$$\text{rem}(2,5) = 2$$

$$\text{rem}(3,5) = 3$$

$$\text{rem}(4,5) = 4$$

$$\text{rem}(5,5) = 0$$

$$\text{rem}(6,5) = 1$$

$$\text{rem}(7,5) = 2$$

\vdots

We see that the numbers start to repeat after 4 – that means there are 5 different numbers modulo 5: 0, 1, 2, 3 and 4. All other numbers are congruent to one of these. For example,

$$29 \equiv 4 \pmod{5}, \quad 42 \equiv 2 \pmod{5} \quad \text{and} \quad 10935 \equiv 0 \pmod{5}$$

Negative numbers in modulo arithmetic

What is the remainder of -4 after division by 3 ? To figure this out, we can use the division algorithm:

The division algorithm

Given integers a and b , we can always find a "quotient" q and a "remainder" $\text{rem}(a, b)$ such that

$$a = q \cdot b + \text{rem}(a, b),$$

where $0 \leq \text{rem}(a, b) < b$.

Let's try to find out what q and $\text{rem}(a, b)$ should be when $a = -4$ and $b = 3$:

$$-4 = (-2) \cdot 3 + 2$$

This shows us that $q = -2$ and $\text{rem}(-4, 3) = 2$.

So

$$-4 \equiv 2 \pmod{3}.$$

Negative numbers in modulo arithmetic

An alternative way to figure out what a negative number is congruent to is to take yet another look at what happens to remainders when we gradually increase or decrease numbers. Let's again take a look at the pattern below:

$$\begin{array}{c} \vdots \\ \text{rem}(-4,3) = 2 \\ \text{rem}(-3,3) = 0 \\ \text{rem}(-2,3) = 1 \\ \text{rem}(-1,3) = 2 \\ \text{rem}(0,3) = 0 \\ \text{rem}(1,3) = 1 \\ \text{rem}(2,3) = 2 \\ \text{rem}(3,3) = 0 \\ \text{rem}(4,3) = 1 \\ \vdots \end{array}$$

and extend this **backwards**. This also shows you that

$$-4 \equiv 2 \pmod{3}.$$

Solving congruences

In many cases we would like to find x in expressions like

$$x - 3 \equiv 9 \pmod{4}$$

$$5 + x \equiv 0 \pmod{2}$$

$$3x \equiv 8 \pmod{10}$$

Doing this is called **solving the congruence**.

In the next slides, we will see what we can and cannot do in order to solve congruences.

Adding and subtracting

We can **add the same number** on each side of a congruence relation:

$$x - 3 \equiv 9 \pmod{4} \Rightarrow$$

$$x - 3 + 3 \equiv 9 + 3 \pmod{4} \Rightarrow$$

$$x \equiv 12 \pmod{4} \Rightarrow$$

$$x \equiv 0 \pmod{4}$$

We can also **subtract the same number** on each side of a congruence relation:

$$5 + x \equiv 0 \pmod{2} \Rightarrow$$

$$5 + x - 5 \equiv 0 - 5 \pmod{2} \Rightarrow$$

$$x \equiv -5 \pmod{2} \Rightarrow$$

$$x \equiv 1 \pmod{2}$$

Multiplying

We are also allowed to **multiply by the same number** on each side:

$$\begin{aligned} 3x &\equiv 8 \pmod{10} \Rightarrow \\ 7 \cdot 3x &\equiv 7 \cdot 8 \pmod{10} \Rightarrow \\ 21x &\equiv 56 \pmod{10} \end{aligned}$$


However, since there are no fractions, this alone does not allow us to solve congruences

Dividing?

In order to solve congruences like

$$5 \cdot x \equiv 3 \pmod{9},$$

it would be very convenient if we were also allowed to divide on both sides. So let's try:

$$x \equiv \frac{3}{5} \pmod{9}$$


Not allowed!

But a remainder of $\frac{3}{5}$ doesn't make any sense!

In the next slide, we will see how we **can** solve the equation above.

Dividing?

We would like to solve the congruence

$$5 \cdot x \equiv 3 \pmod{9}.$$

We can do that by noticing that $2 \cdot 5 = 10$, and $10 \equiv 1 \pmod{9}$. So by multiplying by 2 on each side, we get:

$$\begin{aligned} 5 \cdot x &\equiv 3 \pmod{9} \Rightarrow \\ 2 \cdot 5 \cdot x &\equiv 2 \cdot 3 \pmod{9} \Rightarrow \\ 10 \cdot x &\equiv 6 \pmod{9} \Rightarrow \\ 1 \cdot x &\equiv 6 \pmod{9} \Rightarrow \\ x &\equiv 6 \pmod{9} \end{aligned}$$

Since $2 \cdot 5 \equiv 1 \pmod{9}$, 2 is called **the multiplicative inverse** of 5 modulo 9.

The multiplicative inverse

In general:

To isolate x in an expression like

$$a \cdot x \equiv b \pmod{p},$$

We look for some number, c , such that

$$a \cdot c \equiv 1 \pmod{p},$$

because then

$$\begin{aligned} a \cdot x &\equiv b \pmod{p} \Rightarrow \\ c \cdot a \cdot x &\equiv c \cdot b \pmod{p} \Rightarrow \\ x &\equiv c \cdot b \pmod{p}. \end{aligned}$$

c is then called the **multiplicative inverse** of a .

Examples

Use multiplicative inverses to solve each of the congruences below:

Solve the congruence $5 \cdot x \equiv 6 \pmod{7}$:

Notice that $3 \cdot 5 = 15$ and $15 \equiv 1 \pmod{7}$. That means that 3 is the multiplicative inverse of 5 modulo 7. So

$$5 \cdot x \equiv 6 \pmod{7} \Rightarrow 3 \cdot 5 \cdot x \equiv 3 \cdot 6 \pmod{7} \Rightarrow x \equiv 18 \pmod{7} \Rightarrow x \equiv 4 \pmod{7}$$

Solve the congruence $3 \cdot x \equiv 2 \pmod{4}$:

Notice that $3 \cdot 3 = 9$ and $9 \equiv 1 \pmod{4}$. That means that 3 is its own multiplicative inverse modulo 4. So

$$3 \cdot x \equiv 2 \pmod{4} \Rightarrow 3 \cdot 3 \cdot x \equiv 3 \cdot 2 \pmod{4} \Rightarrow x \equiv 6 \pmod{4} \Rightarrow x \equiv 2 \pmod{4}$$

How to find the multiplicative inverse

We will meet three different ways of finding multiplicative inverses:

- 1) Guessing (as we did in the examples in the previous slides)
- 2) Using the Extended Euclidean Algorithms (EEA)
- 3) Using something called “Euler’s theorem”

Finding the multiplicative inverse with the EEA

Remember that we can always **use the Extended Euclidean Algorithm** to find s and t such that

$$\gcd(a, p) = s \cdot a + t \cdot p.$$

If a and p has $\gcd(a, p) = 1$, that means that we can find numbers s and t such that

$$1 = s \cdot a + t \cdot p \quad \Rightarrow \quad s \cdot a = 1 - t \cdot p$$

Taking the remainder after division by p on both sides, we get

$$\begin{aligned} s \cdot a &\equiv 1 - t \cdot p \pmod{p} \\ &\equiv 1 - t \cdot 0 \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

So s is the multiplicative inverse of a modulo p .

We will see an example in the next slide.

2) Finding the multiplicative inverse with EEA

Example: Find the multiplicative inverse of 7 modulo 19.

Solution:

$$\begin{aligned} \gcd(19, 7) &= \gcd(7, \text{rem}(19, 7)) & 5 &= 1 \cdot 19 - 2 \cdot 7 \\ &= \gcd(7, 5) = \gcd(5, \text{rem}(7, 5)) & 2 &= 1 \cdot 7 - 1 \cdot 5 \\ & & &= 1 \cdot 7 - 1 \cdot (1 \cdot 19 - 2 \cdot 7) \\ & & &= -1 \cdot 19 + 3 \cdot 7 \\ &= \gcd(5, 2) = \gcd(2, \text{rem}(5, 2)) & 1 &= 1 \cdot 5 - 2 \cdot 2 \\ &= \gcd(2, 1) = 1 & &= 1 \cdot (1 \cdot 19 - 2 \cdot 7) - 2 \cdot (-1 \cdot 19 + 3 \cdot 7) \\ & & &= 3 \cdot 19 - 8 \cdot 7 \end{aligned}$$

So $1 \equiv 3 \cdot 19 - 8 \cdot 7 \equiv 3 \cdot 0 - 8 \cdot 7 \equiv -8 \cdot 7 \pmod{19}$.

Therefore, -8 is the multiplicative inverse of 7 modulo 19.

Or, if we prefer a positive number: $-8 \equiv -8 + 0 \equiv -8 + 19 \equiv 11 \pmod{19}$.

Check: $7 \cdot 11 \equiv 77 \equiv 1 \pmod{19}$.

Note:

Not all numbers have multiplicative inverses

In the last slides, we saw how one can find the multiplicative inverse of a number by using the extended Euclidean algorithm. But we only considered cases where $\gcd(a, p) = 1$. What if that isn't the case?

It turns out that if the greatest common divisor is **not** equal to 1, it is not possible to find a multiplicative inverse. We will see an example of this in the next slide.

That means that **only numbers which are relatively prime to the modulus have a multiplicative inverse!**

Note:

Not all numbers have multiplicative inverses

Consider the congruence

$$2 \cdot x \equiv 1 \pmod{4}.$$

Let's try to find a value of x that solves this congruence. We know that there only are 4 different numbers modulo 4: 0, 1, 2 and 3, so we only have to check these:

$$x = 0: \quad 2 \cdot 0 \equiv 0 \not\equiv 1 \pmod{4}$$

$$x = 1: \quad 2 \cdot 1 \equiv 2 \not\equiv 1 \pmod{4}$$

$$x = 2: \quad 2 \cdot 2 \equiv 0 \not\equiv 1 \pmod{4}$$

$$x = 3: \quad 2 \cdot 3 \equiv 2 \not\equiv 1 \pmod{4}$$

We see that no value of x fulfills the congruence. This demonstrates that **2 does not have a multiplicative modulo 4**. This is because $\gcd(2,4) = 2 \neq 1$.

With this in mind, we are now ready to introduce “Euler’s theorem”, which will provide us with the third and last way of finding multiplicative inverses.

Euler's theorem

If a and n are relatively prime positive integers, with $n \geq 2$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Euler's φ – function.

Remember: $\varphi(n)$ counts how many numbers between 1 and n that are relatively prime to n .



Leonhard Euler (1707-1783)

3) Finding the multiplicative inverse with Euler's theorem

If a and n are relatively prime positive integers, with $n \geq 2$, then
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

It follows that $a^{\varphi(n)-1} \cdot a \equiv 1 \pmod{n}$



$a^{\varphi(n)-1}$ is the multiplicative inverse of a .



Leonhard Euler (1707-1783)

Finding the multiplicative inverse using Euler's theorem

Example:

Find the multiplicative inverse of 2 modulo 7.

Solution:

According to Euler's theorem, we can find the multiplicative inverse of 2 modulo 7 as $2^{\varphi(7)-1} = 2^{6-1} = 2^5$. Let's calculate this:

$$2^5 = 32 \equiv 4 \pmod{7}.$$

So 4 is the multiplicative inverse of 2 modulo 7.

Let's check the result: $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Gør tanke til handling

**VIA University
College**

Exponentiation in modular arithmetic

Modular exponentiation

Modular arithmetic is used heavily in cryptography:

A secret message is encrypted by translating it to a number, and then raising this number to some power modulo a third number. The exact procedure is beyond the scope of this course (but if you are interested, you can see this weeks challenge exercise).

It is therefore relevant to be able to calculate exponents modulo some number – this is called **modular exponentiation**. In the following slides, we will see one way to do this.

Modular exponentiation

Assume we want to calculate the number
 $3^{400} \bmod 11$.

Since there are only 11 different numbers modulo 11 (the numbers from 0 to 10), we know that the result is one of these numbers.

To find the result, we might first try to type 3^{400} into a calculator (and then find the remainder after division by 11 afterwards). However, if we type 3^{400} into most calculators, it simply says "Error" – the number is too large!

So we have to do something more clever...

The “square and multiply” algorithm

One way to do fast exponentiation is to use the so-called “square and multiply” algorithm. Below, the steps in the algorithm are listed, and a small example, $3^{18} \bmod 4$, is shown on the right.

You can see a more detailed example in the following slides.

↑
In this example, 3 is called the **base**.

1. Calculate the binary representation of the exponent.
2. Go through the bits one by one, and do the following.
 - The first bit (which is always a 1) is skipped – i.e. you just keep the base.
 - Then, each time you meet a 0, you square the result from the previous bit.
 - Each time you meet a 1, square the result from the previous bit and multiply by the base.

$$18 = 10010_2$$

Below we go through the bits one by one:

1: 3 (we just keep the base)

$$0: 3^2 \equiv 9 \equiv 1 \pmod{4}$$

$$0: 1^2 \equiv 1 \pmod{4}$$

$$1: 1^2 \cdot 3 \equiv 3 \pmod{4}$$

$$0: 3^2 \equiv 9 \equiv \mathbf{1} \pmod{4}$$

↙ This is the result.

The “square and multiply” algorithm

Example: Calculate $3^{400} \pmod{11}$ using the square/multiply algorithm.

Solution:

1. Find the binary representation of the exponent:

$$400 = 256 + 128 + 16 = 110010000_2$$

2. Starting from the left of the binary exponent, skip the first bit and do the following:
 1. Each time you encounter 1, you square your number and multiply by base (in this case 3).
 2. Each time you encounter 0, you square your number.

(Continued on the next slide)

The square and multiply algorithm

Example: Calculate $3^{400} \pmod{11}$ using the square/multiply algorithm.

1 Skip this bit	3	
1 Square and multiply by the base:	$3^2 \cdot 3 = 27$	$\equiv 5 \pmod{11}$
0 Square:	$5^2 = 25$	$\equiv 3 \pmod{11}$
0 Square:	$3^2 = 9$	$\equiv 9 \pmod{11}$
1 Square and multiply by the base:	$9^2 \cdot 3 = 81 \cdot 3 \equiv 4 \cdot 3 \equiv 1 \pmod{11}$	
0 Square:	$1^2 = 1$	$\equiv 1 \pmod{11}$
0 Square:	$1^2 = 1$	$\equiv 1 \pmod{11}$
0 Square:	$1^2 = 1$	$\equiv 1 \pmod{11}$
0 Square:	$1^2 = 1$	$\equiv 1 \pmod{11}$