A short course on Erdős problems in discrete plane: Part I

Alex Iosevich

March 2020

What is this video about?

- This video is the first part of a short course on combinatorial geometry of the finite plane over integer modulo a prime.

What is this video about?

- This video is the first part of a short course on combinatorial geometry of the finite plane over integer modulo a prime.

- We begin by explaining the basic notions of geometry in this setting and compare it with the concepts from the Euclidean plane.

What is this video about?

- This video is the first part of a short course on combinatorial geometry of the finite plane over integer modulo a prime.
- We begin by explaining the basic notions of geometry in this setting and compare it with the concepts from the Euclidean plane.
- In the process, we are going to explore quite a few ideas from areas like abstract algebra, linear algebra, and Fourier analysis.

What is this video about?

- This video is the first part of a short course on combinatorial geometry of the finite plane over integer modulo a prime.
- We begin by explaining the basic notions of geometry in this setting and compare it with the concepts from the Euclidean plane.
- In the process, we are going to explore quite a few ideas from areas like abstract algebra, linear algebra, and Fourier analysis.
- We shall introduce these from a completely elementary standpoint, requiring only a solid knowledge of precalculus, and mostly much less.

What are Erdős problems in geometry?

- Erdős problems in geometry typically involve counting elementary geometric objects satisfying some natural constraints.

What are Erdős problems in geometry?

- Erdős problems in geometry typically involve counting elementary geometric objects satisfying some natural constraints.

- A typical example that we are going to address in the second part of this mini-course is the following.

What are Erdős problems in geometry?

- Erdős problems in geometry typically involve counting elementary geometric objects satisfying some natural constraints.

- A typical example that we are going to address in the second part of this mini-course is the following.

- Let P be a collection of n points and $\mathcal{L}$ be a collections of m lines in the plane.

What are Erdős problems in geometry?

- Erdős problems in geometry typically involve counting elementary geometric objects satisfying some natural constraints.

- A typical example that we are going to address in the second part of this mini-course is the following.

- Let P be a collection of n points and $\mathcal{L}$ be a collections of m lines in the plane.

- What is the largest possible number of **incidences**. defined as the number of elements in the set

$$\{(p, l) \in P \times \mathcal{L} : p \in l\}$$

as a function of n and m?

Incidence theory

- Define $I(P, \mathcal{L})$ denote the number of elements in

$$\{(p, l) \in P \times \mathcal{L} : p \in l\}.$$

Incidence theory

- Define $I(P, \mathcal{L})$ denote the number of elements in

$$\{(p, l) \in P \times \mathcal{L} : p \in l\}.$$

- Since the set we are counting is contained in

$$P \times \mathcal{L} = \{(p, l) \in P \times \mathcal{L}\},$$

we see that $I(P, \mathcal{L}) \leq nm$.

Incidence theory

- Define $I(P, \mathcal{L})$ denote the number of elements in

$$\{(p, l) \in P \times \mathcal{L} : p \in l\}.$$

- Since the set we are counting is contained in

$$P \times \mathcal{L} = \{(p, l) \in P \times \mathcal{L}\},$$

we see that $I(P, \mathcal{L}) \leq nm$.

- But is this estimate realistic? Is it really possible to have every point be on every line and every line pass through every point?

Simple example

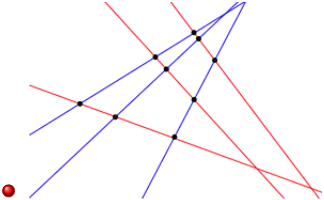

Figure: 6 lines, 9 points, 18 incidences

Simple example

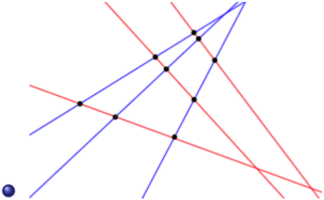

Figure: 6 lines, 9 points, 18 incidences

- In one of lectures of this mini-course we are going to prove the celebrated Szemeredi-Trotter incidence theorem, which says that

$$I(P, \mathcal{L}) \leq C(n + m + (nm)^{\frac{2}{3}}),$$

where recall that n is the number of points in P and m is the number of lines in $\mathcal{L}$.

Prime numbers

- A positive integer is called prime if its only divisors are 1 and itself.

Prime numbers

- A positive integer is called prime if its only divisors are 1 and itself.
- For example, 2 is a prime because its only divisors are 1 and 2.

Prime numbers

- A positive integer is called prime if its only divisors are 1 and itself.
- For example, 2 is a prime because its only divisors are 1 and 2.
- Similarly, 3, 5 and 7 are primes.

Prime numbers

- A positive integer is called prime if its only divisors are 1 and itself.
- For example, 2 is a prime because its only divisors are 1 and 2.
- Similarly, 3, 5 and 7 are primes.
- On the other hand, 8 is not a prime because it is divisible by 4, so 8 has divisors other than 1 and itself.

Prime numbers

- A positive integer is called prime if its only divisors are 1 and itself.
- For example, 2 is a prime because its only divisors are 1 and 2.
- Similarly, 3, 5 and 7 are primes.
- On the other hand, 8 is not a prime because it is divisible by 4, so 8 has divisors other than 1 and itself.
- A question to be explored in a later video is, how many prime numbers are there between 2 and x, where x is a large positive integer?

Prime numbers

- A positive integer is called prime if its only divisors are 1 and itself.
- For example, 2 is a prime because its only divisors are 1 and 2.
- Similarly, 3, 5 and 7 are primes.
- On the other hand, 8 is not a prime because it is divisible by 4, so 8 has divisors other than 1 and itself.
- A question to be explored in a later video is, how many prime numbers are there between 2 and x, where x is a large positive integer?
- The Prime Number Theorem says that there are $\approx \frac{x}{\log(x)}$ prime numbers in this range and this investigation leads to many problems that lie at the heart of modern mathematics.

Remainders

- Let's begin by playing the following game. Given an integer, we are going to divide it by 2 and compute the remainder.

Remainders

- Let's begin by playing the following game. Given an integer, we are going to divide it by 2 and compute the remainder.

- The remainder is either 0 or 1.

Remainders

- Let's begin by playing the following game. Given an integer, we are going to divide it by 2 and compute the remainder.
- The remainder is either 0 or 1.
- Similarly, for each integer, consider the remainder obtained after dividing each integer by 5. This time around the possible remainders are $0, 1, 2, 3, 4$.

Remainders

- Let's begin by playing the following game. Given an integer, we are going to divide it by 2 and compute the remainder.
- The remainder is either 0 or 1.
- Similarly, for each integer, consider the remainder obtained after dividing each integer by 5. This time around the possible remainders are $0, 1, 2, 3, 4$.
- We can play this game with respect to any integer, but we are going to focus on prime numbers for reasons that will become more clear a bit later.

Integers modulo a prime

- We now take all the integers, not necessarily positive, and divide them in accordance with the remainder one obtains after dividing each of these integers by a given prime number p.

Integers modulo a prime

- We now take all the integers, not necessarily positive, and divide them in accordance with the remainder one obtains after dividing each of these integers by a given prime number p.

- As we have discussed above, the possible remainders are

$$\{0, 1, 2, \ldots, p-1\}$$

and we call this the set of **remainders modulo a prime** p.

Integers modulo a prime

- We now take all the integers, not necessarily positive, and divide them in accordance with the remainder one obtains after dividing each of these integers by a given prime number p.

- As we have discussed above, the possible remainders are

$$\{0, 1, 2, \ldots, p-1\}$$

and we call this the set of **remainders modulo a prime** p.

- We define addition on this set of remainders as follows. We add a pair of remainders as we would normally and consider its remainder after dividing by p.

Integers modulo a prime-addition and multiplication

- For example, let $p = 5$. Then the set of remainders is $\{0, 1, 2, 3, 4\}$.

Integers modulo a prime-addition and multiplication

- For example, let $p = 5$. Then the set of remainders is $\{0, 1, 2, 3, 4\}$.

- Then, for instance,

$$1 + 2 = 3, \; 2 + 4 = 1, \; 3 + 4 = 2.$$

Integers modulo a prime-addition and multiplication

- For example, let $p = 5$. Then the set of remainders is $\{0, 1, 2, 3, 4\}$.
- Then, for instance,

$$1 + 2 = 3, \; 2 + 4 = 1, \; 3 + 4 = 2.$$

- This is because $2 + 4 = 6$ and its remainder after dividing by 5 is 1. And so on!

Integers modulo a prime-addition and multiplication

- For example, let $p = 5$. Then the set of remainders is $\{0, 1, 2, 3, 4\}$.

- Then, for instance,

$$1 + 2 = 3,\ 2 + 4 = 1,\ 3 + 4 = 2.$$

- This is because $2 + 4 = 6$ and its remainder after dividing by 5 is 1. And so on!

- We define multiplication on the set of remainders in a similar fashion.

Some more definitions

- We say that integers a and b are congruent modulo p, and write $a \equiv b \mod p$, if there exists an integer k such that

$$a - b = kp.$$

Some more definitions

- We say that integers a and b are congruent modulo p, and write $a \equiv b \mod p$, if there exists an integer k such that

$$a - b = kp.$$

- We say that r is the **canonical remainder** of a after division by p if

$$a \equiv r \mod p \text{ and } 0 \leq r \leq p - 1.$$

Multiplicative inverses modulo a prime

- Let p be an odd prime and consider the set of canonical remainders modulo p:
$$\{0, 1, 2, \ldots, p-1\}.$$

Multiplicative inverses modulo a prime

- Let p be an odd prime and consider the set of canonical remainders modulo p:

$$\{0, 1, 2, \ldots, p-1\}.$$

- Let us start with the case $p = 3$ and note that

$$1 \cdot 1 = 1, \; 2 \cdot 2 = 1.$$

Multiplicative inverses modulo a prime

- Let p be an odd prime and consider the set of canonical remainders modulo p:

$$\{0, 1, 2, \ldots, p-1\}.$$

- Let us start with the case $p = 3$ and note that

$$1 \cdot 1 = 1, \ 2 \cdot 2 = 1.$$

- It follows that every non-zero element in the set of canonical remainders modulo 3 is its own multiplicative inverse.

Multiplicative inverses modulo a prime (continued)

- Now consider the case $p = 5$. We have

$$1 \cdot 1 = 1, \; 2 \cdot 3 = 1, \; 3 \cdot 2 = 1, \; 4 \cdot 4 = 1.$$

Multiplicative inverses modulo a prime (continued)

- Now consider the case $p = 5$. We have

$$1 \cdot 1 = 1,\ 2 \cdot 3 = 1,\ 3 \cdot 2 = 1,\ 4 \cdot 4 = 1.$$

- Once again, every non-zero element has an inverse, but this time, not every element is its own inverse.

Multiplicative inverses modulo a prime (continued)

- Now consider the case $p = 5$. We have

$$1 \cdot 1 = 1,\ 2 \cdot 3 = 1,\ 3 \cdot 2 = 1,\ 4 \cdot 4 = 1.$$

- Once again, every non-zero element has an inverse, but this time, not every element is its own inverse.

- We are going to prove that as long as p is a prime, every non-zero element of the set of remainders has a multiplicative inverse.

Multiplicative inverses modulo a prime (continued)

- Now consider the case $p = 5$. We have

$$1 \cdot 1 = 1, \; 2 \cdot 3 = 1, \; 3 \cdot 2 = 1, \; 4 \cdot 4 = 1.$$

- Once again, every non-zero element has an inverse, but this time, not every element is its own inverse.

- We are going to prove that as long as p is a prime, every non-zero element of the set of remainders has a multiplicative inverse.

- To this end, take a non-zero element a of the set of canonical remainders modulo a prime p and consider

$$a, \; 2a, \; \dots \; (p-1)a.$$

Multiplicative inverses modulo a prime (continued)

- Observe that none of the numbers $a, 2a, \dots, (p-1)a$ are 0 modulo p because p is prime.

Multiplicative inverses modulo a prime (continued)

- Observe that none of the numbers $a, 2a, \dots, (p-1)a$ are 0 modulo p because p is prime.

- Indeed, suppose that $1 \leq k \leq p-1$, and the remainder of ka after the division by p is 0.

Multiplicative inverses modulo a prime (continued)

- Observe that none of the numbers $a, 2a, \ldots, (p-1)a$ are 0 modulo p because p is prime.
- Indeed, suppose that $1 \leq k \leq p-1$, and the remainder of ka after the division by p is 0.
- Then $ka = mp$ for some integer m, but this is impossible because p is prime!

Multiplicative inverses modulo a prime (continued)

- Observe that none of the numbers $a, 2a, \dots, (p-1)a$ are 0 modulo p because p is prime.
- Indeed, suppose that $1 \leq k \leq p-1$, and the remainder of ka after the division by p is 0.
- Then $ka = mp$ for some integer m, but this is impossible because p is prime!
- Our next observation is that the remainders of $a, 2a, \dots, (p-1)a$ after division by p are all distinct.

Multiplicative inverses modulo a prime (continued)

- Observe that none of the numbers $a, 2a, \ldots, (p-1)a$ are 0 modulo p because p is prime.
- Indeed, suppose that $1 \leq k \leq p-1$, and the remainder of ka after the division by p is 0.
- Then $ka = mp$ for some integer m, but this is impossible because p is prime!
- Our next observation is that the remainders of $a, 2a, \ldots, (p-1)a$ after division by p are all distinct.
- Indeed, if $ka \equiv k'a \mod p$ with $1 \leq k, k' \leq p-1$, then $(k-k')a$ is a multiple of p, which is, once again impossible since p is prime.

Multiplicative inverses modulo a prime (continued)

- What did we just prove? We took a non-zero element a of the set of remainder modulo a prime p and considered the set

$$a, \ 2a, \ \dots (p-1)a,$$

Multiplicative inverses modulo a prime (continued)

- What did we just prove? We took a non-zero element a of the set of remainder modulo a prime p and considered the set

$$a, \ 2a, \ \dots \ (p-1)a,$$

- and determined that these $p-1$ elements are distinct and non-zero.

Multiplicative inverses modulo a prime (continued)

- What did we just prove? We took a non-zero element a of the set of remainder modulo a prime p and considered the set

$$a, \; 2a, \; \dots \; (p-1)a,$$

- and determined that these $p-1$ elements are distinct and non-zero.
- This implies that exactly one of them must equal to 1!

Multiplicative inverses modulo a prime (continued)

- What did we just prove? We took a non-zero element a of the set of remainder modulo a prime p and considered the set

$$a,\ 2a,\ \dots\ (p-1)a,$$

- and determined that these $p-1$ elements are distinct and non-zero.
- This implies that exactly one of them must equal to 1!
- Thus we have shown that every non-zero element of the set of remainders modulo a prime p has a multiplicative inverse.

Finite plane

- Denote the set of remainder modulo p by $\mathbb{Z}_p$.

Finite plane

- Denote the set of remainder modulo p by $\mathbb{Z}_p$.

- The finite plane over $\mathbb{Z}_p$, denoted by $\mathbb{Z}_p^2$, is the set of **vectors**

$$\{(x_1, x_2) : x_j \in \mathbb{Z}_p\}.$$

Finite plane

- Denote the set of remainder modulo p by $\mathbb{Z}_p$.

- The finite plane over $\mathbb{Z}_p$, denoted by $\mathbb{Z}_p^2$, is the set of **vectors**

$$\{(x_1, x_2) : x_j \in \mathbb{Z}_p\}.$$

- Note that if $x = (x_1, x_2)$ and $y = (y_1, y_2)$ are both in $\mathbb{Z}_p^2$, then

$$x + y = (x_1 + y_1, x_2 + y_2) \in \mathbb{Z}_p^2.$$

Finite plane

- Denote the set of remainder modulo p by $\mathbb{Z}_p$.

- The finite plane over $\mathbb{Z}_p$, denoted by $\mathbb{Z}_p^2$, is the set of **vectors**

$$\{(x_1, x_2) : x_j \in \mathbb{Z}_p\}.$$

- Note that if $x = (x_1, x_2)$ and $y = (y_1, y_2)$ are both in $\mathbb{Z}_p^2$, then

$$x + y = (x_1 + y_1, x_2 + y_2) \in \mathbb{Z}_p^2.$$

- Also observe that if $x = (x_1, x_2) \in \mathbb{Z}_p^2$ and $\alpha \in \mathbb{Z}_p$ (to be referred to as a **scalar**), then

$$\alpha x = (\alpha x_1, \alpha x_2) \in \mathbb{Z}_p^2.$$

Finite plane-example

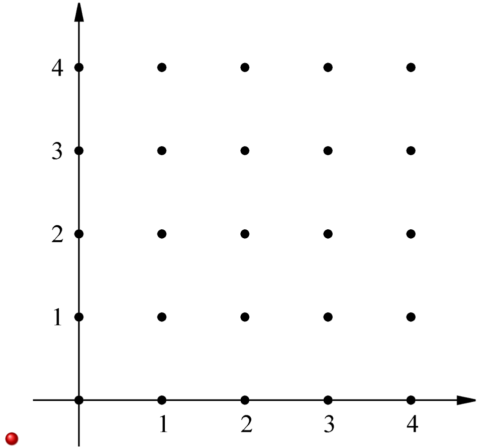

Figure: The grid $\mathbb{Z}_5^2$.

Finite plane: lines

- What is a line in a finite plane?

Finite plane: lines

- What is a line in a finite plane?

- Let $x = (x_1, x_2) \in \mathbb{Z}_p^2$ and let $v = (v_1, v_2) \in \mathbb{Z}_p^2 \backslash (0, 0)$.

Finite plane: lines

- What is a line in a finite plane?

- Let $x = (x_1, x_2) \in \mathbb{Z}_p^2$ and let $v = (v_1, v_2) \in \mathbb{Z}_p^2 \backslash (0, 0)$.

- Define the line
$$L_{x,v} = \{x + tv : t \in \mathbb{Z}_p\},$$
where x shall be referred to as the **starting point** and v the **direction vector**.

Finite plane: lines

- What is a line in a finite plane?

- Let $x = (x_1, x_2) \in \mathbb{Z}_p^2$ and let $v = (v_1, v_2) \in \mathbb{Z}_p^2 \backslash (0, 0)$.

- Define the line
$$L_{x,v} = \{x + tv : t \in \mathbb{Z}_p\},$$
where x shall be referred to as the **starting point** and v the **direction vector**.

- The number of points on $L_{x,v}$, denoted by $|L_{x,v}|$, is equal to p.

Finite plane: lines

- What is a line in a finite plane?

- Let $x = (x_1, x_2) \in \mathbb{Z}_p^2$ and let $v = (v_1, v_2) \in \mathbb{Z}_p^2 \backslash (0,0)$.

- Define the line
$$L_{x,v} = \{x + tv : t \in \mathbb{Z}_p\},$$
where x shall be referred to as the **starting point** and v the **direction vector**.

- The number of points on $L_{x,v}$, denoted by $|L_{x,v}|$, is equal to p.

- It is reasonable to ask whether the basic properties of lines and points we learned in high school geometry are still valid in this setting.

Lines: example

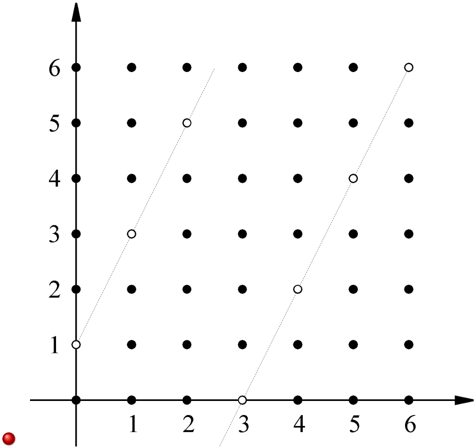

Figure: A line in $\mathbb{Z}_7^2$ with $x = (0,1)$ and $v = (1,2)$.

How many lines are there?

- Each line is determined by the starting point x and the direction v.

How many lines are there?

- Each line is determined by the starting point x and the direction v.
- However, it turns out that if v' is a constant (non-zero) multiple of v, then

$$L_{x,v} = L_{x,v'}.$$

How many lines are there?

- Each line is determined by the starting point x and the direction v.

- However, it turns out that if v' is a constant (non-zero) multiple of v, then
$$L_{x,v} = L_{x,v'}.$$

- Indeed, suppose that $v' = av$, where $a \neq 0$. Then
$$L_{x,v'} = L_{x,av} = \{x + tav : t \in \mathbb{Z}_p\}.$$

How many lines are there?

- Each line is determined by the starting point x and the direction v.

- However, it turns out that if v' is a constant (non-zero) multiple of v, then

$$L_{x,v} = L_{x,v'}.$$

- Indeed, suppose that $v' = av$, where $a \neq 0$. Then

$$L_{x,v'} = L_{x,av} = \{x + tav : t \in \mathbb{Z}_p\}.$$

- As t runs though $\mathbb{Z}_p$, at runs through every element of $\mathbb{Z}_p$ exactly once, just like in the proof above of the fact that every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse.

How many lines are there? (continued)

- We now observe that if we replace the starting point x by any other point y on the same line, then

$$L_{x,v} = L_{y,v}.$$

How many lines are there? (continued)

- We now observe that if we replace the starting point x by any other point y on the same line, then

$$L_{x,v} = L_{y,v}.$$

- Indeed, if y is on the same line, $y = x + av$ for some non-zero a. Then

$$L_{y,v} = \{x + av + tv : t \in \mathbb{Z}_p\} = \{x + (a+t)v : t \in \mathbb{Z}_p\}.$$

How many lines are there? (continued)

- We now observe that if we replace the starting point x by any other point y on the same line, then

$$L_{x,v} = L_{y,v}.$$

- Indeed, if y is on the same line, $y = x + av$ for some non-zero a. Then

$$L_{y,v} = \{x + av + tv : t \in \mathbb{Z}_p\} = \{x + (a + t)v : t \in \mathbb{Z}_p\}.$$

- As before, as t runs through $\mathbb{Z}_p$, $a + t$ runs through all the elements of $\mathbb{Z}_p$ exactly once.

How many lines are there? (conclusion)

- We are now ready to count the total number of lines.

How many lines are there? (conclusion)

- We are now ready to count the total number of lines.

- We have just seen that $L_{x,v}$ and $L_{x',v'}$ constitute the same line if and only if v' is a non-zero multiple of v and the difference between x and x' is a multiple of v.

How many lines are there? (conclusion)

- We are now ready to count the total number of lines.
- We have just seen that $L_{x,v}$ and $L_{x',v'}$ constitute the same line if and only if v' is a non-zero multiple of v and the difference between x and x' is a multiple of v.
- In other words, every v has $(p-1)$ equivalent directions (multiples of v) and given a v, every x has q equivalent starting points on the same line.

How many lines are there? (conclusion)

- We are now ready to count the total number of lines.
- We have just seen that $L_{x,v}$ and $L_{x',v'}$ constitute the same line if and only if v' is a non-zero multiple of v and the difference between x and x' is a multiple of v.
- In other words, every v has $(p-1)$ equivalent directions (multiples of v) and given a v, every x has q equivalent starting points on the same line.
- It follows that the total number of different lines is equal to

$$\frac{\#\text{ starting points} \times \#\text{ directions}}{(p-1)\cdot p} = \frac{p^2\cdot(p^2-1)}{p\cdot(p-1)} = p(p+1).$$

Intersection of lines

- In the Euclidean plane, two lines are either parallel, or they intersect at exactly one point. What about lines in $\mathbb{Z}_p^2$?

Intersection of lines

- In the Euclidean plane, two lines are either parallel, or they intersect at exactly one point. What about lines in $\mathbb{Z}_p^2$?

- We have already seen that whether $v = v'$, or $v' = av$, $a \neq 0$, the line is the same.

Intersection of lines

- In the Euclidean plane, two lines are either parallel, or they intersect at exactly one point. What about lines in $\mathbb{Z}_p^2$?
- We have already seen that whether $v = v'$, or $v' = av$, $a \neq 0$, the line is the same.
- Suppose that $L_{x,v}$ and $L_{x',v}$ intersect. Then

$$x + av = x' + bv \text{ for some } a, b \in \mathbb{Z}_p.$$

Intersection of lines

- In the Euclidean plane, two lines are either parallel, or they intersect at exactly one point. What about lines in $\mathbb{Z}_p^2$?

- We have already seen that whether $v = v'$, or $v' = av$, $a \neq 0$, the line is the same.

- Suppose that $L_{x,v}$ and $L_{x',v}$ intersect. Then

$$x + av = x' + bv \text{ for some } a, b \in \mathbb{Z}_p.$$

- This means that $x' = x + av - bv = x + (a - b)v$, so $x' \in L_{x,v}$.

Intersection of lines (continued)

- The same argument goes through if we consider the intersection of $L_{x,v}$ and $L_{x',av}$, where $a \neq 0$.

Intersection of lines (continued)

- The same argument goes through if we consider the intersection of $L_{x,v}$ and $L_{x',av}$, where $a \neq 0$.

- Thus we see that $L_{x,v}$ and $L_{x',av}$, $a \neq 0$, intersect if and only if $x' \in L_{x,v}$. If $x' \in L_{x,v}$, then $L_{x,v}$ and $L_{x',av}$ are the same line.

Intersection of lines (continued)

- The same argument goes through if we consider the intersection of $L_{x,v}$ and $L_{x',av}$, where $a \neq 0$.
- Thus we see that $L_{x,v}$ and $L_{x',av}$, $a \neq 0$, intersect if and only if $x' \in L_{x,v}$. If $x' \in L_{x,v}$, then $L_{x,v}$ and $L_{x',av}$ are the same line.
- We will now look at the case where there does not exist $a \neq 0$ such that $v' = av$.

  We shall see that for any starting points x and x', the intersection of $L_{x,v}$ and $L_{x',v'}$ consists of exactly one point.

Intersection of lines (continued)

- To see that $L_{x,v}$ and $L_{x',v'}$ intersect at exactly one point if v is not a multiple of v', we consider the equation

$$x + tv = x' + t'v'.$$

Intersection of lines (continued)

- To see that $L_{x,v}$ and $L_{x',v'}$ intersect at exactly one point if v is not a multiple of v', we consider the equation

$$x + tv = x' + t'v'.$$

- More precisely, we must find $t \in \mathbb{Z}_p$ and $t' \in \mathbb{Z}_p$ such that

$$x - x' = t'v' - tv,$$

Intersection of lines (continued)

- To see that $L_{x,v}$ and $L_{x',v'}$ intersect at exactly one point if v is not a multiple of v', we consider the equation

$$x + tv = x' + t'v'.$$

- More precisely, we must find $t \in \mathbb{Z}_p$ and $t' \in \mathbb{Z}_p$ such that

$$x - x' = t'v' - tv,$$

- where x and x' are fixed vectors in $\mathbb{Z}_p^2$ and v and v' are fixed vectors in $\mathbb{Z}_p^2 \backslash \{(0,0)\}$ that are not multiples of one another.

- Note that $x - x'$ is an arbitrary vector in $\mathbb{Z}_p^2$ in this setup.

Intersection of lines (continued)

- Note that $x - x'$ is an arbitrary vector in $\mathbb{Z}_p^2$ in this setup.

- Also note that we must show that t, t' above are unique because we are trying to prove that there is exactly **one** point of intersection!

Intersection of lines (continued)

- Note that $x - x'$ is an arbitrary vector in $\mathbb{Z}_p^2$ in this setup.
- Also note that we must show that t, t' above are unique because we are trying to prove that there is exactly **one** point of intersection!
- As a result, we have reduced matters to the following question. Is it true that if v, v' are non-zero vectors in $\mathbb{Z}_p^2$ that are not multiples of another another, and w is an arbitrary vector in $\mathbb{Z}_p^2$, then there exist unique scalars a, a' such that

$$w = av + a'v'?$$

Intersection of lines (continued)

- Note that $x - x'$ is an arbitrary vector in $\mathbb{Z}_p^2$ in this setup.

- Also note that we must show that t, t' above are unique because we are trying to prove that there is exactly **one** point of intersection!

- As a result, we have reduced matters to the following question. Is it true that if v, v' are non-zero vectors in $\mathbb{Z}_p^2$ that are not multiples of another another, and w is an arbitrary vector in $\mathbb{Z}_p^2$, then there exist unique scalars a, a' such that

$$w = av + a'v'?$$

- If the answer is yes, we recover the answer to the question above by taking $w = x - x'$, $t' = a$, and $t = -a$.

Bases of $\mathbb{Z}_p^2$

- In the process of resolving the question we just raised, we introduce the following notion.

Bases of $\mathbb{Z}_p^2$

- In the process of resolving the question we just raised, we introduce the following notion.

- We say that vectors v and v' form a **basis** of $\mathbb{Z}_p^2$ if every vector w in $\mathbb{Z}_p^2$ can be expressed in exactly one way in the form

$$av + a'v',$$

where a, a' are scalars.

Bases of $\mathbb{Z}_p^2$

- In the process of resolving the question we just raised, we introduce the following notion.

- We say that vectors v and v' form a **basis** of $\mathbb{Z}_p^2$ if every vector w in $\mathbb{Z}_p^2$ can be expressed in exactly one way in the form

$$av + a'v',$$

where a, a' are scalars.

- We claim that v, v' form a basis of $\mathbb{Z}_p^2$ if and only if v and v' are non-zero vectors that are not multiples of one another.

Bases of $\mathbb{Z}_p^2$ (continued)

- We are trying to solve the equation

$$av + a'v' = w,$$

where v, v' and w are given.

Bases of $\mathbb{Z}_p^2$ (continued)

- We are trying to solve the equation

$$av + a'v' = w,$$

where v, v' and w are given.

- Rewriting this as a matrix equation, we get

$$\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot \begin{pmatrix} a \\ a' \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

Bases of $\mathbb{Z}_p^2$ (continued)

- We are trying to solve the equation

$$av + a'v' = w,$$

where v, v' and w are given.

- Rewriting this as a matrix equation, we get

$$\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot \begin{pmatrix} a \\ a' \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

- We can check by a direct calculation that if $v_1 v_2' - v_2 v_1' \neq 0$, then

Bases of $\mathbb{Z}_p^2$ (continued)

- $$\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot \frac{1}{v_1 v_2' - v_2 v_1'} \begin{pmatrix} v_2' & -v_1' \\ -v_2 & v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

  and

Bases of $\mathbb{Z}_p^2$ (continued)

- $$\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot \frac{1}{v_1 v_2' - v_2 v_1'} \begin{pmatrix} v_2' & -v_1' \\ -v_2 & v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

  and

- $$\frac{1}{v_1 v_2' - v_2 v_1'} \begin{pmatrix} v_2' & -v_1' \\ -v_2 & v_1 \end{pmatrix} \cdot \begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Bases of $\mathbb{Z}_p^2$ (continued)

- $$\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot \frac{1}{v_1 v_2' - v_2 v_1'} \begin{pmatrix} v_2' & -v_1' \\ -v_2 & v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

  and

- $$\frac{1}{v_1 v_2' - v_2 v_1'} \begin{pmatrix} v_2' & -v_1' \\ -v_2 & v_1 \end{pmatrix} \cdot \begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

- We shall refer to $\frac{1}{v_1 v_2' - v_2 v_1'} \begin{pmatrix} v_2' & -v_1' \\ -v_2 & v_1 \end{pmatrix}$ as the inverse matrix of $\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix}$.

Bases of $\mathbb{Z}_p^2$ (continued)

- We are now ready to resolve the question that we posed. We are trying to solve the equation

$$av + a'v' = w,$$

where v, v' and w are given. Rewriting this as a matrix equation, we get

$$\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot \begin{pmatrix} a \\ a' \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

Bases of $\mathbb{Z}_p^2$ (continued)

- We are now ready to resolve the question that we posed. We are trying to solve the equation

$$av + a'v' = w,$$

where v, v' and w are given. Rewriting this as a matrix equation, we get

$$\begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} \cdot \begin{pmatrix} a \\ a' \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

- Multiplying both sides by the inverse matrix, we obtain

$$\begin{pmatrix} a \\ a' \end{pmatrix} = \frac{1}{v_1 v_2' - v_2 v_1'} \begin{pmatrix} v_2' & -v_1' \\ -v_2 & v_1 \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

- We just saw that we can solve for the coefficients of a and a' and the question is thus resolved.

Bases of $\mathbb{Z}_p^2$ (back to lines)

- We just saw that we can solve for the coefficients of a and a' and the question is thus resolved.

- Recall that this allows us to conclude that if v and v' are direction vectors that are not multiples of one another, then the lines $L_{x,v}$ and $L_{x',v'}$ intersect at exactly one point.

Bases of $\mathbb{Z}_p^2$ (back to lines)

- We just saw that we can solve for the coefficients of a and a' and the question is thus resolved.
- Recall that this allows us to conclude that if v and v' are direction vectors that are not multiples of one another, then the lines $L_{x,v}$ and $L_{x',v'}$ intersect at exactly one point.
- We now have a reasonably good understanding of what the discrete plane $\mathbb{Z}_p^2$ is, what lines in this plane look like and how they intersect.

Bases of $\mathbb{Z}_p^2$ (back to lines)

- We just saw that we can solve for the coefficients of a and a' and the question is thus resolved.

- Recall that this allows us to conclude that if v and v' are direction vectors that are not multiples of one another, then the lines $L_{x,v}$ and $L_{x',v'}$ intersect at exactly one point.

- We now have a reasonably good understanding of what the discrete plane $\mathbb{Z}_p^2$ is, what lines in this plane look like and how they intersect.

- This puts us in a good position to dive into deeper waters, which we are going to do in the second video of this series.