Linear Algebra 1: Lecture 0

Irena Penev

Winter 2022/2023

Notation: $\mathbb{Z}$ is the set of all integers, and $\mathbb{N}$ is the set of all positive integers.

1 Modular arithmetic

Given $m \in \mathbb{N}$ and $n \in \mathbb{Z}$, we write $m \mid n$ if n is divisible by m, that is, if there exists some $k \in \mathbb{Z}$ such that $n = km$.

Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo* n, and we write $a \equiv b \pmod{n}$ or $a \equiv_n b$, provided that $n|(a-b)$. (Equivalently: $a \equiv b \pmod{n}$ provided that a and b leave the same remainder when divided by n.)

Example 1.1. *We have the following:*

- $2 \equiv 17 \pmod{3}$
- $-13 \equiv 8 \pmod{7}$
- $-1 \equiv 7 \pmod{4}$
- $2 \not\equiv 17 \pmod{2}$
- $-13 \not\equiv 8 \pmod{5}$
- $-1 \not\equiv 7 \pmod{6}$

Observation: For $n \in \mathbb{N}$, every integer is congruent modulo n to exactly one of the following n integers: $0, \dots, n-1$. As we shall see, doing arithmetic modulo n essentially boils down to doing arithmetic with only n values (namely $0, \dots, n-1$), as opposed to infinitely many. This is quite useful for certain applications.

Proposition 1.2. *Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:*

(1) $a \equiv a \pmod{n}$;

(2) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(3) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof. (1) and (2) are obvious. For (3), assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n \mid (a-b)$ and $n \mid (b-c)$, i.e. there exist $k, \ell \in \mathbb{Z}$ such that $a-b = kn$ and $b-c = \ell n$. But then $a-c = (a-b)+(b-c) = kn+\ell n = (k+\ell)n$, i.e. $n \mid (a-c)$. Thus, $a \equiv c \pmod{n}$. □

We remark that Proposition 1.2 establishes that congruence modulo n is an "equivalence relation" on $\mathbb{Z}$.[1]

Proposition 1.3. *Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, and assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:*

(1) $a + c \equiv b + d \pmod{n}$;

(2) $a - c \equiv b - d \pmod{n}$;

(3) $ac \equiv bd \pmod{n}$.

Proof. Since $a \equiv b \pmod{n}$, we have that $n|(a-b)$, and so there exists some $s \in \mathbb{Z}$ such that $a - b = sn$. Similarly, since $c \equiv d \pmod{n}$, there exists some $t \in \mathbb{Z}$ such that $c - d = tn$.

To prove (1), we observe that

$$\begin{aligned}(a+c)-(b+d) &= (a-b)+(c-d)\\ &= sn+tn\\ &= (s+t)n\end{aligned}$$

and so $n \mid \Big((a+c)-(b+d)\Big)$. Thus, $a + c \equiv b + d \pmod{n}$. This proves (1).

For (2), we observe that

$$\begin{aligned}(a-c)-(b-d) &= (a-b)-(c-d)\\ &= sn-tn\\ &= (s-t)n\end{aligned}$$

and so $n \mid \Big((a-c)-(b-d)\Big)$. Thus, $a - c \equiv b - d \pmod{n}$. This proves (2).

Finally, for (3), we have that

$$\begin{aligned}ac-bd &= ac-ad+ad-bd\\ &= a(c-d)+(a-b)d\\ &= atn+snd\\ &= (at+ds)n\end{aligned}$$

and so $n \mid (ac - bd)$. Thus, $ac \equiv bd \pmod{n}$. This proves (3). □

[1] If you are not already familiar with equivalence relations, you will soon learn about them in Discrete Math.

Proposition 1.4. *Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Assume that $a \equiv b \pmod{n}$. Then $a^t \equiv b^t \pmod{n}$ for all integers $t \geq 0$.*

Proof. The statement obviously holds for $t = 0$ and $t = 1$.[2] For integers $t \geq 2$, we repeatedly apply Proposition 1.3 to get the following:

$$\begin{aligned}
a \equiv b \pmod{n} &\implies a^2 \equiv b^2 \pmod{n} && \text{by Proposition 1.3, since } a \equiv b \pmod{n} \\
&\implies a^3 \equiv b^3 \pmod{n} && \text{by Proposition 1.3, since } a \equiv b \pmod{n} \\
&\vdots \\
&\implies a^t \equiv b^t \pmod{n} && \text{by Proposition 1.3, since } a \equiv b \pmod{n},
\end{aligned}$$

which is what we needed. □

Warning: Do not divide!!! For example, we have that $4 \equiv 8 \pmod{4}$, but if we divide both sides by 2, we get $2 \not\equiv 4 \pmod{4}$.

Example 1.5. *Compute the last digit of* 2018^{2019}.

Solution. In principle, we could compute the value of 2018^{2019}, and then simply check what its last digit is. However, 2018^{2019} is an enormous number, and so this is impractical (even with the help of a computer). However, note that the last digit of a positive integer is simply its remainder when divided by 10. So, we need only figure out which of $0, 1, \ldots, 9$ the number 2018^{2019} is congruent to modulo 10.[3]

Clearly, $2018 \equiv 8 \pmod{10}$, and so $2018^{2019} \equiv 8^{2019} \pmod{10}$. Now, note the following:

- $8^1 \equiv 8 \pmod{10}$;
- $8^2 \equiv 4 \pmod{10}$;
- $8^3 \equiv 2 \pmod{10}$;
- $8^4 \equiv 6 \pmod{10}$;
- $8^5 \equiv 8 \pmod{10}$.

[2] For $t = 0$, we area using the fact that $r^0 := 1$ for all real numbers r.

[3] If we were looking for the last two digits, then we'd be considering congruence modulo 100; for the last three digits, we'd need congruence modulo 1000, etc.

So, we get a periodic pattern! In general, for an integer $k \geq 0$, we have:[4]

- $8^{4k+1} \equiv 8 \pmod{10}$;
- $8^{4k+2} \equiv 4 \pmod{10}$;
- $8^{4k+3} \equiv 2 \pmod{10}$;
- $8^{4k+4} \equiv 6 \pmod{10}$.

Since $2019 = 4 \cdot 504 + 3$, we see that $8^{2019} \equiv 2 \pmod{10}$. Thus, $2018^{2019} \equiv 2 \pmod{10}$, and it follows that the last digit of 2018^{2019} is 2. □

Notation: For $a_n, a_{n-1}, \ldots, a_0 \in \{0, 1, \ldots, 9\}$, we define:

$$\overline{a_n a_{n-1} \ldots a_0} \quad := \quad \sum_{i=0}^{n} a_i 10^i.$$

Thus, $\overline{a_n a_{n-1} \ldots a_0}$ is the number whose first digit is a_n,[5] whose second digit is a_{n-1}, and so on.

Proposition 1.6. *Let $a = \overline{a_n a_{n-1} \ldots a_0}$. Then $a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod{9}$. Therefore, a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.*

Proof. The second statement obviously follows from the first. It remains to prove the first statement.

Note that $10 \equiv 1 \pmod{9}$. So, by Proposition 1.4, we have that $10^k \equiv 1 \pmod{9}$ for all non-negative integers k. It follows that for all $i \in \{0, \ldots, n\}$, we have that $a_i \cdot 10^i \equiv a_i \pmod{10}$. Consequently,

$$a \quad = \quad \overline{a_n a_{n-1} \ldots a_0} \quad = \quad \sum_{i=0}^{n} a_i 10^i \quad \equiv_9 \quad \sum_{i=0}^{n} a_i \quad = \quad a_n + a_{n-1} + \cdots + a_0,$$

which is what we needed to show. □

Proposition 1.7. *Let $a = \overline{a_n a_{n-1} \ldots a_0}$. Then $a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod{3}$. Therefore, a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.*

Proof. The proof is completely analogous to that of Proposition 1.6: just replace (mod 9) by (mod 3) throughout. □

[4] To give a fully formal proof of the fact that this pattern holds, we would need to use "mathematical induction." If you are not already familiar with mathematical induction, you will learn about it soon in the Mathematical Skills seminar.

[5] It's possible that this first digit is zero. We could eliminate this possibility, but that would result in a messier definition.

Example 1.8. *Show that the following equation has no non-negative integer solutions:*

$$x^2 + y^2 = 10^{z+2} - 1$$

Solution. We will show that for all non-negative integers x, y, z, we have that $x^2 + y^2 \not\equiv 10^{z+2} - 1 \pmod 4$. This immediately implies that the equation $x^2 + y^2 = 10^{z+2} - 1$ has no positive integer solutions.

First, note that $100 \equiv 0 \pmod 4$, and so for a non-negative integer z, we have that

$$10^{z+2} - 1 \equiv 100 \cdot 10^z - 1 \equiv 0 \cdot 10^z - 1 \equiv -1 \pmod 4.$$

On the other hand:

- $0^2 \equiv 0 \pmod 4$;
- $1^4 \equiv 1 \pmod 4$;
- $2^2 \equiv 0 \pmod 4$;
- $3^2 \equiv 1 \pmod 4$.

Since every integer is congruent to one of $0, 1, 2, 3$ modulo 4, it follows that the square of any integer is congruent to either 0 or 1 modulo 4. It follows that the sum of two squares is congruent to 0, 1, or 2 modulo 4, and none of these three numbers (0 , 1, or 2) is congruent to -1 modulo 4. Consequently, for integers x and y, we have that

$$x^2 + y^2 \not\equiv -1 \pmod 4$$

Thus, for non-negative integers x, y, z, we have that $x^2 + y^2 \not\equiv 10^{z+2} - 1 \pmod 4$, and we are done. □

2 Arithmetic in $\mathbb{Z}_n$

Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, we set

$$[a]_n \quad := \quad \{x \in \mathbb{Z} \mid x \equiv a \pmod n\};$$

note that $[a]_n = \{a + tn \mid t \in \mathbb{Z}\}$.[6] We define

$$\mathbb{Z}_n \quad := \quad \{[a]_n \mid a \in \mathbb{Z}\}.$$

[6] For example:

- $[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$;
- $[1]_2 = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$;
- $[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$;
- $[1]_3 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$;
- $[2]_3 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Note that for $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we have that $a \equiv b \pmod{n}$ if and only if $[a]_n = [b]_n$. Recall that every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n; consequently, for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$. This implies that, in fact:

$$\mathbb{Z}_n = \{[0]_n, \ldots, [n-1]_n\}.$$

Remark: Sets $[0]_n, \ldots, [n-1]_n$ form a *partition* of $\mathbb{Z}$, that is:

- $\mathbb{Z} = [0]_n \cup \cdots \cup [n-1]_n$, and
- the sets $[0]_n, \ldots, [n-1]_n$ are pairwise disjoint.[7]

If you are familiar with "equivalence relations," then note that congruence modulo n is an equivalence relation on $\mathbb{Z}$ (by Proposition 1.2), and the sets $[0]_n, \ldots, [n-1]_n$ are the related equivalence classes.

Notation: When working in $\mathbb{Z}_n$, we often write simply $0, \ldots, n-1$ instead of $[0]_n, \ldots, [n-1]_n$, respectively. We may do this **only** if we have previously made it clear that our numbers (which are technically sets of integers) are in $\mathbb{Z}_n$.

Example 2.1. *For $n = 2$, $[0]_2 = \{2t \mid t \in \mathbb{Z}\}$ and $[1]_2 = \{1 + 2t \mid t \in \mathbb{Z}\}$[8], and we have that $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. Sometimes we simply write $\mathbb{Z}_2 = \{0, 1\}$, but technically, 0 stands for the set $[0]_2$, and 1 stands for $[1]_2$.*

Recall that for $n \in \mathbb{N}$ and $a, a', b, b' \in \mathbb{Z}$, if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$;[9] equivalently, if $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then $[a + b]_n = [a' + b']_n$ and $[ab]_n = [a'b']_n$. Thus, we may define addition and multiplication in $\mathbb{Z}_n$ as follows. For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we define

$$[a]_n + [b]_n = [a + b]_n \quad \text{and} \quad [a]_n[b]_n = [ab]_n.$$

We can now make addition and multiplication tables for $\mathbb{Z}_n$, for various values of n.

Example 2.2. *The addition and multiplication tables for $\mathbb{Z}_2$ are:*

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

[7] This means that no two of $[0]_n, \ldots, [n-1]_n$ have an element in common. In other words, for all distinct $i, j \in \{0, \ldots, n-1\}$, we have $[i]_n \cap [j]_n = \emptyset$.

[8] In other words, $[0]_2$ is the set of all even numbers, and $[1]_2$ is the set of all odd numbers.

[9] See Proposition 1.3.

If we omit subscripts and square brackets, this produces the following addition and multiplication tables for $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Example 2.3. *The addition and multiplication tables for $\mathbb{Z}_3$ are:*[10]

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Example 2.4. *The addition and multiplication tables for $\mathbb{Z}_4$ are:*[11]

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Remark: Note that for $n = 2, 3$, every non-zero member of $\mathbb{Z}_n$ has a "multiplicative inverse," i.e. a number that we can multiply it by to get 1. However, for $n = 4$, this is not the case. This is not an accident!

Theorem 2.5. *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.*[12] *Then there exists some $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.*

Proof. Let us show that no two of $0, a, 2a, \ldots, (n-1)a$ are congruent modulo n.[13] Suppose otherwise, and fix distinct $i, j \in \{0, \ldots, n-1\}$ such that $ia \equiv ja \pmod{n}$. Then $(i-j)a \equiv 0 \pmod{n}$, that is, $n|(i-j)a$. Since n and a are relatively prime, it follows that $n|(i-j)$. But this is impossible because $i, j \in \{0, \ldots, n-1\}$ and $i \neq j$, and so $0 < |i-j| < n$. Thus, no two of $0, a, 2a, \ldots, (n-1)a$ are congruent modulo n.

We know that every integer is congruent modulo n to one of the following n integers: $0, 1, 2, \ldots, n-1$. We showed above that no two of the following n integers are congruent to each other modulo n: $0, a, 2a, \ldots, (n-1)a$. It follows that (exactly) one of $0, a, 2a, \ldots, (n-1)a$ is congruent to 1 modulo n. This completes the argument. □

[10] Remember, in this context, 0 stands for $[0]_3$, 1 stands for $[1]_3$, and 2 stands for $[2]_3$.

[11] Remember, in this context, 0 stands for $[0]_4$, 1 stands for $[1]_4$, 2 stands for $[2]_4$, and 3 stands for $[3]_4$.

[12] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1.

[13] Note that this implies that $[a]_n, [2a]_n, \ldots, [(n-1)a]_n$ are pairwise distinct.

Corollary 2.6. *Let $p \in \mathbb{N}$ be a prime number. Then:*

(a) for all $a \in \mathbb{Z}$ such that a is not a multiple of p, there exists some $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ such that $ab = 1$.[14]

Proof. We first prove (a). Since p is a prime number, every integer that is not a multiple of p is relatively prime to p; (a) now follows from Theorem 2.5.

Statement (b) immediately follows from (a). Indeed, fix $a \in \mathbb{Z}_p \setminus \{0\}$. Then there exists an integer $a' \in \{1, \ldots, p-1\}$ such that $a = [a']_p$. By (a), there exists an integer b' such that $a'b' \equiv 1 \pmod{p}$. We now set $b := [b']_p$, and we see that $ab = [a']_p[b']_p = [a'b']_p = [1]_p$. Moreover, $b \neq 0$, since (in $\mathbb{Z}_p$) we have that $a \cdot 0 = 0 \neq 1 = ab$. This proves (b). □

Fermat's Little Theorem (below) is a strengthening of Corollary 2.6. Before stating and proving Fermat's Little Theorem, we need some notation. We define $0! := 1$, and for a positive integer n, we define $n! := 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$. "$n!$" is read "$n$ factorial."

Fermat's Little Theorem. *If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Fix a prime number $p \in \mathbb{N}$. Let $a \in \mathbb{Z}$, and assume that a is not a multiple of p. As in the proof of Theorem 2.5, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p.[15] Since every integer is congruent to exactly one of $0, 1, \ldots, p-1$ modulo p, it follows that there exists some rearrangement (i.e. permutation) $r_1, \ldots, r_{p-1}$ of the sequence $1, \ldots, p-1$ such that

- $a \equiv r_1 \pmod{p}$;
- $2a \equiv r_2 \pmod{p}$;

  $\vdots$

- $(p-1)a \equiv r_{p-1} \pmod{p}$.

It now follows that

$$\underbrace{a \cdot 2a \cdot \cdots \cdot (p-1)a}_{=(p-1)!a^{p-1}} \equiv \underbrace{r_1 r_2 \ldots r_{p-1}}_{=(p-1)!} \pmod{p},$$

[14] Here, $0 = [0]_p$ and $1 = [1]_p$.

[15] This is exactly the same as in the proof of Theorem 2.5, but for the sake of completeness, here is the full proof. Suppose some two of $0, a, \ldots, (p-1)a$ are congruent modulo p. Fix distinct $i, j \in \{0, 1, \ldots, p-1\}$ such that $ia \equiv ja \pmod{p}$. Then $(i-j)a \equiv 0 \pmod{p}$, that is, $p|(i-j)a$. Since p is prime and does not divide a, we see that $p|(i-j)$. But this is impossible because $i, j \in \{0, \ldots, p-1\}$ and $i \neq j$, and so $0 < |i-j| < p$. Thus, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p.

and so $(p-1)!a^{p-1} \equiv (p-1)!\pmod{p}$. But now

$$(a^{p-1}-1)(p-1)! \;\equiv\; 0 \pmod{p},$$

that is, $p \mid \Big((a^{p-1}-1)(p-1)!\Big)$. Since p is prime, we see that p and $(p-1)!$ are relatively prime. It follows that $p \mid (a^{p-1}-1)$, and consequently, $a^{p-1} \equiv 1 \pmod{p}$, which is what we needed to show. □

Fermat's Little Theorem can be restated as follows:

> *If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is not a multiple of p, then $([a]_p)^{p-1} = [1]_p$.*

Here is another way to restate Fermat's Little Theorem:

> *If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.*[16]

3 Exercises (optional, not to be turned in)

Exercise 3.1. *Prove that a positive integer is divisible by 11 if and only if the difference between the sum of the digits at odd places and the sum of the digits at even places of the number, is divisible by 11.*

Exercise 3.2. *Prove that the number $2222^{5555} + 5555^{2222}$ is divisible by 7.*

Exercise 3.3. *Find all the positive integers n for which $2^n - 1$ is a perfect square (and prove that your answer is correct).*

Exercise 3.4. *Suppose that the decimal representation of a positive integer n consists of exactly 300 ones and a certain number of zeros (and of no other digits). Prove that n is **not** a perfect square.*

Exercise 3.5. *Prove that $n^7 - n$ is divisible by 42 for every integer n. (**Hint:** Find a way to apply Fermat's Little Theorem.)*

[16] In the equality $a^{p-1} = 1$, numbers a and 1 are elements of $\mathbb{Z}_p$, but the exponent $p-1$ is a positive integer, so that $a^{p-1} = \underbrace{a \cdot \cdots \cdot a}_{p-1}$, i.e. a is multiplied by itself $p-1$ times, and the multiplication is in $\mathbb{Z}_p$.