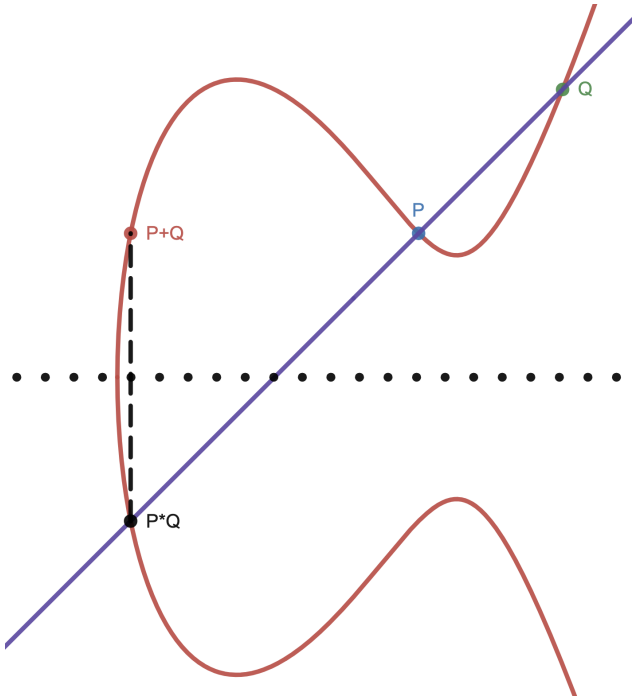
Torsion points on Elliptic Curves

Rohan Ramkumar

July 14,2023

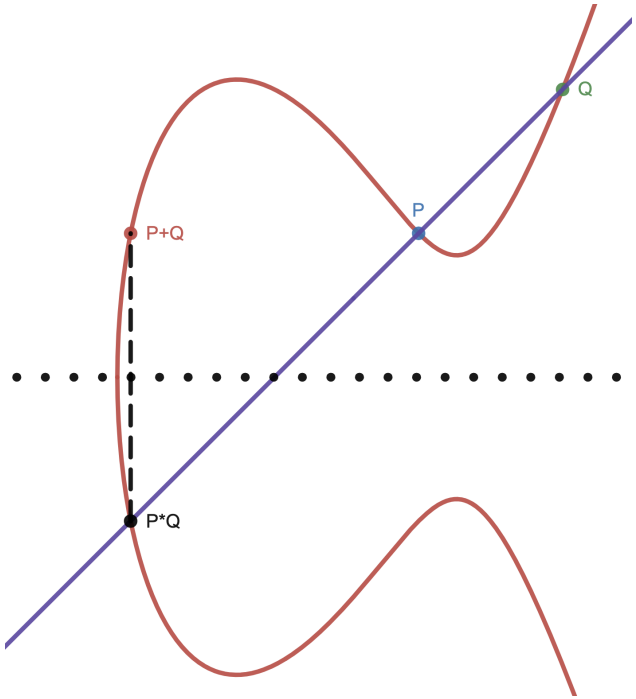
What are Elliptic Curves?

An elliptic curve is a curve with the equation $y^2 = x^3 + ax^2 + bx + c$. With a linear transformation, we can turn it into the more common form $y^2 = x^3 + ax + b$.



What are Elliptic Curves?

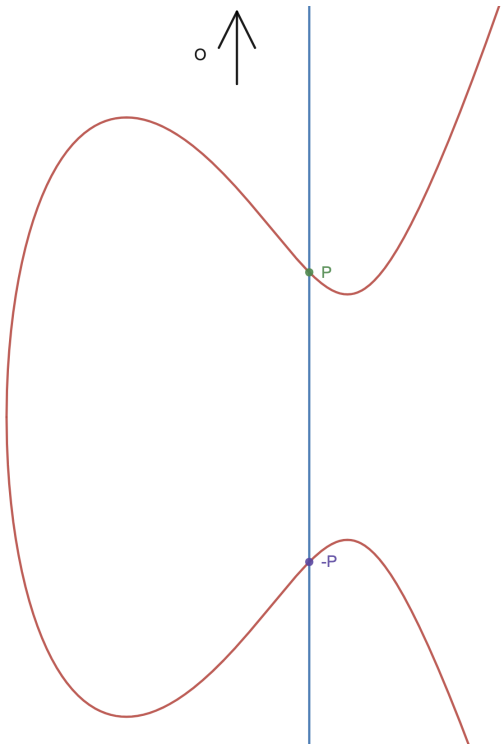
An elliptic curve is a curve with the equation $y^2 = x^3 + ax^2 + bx + c$. With a linear transformation, we can turn it into the more common form $y^2 = x^3 + ax + b$.



We define the sum of two points to be the reflection over the $x-$axis of the intersection of the line joining those points and the curve. This new point must be rational. It turns out that this operation forms an Abelian group.

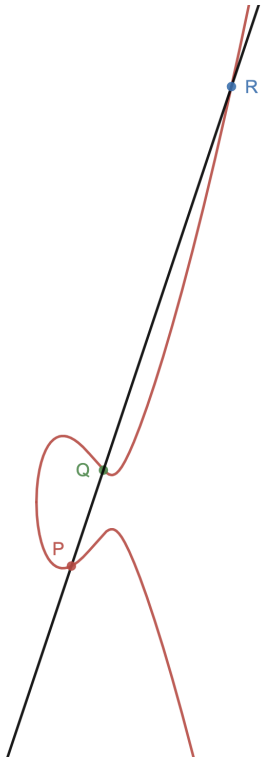
What are Elliptic Curves?

In addition to the sets of rational points, we choose to include the point at infinity, $\mathbb{O}$. We define the line through P and $\mathbb{O}$ to be the vertical line through P. We can see that $P + \mathbb{O} = P$, so we can treat $\mathbb{O}$ as the identity element of our group. If we define the negative of a point to be the point's reflection over the x-axis, we see that $P + (-P) = \mathbb{O}$, which agrees with the definition of an additive inverse.



What are Elliptic Curves?

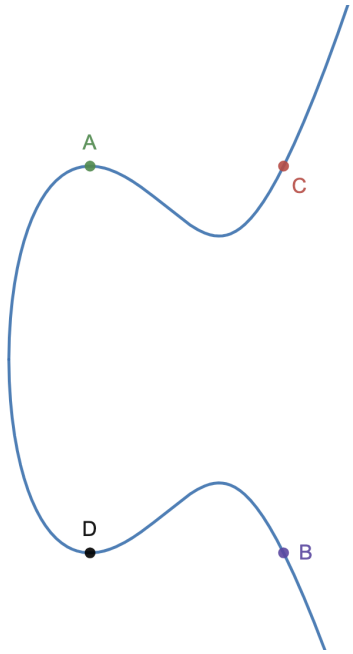
If our two points that we are adding coincide, we use the tangent line at that point instead. Also, note that if three points P, Q, R lie on a line, then $P + Q + R = \mathbb{O}$.



We can see this by noting that $P + Q = -R$, by the construction of point addition, so $P + Q + R = \mathbb{O}$.

What are torsion points?

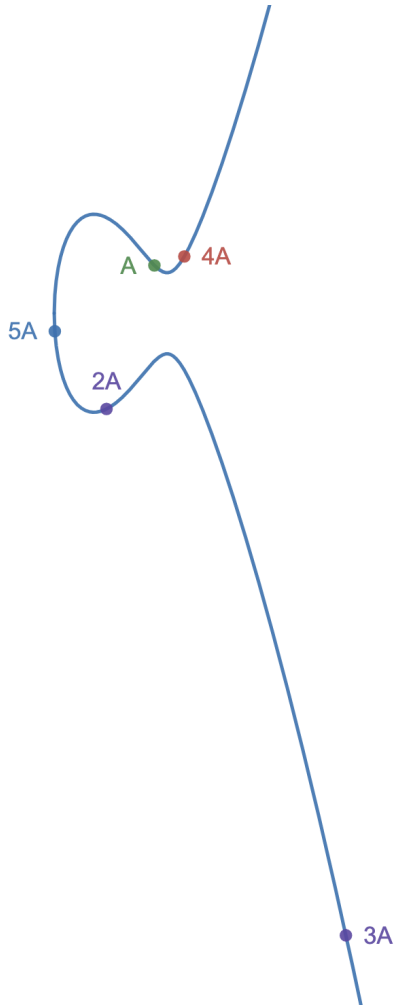
A point P is called a torsion point if there is some n such that $nP = \mathbb{O}$.



Here, we see that $B = 2A, C = 3A, D = 4A, \mathbb{O} = 5A$, so A has order 5.

What are torsion points?

Not all rational points are torsion points.



I have only shown the first 5 multiples of A, but it can be shown that no multiple of A will bring it back to itself.

Important theorems about Torsion Points

Theorem

(Mordell-Weil) The additive group of an elliptic curve is finitely generated; that is, its group can be represented as the direct sum:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors} \cong \mathbb{Z}^r \oplus C_{p_1} \oplus \cdots \oplus C_{p_n},$$

where C_n is the cyclic group of order n.

Important theorems about Torsion Points

Theorem

(Mordell-Weil) The additive group of an elliptic curve is finitely generated; that is, its group can be represented as the direct sum:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors} \cong \mathbb{Z}^r \oplus C_{p_1} \oplus \cdots \oplus C_{p_n},$$

where C_n is the cyclic group of order n.

$\mathbb{Z}^r$ is called the free part and the rest, which has finite order, is called the torsion part. We call r the rank of the elliptic curve. The rank of an elliptic curve is related to many challenging questions in number theory, including one of the Millenium prize problems, the Birch and Swinnterton-Dyer conjecture. Additionally, the question about whether or not there is an upper bound for ranks of elliptic curves still remains unanswered (the largest known rank is 28).

Important theorems about Torsion Points

Theorem

(Nagell-Lutz) If (x, y) is a rational point of finite order on an elliptic curve, then the following is true:

1. *Both x and y are integers,*
2. *Either $y = 0$ or $y^2 \mid \Delta$, where Δ is the discriminant of the cubic function $x^3 + ax + b$.*

Important theorems about Torsion Points

Theorem

(Nagell-Lutz) If (x, y) is a rational point of finite order on an elliptic curve, then the following is true:

1. *Both x and y are integers,*
2. *Either $y = 0$ or $y^2 \mid \Delta$, where Δ is the discriminant of the cubic function $x^3 + ax + b$.*

Recall that the discriminant of a quadratric equation is $b^2 - 4ac$. Similarly, we can define an expression for any polynomial called the discriminant. Although the converse of Nagell-Lutz is not true, this theorem is a very useful way of checking a priori if a point has finite order. For example, for the elliptic curve $y^2 = x^3 - 7x + 10$, the point $(9, -26)$ cannot possibly be of finite order because $(26)^2 \nmid \Delta = -1328$.

Important theorems about Torsion Points

Theorem

(Mazur) Any elliptic curve can only have the following torsion subgroups:

- C_n *for* $1 \leq n \leq 10$ *or* $n = 12$, *where* C_n *is the cyclic subgroup of order* n.
- $C_{2n} \oplus C_2$ *for* $1 \leq n \leq 4$.

Important theorems about Torsion Points

Theorem

(Mazur) Any elliptic curve can only have the following torsion subgroups:

- C_n *for* $1 \leq n \leq 10$ *or* $n = 12$, *where* C_n *is the cyclic subgroup of order* n.
- $C_{2n} \oplus C_2$ *for* $1 \leq n \leq 4$.

With this theorem, we are able to fully classify the groups of points on all elliptic curves, as, by Mordell-Weil, they all elliptic curves are of the form $\mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$.

$n = 11$ is impossible

$n = 11$ is the smallest value of n such that C_n is not a possible torsion group, so we will investigate that case. Let P be a point of order 11 and define $P_n = nP$. After a change of variables we have the following in homogeneous coordinates:

$$P_0 = (0, 1, 0), P_1 = (1, 0, 0), P_2 = (0, 0, 1), P_3 = (1, 1, 1).$$

If we let $P_4 = (x_1, x_2, x_3)$, we can calculate

$$P_5 = ((x_1 - x_3)x_2, -x_1x_2 + x_1x_3 + x_2^2 - x_3^2, (x_1 - x_3)x_3).$$

Since $P_2 + P_4 + P_5 = 2P + 4P + 5P = 11P = \mathbb{O}$, these three points must be collinear.

$n = 11$ is impossible

Lemma

(Collinearity Lemma) In homogeneous coordinates, if points $(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3)$ are collinear, then the determinant

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = 0.$$

This can be proved using some linear algebra. Applying this lemma to P_2, P_4, and P_5, we have

$$\begin{vmatrix} 0 & 0 & 1 \\ x_1 & x_2 & x_3 \\ (x_1 - x_3)x_2 & -x_1x_2 + x_1x_3 + x_2^2 - x_3^2 & (x_1 - x_3)x_3 \end{vmatrix} = 0.$$

Solving this, we get

$$x_1^2x_2 - x_1^2x_3 + x_1x_3^2 - x_2^2x_3 = 0.$$

$n = 11$ is impossible

Define the cubic curve

$$C : u^2v - u^2w + uw^2 - v^2w = 0.$$

We can verify that the five points

$$(0, 1, 0), (1, 0, 0), (0, 0, 1), (1, 1, 1), (1, 0, 1)$$

satisfy this equation, but from our construction, some other point (x_1, x_2, x_3) must also satisfy it. We want to prove that this is impossible; in other words, C has exactly 5 rational points.

$n = 11$ is impossible

Define the cubic curve

$$C : u^2v - u^2w + uw^2 - v^2w = 0.$$

We can verify that the five points

$$(0, 1, 0), (1, 0, 0), (0, 0, 1), (1, 1, 1), (1, 0, 1)$$

satisfy this equation, but from our construction, some other point (x_1, x_2, x_3) must also satisfy it. We want to prove that this is impossible; in other words, C has exactly 5 rational points. With the transformation

$$f(u, v, w) = (4uv, 8v^2 - 4uw, uw),$$

we can turn C into a new curve

$$E : y^2z = x^3 - 4x^2z + 16z^3.$$

Dehomogenizing by setting $z = 1$, we get a more familiar form

$$E : y^2 = x^3 - 4x^2 + 16.$$

$n = 11$ is impossible

We have just turned our curve C into an elliptic curve! First we will check torsion points. Using Nagell-Lutz, we see that $y = 0$ or $y^2 \mid -2816$. We can determine from trial and error that the set of torsion points is the following:

$$\{\mathbb{O}, (0, 4), (0, -4), (4, 4), (4, -4)\}.$$

$n = 11$ is impossible

We have just turned our curve C into an elliptic curve! First we will check torsion points. Using Nagell-Lutz, we see that $y = 0$ or $y^2 \mid -2816$. We can determine from trial and error that the set of torsion points is the following:

$$\{\mathbb{O}, (0, 4), (0, -4), (4, 4), (4, -4)\}.$$

As desired, there are exactly 5 torsion points! But we aren't done yet. Remember Mordell-Weil:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}.$$

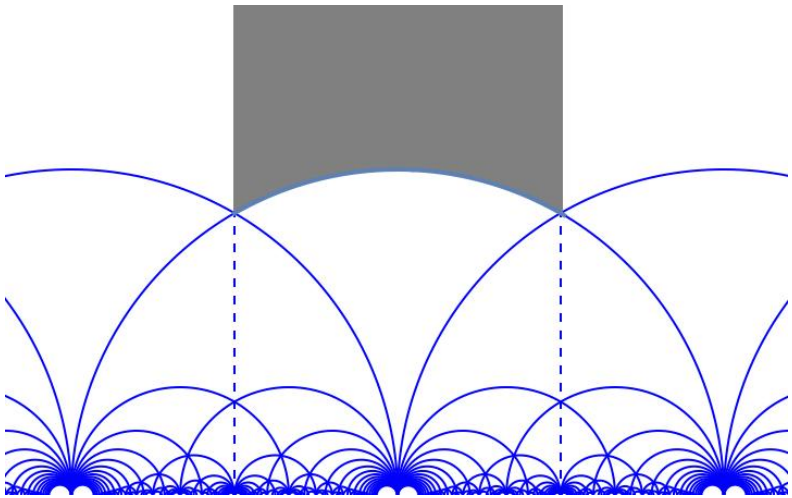
We have shown that there are exactly 5 points in $E(\mathbb{Q})_{tors}$, but we also need to show that $r = 0$ in order to show that there are no more than 5 points in $E(\mathbb{Q})$.

$n = 11$ is impossible

However, proving that $r = 0$ turns out to be extremely difficult, requiring a lot of algebraic number theory. The main idea of the proof is that we want to show that every point in $E(\mathbb{Q})$ is a multiple of 2. If this is true, then there cannot be a free part of $E(\mathbb{Q})$, as not all integers are multiples of 2. However, for $E(\mathbb{Q})_{tors} \cong C_5$, each point is a multiple of 2 (think of integers modulo 5).

$n = 11$ is impossible

Thus, we have proved that C_{11} is not a possible torsion group of an elliptic curve E. If we try to apply this procedure to higher values of n, such as $n = 13$, we run into problems; for example, instead of a cubic elliptic curve, we end up with a hyperelliptic 7-degree curve. We have to instead use modular curves to study these.



Significance

Elliptic curves have many uses, including factorization and primality testing, but by far the most popular use of it is in cryptography. Instead of looking at elliptic curves over $\mathbb{Q}$, they are considered in the finite field $\mathbb{F}_p$. In this field, given the points P and nP, it is very difficult to figure out the value of n, which provides a safe algorithm that is used throughout the world, including things like bitcoin.