

Welcome back to Extensions!

Here are some things to do whilst we wait for everyone to join us...

1. For each pair of cards, find the symbol that appears on both of them.

a.



b.



2. Give three solutions to the congruence: $x \equiv 3 \pmod{7}$.

3. Find a solution to the **simultaneous congruences**: $x \equiv 2 \pmod{5}$ and $x \equiv 4 \pmod{7}$.

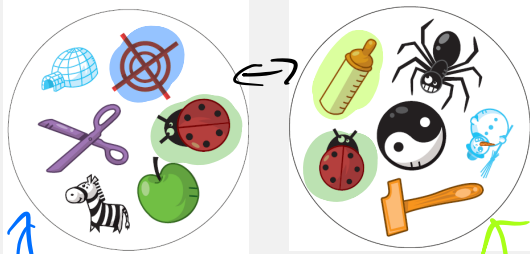
4. Find the equation of the line going through $(2, 1)$ and $(4, 5)$.

5. Find the equation of the line going through (x_1, y_1) and (x_2, y_2) .

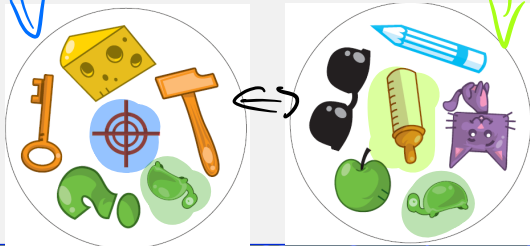
Intro Problems

1. For each pair of cards, find the symbol that appears on both of them.

a.



b.



a) Ladybug / Ladybird
b) Turtle

Target/crosshairs
Baby bottle

These are
taken from
the card
game "Dobble"

Intro Problems

2. Give three solutions to the congruence: $x \equiv 3 \pmod{7}$. \rightarrow remainder 3 when you divide by 7
eg. 3, 10, 17, 24,

3. Find a solution to the **simultaneous congruences**: $x \equiv 2 \pmod{5}$ and $x \equiv 4 \pmod{7}$.

$2 \pmod{5} \rightarrow 2, 7, 12, 17, 22, 27, 32, 37, \dots$ $5a + 2 = 7b + 4$

$4 \pmod{7} \rightarrow 4, 11, 18, 25, 32, \dots$

"Simultaneous equations in modular arithmetic"

Intro Problems

4. Find the equation of the line going through $(2, 1)$ and $(4, 5)$.

$$y - y_1 = m(x - x_1)$$

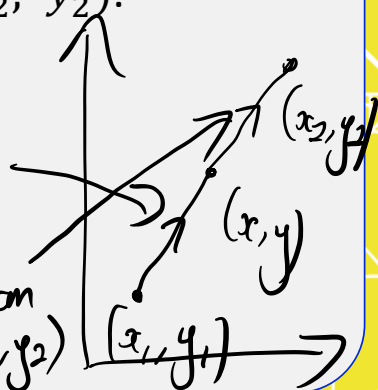
$$\boxed{y = 2x - 3}$$

$$\begin{aligned} &\rightarrow (x_1, y_1) = (2, 1) \\ &\leftarrow m = 2 \end{aligned}$$

5. Find the equation of the line going through (x_1, y_1) and (x_2, y_2) .

$$\frac{y - y_1}{y_2 - y_1} = \frac{x - x_1}{x_2 - x_1}$$

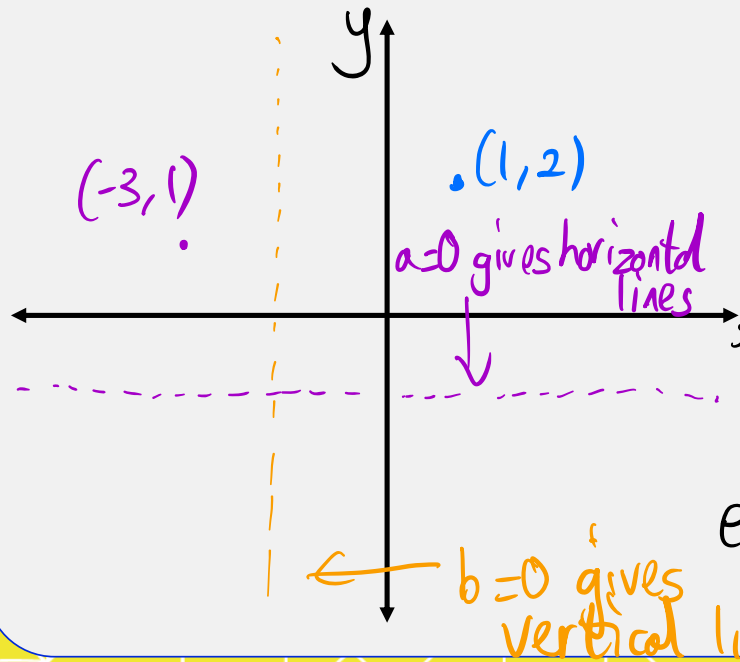
Gradient of
first part
= gradient
of overall
segment from
 (x_1, y_1) to (x_2, y_2)



$$\rightarrow (y_2 - y_1)x - (x_2 - x_1)y + (x_2 y_1 - x_1 y_2) = 0$$

Recap of (Euclidean) plane geometry

Here's a picture of the usual (Euclidean) 2D plane:



Points: (x, y) , x and y real numbers.

eg. $(1, 2)$

eg. $(-3, 1)$

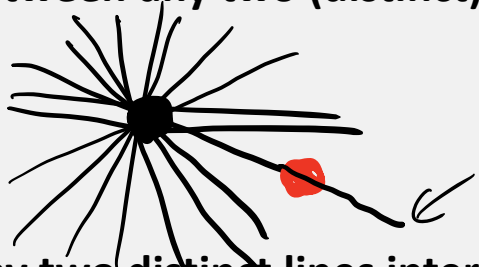
Lines: $ax + by + c = 0$, where a, b, c are real numbers (not all zero).

and at least
one of $a, b \neq 0$.

eg. $2x + 4y - 3 = 0$

Recap of (Euclidean) plane geometry

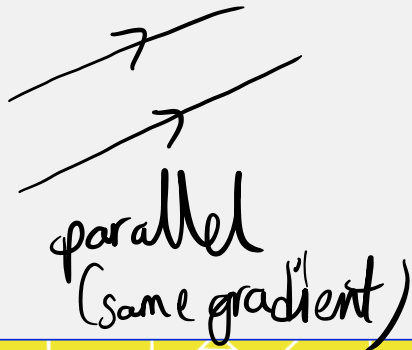
Between any two (distinct) points, there's a unique line going through them.



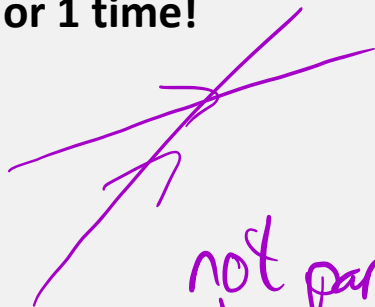
2 points \rightarrow determines gradient m .

$$y - y_1 = m(x - x_1)$$

Any two distinct lines intersect 0 times or 1 time!



parallel
(same gradient)



not parallel/
different gradients

Projective (plane) geometry: points

Points: $(x: y: z)$, where x, y, z are real numbers (not all equal to zero).
There are infinitely many “representations” of a point: $(\alpha x: \alpha y: \alpha z)$ also represents the same point as $(x: y: z)$, for any non-zero real number α .

$$\begin{aligned}\text{eg. } (1:2:3) &= (2:4:6) = (3:6:9) \\ &= (10:20:30) = (-5:-10:-15) \\ &= (1.5:3:4.5)\end{aligned}$$

But $(1:3:2)$ is a different point, so their order matters.

Projective (plane) geometry: lines

Lines: $ax + by + cz = 0$, where a, b, c are real numbers (not all equal to zero).

eg. $x + 2y - 3z = 0 \rightarrow$ has multiple representations, eg. $2x + 4y - 6z = 0$
eg. $3x + 6y - 9z = 0$

$(1:1:1)$ is on this line, because $(1) + 2(1) - 3(1) = 1 + 2 - 3 = 0$

$(1:4:3)$ is on this line, because $(1) + 2(4) - 3(3) = 1 + 8 - 9 = 0$

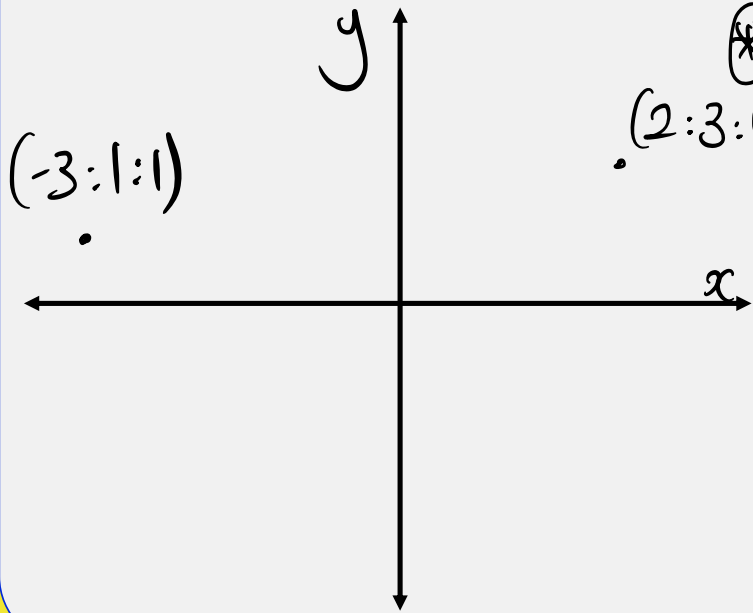
$(6:3:4)$ is on this line, because $(6) + 2(3) - 3(4) = 6 + 6 - 12 = 0$

$(1:7:5)$ is on this line, because $(1) + 2(7) - 3(5) = 1 + 14 - 15 = 0$

$(7:10:9)$ is on this line, etc.

Projective (plane) geometry

The projective plane can be visualised like so:



plot at (x, y)

*** "Regular" points:** $(x: y: 1)$, where x and y are real numbers.

$(2:3:1)$

Why? Well, $(X:Y:Z) = \left(\frac{X}{Z} : \frac{Y}{Z} : 1\right)$

Points "at infinity": $(x: y: 0)$ where x and y are not both zero.

↳ These can't be visualised/plotted like the regular points...

Projective (plane) geometry: some examples

“Regular” points: $(x: y: 1)$, where x and y are real numbers.

Points “at infinity”: $(x: y: 0)$ where x and y are not both zero.

1. What points are on the line $4x - 2y - z = 0$?

Regular points: $(1:0:4)$ and $(2:1:4)$ are on this line

Points at infinity: only $(1:2:0)$ → observation: only one point “at infinity”

Projective (plane) geometry: some examples

“Regular” points: $(x: y: 1)$, where x and y are real numbers.

Points “at infinity”: $(x: y: 0)$ where x and y are not both zero.

2. Where do the lines $4x - 2y - z = 0$ and $6x + 3y + z = 0$ intersect?

We try to “solve” the simultaneous equations.

$$4x - 2y - z = 0$$

$$6x + 3y + z = 0$$

$$10x + y = 0$$

$(+)$

$\rightarrow y = -10x$, hence $4x - 2(-10x) - z = 0$
so $z = -24x$.

Hence the intersection point is $(x: -10x: -24x)$
which is the same as $(1: -10: -24)$

Projective (plane) geometry: some examples

“Regular” points: $(x: y: 1)$, where x and y are real numbers.

Points “at infinity”: $(x: y: 0)$ where x and y are not both zero.

3. What's an equation of the line going through $(-2: 5: 11)$ and $(4: -6: 10)$?

The equation of a line is $ax + by + cz = 0$. We need to find a, b, c . We know they satisfy:

$$\textcircled{1} -2a + 5b + 11c = 0 \xrightarrow{\times 2} -4a + 10b + 22c = 0$$

$$\textcircled{2} 4a - 6b + 10c = 0 \rightarrow \underline{4a - 6b + 10c = 0} \quad (+)$$

$$4b + 32c = 0, \text{ ie. } b = -8c$$

$$\text{In } \textcircled{1}: -2a + 5(-8c) + 11c = 0 \rightarrow a = -\frac{29}{2}c \rightarrow \text{so } c = 2, b = -16, a = -29 \text{ is a solution.}$$

Projective (plane) geometry: problems

1. Separate the following into different representations of the same point.
(1: 1: 2) (3: -9: 3) (-3: -3: -6) ($a/3$: $-a$: $a/3$) (1: 0: 10) (0.5: 1.5: 0.5)
2. Find an equation of the line which goes through the following two points:
 - a. (1: 2: 1) and (1: 2: 0)
 - b. (3: -2: -1) and (5: -3: -2)
 - c. (6: -3: -1.5) and (-10: 5: -2.5).
3. Where do the lines $4x - 2y - z = 0$ and $6x - 3y + z = 0$ intersect?

$$ax + by + cz = 0$$

Want to find a, b, c .

Projective (plane) geometry: solutions

1. Separate the following into different representations of the same point.

$(1: 1: 2)$ $(3: -9: 3)$ $(-3: -3: -6)$ $(a/3: -a: a/3)$ $(1: 0: 10)$ $(0.5: 1.5: 0.5)$

Arrows indicate scaling factors:

- From $(1: 1: 2)$ to $(-3: -3: -6)$ with factor $\times (-3)$
- From $(-3: -3: -6)$ to $(a/3: -a: a/3)$ with factor $(\frac{a}{9})$

2. Find an equation of the line which goes through the following two points:

a. $(1: 2: 1)$ and $(1: 2: 0)$

$$y = 2x$$

$$\text{or } 2x - y = 0$$

→ method: find a, b, c that satisfy

$$a(1) + b(2) + c = 0$$

and

$$a(1) + b(2) + c(0) = 0.$$

Projective (plane) geometry: solutions

2. Find an equation of the line which goes through the following two points:

b. $(3: -2: -1)$ and $(5: -3: -2)$

$$3a - 2b - c = 0 \rightarrow 6a - 4b - 2c = 0$$

$$5a - 3b - 2c = 0 \rightarrow 5a - 3b - 2c = 0 \quad \ominus$$

$$\underline{a - b = 0} \rightarrow \underline{a = b = 1}$$

$$\downarrow \\ c = 1$$

c. $(6: -3: -1.5)$ and $(-10: 5: -2.5)$.

→ Similar method to 2b;
solve for a, b, c in the simultaneous equations

$$x + 2y = 0$$

$$ax + by + cz = 0$$

$$x + y + z = 0$$

Projective (plane) geometry: solutions

3. Where do the lines $4x - 2y - z = 0$ and $6x - 3y + z = 0$ intersect?

$$\begin{array}{rcl} \textcircled{1} & 4x - 2y - z = 0 & \\ & 6x - 3y + z = 0 & \textcircled{+} \\ \hline & 10x - 5y = 0 & \\ & 2x = y & \end{array}$$

In $\textcircled{1}$, $4x - 2(2x) - z = 0$
 $\Rightarrow z = 0$. Hence the intersection
is at $(x : 2x : 0)$

\rightarrow all of these
represent the same
point, $(1 : 2 : 0)$

$$\begin{array}{l} 4x - 2y - 1 = 0 \\ 6x - 3y + 1 = 0 \end{array} \left. \vphantom{\begin{array}{l} 4x - 2y - 1 = 0 \\ 6x - 3y + 1 = 0 \end{array}} \right\} \text{parallel lines}$$

So parallel lines intersect
at a point at infinity!

Modular arithmetic recap

Remember that if n is a positive integer, then any integer x is congruent to exactly one of $0, 1, \dots, n - 1$ modulo n .

This is because... the remainder when you divide by n is one of $0, 1, 2, \dots, n-1$

This means we can focus on "arithmetic modulo n " with only the numbers $0, 1, 2, \dots, n - 1$. For example.

eg. $n = 7 \rightarrow$ instead of 10, $10 \equiv 3 \pmod{7}$
instead of 100, $100 \equiv 2 \pmod{7}$

Modular arithmetic recap

This means we can focus on “arithmetic modulo n ” with only the numbers $0, 1, 2, \dots, n - 1$. For example.

eg. $n = 13$.

Then: $7 \times 5 = 35 \equiv 9 \pmod{13}$ “9 is smaller than 35, easier to manage in calculations”

$$6^4 = 6^2 6^2 = 36 \times 36 \equiv (-4) \times (-4) \pmod{13} \quad \text{“3 is smaller than 6”}$$
$$\equiv 16 \pmod{13} \equiv 3 \pmod{13} \quad \text{than } 6^4$$

Modular arithmetic recap

If n is actually a prime number (say, p), then it's also true that:

between 1 and $p-1$

If a is an integer such that $0 < a < p-1$, then there exists an integer b such that $0 < b < p-1$ such that:

$$ab \equiv 1 \pmod{p}$$

$$3b \equiv 1 \pmod{7}$$

eg. $b=5$ is a solution here.

prime
↑

We call the number b a “multiplicative inverse of a , modulo p ”. This can be proven and obtained using the [extended version of Euclid's algorithm](#), but we won't do it here.

This makes the integers $0, 1, 2, \dots, p-1$ a “field” under the operation of addition and multiplication modulo p .

Projective geometry over other fields

We can work with the projective plane over this new field!

“Regular” points: $(x: y: 1)$, where x and y are one of $0, 1, 2, \dots, p - 1$.

Points “at infinity”: $(x: y: 0)$ where x and y are one of $0, 1, 2, \dots, p - 1$ (not both zero).

There are multiple “representations” of a point: $(\alpha x: \alpha y: \alpha z)$ also represents the same point as $(x: y: z)$, for any integer α ($1, 2, \dots, p - 1$).

eg. $p = 7$

$$(1: 2: 3) \xrightarrow{\times 2} (2: 4: 6) \xrightarrow{\times 3} (3: 6: 2) \xrightarrow{\times 4} (4: 1: 5)$$

because $8 \equiv 1 \pmod{7}$

because $9 \equiv 2 \pmod{7}$

because $12 \equiv 5 \pmod{7}$

Projective geometry over other fields: problems

If $p = 3$:

- 1) How many points are on the projective line $x - 2y - z = 0$?
- 2) How many points are there in this projective plane?

If $p = 5$:

- 3) How many points are on the projective line $4x - 2y - z = 0$?
- 4) How many points are there in this projective plane?

If you get done: answer the two questions for a general prime p .

Projective geometry over other fields

If $p = 3$:

1) How many points are on the projective line $x - 2y - z = 0$?

2) How many points are there in this projective plane?

① If $z=0 \rightarrow x=2y \quad (x \equiv 2y \pmod{7})$
 $y=0$ means $x=0 \rightarrow (0:0:0)$ not allowed

$y=1$ means $x=2 \rightarrow (2:1:0)$
 $y=2$ means $x=1 \rightarrow (1:2:0)$ same $(\times 2)$

If $z=1 \rightarrow x=2y+1 \quad (x \equiv 2y+1 \pmod{7})$ 4 points in total
 $y=0 \rightarrow x=1$
 $y=1 \rightarrow x=0$
 $y=2 \rightarrow x=2$ (3 regular one at infinity)

Projective geometry over other fields

If $p = 5$:

3) How many points are on the projective line $4x - 2y - z = 0$?

4) How many points are there in this projective plane?

③ If $z=0 \rightarrow 4x \equiv 2y \pmod{5} \rightarrow$ multiply both sides by 3
 $\rightarrow 12x \equiv 6y \pmod{5} \rightarrow$ but $12 \equiv 2 \pmod{5}$
 $\Rightarrow 2x \equiv y \pmod{5}$ and $6 \equiv 1 \pmod{5}$

As before, this gives only one point $(1:2:0)$.

If $z=1$, then we can plug in $y=0, y=1, y=2, y=3, y=4$ to get a different point each time.

So in total there are $5+1 = 6$ points on this line!

Projective geometry over other fields

General results when working over the field of integers modulo p :

Projective line: contains $p + 1$ points

Entire projective plane: contains $p^2 + p + 1$ points

→ one point at infinity and p regular points

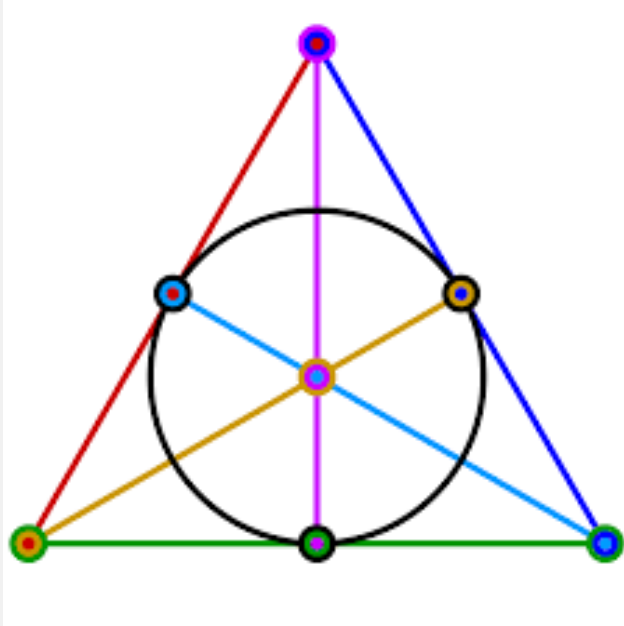
↳ p^2 regular points $(x:y:1)$ and $p+1$ at infinity $(x:y:0)$

Any two lines intersect at exactly one point!

Any two points lie on a unique line!

Projective geometry over other fields

Projective plane over the field of integers modulo 2: $\phi = 2$.



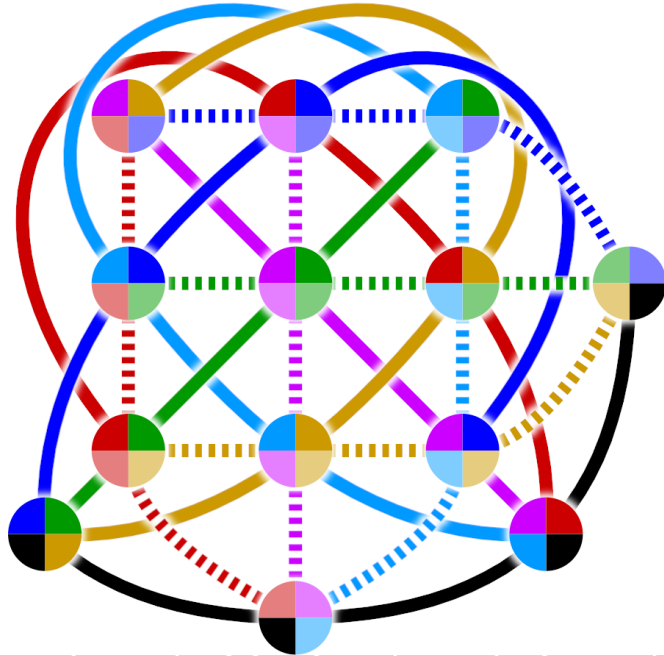
Each colour represents a different “line”

Observe how any two points lie on a unique line!

[This picture is sometimes called the “Fano plane”, and is of interest in other mathematical areas too]

Projective geometry over other fields

Projective plane over the field of integers modulo 3: $p = 3$.



More complicated picture, but the same properties as before!

[Pictures for fields of larger primes steadily become messier...]

Relation to Dobble

$$\rightarrow p = 7$$

Any two lines intersect at exactly one point!

Any two Dobble cards have exactly one symbol in common.

Any two points lie on a unique line!

If you pick any two symbols there is exactly one Dobble card with both of them on it!

Projective line: contains $p + 1$ points

↳ Each card has 8 symbols

Entire projective plane:

contains $p^2 + p + 1$ points

→ Across the whole deck, there are 57 different symbols.

BONUS: there are $p^2 + p + 1$ different lines! There are 57 different cards

→ actually, the Dobble manufacturers only print 55, due to printing reasons.

SPARE SLIDE

SPARE SLIDE

Additional info and other links

More on projective geometry:

<https://www.math.toronto.edu/mathnet/questionCorner/projective.html>

Extended Euclidean algorithm: <https://www.youtube.com/watch?v=fz1vxq5ts5I>

Video by Matt Parker about Dobble: https://www.youtube.com/watch?v=VTDKqW_GLkw

Dobble resources and website:

<https://connect-and-play.asmodee.fun/spotit/>

You can have “finite fields” of different sizes too (in general, they can be a power of a prime, but are much harder to construct), to enable you to make Dobble decks with different numbers of symbols on each card!