Math 319NT Fall 2024 **Name: Aby Soumare :3**
Lab 9: Elliptic Curves!!! :D
Collaborators:

Introduction

In this lab, we were tasked with studying the ideas of elliptic curves. To aid us in our journey, Professor Day assigned us multiple questions with instructions. The tool Magma was used to do most of the computational work for us, and Professor Day was available to ask questions to.

Background

Definition 0.1. *An elliptic curve is a curve of the form:*

$$y^2 = x^3 + a_1x^2 + a_2x + a_3$$

Example 0.2. *The equation* $l := x^3 + 2 * x^2 + x + 5$ *is an elliptic curve.*

For a point to be on the curve means that it "solves" this equation. If we were to assign $4 = x$ in the equation of a curve, the y output we would write as the (x, y) coordinate point on the curve.

Example 0.3. *For the curve* $l := x^3 + 2 * x^2 + x + 5$*, if we were to put* $x = 4$*, then a point on that curve would then be* $(4, 11, 025)$.

For this lab, we must also know that the group of points on the elliptic curve added with the "point at infinity" (the identity) form a group.

The explicit formulas for adding points on an elliptic curve are thus:

1. $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$,
2. $x_3 = \lambda^{2-a} - x_1 - x_2$,
3. $y_3 = \lambda(x_3 - x_1) + y_1$.

Note the order of these items, since addition is closed here.

Analysis

To study the topic of elliptic curves, Professor Day assigned multiple exercises to facilitate in understanding. See the first exercise here:

Exercise 0.1. *Use magma to create the elliptic curve* $y^2 = x^3 + 17$.

This code was used:

Code 0.4. *Code used:*

```
> E:= EllipticCurve([0,0,0,0,17]);
> print E;
Elliptic Curve defined by y^2 = x^3 + 17 over Rational Field
```

Now we want to create a point on this curve. See this:

Exercise 0.2. *Create the point $P = (2, 5)$ on the curve.*

The code used to do this is here:

Code 0.5. *Printing and naming our point:*

```
> P:=E![2,5];
> P;
(2 : 5 : 1)
```

Now, since this point was given to us by Professor Day, we now want to try finding a point on the curve ourselves. See this excerise:

Exercise 0.3. *Find another point with integer coordinates on the curve. Call it Q and input it into magma as a point on the curve.*

The function `IsPoint(E,[x,y]);` was used to check if the point was truly on the curve. In order to find your own point on the curve, simply substitute x for integers and see if an integer solution for y is the result. The integer -1 was inputted in the function to yield $y = 4$, so now we know $(-1, 4)$ is a point on the curve. We will do this again with the numbers $y = -5$, and $x = 2$ is our output. See the code here that checks that this point is truly on the curve:

Code 0.6. *Checking if the point is truly on the curve:*

```
> IsPoint(E,[2,-5]);
true (2 : -5 : 1)
> Q:= E![2,-5];
```

Now we are going to do some operations on these points we found on the curve. The operations are listed here:

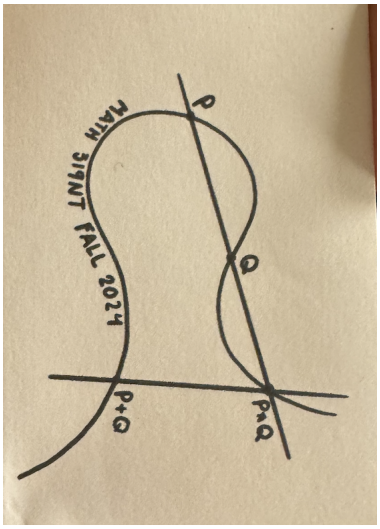
Exercise 0.4. *Use magma to compute the following:*

1. $P + Q$,
2. $P + Q + P$,
3. $P + Q + Q$.

The work for this is here:

Code 0.7. *Operations on the points:*

```
> P+Q;
(0 : 1 : 0)
> P+Q+Q;
(2 : -5 : 1)
> P+Q+P;
(2 : 5 : 1)
```



Graphic of an elliptic curve given to all students by Professor Tori Day on the last day of class.

You can see how this works by looking at the diagram Professor Day gifted all students on the last day of class.

To continue this trend of doing operations on the points, we now want to try multiplication on these points. See this:

Exercise 0.5. *Use magma to compute:*

1. $2 * P$,
2. $3 * Q$,

3. $2P + 5Q$,

4. $3P - 2Q$.

The work for this is here:

Code 0.8. *Operations on the points:*

```
> twop:= 2*P;
> twop:= E!twop;
> print twop;
(-64/25 : 59/125 : 1)
> threeq:= 3*Q;
> threeq:= E!threeq;
> print threeq;
(298927/40401 : 166830380/8120601 : 1)
> fiveq:= 5*Q;
> fiveq:= E!fiveq;
> thwfivepq:= E!twop+fiveq;
> print thwfivepq;
(-77411021500244602694/63529194761351407449 :
19735595890194195395136504397 43/506360740109169149902855939293 : 1)
> threep:= 3*P;
> threep:= E!threep;
> twoq:= 2*Q;
> twoq:= E!twoq;
> threetwopq:= E!threep-twoq;
> print threetwopq;
(76271/289 : -21063928/4913 : 1)
```

Part two:

In the first part of this lab, we went through some basic definitions and operations on elliptic curves. Now, we want to more deeply study their behavior and go into more detailed topics. IN this section of the report, we are going to be studying Two Torsion points and their behavior. In order to do that, we first stared out with this question:

Exercise 0.6. *The integers $\mathbb{Z}$ are a group under addition. Are there any non-trivial elements of finite order in this group? Explain.*

The answer to this is simple, there are no non-trivial elements within $\mathbb{Z}$ for finite order. We know that the only way to get a finite order element within $\mathbb{Z}$ is to multiply a number by 0, and this is trivial.

Now that we can see different behaviors of different groups, we want to be able to answer some questions posed by Professor Day:

Exercise 0.7. *Answer the following questions to learn more about P, a point of order 2 on an elliptic curve given the equation:*

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

1. *What is $P + P$?*
2. *Based on 1, what is the relationship between P and $-P$?*
3. *Based on 2, what is the y-coordinate of P?*
4. *Based on 3, what is a cubic equation that the x-coordinate of P must satisfy?*

The answers for this question are here:

1. $P + P$ is the identity, $\mathcal{O}$. You can see how that will be in this example:

$$P = (-1, 4)$$
$$-P = (-1, -4).$$

   From this, we can see that $-(x, y) = (x, -y)$.

2. So, $P = -P$.
3. The y-coordinate of P is $-y$ in $-P$, forcing $y = 0$.
4. The x-coordinate of P satisfies the cubic equation. So, we have $0 = x$ since we know y will be 0.

Now we want to continue to study this idea with another example. See this:

Exercise 0.8. *Use magma to find the x-coordinates of the rational two torsion points of our elliptic curve $y^2 = x^3 - 4x$*

We were given code by Professor Day to aid us:

Code 0.9. *Code from Professor Day:*

```
R<x>:= PolynomialRing(Rationals()); %creates the polynomial ring R[x]
Factorization(f); %factors our polynomial
```

So, since we know x needs to "solve" the equation, then by this we can deduce that we need to do these steps:

Code 0.10. *Factoring the equation:*

```
> g:= x^3 -4*x;
> Factorization(g);
[
    <x - 2, 1>,
    <x, 1>,
    <x + 2, 1>
]
```

To expand on this process, we were then given this exercise to complete:

Exercise 0.9. *Use your answers from the previous exercise to create all the two torsion points on the elliptic curve. Then use magma to do the needed computation to create an addition table for this group.*

Since the factorizations in the last example are all the factorizations for that curve, then we know those are all the two torsion points for that elliptic curve. The points written out are: $(-2,0),(0,0),(2,0)$.

$(0,0)$	$(-2,0)$	$(0,0)$	$(-2,0)$
$(-2,0)$	$(0,0)$	$(2,0)$	$(0,0)$
$(0,0)$	$(2,0)$	$(0,0)$	$(2,0)$
$(-2,0)$	$(0,0)$	$(2,0)$	$+$

Table 1: An Example table

After finishing that problem, we should now want to move on to another similar curve. See this exercise:

Exercise 0.10. *Consider the curve: $y^2 = x^3 + x$. Find the rational two torsion points of this curve.*

From the last example, we know how to solve this already. See this:

Code 0.11.

```
> e:= x^3 +x;
> Factorization(e);
[
    <x, 1>,
    <x^2 + 1, 1>
]
```

To try and connect the first and second example, we were posed this question:

Exercise 0.11. *How does the number of rational two torsion points on E_2 compare to the number of rational two torsion points on E_1?*

It depends on the number of factors of the equation. If the equation factors into 3 different parts, then there will be 3 different torsion points. Same for other number of factors.

Finally, to conclude our findings in this lab, we were asked these couple of questions:

Exercise 0.12. *Last questions:*

1. *Do you think every elliptic curve with coefficients in $\mathbb{R}$ has a non-trivial rational two torsion point? Explain your reasoning.*
2. *Do you think every elliptic curve with coefficients in $\mathbb{R}$ has a non-trivial real two torsion point? Explain your reasoning.*

For the first question, we can see that this is not true. If we are given a polynomial that cannot be factored, like x^3+2*x^2+x+5, then we will only be able to make trivial solutions for the points. For the second question, if the equation can be factored into any real number, then of course we will then have non-trivial points (also, every real cubic has a real root by the intermediate value theorem).

Future Directions

In this lab, we worked with polynomials with fairly simple equations. However, we saw an equation that could not be factored near the end of this lab. This begs the question, do we know for certain that a polynomial that cannot be factored will not have torsion points? Additionally, what if we were to observe three different points P, Q, Z on the line? What would the relationship between multiplication and addition look for those?

Source: `https://magma.maths.usyd.edu.au/magma/pdf/examples.pdf`