The Group of Rational Points on a Cubic

Sanjana Das   Espen Slettnes   Sophie Zhu

December 9, 2020

Introduction

Definition (Diophantine Equations)

Diophantines are polynomials with rational coefficients where rational solutions in the real projective space are sought.

- Solutions to one-variable Diophantine equations are just the rational roots of a one-variable polynomial.
  - Formulas exist for such equations of degree ≤ 4.
- Two-variable Diophantines are more complicated:
  - Those with degree 1 are simply lines, and are thus parameterizable.
  - What about those with degree 2?

Introduction (cont.)

Given a conic C with degree 2, and rational $\mathcal{O} \in C$, any rational line through $\mathcal{O}$ reintersects C at a rational point by Vieta's formulæ. We can thus parameterize the rational points on C in terms of the slopes of the lines between them and $\mathcal{O}$.

Here we go one degree further: given a rational cubic curve in the projective plane of the form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

with rational coefficients, we explore its solutions with rational coordinates.

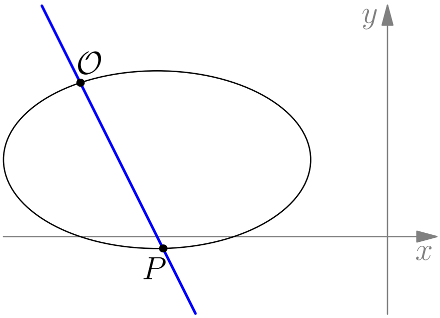

Figure: A line through a point $\mathcal{O}$ re-intersecting a conic at another rational point P.

Transforming a Cubic

Assume that we have a rational non-singular point $\mathcal{O}$ on our curve. Let $X, Y, Z : \mathbb{R}^2 \to \mathbb{R}$ be affine transformations such that

- the kernel of X is the tangent to the curve at $\mathcal{P}$ (or, if $\mathcal{P} = \mathcal{O}$, any rational line not passing through $\mathcal{O}$),
- the kernel of Y is a line through $\mathcal{O}$ with rational slope, and
- the kernel of Z is tangent $\overline{\mathcal{O}\mathcal{P}}$.

Taking the projective transformation

$$T : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x, y) \longmapsto \left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

gives a curve of the form

$$\boxed{x_1 y_1^2 + (Ax_1 + B)y_1 = Cx_1^2 + Dx_1 + E}.$$

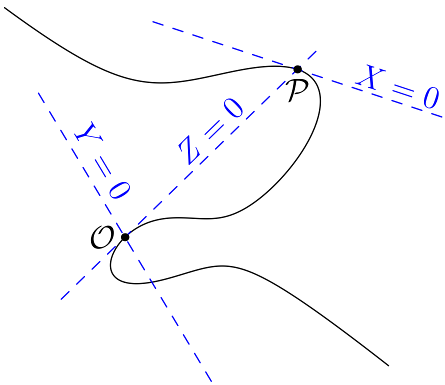

Figure: Choosing axes to put a cubic into Weierstraß form

Weierstraß Normal Form

$$\boxed{x_1 y_1^2 + (Ax_1 + B)y_1 = Cx_1^2 + Dx_1 + E}$$

Multiplying this equation by x_1 gives

$$(x_1 y_1)^2 + (Ax_1 + B)x_1 y_1 = Cx_1^3 + Dx_1^2 + Ex_1.$$

Setting $x_2 = Cx_1$ and $y = C\left(x_1 y_1 + \frac{1}{2}(Ax_1 + B)\right)$ then turns this equation into the form

$$y_2^2 = \text{a monic rational cubic in } x_2.$$

Definition

Given a cubic polynomial $f(x) = x^3 + ax^2 + bx + c$, the *elliptic curve* with equation $y^2 = f(x)$ is the union of the equation's set of solutions and $\mathcal{O}$, the vertical point at infinity. It is said to be *singular* if f has a double root and *non-singular* otherwise.

Weierstraß Normal Form (cont.)

Given $a, b, c \in \mathbb{Q}$, let $X = d^2x$ and $Y = d^3y$. The equation of the curve then becomes

$$Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c.$$

By choosing sufficiently large d, we can assume a, b, and c are integers.

Until further notice, C will be an non-singular elliptic curve with equation

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

for $a, b, c \in \mathbb{Z}$.

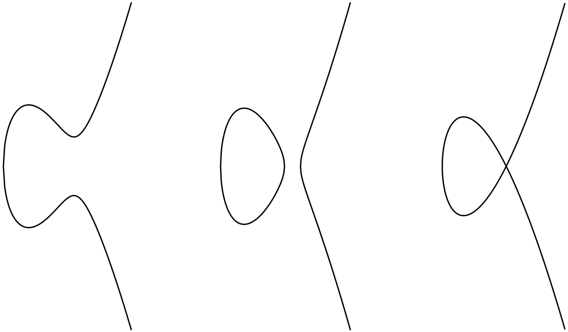

Figure: The elliptic curves with equations $y^2=x^3-6x+9$, $y^2=x^3-7x+6$, $y^2=x^3+x^2-5x+3$.

The intersections of a Line and a Cubic

Lines and cubics can intersect at one or three points.

Definition

$P * Q$ is the third intersection of line $\overline{PQ}$ with C.

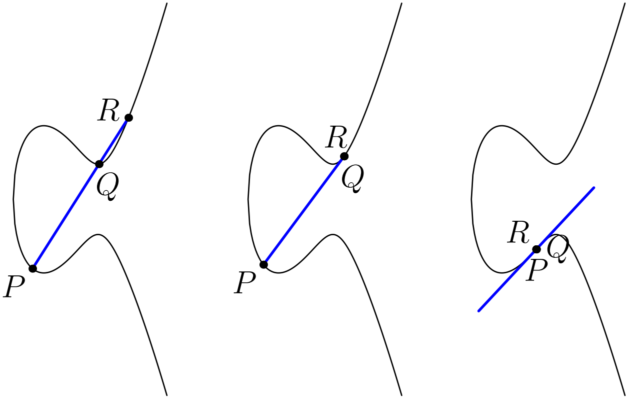

Figure: Intersections of various lines with C.

The Group of Points on a Cubic

Definition

$\mathcal{O}$ is the vertical point at infinity.

Proposition

There is a unique group $(C, +)$ *with identity* $\mathcal{O}$ *where for collinear* P, Q, R,

$$P + Q + R = \mathcal{O}.$$

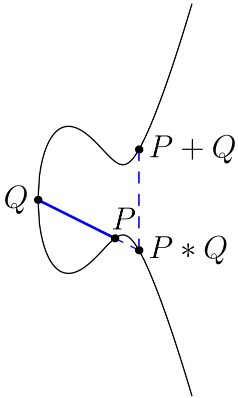

Figure: Group addition

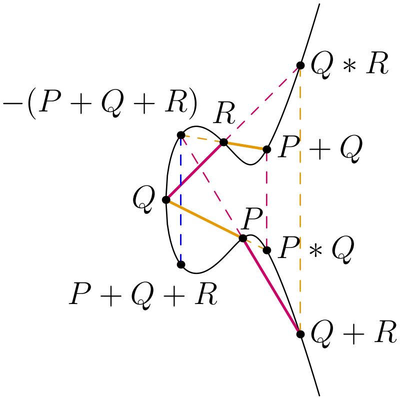

Figure: Associativity of addition

Formulæ for the Group Addition Law

By writing the line through two points as $y = \lambda x + \nu$, we can get a cubic in x that gives the intersections of a line in a cubic and the elliptic curve and use Vieta's formulæ to find the third root. The results are as follows:

Proposition (Addition Formula)

If $x_1 \neq x_2$, the sum of $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ is $P + Q = (x_3, y_3)$, where

- $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$,
- $\nu = \dfrac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$,
- $x_3 = \lambda^2 - a - x_1 - x_2$, *and*
- $y_3 = \lambda x_3 + \nu$.

Proposition (Duplication Formula)

If $P = (x, y)$ where $y \neq 0$, the sum of P with itself is $2P = (x_1, y_1)$, where

- $x_1 = \dfrac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$,
- $\lambda = \dfrac{f'(x)}{2y}$, *and*
- $y_1 = \lambda(x_1 - x) + y$.

Points of Finite Order

- The point of order 1 is the identity.
- Points of order 2 are those with a vertical tangent, i.e. those with y coordinate 0.
- Points of order 3 are inflection points, i.e., triple intersections of their tangent.

Theorem (Nagell-Lutz)

- *If (x, y) has finite order, $x, y \in \mathbb{Z}$.*
- *$y = 0$ or y divides the discriminant of f.*

The proof is basically a ν_p bash with the addition and duplication formulæ.

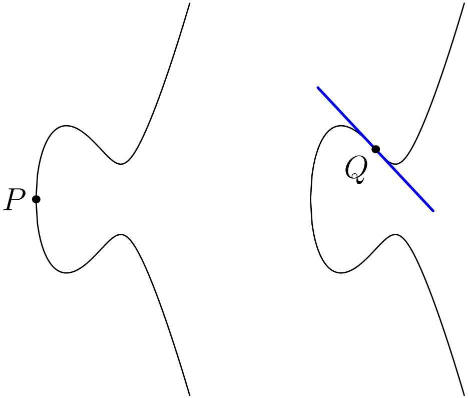

Figure: P has order 2, Q has order 3.

The Group Structure

We will outline the proof of Mordell's theorem, which states that the group of rational points on a non-singular cubic curve is finitely generated. We do so using the Descent theorem, which gives four conditions that suffice to show that an Abelian group is finitely generated:

Descent Theorem

Let Γ be a commutative group, and let $h\colon \Gamma \to \mathbb{R}_{\geq 0}$ be a function. If

1. for every real number M, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite,
2. for every $P_0 \in \Gamma$ there is a constant κ_0 so that
$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \text{for all } P \in \Gamma, \text{ and}$$
3. there is a constant κ so that
$$h(2P) \geq 4h(P) - \kappa \qquad \text{for all } P \in \Gamma.$$

Then, if the index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite, Γ is finitely generated.

Height

Definition

Given a rational number $r = p/q$ for p, q co-prime, we define the *height* of r to be

$$h(r) = \log H(r)$$

where

$$H(r) = \max\{|p|, |q|\}.$$

We also define the height of a point $P = (x, y)$ to be

$$h(P) = h(x).$$

Descent Theorem, Condition 1 ✓

For every real number M, the set $\{P \in C : h(P) \leq M\}$ is indeed finite.

Height of $P + P_0$

Proposition (Descent Theorem, Condition 2)

For a fixed point P_0, $h(P + P_0) \leq 2h(P) + \kappa$ for some constant κ.

By considering primes individually, we get $(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ for rational points on the curve. So $m \leq H(P)$, $e \leq H(P)^{1/2}$, and $n \leq k \cdot H(P)^{3/2}$.
The rest is the addition formula and the triangle inequality – the x-coordinate is

$$\frac{(y - y_0)^2 - (x - x_0)^2(x + x_0 + a)}{(x - x_0)^2} = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

Clearing denominators gets this is $\frac{Ane+Bm^2+Cme^2+De^4}{Em^2+Fme^2+Ge^4}$, and using the above bounds on m, e, n and the triangle inequality gets $H(P + P_0) \leq CH(P)^2$ for some constant C.

Height of $2P$

Proposition (Descent Theorem, Condition 3)

There is a constant κ such that $h(2P) \geq 4h(P) - \kappa$.

Again, the explicit formulas get the x-coordinate of $2P$ is

$$\frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c},$$

but getting a lower bound means we have to bound cancellation.
The numerator and denominator cannot have common roots, since if f' and f shared a root, the curve would be singular.

Height of $2P$ (cont.)

We want $h\left(\frac{f(m/n)}{g(m/n)}\right) \geq d \cdot h\left(\frac{m}{n}\right) - \kappa$, where these have no common roots and maximum degree d. We can bound the gcd of $n^d f(m/n)$ and $n^d g(m/n)$ by a constant R, and some manipulation gets

$$\frac{H\left(\frac{f(m/n)}{g(m/n)}\right)}{H(m/n)^d} \geq \frac{1}{2R} \cdot \frac{|f(m/n)| + |g(m/n)|}{\max\left(|m/n|^d, 1\right)}.$$

We want to bound this below by $C > 0$. But it's a continuous function in $t = \frac{m}{n}$, and it's never 0 and approaches some positive constant as $|t| \to \infty$.

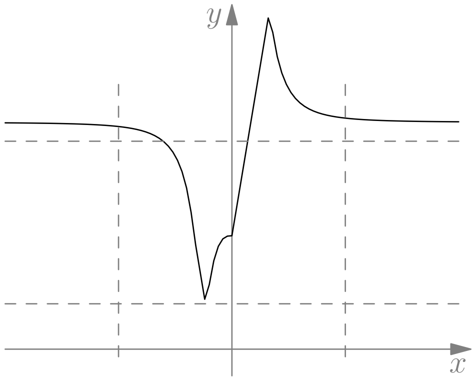

Figure: Bounding the function in t above 0

Duplication as a composition of homomorphisms

Definition

If C is $y^2 = x^3 + ax^2 + bx$, then $\overline{C}$ is $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$.

Note that $\overline{\overline{C}} = x^3 + 4ax^2 + 16bx$ is isomorphic to C, since (x, y) on $\overline{\overline{C}}$ corresponds to $\left(\frac{x}{4}, \frac{y}{8}\right)$ on C. Also, let $T = (0, 0)$, which is on C.

Definition

Let $\phi : C \to \overline{C}$ be a function with $\phi(T) = \overline{\mathcal{O}}$, $\phi(\mathcal{O}) = \overline{\mathcal{O}}$, and

$$\phi(x, y) = \left(\frac{y^2}{x^2}, y\left(\frac{x^2 - b}{x^2}\right)\right).$$

We can check $\phi(x, y)$ is on $\overline{C}$ by plugging into the equation.

Duplication as a composition of homomorphisms (cont.)

Proposition

ϕ is a homomorphism.

We want to show

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2).$$

We immediately get $\phi(-P) = -\phi(P)$. So then it suffices to show

$$P_1 + P_2 + P_3 = \mathcal{O} \implies \phi(P_1) + \phi(P_2) + \phi(P_3) = \overline{\mathcal{O}}.$$

Duplication as a composition of homomorphisms (cont.)

Since $P_1 + P_2 + P_3 = \mathcal{O}$ if and only if P_1, P_2, P_3 are collinear, we can assume they're collinear on a line $y = \lambda x + \nu$ and show their images are collinear on a line $\overline{y} = \overline{\lambda}\overline{x} + \overline{\nu}$.

By some computation, if P_1, P_2, P_3 are the intersections of C with $y = \lambda x + \nu$, then their images are the intersections of $\overline{C}$ with $y = \overline{\lambda} x + \overline{\nu}$ for

$$\overline{\lambda} = \frac{\nu\lambda - b}{\nu} \text{ and } \overline{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}.$$

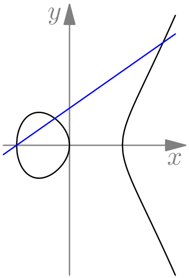

Figure: Three collinear points on C

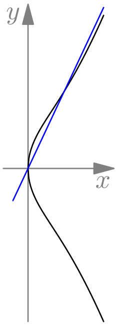

Figure: Collinear images on $\overline{C}$

Duplication as a composition of homomorphisms (cont.)

Finally, there is a corresponding homomorphism $\overline{\phi}$ from $\overline{C}$ to $\overline{\overline{C}}$, which gives the function $\psi : \overline{C} \to C$ defined as $\psi(\overline{x}, \overline{y}) = \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2} \right)$.

Proposition

$\psi \circ \phi(P) = 2P$.

This can be shown by straightforward computation. Similarly, we get $\phi \circ \psi(\overline{P}) = 2\overline{P}$. So then we've split the duplication map into two homomorphisms between C and $\overline{C}$.

Finiteness of the Index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$

Now we prove the fourth condition in the Descent Theorem, stated as follows:

Theorem

$(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ *is finite.*

Recall the splitting of the duplication map into the two homomorphisms, shown below.

$$C(\mathbb{Q}) \xrightarrow{\phi} \overline{C}(\mathbb{Q}) \xrightarrow{\psi} C(\mathbb{Q})$$
$$P \overset{\phi}{\mapsto} \overline{P} \overset{\psi}{\mapsto} 2P$$

Using the two homomorphisms, we split the index as

$$(C(\mathbb{Q}) : 2C(\mathbb{Q})) \leq (C(\mathbb{Q}) : \psi(\overline{C}(\mathbb{Q})))(\overline{C}(\mathbb{Q}) : \phi(C(\mathbb{Q}))).$$

(Proof is simple and just group theory.) It suffices to show $(C(\mathbb{Q}) : \psi(\overline{C}(\mathbb{Q}))$ is finite (the other is symmetric). To do this, we find a homomorphism α from $C(\mathbb{Q})$ to another group, where

1. $\ker(\alpha) = \psi(\overline{C}(\mathbb{Q}))$,
2. $\alpha(C(\mathbb{Q}))$ is finite.

Then the result follows by the First Isomorphism Theorem.

Note that we denote $\overline{a} = -2a$, and $\overline{b} = b^2 - 4a$ from here on.

Finiteness of the Index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ (cont.)

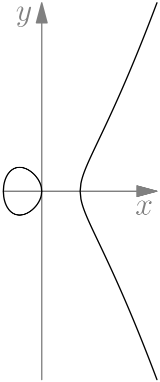

Figure: The elliptic curve C defined by $y^2 = x^3 - x$.

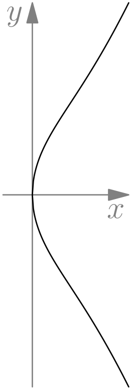

Figure: The elliptic curve $\overline{C}$ defined by $y^2 = x^3 + 4x$.

Via straightforward computation, we observe the following:

Proposition (Image of $C(\mathbb{Q})$ under ϕ)

The image $\phi(C(\mathbb{Q}))$ consists precisely of

1. $\overline{\mathcal{O}}$,
2. $\overline{T} = (0,0)$ *iff* $\overline{b} \in \mathbb{Z}^2$,
3. *nonzero* (x, y) *iff* $x \in \mathbb{Q}^2$.

Similarly, the image $\psi(\overline{C}(\mathbb{Q}))$ consists precisely of

1. $\mathcal{O}$,
2. $T = (0,0)$ iff $b \in \mathbb{Z}^2$,
3. nonzero (x, y) iff $x \in \mathbb{Q}^2$.

Finiteness of the Index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ (cont.)

Define the map
$\alpha : C(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by

$$\mathcal{O} \mapsto 1 \mod (\mathbb{Q}^*)^2$$
$$T \mapsto b \mod (\mathbb{Q}^*)^2$$
$$(x, y) \mapsto x \mod (\mathbb{Q}^*)^2 \text{ for nonzero } x$$

Weak Mordell's Theorem

$(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite.

Proposition

1. α *is a (group) homomorphism.*
2. *The kernel of* α *is* $\psi(\overline{C}(\mathbb{Q}))$.
3. $\alpha(C(\mathbb{Q})) \subseteq \{(\pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k})(\mathbb{Q}^*)^2 \mid \epsilon_i = 0, 1$ *for all* $1 \le i \le k\}$, *where* p_i *are distinct prime factors of* b.

For (3), we write $(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, $m, n, e \in \mathbb{Z}, e \neq 0$.

Via the Descent Theorem, $C(\mathbb{Q})$ must be finitely generated, giving

Mordell's Theorem

Let C be a non-singular cubic curve defined by $y^2 = x^3 + ax^2 + bx$ for $a, b \in \mathbb{Z}$. Then the abelian group $C(\mathbb{Q})$ is finitely generated.

The Explicit Group Structure of $C(\mathbb{Q})$

We now have

$$\boxed{C(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{\upsilon_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{\upsilon_s}\mathbb{Z}.}$$

To find a formula for rank r, we apply a slew of computations and group theory to show the following:

Proposition

Let $\overline{\alpha} : \overline{C}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ be the analogy of α. Then $2^r = \frac{\#\alpha(C(\mathbb{Q}))\cdot\#\overline{\alpha}(\overline{C}(\mathbb{Q}))}{4}$.

We later explicitly compute r and $C(\mathbb{Q})$ for the curve $C : y^2 = x^3 - x$. We prepare the next proposition to compute that $\#\alpha(C(\mathbb{Q})) = \#\overline{\alpha}(\overline{C}(\mathbb{Q})) = 2$, which gives $r = 0$.

The Explicit Group Structure of $C(\mathbb{Q})$ (cont.)

For any rational point (x, y) on $C : y^2 = x^3 + ax^2 + bx$, we can write $(x, y) = (m/e^2, n/e^3)$ for integers m and n coprime, $e \in \mathbb{Z}_{\neq 0}$. Via substitution, we get

Proposition

The set of all nonzero points $(x, y) \in C(\mathbb{Q})$ *consists precisely of all*

$$(x, y) = \left(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3}\right),$$

where b_1, b_2, M, N, e *satisfy*

$$N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4$$

and $b_1 b_2 = b$. *Moreover, we must have* $(M, e, N) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z} \times \mathbb{Z}$ *and* $gcd(M, e) = \gcd(e, N) = \gcd(N, M) = \gcd(b_1, e) = \gcd(b_2, M) = 1.$

An Explicit Computation of $C(\mathbb{Q})$

We prove that for the curve $C : y^2 = x^3 - x$, whose analogy is $y^2 = x^3 + 4x$,

$$C(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

1. *Find images $\alpha(C(\mathbb{Q}))$ and $\overline{\alpha}(\overline{C}(\mathbb{Q}))$ to determine rank.*
   - $b = 1$ gives $b_1 = \pm 1$. Hence we seek solutions to

     $$N^2 = M^4 - e^4$$
     $$N^2 = -M^4 + e^4,$$

     which easily give $\alpha(C(\mathbb{Q})) = \{\pm 1 \mod (\mathbb{Q}^*)^2\}$.
   - $\overline{b} = 4$ gives $b_1 = \pm 1, \pm 2, \pm 4$. Because $\pm 1 \equiv \pm 4 \mod (\mathbb{Q}^*)^2$, we need only find solutions to the Diophantine equations for $b_1 = \pm 1, \pm 2$:

     $$N^2 = M^4 + 4e^4$$
     $$N^2 = -M^4 - 4e^4$$
     $$N^2 = 2M^4 + 2e^4$$
     $$N^2 = -2M^4 - 2e^4$$

     A speedy analysis gives $(M, e, N) = (1, 0, 1)$, $(1, 1, 2)$ so $\#\alpha(C(\mathbb{Q})), \#\overline{\alpha}(\overline{C}(\mathbb{Q})) = 2$. Hence, $\text{rank}(C(\mathbb{Q})) = 0$.
2. *Use Nagell-Lutz to determine torsion subgroup.*
   - Because $D = 4$, by Nagell-Lutz, $\mathcal{O}$, $(0,0), (\pm 1, 0)$ are the only points of finite order.

The Group of Rational Points on a Singular Cubic Curve

Mordell's Theorem has provided us the structure of the group of rational points on a non-singular cubic curve. Naturally, we turn to singular cubic curves as well. We form a group of points lying on a singular curve by excluding the singular point.

Definition

1. Let C be a cubic curve. Let $C_{ns} = \{P \in C \mid P \text{ is not singular}\}$.
2. $C_{ns}(\mathbb{Q}) = \{(x, y) \in C_{ns} \mid (x, y) \in \mathbb{Q}^2\}$.

Theorem

1. *Let C be the curve defined by $y^2 = x^3 + x^2$. Then $(C_{ns}(\mathbb{Q}), +) \cong (\mathbb{Q}^*, \times)$.*
2. *Let C be the curve defined by $y^2 = x^3$. Then $(C_{ns}(\mathbb{Q}), +) \cong (\mathbb{Q}, +)$.*

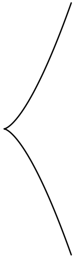

Figure: The singular elliptic curve with equation $y^2 = x^3$.

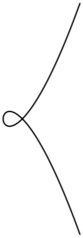

Figure: The singular elliptic curve with equation $y^2 = x^3 + x^2$.

Acknowledgements

We thank

- Our mentor Kaavya Valiveti of MIT for her valuable guidance and feedback.
- Dr. Pavel Etingof, Dr. Slava Gerovitch, Dr. Tanya Khovanova, the MIT Math Department, and the MIT PRIMES program, for providing us with the opportunity to work on this project.
- You for listening.