Facet of Mathematics: Poster Topics

1 Image Processing

The following is a list of Image Processing poster topics for the Facets of Mathematics group poster. Each topic includes a brief description, some suggested topics you might want to focus on, and one or more starting point references.

For the Image Processing poster topics you should

- Do some further reading beyond the given starting point references – the poster should typically have about three references.
- Include some equations.
- Perform some relevant Python calculations and include at least one resulting image in the poster.

IP-P-1: JPEG compression

In week 1 we saw how images can be compressed using *lossy* and *lossless* compression. The widely used JPEG image format is a *lossy* format that is based on a mathematical technique known as the Discrete Cosine Transform, which splits up (small pieces of) the image into contributions which have different spatial frequencies.

In this project you can investigate how images are stored in the JPEG format.

Suggested topics to consider:

- The definition of the Discrete Cosine Transform (DCT).
- How the DCT is used in the JPEG format.
- How the DCT is used for lossy image compression.

Starting point reference:

- David Salomon, *Data Compression: The Complete Reference*, Fourth Edition, Springer-Verlag London Limited, 2007, sections 4.6.1 and 4.8

IP-P-2: Edge detection

In weeks 3–4 we introduced derivative filters, briefly relating these to numerical derivatives, and showing how these could be used to highlight edges in the image.

In this project you can consider edge detection using derivative filters in more detail, exploring the link to numerical differentiation.

Suggested topics to consider:

- First and second order derivative filters.
- The relation between edge detection and numerical differentiation.

- The effect of different types of derivative filters in detecting edges.

Starting point reference:

- Chris Solomon and Toby Breckon, *Fundamentals of Digital Image Processing: A Practical Approach with Examples in Matlab*, John Wiley & Sons, Ltd, 2011, section 4.5

IP-P-3: Colour models

In the Image Processing theme we have primarily focused on the RGB representation of 24-bit true colour images – using the RGB "colour model". However there are different ways to encode the colour of a pixel. Two other important colour models are the CMYK colour model, useful for printing, and the HSV colour model briefly mentioned in week 1.

In this project you can explore different colour models, where these are useful, and how to convert between them.

Suggested topics to consider:

- Encoding of colours
  - in greyscale images.
  - using the "RGB" colour model.
  - using the "CMYK" colour model.
  - using the "HSV" colour model.
- The difference between additive and subtractive colour models.
- Converting between different colour models.

Starting point references:

- Chris Solomon and Toby Breckon, *Fundamentals of Digital Image Processing: A Practical Approach with Examples in Matlab*, John Wiley & Sons, Ltd, 2011, section 1.4
- Luiz Velho, Alejandro C. Frery, and Jonas Gomes, *Image Processing for Computer Graphics and Vision*, second edition, Springer-Verlag London Limited, 2009, sections 5.6 and 16.6

IP-P-4: Image histograms

In week 2 we briefly considered the use of an image "histogram", constructed for a greyscale image by counting the number of pixels of a given intensity. This was used to guide changes to the image brightness and contrast through addition and multiplication.

In this project you can explore how histograms can be used in other applications, including thresholding, and in more advanced applications.

Suggested topics to consider:

- Defining histograms for greyscale and colour images.
- Using histograms to guide thresholding.
- Histogram equilization.

Starting point references:

- Chris Solomon and Toby Breckon, *Fundamentals of Digital Image Processing: A Practical Approach with Examples in Matlab*, John Wiley & Sons, Ltd, 2011, section 3.4
- Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, Fourth Edition, Pearson Education Limited, 2018, section 3.3

IP-P-5: Dithering

In weeks 1 and 3 we considered changing the image "colour depth", by reducing the number of bits used to encode a pixel colour. However this is is a lossy procedure, and the lower colour depth image may have lower quality than the original. "Dithering" can be used to improve the appearance of the resulting lower colour depth image.

In this project you can explore the effect of reducing the colour depth of an image, making use of colour palettes, and the use of dithering.

Suggested topics to consider:

- Colour quantization.
- Choosing a colour palette.
- Floyd-Steinberg dithering.

Starting point reference:

- Luiz Velho, Alejandro C. Frery, and Jonas Gomes, *Image Processing for Computer Graphics and Vision*, second edition, Springer-Verlag London Limited, 2009, sections 11.1–11.3, 12.1, 12.4.1

IP-P-6: High dynamic range

The dynamic range of a camera is the ratio between the maximum and minimum intensities that the camera can capture. The dynamic range of a camera may be too low for a single image to capture both low and high intensity features in an image – for example an image may be dominated by a single bright part of the image, and then other details are obscured in the remaining much darker parts of the image. High Dynamic Range imaging can be used to address this.

In this project you can explore different steps in High Dynamic Range imaging.

Suggested topics to consider:

- Constructing a High Dynamic Range image.
- Storing a High Dynamic Range image.
- Using tone mapping.

Starting point reference:

- Yasir Salih, Wazirah bt. Md-Esa, Aamir S. Malik, and Naufal Saad, *Tone mapping of HDR images: A review*, 2012 4th International Conference on Intelligent and Advanced Systems (ICIAS2012), Kuala Lumpur, Malaysia, 2012, 368–373, doi: 10.1109/ICIAS.2012.6306220

2 Cubic Curves

Below are the topics for the posters in the Cubic Curves theme. Each topic contains some suggested resources to get you started on the topic, but you should certainly read around the subject. There are also some suggested subtopics to look at. It is not necessary to include *all* the suggestions in your poster: they are there to give you some ideas of the sort of topics you could look at. Your poster must include a bibliography (typically around three references). It must include some figures. It must include some equations, and should also include some results from your own Python computations.

CC-P-1: Projective Geometry and Dobble

Dobble is a game involving 55 cards which looks like this:

Each card contains 8 distinct funny symbols, and there are 57 symbols in all the Dobble cards in total. The key feature of the game is the following condition:

every two distinct Dobble cards have exactly one symbol in common.

Players compete with each other to find the unique common symbol between two cards.

How can we generate a pack of Dobble cards? We have to choose 55 cards consisting of 8 symbols in a way such that every pair of cards has exactly one symbol in common. Simple combinatorics tells us that there are

$$\binom{57}{8} = 1652411475$$

cards in total. We have to choose 55 of them. How do we do this?

We can use the following idea: the symbols are the points in the projective plane $\mathbb{P}^2_{\mathbb{F}_7}$, and the cards are the lines in this plane. Here $\mathbb{F}_7$ is the *finite field* of 7 elements, which can be thought of as just the set of 7 integers

$$\{0, 1, 2, 3, 4, 5, 6\}$$

equipped with addition and multiplication, which can be described as

$$a + b = \text{the remainder of the integer } a + b \text{ when divided by } 7$$

and

$$a * b = \text{the remainder of the integer } a * b \text{ when divided by } 7$$

for every a and b in the set $\mathbb{F}_7$. The plane $\mathbb{P}^2_{\mathbb{F}_7}$ contains 57 points. Furthermore, there are 57 lines in $\mathbb{P}^2_{\mathbb{F}_7}$ and each line contains exactly 8 points. So, if we index the points in $\mathbb{P}^2_{\mathbb{F}_7}$ by integers between 1 and 57, we get 55 cards we

are looking for. In fact, we obtain 57 such cards. Why does Dobble have 55 cards? Apparently, for marketing reasons: 55 sounds better than 57

Instead of $\mathbb{F}_7$, we can consider another finite field consisting of q elements, where $q = p^n$ for some prime $p \geqslant 1$ and some positive integer n. Then, considering points and lines in the projective plane $\mathbb{P}^2_{\mathbb{F}_q}$, we can construct a Dobble game such that

- it consists of exactly $q^2 + q + 1$ cards,
- each card contains exactly $q + 1$ symbols,
- each two cards has exactly one symbol in common,
- there are $q^2 + q + 1$ symbols in total on all cards.

The simplest example of a finite field is the field $\mathbb{F}_2$ that consists of just two elements: 0 and 1. In this case, the plane $\mathbb{P}^2_{\mathbb{F}_2}$, also known as the Fano plane, consists of the following 7 points:

$$[0:0:1],\ [0:1:0],\ [1:0:0],\ [0:1:1],\ [1:0:1],\ [1:1:0],\ [1:1:1].$$

Similarly, there are just 7 lines in $\mathbb{P}^2_{\mathbb{F}_2}$. Their equations are

$$x = 0,\ y = 0,\ z = 0,\ x + y = 0,\ x + z = 0,\ y + z = 0,\ x + y + z = 0.$$

Substituting points of the plane $\mathbb{P}^2_{\mathbb{F}_2}$ into these equations, we obtain the following incidence table:

	$[0:0:1]$	$[0:1:0]$	$[1:0:0]$	$[0:1:1]$	$[1:0:1]$	$[1:1:0]$	$[1:1:1]$
$x = 0$	★	★		★			
$y = 0$	★		★		★		
$z = 0$		★	★			★	
$x + y = 0$	★					★	★
$x + z = 0$		★			★		★
$y + z = 0$			★	★			★
$x + y + z = 0$				★	★	★	

In this table, we put symbol ★ in a cell if the line in its row contains the point in its column. Indexing the points in this table by seven funny symbols, we obtain Dobble game with 7 cards such that each card contains 3 symbols with 7 symbols in total on all cards.

In your poster, you should define finite fields and projective planes over them in an accessible way, and explain the relation between them and the Dobble card game. You should provide explicit examples and explain how to produce Dobble card games with different numbers of cards. This is done in [1] in detail. If you wish, you can explain how to approach this problem from combinatorial point of view.

CC-P-2: Pappus, Pascal and Cayley–Bacharach

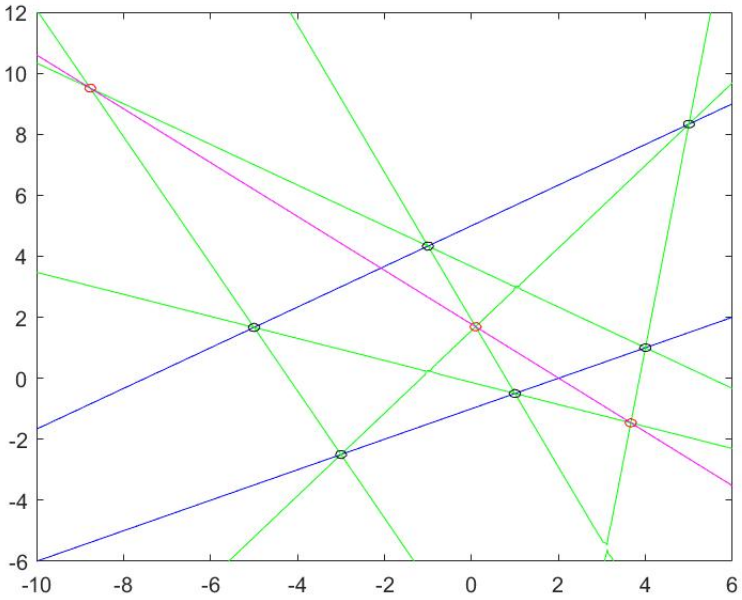
Pappus' hexagon theorem (attributed to Pappus of Alexandria) states that given three distinct collinear points P_1, P_2, P_3 in the plane, and another (disjoint) set of three collinear points Q_1, Q_2, Q_3, the intersection points

$$\{O_{12}\} = L_{12} \cap L_{21}, \quad \{O_{13}\} = L_{13} \cap L_{31}, \quad \{O_{23}\} = L_{23} \cap L_{32}$$

are collinear, where L_{12}, L_{13}, L_{23}, L_{21}, L_{31}, L_{32} are the lines defined as follows:

- L_{12} is the line that passes through the points P_1 and Q_2;
- L_{13} is the line that passes through the points P_1 and Q_3;
- L_{23} is the line that passes through the points P_2 and Q_3;
- L_{21} is the line that passes through the points P_2 and Q_1;
- L_{31} is the line that passes through the points P_3 and Q_1;
- L_{32} is the line that passes through the points P_3 and Q_2.

This result is illustrated by the following picture:



Here, we have $P_1 = (1, -\frac{1}{2})$, $P_2 = (-3, -\frac{5}{2})$ and $P_3 = (4, 1)$. These points are contained in the blue line given by $x - 2y - 2 = 0$. Similarly, we have $Q_1 = (5, \frac{25}{3})$, $Q_2 = (-1, \frac{13}{3})$ and $Q_3 = (-5, \frac{5}{3})$, which are contained in another blue line, given by the equation $2x - 3y + 15 = 0$. Using Python, we see that $O_{12} = (\frac{102}{1086}, \frac{1835}{1086})$, $O_{13} = (\frac{1015}{277}, -\frac{405}{277})$ and $O_{23} = (-\frac{447}{51}, \frac{485}{51})$. These points are indeed collinear: they are contained in the pink line, which is given by $625x + 708y - 1255 = 0$. The green lines in this picture are the lines L_{12}, L_{13}, L_{23}, L_{21}, L_{31}, L_{32}.

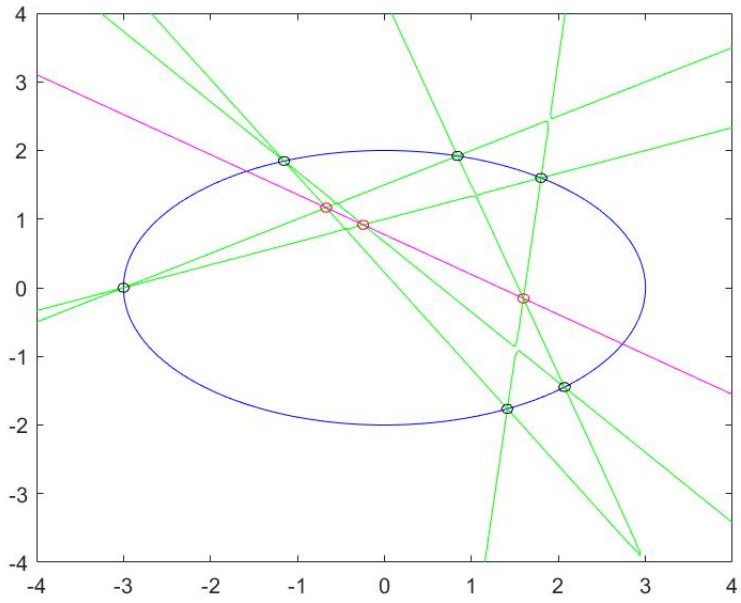
Pappus' theorem is a special case of Pascal's hexagrammum mysticum theorem (see [1, 7]). To explain it, fix a conic C in $\mathbb{R}^2$ such that C is either an ellipse, parabola, hyperbola or a union of two distinct lines. Then choose six points P_1, P_2, P_3, Q_1, Q_2, Q_3 in the conic C. If C is a union of two distinct lines, assume further that P_1, P_2, P_3 are contained in only one of them, and also Q_1, Q_2, Q_3 are contained only in the other line. Then we can define the lines L_{12}, L_{13}, L_{23}, L_{21}, L_{31}, L_{32} as above. This gives us three points

$$\{O_{12}\} = L_{12} \cap L_{21} \quad \{O_{13}\} = L_{13} \cap L_{31}, \quad \{O_{23}\} = L_{23} \cap L_{32}.$$

Pascal's theorem states that the points O_{12}, O_{13} and O_{23} are contained in one line, which is usually called the Pascal line. If C is an ellipse given by $4x^2 + 9y^2 = 36$, and the points P_1, P_2, P_3, Q_1, Q_2 and Q_3 are the points

$$(\tfrac{21}{25}, \tfrac{48}{25}), (\tfrac{9}{5}, \tfrac{8}{5}), (-\tfrac{15}{13}, \tfrac{24}{13}), (\tfrac{24}{17}, -\tfrac{30}{17}), (\tfrac{60}{29}, -\tfrac{42}{29}), (-3, 0),$$

respectively, then Pascal's theorem is illustrated by



Here, the lines L_{12}, L_{13}, L_{23}, L_{21}, L_{31}, L_{32} are the green lines, and the points $O_{12} = (\frac{123}{77}, -\frac{12}{77})$, $O_{13} = (-\frac{69}{103}, \frac{120}{103})$, $O_{23} = (-\frac{15}{61}, \frac{56}{61})$ are contained in the pink line, which is given by the equation $194x + 333y - 258 = 0$.

Both Pappus's theorem and Pascal's hexagrammum mysticum theorem follow from the famous Cayley–Bacharach theorem.

Theorem (Cayley–Bacharach)**.** Let C_1 and C_2 be cubic curves such that the intersection $C_1 \cap C_2$ consists of 9 points. Let C_3 be a cubic curve containing 8 of them. Then C_3 contains the ninth intersection point.

For example, if C_1 is given by the equation

$$\begin{aligned} &-5913252577x^3 + 30222000280x^2y - 21634931915xy^2 + \\ &\quad + 5556266591y^3 - 73906985473x^2 + 102209537669xy - 37300172365y^2 + \\ &\quad + 1389517162x - 88423819400y + 204616284808 = 0, \end{aligned}$$

and C_2 is given by the equation

$$\begin{aligned} &-4844332x^3 - 8147864x^2y - 4067744xy^2 - \\ &\quad - 1866029y^3 + 32668904x^2 - 28226008xy + 41719157y^2 + \\ &\quad + 252639484x + 126319742y - 960898976 = 0, \end{aligned}$$

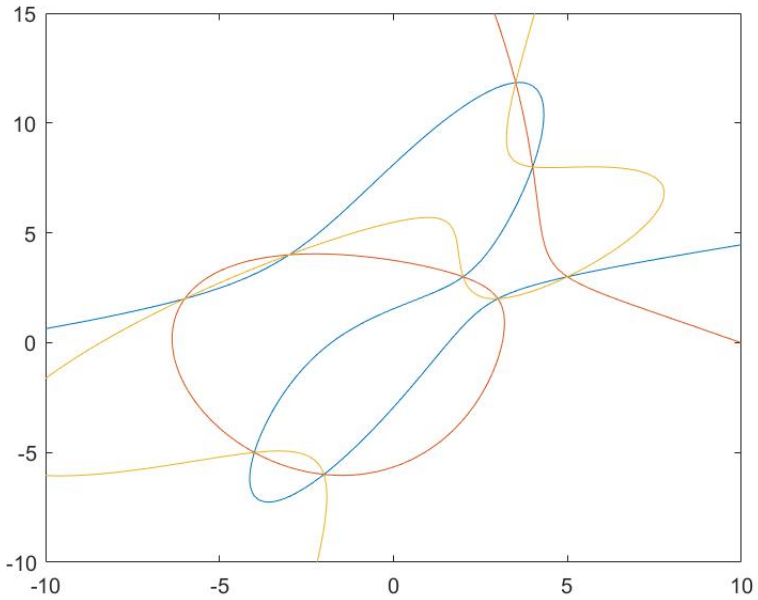
then the intersection $C_1 \cap C_2$ consists of the exactly nine points: $(2,3)$, $(-3,4)$, $(-4,-5)$, $(-6,2)$, $(5,3)$, $(3,2)$, $(-2,-6)$, $(4,8)$ and

$$\left(\frac{1439767504290697562}{409942054104759719}, \frac{4853460637572644276}{409942054104759719}\right). \qquad (\bigstar)$$

Then every cubic curve C_3 that contains the points

$$(2,3), (-3,4), (-4,-5), (-6,2), (5,3), (3,2), (-2,-6), (4,8)$$

must also contain the point ($\bigstar$). This can be explicitly checked by Python (see [1]). In fact, you can use Python to construct the curves C_1, C_2 and C_3 as distinct cubic curves in $\mathbb{R}^2$ that contains eight points $(2,3)$, $(-3,4)$, $(-4,-5)$, $(-6,2)$, $(5,3)$, $(3,2)$, $(-2,-6)$ and $(4,8)$. Then you can use Python to find the coordinates of the remaining ninth point ($\bigstar$) of the intersection $C_1 \cap C_3$. This example is illustrated by the following picture, where C_1 is a blue curve, C_2 is a red curve, and C_3 is an orange curve.



In its turn, the Cayley–Bacharach theorem is implied, via *Chasles' theorem*, by the following lemma, which is proved in [1].

Lemma. Let Σ be a finite subset in $\mathbb{P}^2_{\mathbb{C}}$ consisting of at most 8 points such that at most 3 points in Σ are contained in a line, and at most 6 points in Σ are contained in a conic. Then the points of Σ impose independent linear conditions on cubic curves in $\mathbb{P}^2_{\mathbb{C}}$.

In your poster, you should describe Pappus' theorem, Pascal's hexagrammum mysticum theorem and the Cayley–Bacharach theorem, and illustrate them by explicit examples, pictures and Python computations. You should explain how to use the Cayley–Bacharach theorem to prove Pappus' theorem and Pascal's hexagrammum mysticum theorem (see [1]). You can explain how to use our lemma to prove the Cayley–Bacharach theorem, and you can illustrate this lemma by explicit examples.

CC-P-3: Group Law on Cubic Curves

Let $\mathcal{C}$ be a smooth irreducible cubic curve in $\mathbb{R}^2$, and let O be a point in $\mathcal{C}$. Then we can equip the curve $\mathcal{C}$ with an addition operation $+$ that takes any two points A and B in $\mathcal{C}$ and produces a point $A+B$ in $\mathcal{C}$ such that the following conditions are satisfied:

(a) For every triple of points A, B and C in $\mathcal{C}$, one has $(A+B)+C=A+(B+C)$.

(b) For every point A in $\mathcal{C}$, one has $A+O=O+A=A$.

(c) For every point $A\in\mathcal{C}$ there is a unique point $B\in\mathcal{C}$ such that

$$A+B=B+A=O.$$

This point B is usually denoted by $-A$.

(d) For every pair of points A and B in $\mathcal{C}$, one has $A+B=B+A$.

The first three conditions are axioms of a *group*, so that the curve $\mathcal{C}$ equipped with $+$ is a group. The fourth conditions means that this group is *commutative*.

Given two points A and B in the curve $\mathcal{C}$, there is an explicit algorithm for constructing the point $A+B$ in the curve $\mathcal{C}$. It is described in, for instance, [1]. Namely, we can define $A+B$ as follows:

- If $A \neq B$, let L be the line in $\mathbb{R}^2$ that passes through A and B. If $A = B$, let L be the line in $\mathbb{R}^2$ that is tangent to $\mathcal{C}$ at the point $A = B$.
- The intersection $L \cap \mathcal{C}$ consists of the points A, B and some point P. It may happen that the point P lies at infinity, so projective geometry comes in handy to deal with this problem. Moreover, we may have $P = A$. In this case, the line L is tangent to the curve $\mathcal{C}$ at the point A. Similarly, we may have $P = B$. Furthermore, we may even encounter the case $P = A = B$, which means that L is tangent to $\mathcal{C}$ at the point $A = B = P$ and this point is an inflection point of the curve $\mathcal{C}$.
- If $P \neq O$, let L' be the unique line that contains both P and O. If $P = O$, let L' be the line that is tangent to the curve $\mathcal{C}$ at the point O. Then $L' \cap \mathcal{C}$ consists of the point P, the point O and the third point Q. We let $A + B = Q$. It may happen that $Q = P$ or $Q = O$ (or both), and we should be ready to deal with the case when Q lies at infinity.

Let us illustrate this algorithm using one explicit example. Suppose that the curve $\mathcal{C}$ is the cubic curve given by

$$x^3 + y^3 + 4xy + 1 = 0.$$

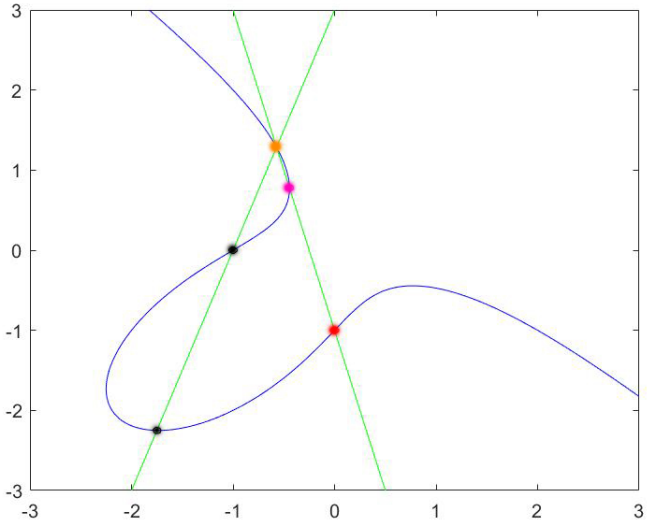
Then $\mathcal{C}$ contains points

$$(0,-1),\ (-1,0),\ (-\frac{1}{2},\frac{1}{2}),\ (-1,2),(2,-1),\ (-\frac{7}{4},-\frac{9}{4}),\ (\frac{7}{9},-\frac{4}{9}),\ (-\frac{4}{7},\frac{9}{7}),\ \text{etc.}$$

First, we have to choose the point O in $\mathcal{C}$ such that $O + P = P + O$ for every point $P \in \mathcal{C}$. For simplicity, let $O = (0,-1)$. Let $A = (-1,0)$ and $B = (-\frac{7}{4},-\frac{9}{4})$; our goal is to compute $A + B$. The line that contains the points A and B is given by $3x - y + 3 = 0$. This line intersects $\mathcal{C}$ at three distinct points: A, B and $P = (-\frac{4}{7},\frac{9}{7})$. The line that contains the points P and O is given by $4x + y + 1 = 0$. It intersects the curve $\mathcal{C}$ by three distinct points: P, O and $Q = (-\frac{4}{9},\frac{7}{9})$. Thus, we have

$$A + B = \Big(-\frac{4}{9},\frac{7}{9}\Big).$$

These computations are illustrated by the following picture:



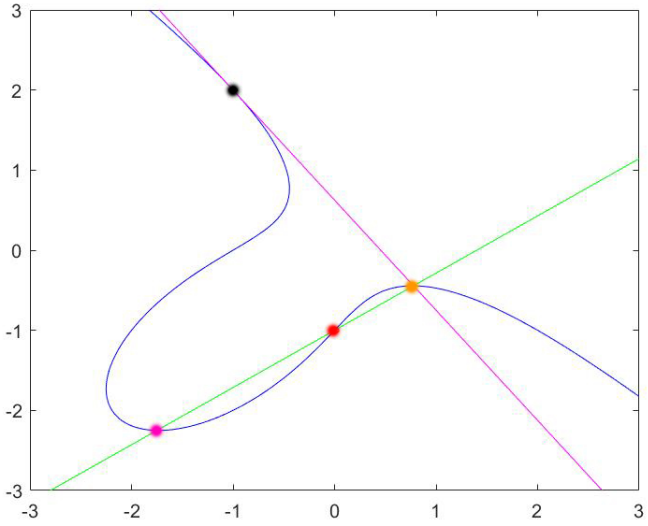
Here the red point is O, the black points are A and B, the orange point is P, the pink point is $A + B$, and the green lines are the lines $3x - y + 3 = 0$ and $4x + y + 1 = 0$.

In your poster, you should describe the algorithm for addition of points on cubic curves, and illustrate it by an explicit example, pictures and Python computations. You can try to prove that + satisfies 4 conditions above, or provide explicit examples and computations to convince people that this is indeed the case.

You can show in your poster how to compute *orders* of points in $\mathcal{C}$. The order of a point $P \in \mathcal{C}$ is the smallest $n \in \mathbb{N}$ such that $nP = O$, where

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}}.$$

If such integer does not exists, we say that the order is ∞. If all coefficients of the equation of the curve $\mathcal{C}$ are rational numbers (like in our example), then Mazur's theorem (see [10]) says that the orders of points with rational coordinates are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 or ∞. In our example we can use this theorem to show that $(-1, 2)$ is of infinite order. Namely, let $P = (-1, 2)$. Then $2P = P + P = (-\frac{7}{4}, -\frac{9}{4})$. This can be illustrated by



Here the red point is O, the black point is P, the orange point is $(-1, 2)$, the pink point is $2P$, the green line is the line $5x - 7y - 7 = 0$, and the pink line is the line $11x + 8y - 5 = 0$. This is the tangent line to $\mathcal{C}$ at the point P. Since $2P \neq O$, we see that the order of P is not 2. Applying the same algorithm to $2P$, we compute the point

$$4P = 2 \cdot 2P = 2P + 2P = \Big(-\frac{5551}{3663}, -\frac{1544}{3663} \Big).$$

Thus, the order of P is not 4 either. Similarly, we see that and

$$8P = 2 \cdot 4P = 4P + 4P = \Big(-\frac{293255735344481}{339980855190512}, \frac{613059833705121}{339980855190512} \Big).$$

Hence, the order of P is not 8. Similarly, we can compute $16P$. This is the point whose x-coordinate is

$$\frac{5604600786263095192403201029073533468015208082860948938067 3}{3955280540187997423866501954312028549601079671696576840364 9}$$

and whose y-coordinate is

$$-\frac{8691050713519283193228455499869582129421169834615784385942 4}{3955280540187997423866501954312028549601079671696576840364 9}.$$

Thus, we found P, $2P$, $4P$, $8P$ and $16P$. All these points are distinct. This implies that the order of P is not 3, 5, 6, 7 or 12. Indeed, if the order of P is 3, then $4P = P + 3P = P + O = P$, but we know that $4P \neq P$. Similarly, if $5P = O$, then

$$16P = 5P + 5P + 5P + P = O + O + O + P = P,$$

which is not the case. If $6P = O$, then

$$8P = 6P + 2P = O + 2P = 2P,$$

which is not true. Likewise, if $7P = O$, then

$$P \neq 8P = 7P + P = O + P = P.$$

If $12P = O$, then

$$16P = 12P + 4P = O + 4P = 4P,$$

which is not the case. Thus, it follows from Mazur's theorem that either the order of P is infinite, or the order of P is 9, or the order of P is 10. If $9P = O$, then

$$\Big(-\frac{293255735344481}{339980855190512}, \frac{613059833705121}{339980855190512}\Big) = 8P = -P + 9P = -P + O = -P.$$

But we can compute $-P$ explicitly (see [1]). This gives

$$-P = \Big(-\frac{1}{2}, \frac{1}{2}\Big),$$

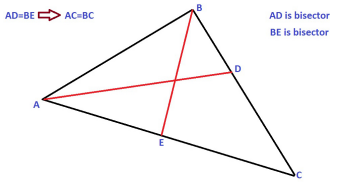
so that $10P \neq O$. Likewise, if $10P = 0$, then

$$8P = -2P = (\frac{7}{9}, -\frac{4}{9}),$$

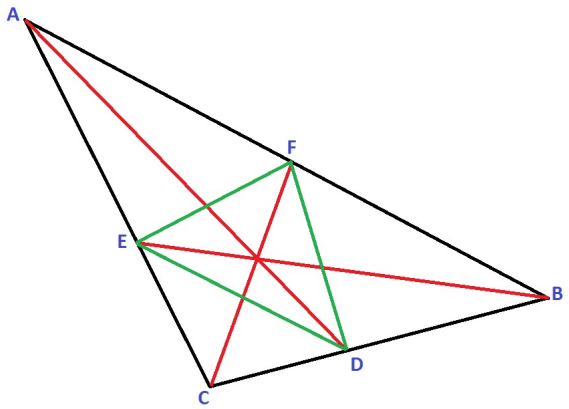
which is absurd. Thus, we have $10P \neq O$, so that the order of P is infinite.

CC-P-4: Sharygin Triangles and Cubic Curves

The Steiner–Lehmus theorem says that every triangle with two angle bisectors of equal lengths is isosceles:



The Steiner–Lehmus theorem is one of 498 problems in the book [9] by Igor Sharygin. This book contains a similar problem about isosceles triangles, which is much less known. To describe it, let $\triangle ABC$ be a triangle in $\mathbb{R}^2$, and let AD, BE, CF be its angle bisectors. This gives us another triangle $\triangle DEF$ as in this picture:



The problem in Sharygin's book asks the following question: if $\triangle DEF$ is isosceles, can $\triangle ABC$ be non-isosceles? Surprisingly, the answer is yes. We have all seen an example of such a triangle:

We say $\triangle ABC$ is a *Sharygin triangle* if $\triangle DEF$ is isosceles and $\triangle ABC$ is not isosceles. Using algebra and Python, we can produce many Sharygin triangles. Namely, let

$$\begin{cases} x = AC, \\ y = BC, \\ z = AB. \end{cases}$$

Then

$$DF - EF = (x-y)\frac{xyz}{(x+y)(x+z)^2(y+z)^2} f_3(x,y,z),$$

where

$$f_3(x,y,z) = x^3 + x^2y + xy^2 + y^3 + z(y^2+xy+x^2) - z^2(x+y) - z^3.$$

This shows that $\triangle ABC$ is a Sharygin triangle $\iff$ $f_3(x,y,z) = 0$ and $x \neq y$.

Note that $f_3(x,y,z)$ is a homogeneous polynomial of degree 3. Thus, it defines a cubic curve in $\mathbb{P}^2_{\mathbb{C}}$. Namely, let $\mathcal{C}$ be the curve given by

$$x^3 + x^2y + xy^2 + y^3 + z(y^2+xy+x^2) - z^2(x+y) - z^3 = 0. \qquad (\blacklozenge)$$

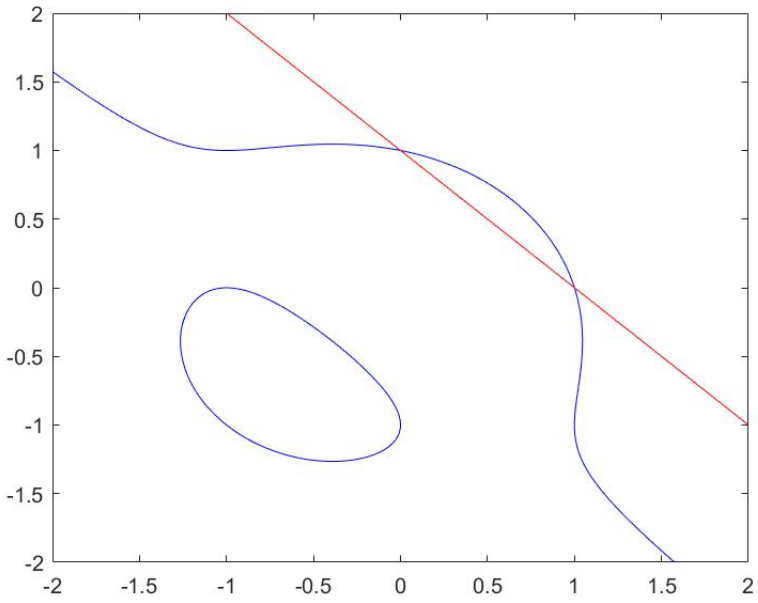
Keeping in mind that every triangle satisfies *triangle inequality*, we see that (up to similarity) Sharygin triangles are points $[x:y:z] \in \mathcal{C}$ such that x, y and z are real numbers, $x \neq y$ and

$$\begin{cases} 0 < x < y + z, \\ 0 < y < x + z, \\ 0 < z < y + z. \end{cases}$$

Let U_z be the subset in $\mathbb{P}^2_{\mathbb{C}}$ given by $z \neq 0$. Then we can identify U_z with $\mathbb{C}^2$ with coordinates $\overline{x} = \frac{x}{z}$ and $\overline{y} = \frac{y}{z}$. Then $\mathcal{C} \cap U_z$ is a cubic curve in $\mathbb{C}^2$ that is given by

$$\overline{x}^3 + \overline{x}^2\overline{y} + \overline{x}\overline{y}^2 + \overline{y}^2 + \overline{y}^2 + \overline{x}\overline{y} + \overline{x}^2 - \overline{x} - \overline{y} - 1 = 0.$$

Using Python, we can plot its real part:



All points in the blue curve in this picture that lie above the red line are Sharygin triangles. This gives complete description of them.

Are there Sharygin triangles with integer sides? Actually, yes. A computer search gives one Sharygin triangle with integer sides:

$$\Big[1481089 : 18800081 : 19214131\Big]$$

Do we have more Sharygin triangle with integer sides? If yes, how many of them exist? These questions are too complicated for a computer search.

Observe that the curve $\mathcal{C}$ contains the point $[1 : -1 : 0]$. Moreover, the point $[1 : -1 : 0]$ is an *inflection* point of the curve $\mathcal{C}$. In particular, we can use the algorithm described in [1] and find a *projective transformation* $\phi\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ such that $\phi(\mathcal{C})$ is given by

$$zy^2 = x^3 + 5x^2z + 32xz^2.$$

In particular, the curve $\mathcal{C}$ is smooth.

Let $O = [1 : -1 : 0]$. Using the algorithm described in [1], equip the curve $\mathcal{C}$ with an addition $+$ such that

$$O + P = P + O = P$$

for every point $P \in \mathcal{C}$. Observe that the curve $\mathcal{C}$ also contains the points $[1 : 1 : -1]$ and $[1 : 0 : 1]$. Moreover, we have $2[1 : 1 : -1] = [1 : -1 : 0] = O$ and $2[1 : 0 : 1] = [-32 : 25 : 1]$. Similarly, we have

$$4\big[1 : 0 : 1\big] = \big[-622895 : 600608 : 600153\big].$$

Computing $n[1 : 0 : 1]$ and $n[1 : 0 : 1] + [1 : 1 : -1]$ for small n, we rediscover the first Sharygin triangle with integer sides:

$$9\big[1 : 0 : 1\big] + \big[1 : 1 : -1\big] = \Big[1481089 : 18800081 : 19214131\Big].$$

Moreover, we discover the second Sharygin triangle with integer sides:

$$16\big[1 : 0 : 1\big] = \Big[3013615334499004588376 00 : \\ : 49105016933436320224063 : \\ : 31662903325350128110280 7\Big].$$

Furthermore, the point $23[1:0:1]+[1:1:-1]$ is the third Sharygin triangle with integer sides:

$$\Big[119361397031607967398713496044789535174585032475 35 :$$
$$: 109775670610677902190285796706340213216430218851 03 :$$
$$: 27858275333008732470444727412454885009141926482 09\Big].$$

The next two Sharygin triangle with integer sides are $30[1:0:1]$ and

$$37\big[1:0:1\big]+\big[1:1:-1\big].$$

However, their decimal expansions do not fit into the screen.

In your poster, you should describe the history of the problem and its links to cubic curves. You should use Python to produce at least one Sharygin triangle with integer sides. You can indicate why there are infinitely many Sharygin triangles with integer sides (see [5]).

CC-P-5: Bézout's Theorem

Two lines in the plane $\mathbb{R}^2$ usually intersect at one point. However, some lines are parallel and do not intersect. Similarly, two ellipses in $\mathbb{R}^2$ can intersect each other at up to 4 points. But sometimes they do not intersect at all. To solve these nuisances, we can do two things: use the projective plane and use complex numbers.

The only reasonable subsets we can define in the complex projective plane $\mathbb{P}^2_{\mathbb{C}}$ are given by homogeneous polynomial equations in x, y and z. The simplest case is when we have one equation:

$$f_d(x,y,z)=0,$$

where $f_d(x,y,z)$ is an homogeneous polynomial of degree $d\geqslant 1$. Such subsets are called *plane projective complex curves* of degree d or simply *plane curves*. Plane curves of degree 1 are just lines in $\mathbb{P}^2_{\mathbb{C}}$. Plane curves of degree 2 are called *conics*, and plane projective curves of degree 3 are called *cubic curves*. If $f_d(x,y,z)$ is *irreducible*, we say that the curve it defines is *irreducible*. Lines are always irreducible. Conics can be reducible. In this case, they consist of two lines.

Two distinct lines in $\mathbb{P}^2_{\mathbb{C}}$ always intersect at a single point. Likewise, a line and an irreducible conic in $\mathbb{P}^2_{\mathbb{C}}$ always share a common point. Usually, they intersect at two distinct points. In the case where they have only one common point, we say that the line and the conic are *tangent* at that point.

Let $\mathcal{C}$ and $\mathcal{C}'$ be two distinct irreducible conics in $\mathbb{P}^2_{\mathbb{C}}$. Then $\mathcal{C}\cap\mathcal{C}'$ can consist of one, two, three or four points. All of these cases are possible:

Suppose that $\mathcal{C}$ is given by $f_2(x,y,z)=0$, where

$$f_2(x,y,z):=511x^2+709xy-131y^2-1932xz+981yz-448z^2.$$

- If the conic $\mathcal{C}'$ is given by $g_2(x,y,z)=0$ for

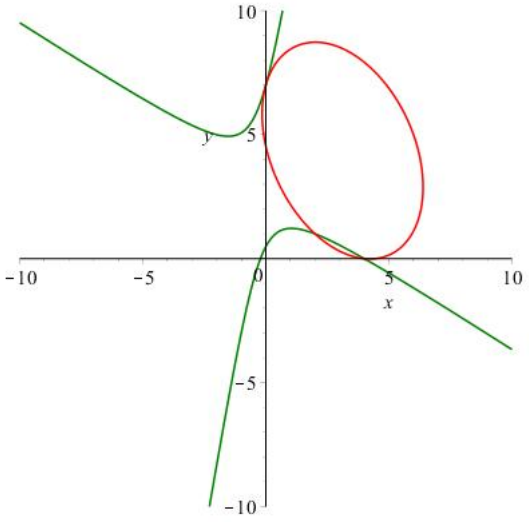
  $$g_2(x,y,z):=1217x^2-394xy-541y^2-6555xz+2823yz+6748z^2,$$

  then $\mathcal{C}\cap\mathcal{C}'$ consists of the four points $[4:0:1]$, $[1:3:-1]$, $[0:7:1]$, $[2:1:1]$.

- If the conic $\mathcal{C}'$ is given by $g_2(x,y,z)=0$ for

  $$g_2(x,y,z):=42049x^2+21271xy+23536y^2-355005xz-271500yz+747236z^2,$$

  then $\mathcal{C}\cap\mathcal{C}'$ consists of just three points $[4:0:1]$, $[0:7:1]$, $[2:1:1]$. Plotting the real part of the plane $\mathbb{P}^2_{\mathbb{C}}$ away from the line $z=0$, we obtain the following picture:



These conics are tangent at $[0:7:1]$, so that we should count this intersection point with appropriate multiplicity.

- If the conic $\mathcal{C}'$ is given by is given by $g_2(x,y,z)=0$ for

$$g_2(x,y,z) := (3031x - 853y + 5971z)(821x - 3779y + 2137z) - 9700f_2(x,y,z),$$

then then $\mathcal{C} \cap \mathcal{C}'$ consists of just two points $[0:7:1]$ and $[2:1:1]$. This is easy to explain algebraically. In this case, the intersection $\mathcal{C} \cap \mathcal{C}'$ is given by the following system of polynomial equations:

$$\begin{cases} f_2(x,y,z) = 0, \\ (3031x - 853y + 5971z)(821x - 3779y + 2137z) - 9700f_2(x,y,z) = 0. \end{cases}$$

To solve this system, we can separately solve the system

$$\begin{cases} f_2(x,y,z) = 0, \\ 3031x - 853y + 5971z = 0, \end{cases}$$

and then solve the system

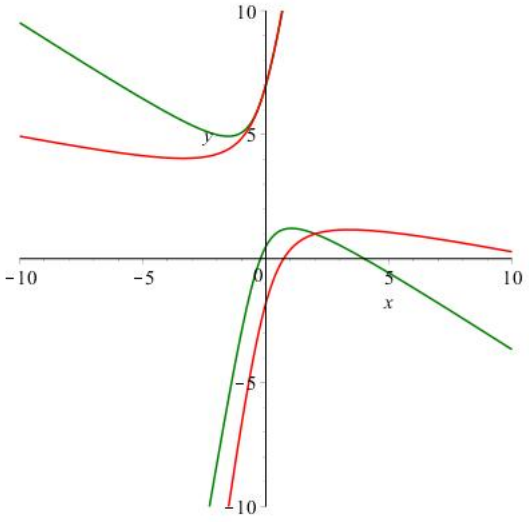
$$\begin{cases} f_2(x,y,z) = 0, \\ 821x - 3779y + 2137z = 0. \end{cases}$$

Then $\mathcal{C} \cap \mathcal{C}'$ consists of the points $[0:7:1]$ and $[2:1:1]$, which should be counted with multiplicity 2.

- If the conic $\mathcal{C}'$ is given by $g_2(x,y,z)=0$ for

$$g_2(x,y,z) := (3031x - 853y + 5971z)(6x + 2y - 14z) - 50f_2(x,y,z) = 0,$$

then we get the following picture:



These conics are tangent at the point $[0:7:1]$, and they intersect *transversally* at the point $[2:1:1]$. In this case, we should count $[0:7:1]$ in the intersection $\mathcal{C} \cap \mathcal{C}'$ with multiplicity 3.

- Finally, if conic $\mathcal{C}'$ is given by $g_2(x,y,z) = 0$ for

$$g_2(x,y,z) := (3031x - 853y + 5971z)^2 - 5000 f_2(x,y,z),$$

then $\mathcal{C} \cap \mathcal{C}'$ consists of the point $[0:7:1]$. We should count it with multiplicity 4.

Our examples are parts of a powerful algebraic result known as Bézout's Theorem (see [1, 3]). To state it, let $f_{d_1}(x,y,z)$ be a homogeneous polynomial of degree $d_1 \geqslant 1$, and let $g_{d_2}(x,y,z)$ be a homogeneous polynomial of degree $d_2 \geqslant 1$. Consider the system of equations

$$\begin{cases} f_{d_1}(x,y,z) = 0 \\ g_{d_2}(x,y,z) = 0 \end{cases} \qquad (\bigstar)$$

How many solutions in $\mathbb{P}^2_{\mathbb{C}}$ does $(\bigstar)$ have? Clearly there are infinitely many solutions if the polynomials $f_{d_1}(x,y,z)$ and $g_{d_2}(x,y,z)$ have a common (non-constant) polynomial factor. Otherwise, we have:

Theorem (Bézout)**.** Suppose that $f_{d_1}(x,y,z)$ and $g_{d_2}(x,y,z)$ do not have a common (non-constant) polynomial factor. Then $(\bigstar)$ has $d_1 d_2$ solutions in $\mathbb{P}^2_{\mathbb{C}}$ counted with multiplicities.

How can we find all points in $\mathbb{P}^2_{\mathbb{C}}$ that satisfy $(\bigstar)$? This can be done using resultants (see [1]).

In your poster, you should describe the history of the problem, and use examples of conics or cubic curves to illustrate Bézout's Theorem. You can use Python to compute resultants to find intersection points.

CC-P-6: Cubic Curves and Number Theory

Let $\mathcal{C}$ be an irreducible cubic curve in the plane $\mathbb{P}^2_{\mathbb{C}}$. Then it is given by

$$f_3(x,y,z) = 0,$$

where $f_3(x,y,z)$ is a homogeneous polynomial of degree 3 with complex coefficients. Suppose that its coefficients are all integers. In this case, we say that $\mathcal{C}$ is defined over $\mathbb{Q}$. Then we can consider the equation $f_3(x,y,z) = 0$ as a *Diophantine equation* and look for its solutions in the integers. To do this in a consistent way, denote by $\mathcal{C}(\mathbb{Q})$ the set of *rational points* of the curve $\mathcal{C}$. This set consists of all points $P \in \mathcal{C}$ such that $P = [\alpha : \beta : \gamma]$ for some integers α, β and γ.

If the curve $\mathcal{C}$ is singular, then the set $\mathcal{C}(\mathbb{Q})$ is infinite and is easy to describe. However, the case of smooth cubic curves is very different. For example, there are smooth cubic curves in $\mathbb{P}^2_{\mathbb{C}}$ defined over $\mathbb{Q}$ that do not have rational points. Among them is the cubic curve given by

$$3x^3 + 4y^3 + 5z^3 = 0.$$

This Diophantine equation has only one integer solution given by $x = y = z = 0$ (see [8]), which does not corresponds to any point in $\mathbb{P}^2_{\mathbb{C}}$. Some smooth cubic curves defined over $\mathbb{Q}$ have finitely many rational points. For example, the points $[1 : 0 : 1]$, $[0 : 1 : 1]$ and $[1 : -1 : 0]$ are the only rational points on the cubic curve in $\mathbb{P}^2_{\mathbb{C}}$ given by

$$x^3 + y^3 = z^3.$$

This was proven by Euler using the method of *infinite descent* (see [2]). A similar method can be applied to the smooth cubic curve $zy^2 = x^3 - xz^2$ to show that it contains only four rational points: $[0 : 1 : 0]$, $[-1 : 0 : 1]$, $[0 : 0 : 1]$ and $[1 : 0 : 0]$.

There are smooth cubic curves defined over $\mathbb{Q}$ that have infinitely many rational points. For instance, let $\mathcal{C}$ be the cubic curve that is given by

$$zy^2 = x^3 + xz^2 + z^3.$$

Then $\mathcal{C}(\mathbb{Q})$ contains $[0 : 1 : 0]$, $[0 : \pm 1 : 1]$ and $[2 : \pm 9 : 8]$. In fact, it contains infinitely many points. To show this, let $O = [0 : 1 : 0]$, and equip $\mathcal{C}$ with an operation $+$ such that O plays the role of zero (see [1]). Then the sum of two points in $\mathcal{C}(\mathbb{Q})$ is a point in $\mathcal{C}(\mathbb{Q})$. Now, taking a point in $\mathcal{C}(\mathbb{Q})$, say $[2 : 9 : 8]$, we compute

$$n[2 : 9 : 8] = \underbrace{[2 : 9 : 8] + [2 : 9 : 8] + \cdots + [2 : 9 : 8]}_{n \text{ times}},$$

for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$. This gives 10 distinct points in the curve $\mathcal{C}$, which are all different from $[2 : 9 : 8]$ and O. For instance, we have

$$2\big[2 : 9 : 8\big] = \big[-10332 : -40879 : 46656\big],$$

and

$$3\big[2 : 9 : 8\big] = \big[32826479686 : -139455877527 : 1824793048\big].$$

Now we can apply Mazur's Theorem (see [4, 10]) to deduce that the sequence

$$[2 : 9 : 8],\ 2[2 : 9 : 8],\ 3[2 : 9 : 8],\ 4[2 : 9 : 8],\ 5[2 : 9 : 8],\ 6[2 : 9 : 8],\ 7[2 : 9 : 8], \ldots$$

is actually infinite, so that $\mathcal{C}(\mathbb{Q})$ is infinite as well.

A similar approach can be used to study the set $\mathcal{C}(\mathbb{Q})$ in the case when $\mathcal{C}$ is smooth and it contains at least one rational point. Namely, we can fix a point $O \in \mathcal{C}(\mathbb{Q})$ and equip the curve $\mathcal{C}$ with an addition operation $+$ such that O plays the role of zero. Then for a point $P \in \mathcal{C}(\mathbb{Q})$, we have

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

is a point in $\mathcal{C}(\mathbb{Q})$ for every positive integer n. If $nP = O$ for some $n \geqslant 1$, then P is said to be a *torsion* point. For instance, the point O is torsion.

By a theorem of Mordell (see [6, 10]), the set $\mathcal{C}(\mathbb{Q})$ contains finitely many torsion points. How can we find all of them? This can be done using *Nagell–Lutz theorem* if $O = [0 : 1 : 0]$ and the curve $\mathcal{C}$ is given by

$$zy^2 = x^3 + ax^2z + bxz^2 + cz^3,$$

for some *integers* a, b and c. In this case, the Nagell–Lutz theorem says the following: if P is a torsion point in the set $\mathcal{C}(\mathbb{Q})$ and $P \neq O$, then $P = [\alpha : \beta : 1]$ for some integers α and β such that

(i) either $\beta = 0$ and $2P = O$,

(ii) or $\beta \neq 0$ and β^2 divides $-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

In the language of algebra, the pair $(\mathcal{C}(\mathbb{Q}), +)$ is an *abelian group*. Denote by $\mathcal{C}(\mathbb{Q})_{tors}$ the subset in $\mathcal{C}(\mathbb{Q})$ consisting of all torsion points. Then $P + Q$ is a point in $\mathcal{C}(\mathbb{Q})_{tors}$ for every two points P and Q in $\mathcal{C}(\mathbb{Q})_{tors}$, so that the pair $(\mathcal{C}(\mathbb{Q})_{tors}, +)$ is a *finite abelian group*. All possibilities for this group were found by Barry Mazur [4]. What can

we say about the points of the set $\mathcal{C}(\mathbb{Q})$ that are not torsion? In [6], Mordell proved that there are finitely many points $P_1, \ldots, P_r$ in $\mathcal{C}(\mathbb{Q})$ such that every point $P \in \mathcal{C}(\mathbb{Q})$ can be uniquely written as

$$P = n_1 P_1 + n_2 P_2 + \cdots + n_r P_r + T,$$

where T is a point in $\mathcal{C}(\mathbb{Q})_{tors}$. This implies an *isomorphism* of abelian groups

$$\mathcal{C}\big(\mathbb{Q}\big) \cong \mathbb{Z}^r \times \mathcal{C}\big(\mathbb{Q}\big)_{tors}.$$

The number r here is called the *rank* of the cubic curve $\mathcal{C}$. Thus, if the rank of the curve $\mathcal{C}$ is zero, then $\mathcal{C}$ has finitely many rational points. If the rank is positive, then the cubic curve $\mathcal{C}$ has infinitely many rational points. In every case, this can be checked either by using the Nagell–Lutz theorem or by using Mazur's theorem (see [10]). Unfortunately, there is no known algorithm that can determine the exact value of the rank of the curve $\mathcal{C}$. It is also not known which ranks can occur. Currently the largest known rank is the rank of the cubic curve

$$zy^2 = x^3 + axz^2 + bz^3,$$

where $a = -32108419864920842536053133134941668401488368499486330402 7$ and

$$b = 22068231548819556138901110838639219053415720136358962117716078469478004397240002754 46.$$

This cubic curve was discovered by Noam Elkies who proved that its rank is at least 28, but the exact value of its rank is unknown.

In your poster, you should state Mordell's theorem and describe either Mazur's theorem or the Nagell–Lutz theorem (or both). You do not need to provide proofs of these results, but you should illustrate at least one of them by using explicit examples.

References

[1] I. Cheltsov, *Algebraic Geometry for sophomores.*
Learn, University of Edinburgh, 2019.

[2] G. Hardy, E. Wright, *An introduction to the theory of numbers.*
Sixth edition, Oxford at the Clarendon Press, 2009.

[3] F. Kirwan, *Complex Algebraic Curves.*
Cambridge University Press, 1992.

[4] B. Mazur, *Modular curves and the Eisenstein ideal.*
Publications Mathematiques de l'IHES **47** (1977), 33–186.

[5] I. Netay, A. Savvateev, *Sharygin triangles and elliptic curves.*
Magadan Volume, Bulletin of the Korean Mathematical Society **54** (2017) 1597–1617.

[6] L. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.*
Proceedings of the Cambridge Philosophical Society **21** (1922), 179–192.

[7] M. Reid, *Undergraduate Algebraic Geometry.*
Cambridge University Press, 1988.

[8] E. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$.
Acta Mathematica **85** (1951), 203–362.

[9] I. Sharygin, *Problems in Plane Geometry.*
Mir Publishers, 1988

[10] J. Silverman, J. Tate, *Rational Points on Elliptic Curves.*
Undergraduate Texts in Mathematics, Springer, 2015.