Discrete Mathematics, Section 001, Fall 2016

Lecture 19: Modular arithmetic and congruences

Zsolt Pajor-Gyulai
zsolt@cims.nyu.edu

Courant Institute of Mathematical Sciences

November 28, 2016

Outline

1. Modular arithmetic
2. Congruences

New context for basic operations

- Arithmetic is the study of basic operations: $+, -, \cdot, /$.
- The usual context for studying these are number systems like $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

For example, look at divison $/$:

- In the context of rational numbers $\mathbb{Q}$, x/y makes sense whenever $y \neq 0$.
- In the context of integers, $\mathbb{Z}$, x/y makes sense if and only if $y|x$.

Division takes on slightly different meaning depending on the context!

In this lecture: We introduce a new context for these operations, by performing arithmetic in the set

$$\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$$

Modular addition and multiplication

Definition

Let n be a positive integer and $a, b \in \mathbb{Z}_n$ We define

$$a \oplus b := (a + b) \bmod n$$
$$a \otimes b := (ab) \bmod n$$

$\oplus$ is called **addition modulo** n, while $\otimes$ is called **multiplication modulo** n.

For example in $\mathbb{Z}_{10}$,

$$5 \oplus 5 = 0 \quad 9 \oplus 8 = 7$$
$$5 \otimes 5 = 5 \quad 9 \otimes 8 = 2$$

Do Problem 1-2.

Closure property

Let $a, b \in \mathbb{Z}_n$. Then $a \oplus b \in Z_n$ and $a \otimes b \in \mathbb{Z}_n$.

Proof.

Straightforward by the definition of mod. $\square$

What about other properties? (Homework)

Proposition

Let n be an integer with $n \geq 2$.

1. For all $a, b \in \mathbb{Z}_n$, $a \oplus b = b \oplus a$ and $a \otimes b = b \otimes a$
2. For $a, b, c \in \mathbb{Z}_n$, $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
3. For $a \in \mathbb{Z}_n$, $a \oplus 0 = a$, $a \otimes 1 = a$ and $a \otimes 0 = 0$.
4. For $a, b, c \in \mathbb{Z}_n$, $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

In other words $\oplus$ and $\otimes$ are commutative, associative operations with identities 0 and 1 respectively. The last bulletpoint is called the distributive property.

Modular substraction

Ordinary substraction in terms of addition:

Definition

Let $a, b \in \mathbb{Z}$. We define $a - b$ to be the solution of the equation $a = b + x$.

Then we would prove

1. The equation $a = b + x$ has a solution.
2. The equation $a = b + x$ has only one solution.

We want to use the same approach defining modular substraction.

Modular substraction

Proposition

Let n be a positive integer, and let $a, b \in \mathbb{Z}_n$. Then there is one and only one $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.

Let $x = (a - b) \bmod n$.

- By the definition of mod, $x \in \mathbb{Z}_n$.
- Note that $x = (a - b) + kn$ for some $k \in \mathbb{Z}$. We calculate

$$\begin{aligned} b \oplus x &= (b + x) \bmod n = \\ &= [b + (a - b + kn)] \bmod n = (a + kn) \bmod n = a \end{aligned}$$

So the existence part is proved.
[...]

Modular substraction

Proposition

Let n be a positive integer, and let $a, b \in \mathbb{Z}_n$. Then there is one and only one $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.

[...]

FTSC, suppose there were two $x, y \in \mathbb{Z}_n$ with $x \neq y$ for which

$$a = b \oplus x, \qquad a = b \oplus y.$$

This means that there are $k, j \in \mathbb{Z}$, such that

$$a = b \oplus x = (b + x) \bmod n = b + x + kn$$

$$a = b \oplus y = (b + y) \bmod n = b + y + jn$$

Combining these

$$b + x + kn = b + y + jn$$

[...]

Proposition

Let n be a positive integer, and let $a, b \in \mathbb{Z}_n$. Then there is one and only one $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.

[...] Combining these

$$b + x + kn = b + y + jn$$

which in turn implies

$$x = y + (k - j)n \qquad \Rightarrow \qquad x \equiv y \pmod{n}.$$

But since $0 \leq x, y < n$, this implies $x = y$.$\Rightarrow\Leftarrow$ $\square$

Definition

Let n be a positive integer and let $a, b \in \mathbb{Z}_n$. Then $a \ominus b$ is the unique $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.

Note that the above proof also shows $a \ominus b = (a - b) \bmod n$.

Do Problem 3 on the worsheet. This shows that $\ominus$ is not commutative.

Modular division

This operation is very different from its usual counterpart:

- In ordinary division the only division not allowed is by zero.
- In the context of $\mathbb{Z}_{10}$,

$$5 \otimes 2 = 5 \otimes 4 = 0 \qquad \text{but} \qquad 2 \neq 4$$

  and so we can't just $\oslash$ by 5.

Given $a, b \in \mathbb{Z}_{10}$ with $b \neq 0$, must there be a solution to $a = b \otimes x$?

- Let $a = 6$, $b = 2$. Then $x = 3$ and $x = 8$ are both solutions.
- Let $a = 7$, $b = 2$. There are no solutions (check all options).
- Let $a = 7$, $b = 3$. There is only one solution $x = 9$.

We need to do something more elaborate!

Modular division

In the context of $\mathbb{Q}$, we define divison by multiplication by the reciprocal:

$$\frac{a}{b} = a \cdot b^{-1}$$

Then we cannot divide by 0 as it doesn't have a reciprocal.

Modular reciprocal

Let n be a positive integer and let $a \in \mathbb{Z}_n$. A **reciprocal** of a is an element $b \in \mathbb{Z}_n$ such that $a \otimes b = 1$. An element of $\mathbb{Z}_n$ that has a reciprocal is called **invertible**.

Natural questions:

- What elements have reciprocals?
- Can an element have more than one reciprocals?

Modular division

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Now we make use of these observations!

0 has no reciprocal.

$2, 4, 6, 8$ have no reciprocals either.

$1, 3, 7, 9$ are invertible.

The invertible ones have ony one reciprocal.

The invertible ones are precisely the ones relatively primes to 10.

$3^{-1} = 7$ and $7^{-1} = 3$, $1^{-1} = 9$ and $9^{-1} = 1$.

Modular division

Proposition

Let n be a positive integer and $a \in \mathbb{Z}_n$. If a has a reciprocal in $\mathbb{Z}_n$, then it has only one reciprocal.

Proof.

FTSC, suppose a had two reciprocals, $b, c \in \mathbb{Z}_n$ with $b \neq c$. Then

$$b \otimes (a \otimes c) = b \otimes 1 = b,$$

$$(b \otimes a) \otimes c = 1 \otimes c = c.$$

By the associative property, these two are equal and so $b = c$. $\Rightarrow\Leftarrow$. $\square$

Therefore it make sense to talk about *the* reciprocal of an element a.

Modular division

Propostition

Let n be a positive integer and $a \in \mathbb{Z}_n$. Suppose a is invertible. $b = a^{-1}$, then b is invertible and $a = b^{-1}$. In other words $(a^{-1})^{-1} = a$.

Proof.

Since a^{-1} is the reciprocal of a,

$$a^{-1} \otimes a = 1.$$

But this also shows that the reciprocal of a^{-1} is a. □

Modular division

Modular division

Let n be a positive integer and let b be an invertible element of $\mathbb{Z}_n$. Let $a \in \mathbb{Z}_n$ be arbitrary. Then $a \oslash b$ is defined to be $a \otimes b^{-1}$.

For example, in the context of $\mathbb{Z}_{10}$,

$$7^{-1} = 3 \qquad \Rightarrow \qquad 2 \oslash 7 = 2 \otimes 3 = 6$$

Practice some by doing Problem 4 on the Worksheet.

We still have not answered:

- In $\mathbb{Z}_n$, which elements are invertible?
- In $\mathbb{Z}_n$, given that a is invertible, how do we calculate a^{-1}?

We could just write out the multiplication table, like we did for $\mathbb{Z}_{10}$. However, good luck with $\mathbb{Z}_{1000}$.

Invertible elements of $\mathbb{Z}_n$

Theorem

Let n be a positive integer and let $a \in \mathbb{Z}_n$. Then a is invertible if and only if a and n are relative primes.

Recall:

$gcd(a, n) = 1$ if and only if there are $b, k \in \mathbb{Z}_n$ such that $ab + kn = 1$.

($\Rightarrow$): Suppose a is invertible. This means there is a $b \in \mathbb{Z}_n$ such that

$$1 = a \otimes b = (ab) \bmod n.$$

This means that there is $k \in \mathbb{Z}$ such that

$$ab + kn = 1$$

and therefore a and n are relative primes.
[...]

Invertible elements of $\mathbb{Z}_n$

Theorem

Let n be a positive integer and let $a \in \mathbb{Z}_n$. Then a is invertible if and only if a and n are relative primes.

[...]
($\Leftarrow$) Suppose a and n are relative primes. Then there are integers x, y such that $ax + ny = 1$. Let

$$b = x \bmod n \qquad \Rightarrow \qquad b = x + kn$$

for some $k \in \mathbb{Z}$. Therefore

$$1 = ax + ny = a(b - kn) + ny = ab + (y - ka)n,$$

and $a \otimes b = (ab) \bmod n = 1$ and $b = a^{-1}$. $\square$.

Invertible elements of $\mathbb{Z}_n$

This also helps us find a^{-1} for invertible a-s in $\mathbb{Z}_n$.

1. Use Euclid's algorithm to find x, y such that
$$ax + ny = 1.$$
2. Then $a^{-1} = x \bmod n$.

For example, in $\mathbb{Z}_{431}$, let's find 29^{-1}.

This is problem 5 on the worksheet.

Solving equations in $\mathbb{Z}_n$

- Consider $2 \otimes x = 4$ in $\mathbb{Z}_{11}$. Then clearly $gcd(2, 11) = 1$ and $2^{-1} = 6$ and so

$$x = (2^{-1} \otimes 2) \otimes x = 2^{-1} \otimes (2 \otimes x) = 2^{-1} \otimes 4 = 6 \otimes 4 = 2$$

- Consider, however, $2 \otimes x = 4$ in $\mathbb{Z}_{10}$. Now 2 doesn't have a reciprocal and the only thing we can do at this point is guess. Checking all the values, we see that $x = 2$ and $x = 7$ are the two solutions.

Do Problem 6 on the Worksheet.

Outline

1. Modular arithmetic
2. Congruences

An application: Solving congruences

For example, try to find all integers x such that

$$3x \equiv 4 \pmod{11}.$$

Note that if x_0 is a solution, then

$$3(x_0 + k \cdot 11) = 3x_0 + 33k \equiv 3x_0 \equiv 4 \pmod{11}$$

for any $k \in \mathbb{Z}$ and therefore $x + k \cdot 11$ is also a solution.

This means that it is enough to find the solutions in $\mathbb{Z}_{11}$, then all other solutions can be obtained by adding (or substracting) some multiple of 11.

An application: Solving congruences

We need to find $x \in \mathbb{Z}_{11}$ for which $3x \equiv 4 \pmod{11}$. Note

$$3x \equiv 4 \bmod 11 \qquad \Leftrightarrow \qquad (3x) \bmod 11 = 4 \qquad \Leftrightarrow \qquad 3 \otimes x = 4.$$

But we know how to solve this as $3^{-1} = 4$ in $\mathbb{Z}_{11}$ and therefore

$$x = (3^{-1} \otimes 3) \otimes x = 3^{-1} \otimes (3 \otimes x) = 3^{-1} \otimes 4 = 4 \otimes 4 = 5$$

Therefore the solutions to the original congruence is

$$\{5 + k \cdot 11 : k \in \mathbb{Z}\}.$$

An application: Solving congruences

Proposition

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose a and n are relatively prime and consider the equation

$$ax \equiv b \pmod{n}.$$

The set of solutions to this equation is

$$\{x_0 + kn : k \in \mathbb{Z}\}$$

where $x_0 = a_0^{-1} \otimes b_0$ with $a_0 = a \bmod n$ and $b_0 = b \bmod n$ and $\otimes$ is meant in the context of $\mathbb{Z}_n$.

Practice this by Problem 7 on the worksheet.

For quiz

- Understand the operations $\oplus, \ominus, \otimes$ within the context of $\mathbb{Z}_n$.
- Understand the notion of the reciprocal within the context of $\mathbb{Z}_n$ and how to compute this.
- Understand how to use the reciprocals to solve equations in $\mathbb{Z}_n$.