Counting Points on Elliptic Curves in Small Boxes

Christian Bagshaw
Postgraduate Conference 2024

Elliptic Curves over $\mathbb{R}$

I am sure many of you have heard the term "elliptic curve" at some point.

There is a more formal definition, but for our purposes we can think of an elliptic curve E over a field $\mathbb{F}$ as a curve of the form

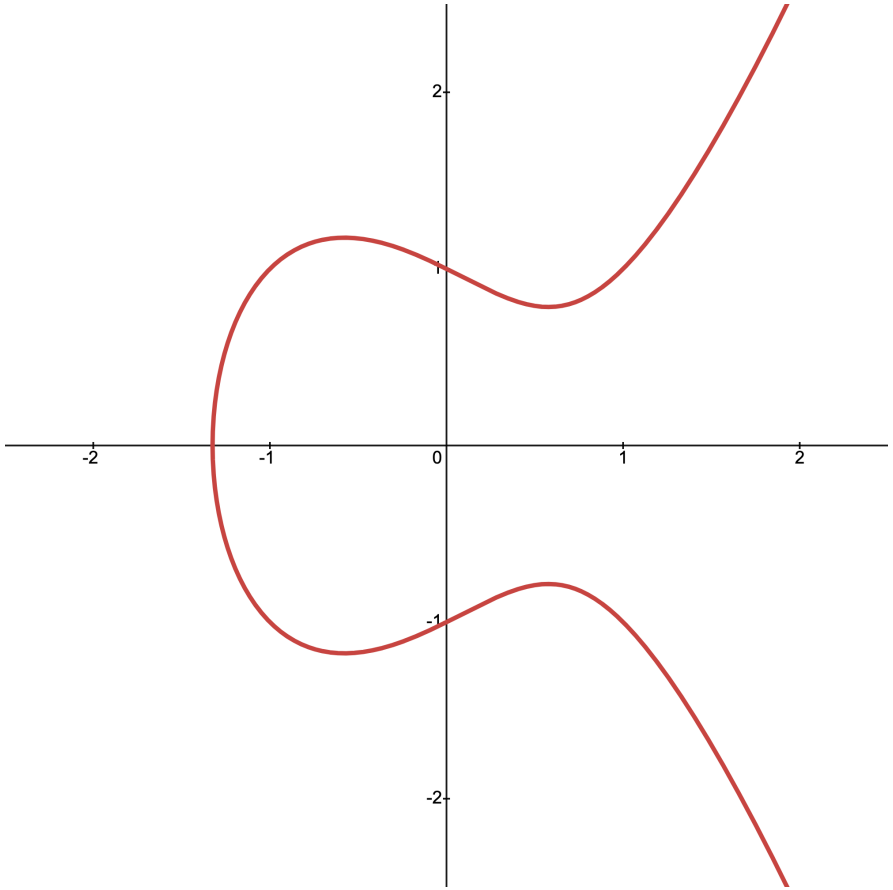
$$E : y^2 = x^3 + Ax + B$$

for some $A, B \in \mathbb{F}$ (with some minor restrictions on $\mathbb{F}$, A and B).

We will refer to the points on the curve as $E(\mathbb{F})$.

Elliptic Curves over $\mathbb{R}$

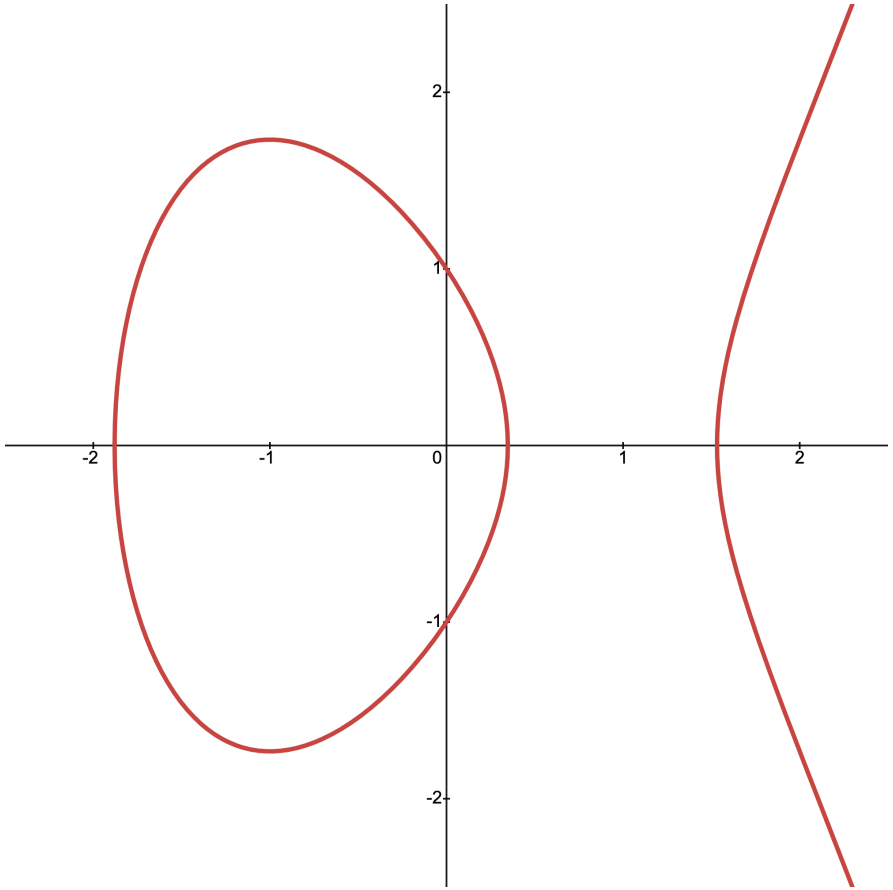
$$E : y^2 = x^3 - x + 1$$



An elliptic curve over $\mathbb{R}$ will typically look like this.

Elliptic Curves over $\mathbb{R}$

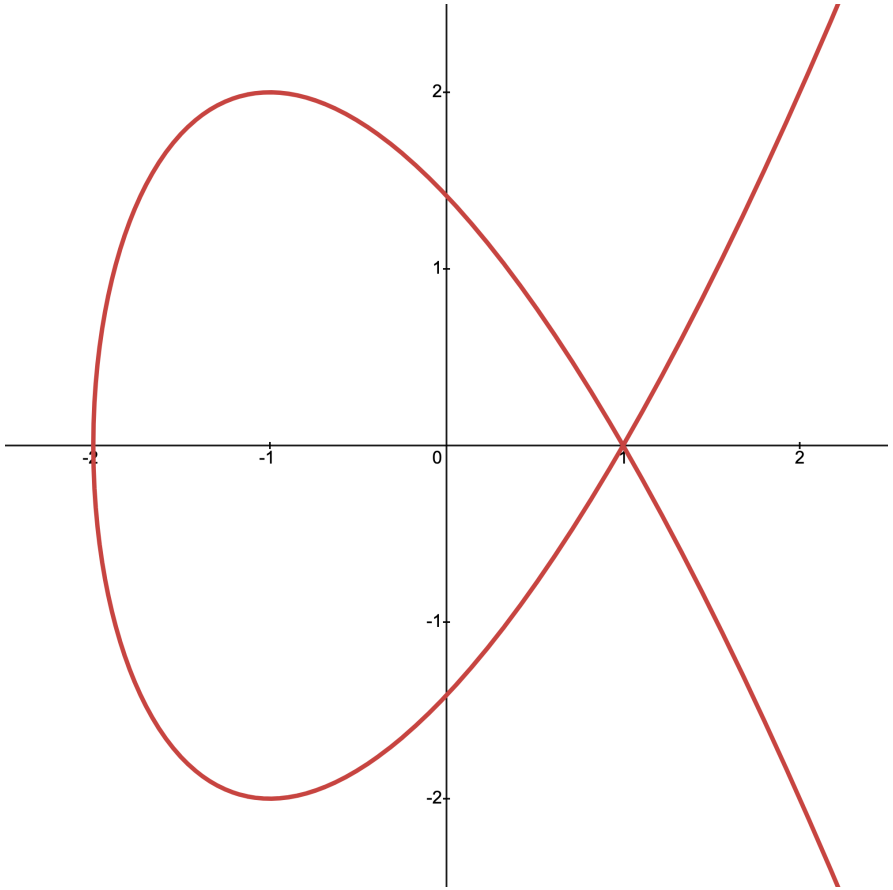
$$E : y^2 = x^3 - 3x + 1$$



Or it may look like this.

Elliptic Curves over $\mathbb{R}$

$E : y^2 = x^3 - 3x + 2$

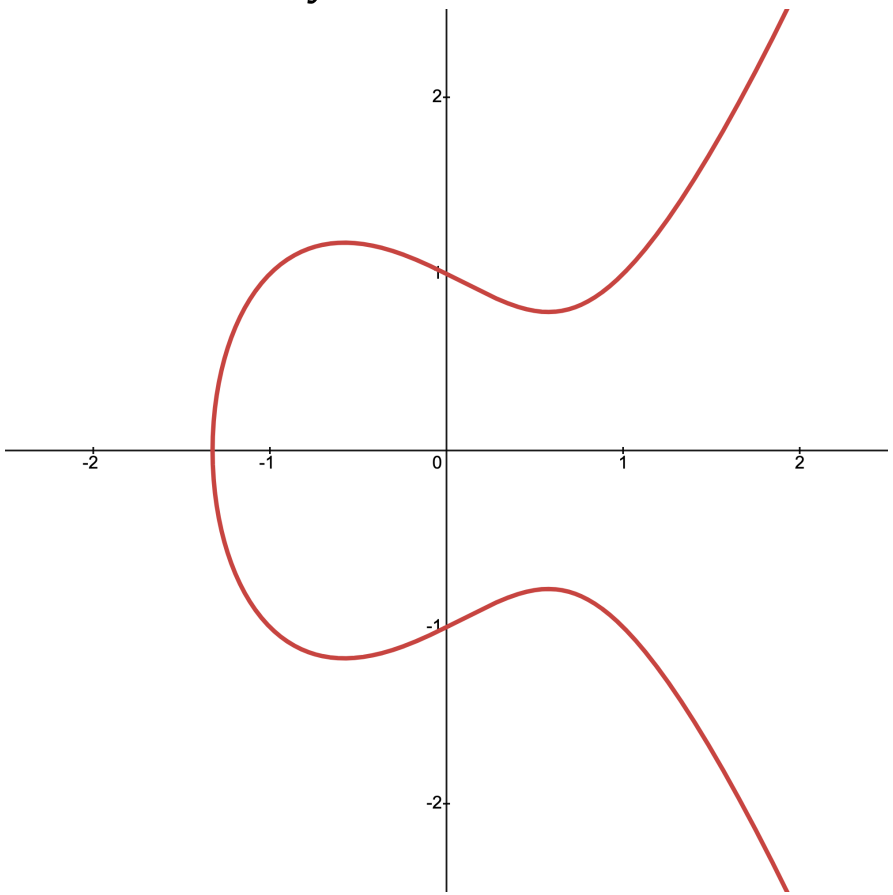


But we want to avoid "singularities" like this.

So if our curve is $y^2 = x^3 + Ax + B$ then we want $4A^3 + 27B^2 \neq 0$.

Elliptic Curves over $\mathbb{R}$

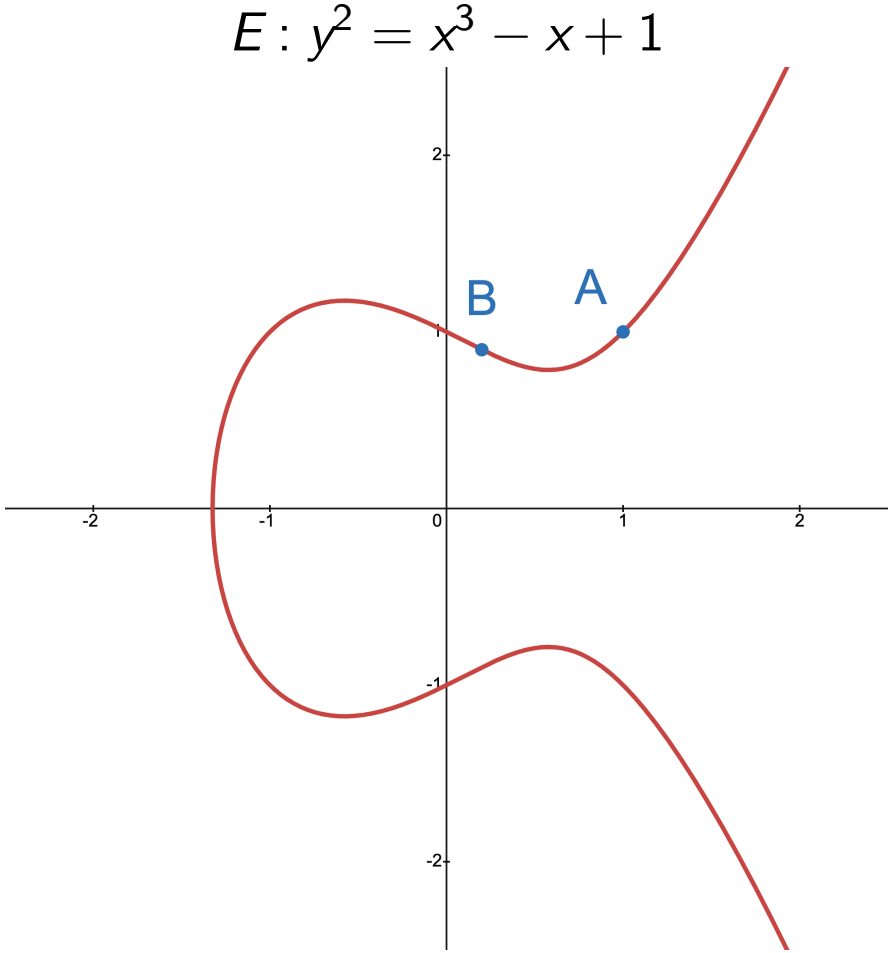
$$E : y^2 = x^3 - x + 1$$



Why do people care about a curve like this?

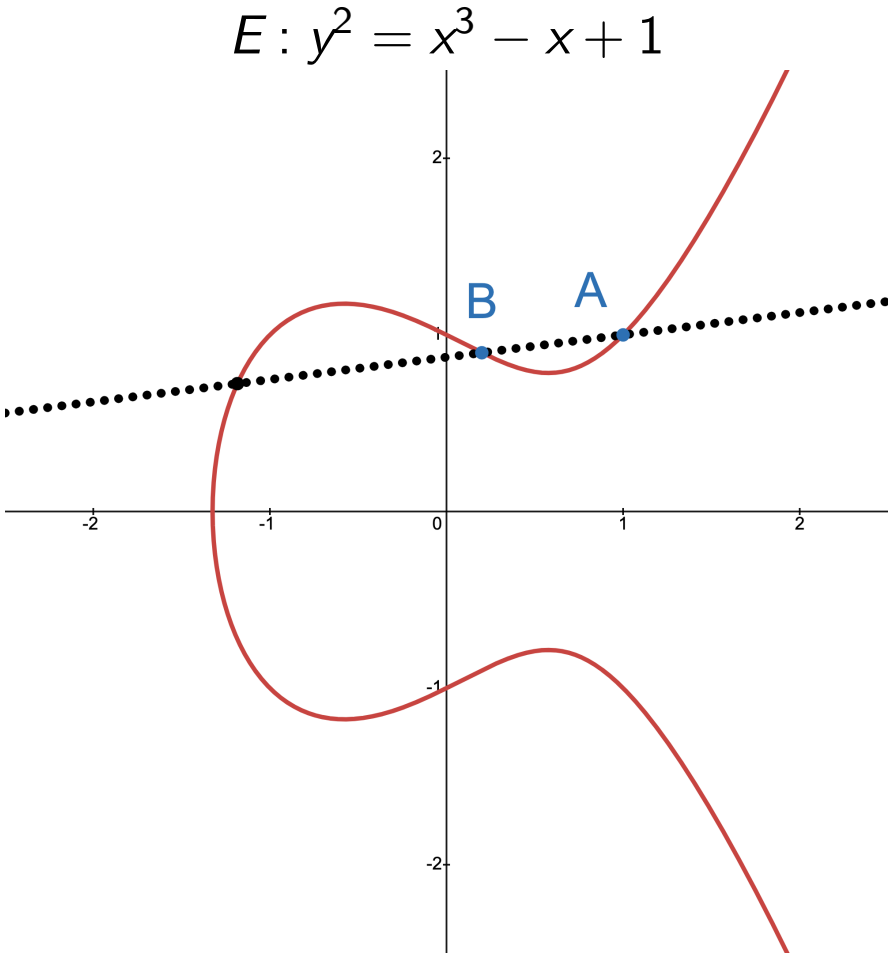
It turns out that the points on the curve can form a "group". There is a natural way to "add" two points on the curve to get another point on the curve.

Elliptic Curves over $\mathbb{R}$



Suppose we have some points A and B.

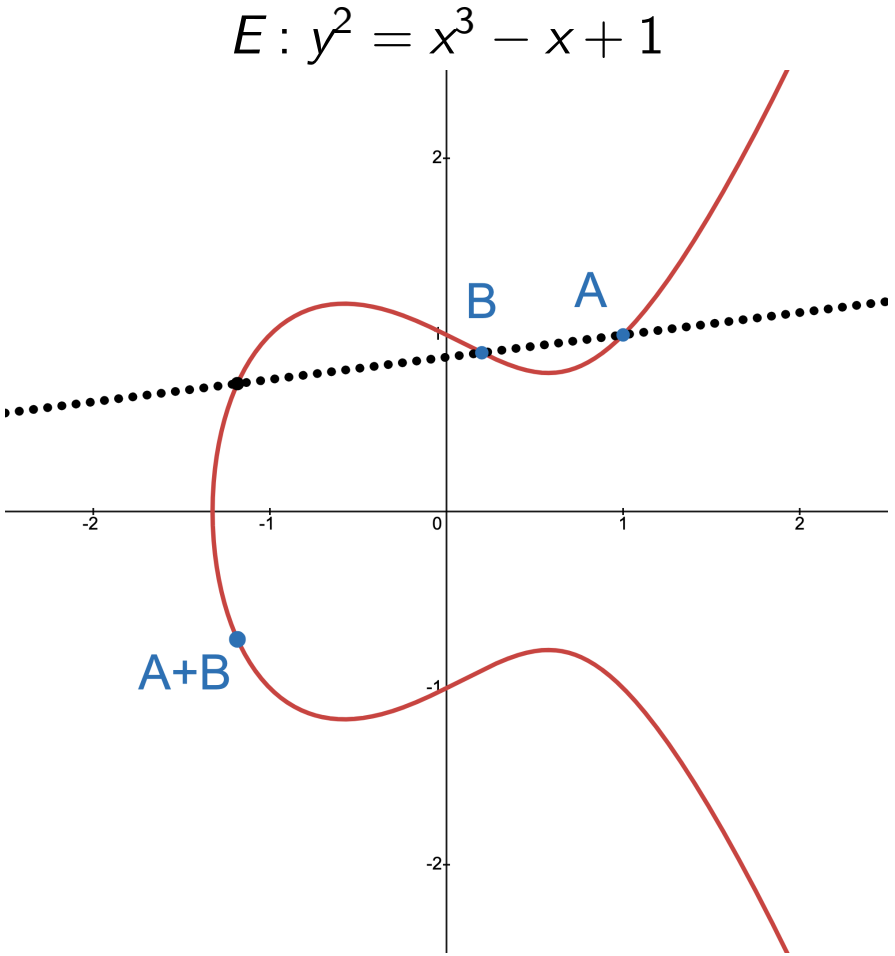
Elliptic Curves over $\mathbb{R}$



Suppose we have some points A and B.

Because this curve is a cubic, the line through A and B should intersect the curve at another point.

Elliptic Curves over $\mathbb{R}$

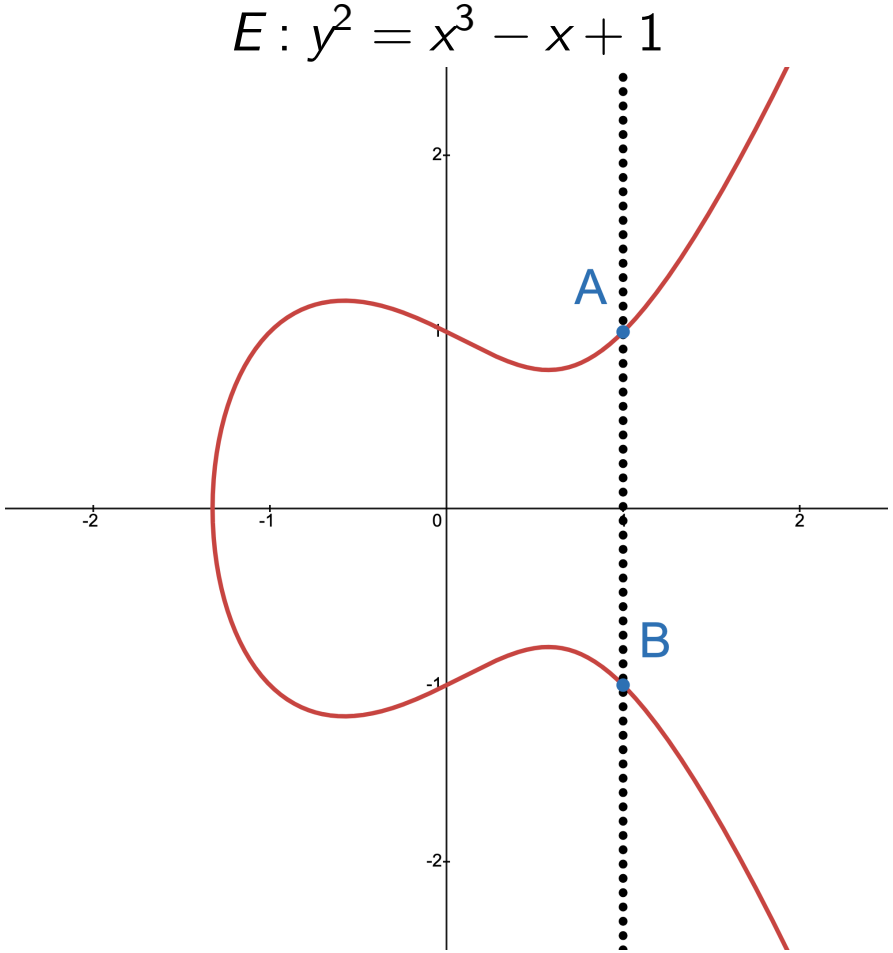


Suppose we have some points A and B.

Because this curve is a cubic, the line through A and B should intersect the curve at another point.

Let's reflect this point across the x-axis, and call this new point $A + B$.

Elliptic Curves over $\mathbb{R}$



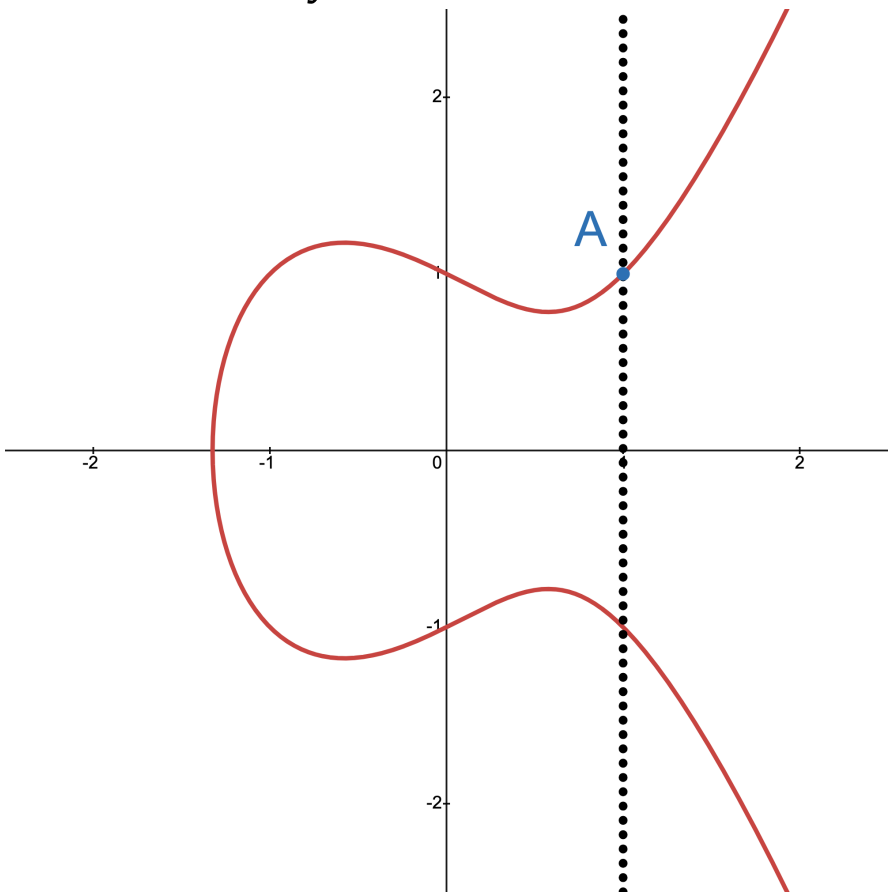
Unfortunately, this operation isn't quite closed as we have defined things thus far.

We will add an extra point O to the curve E, which we will call the "point at infinity", and it intersects all vertical lines.

So if A and B lie on a vertical line, then we will just say $A + B = O$.

Elliptic Curves over $\mathbb{R}$

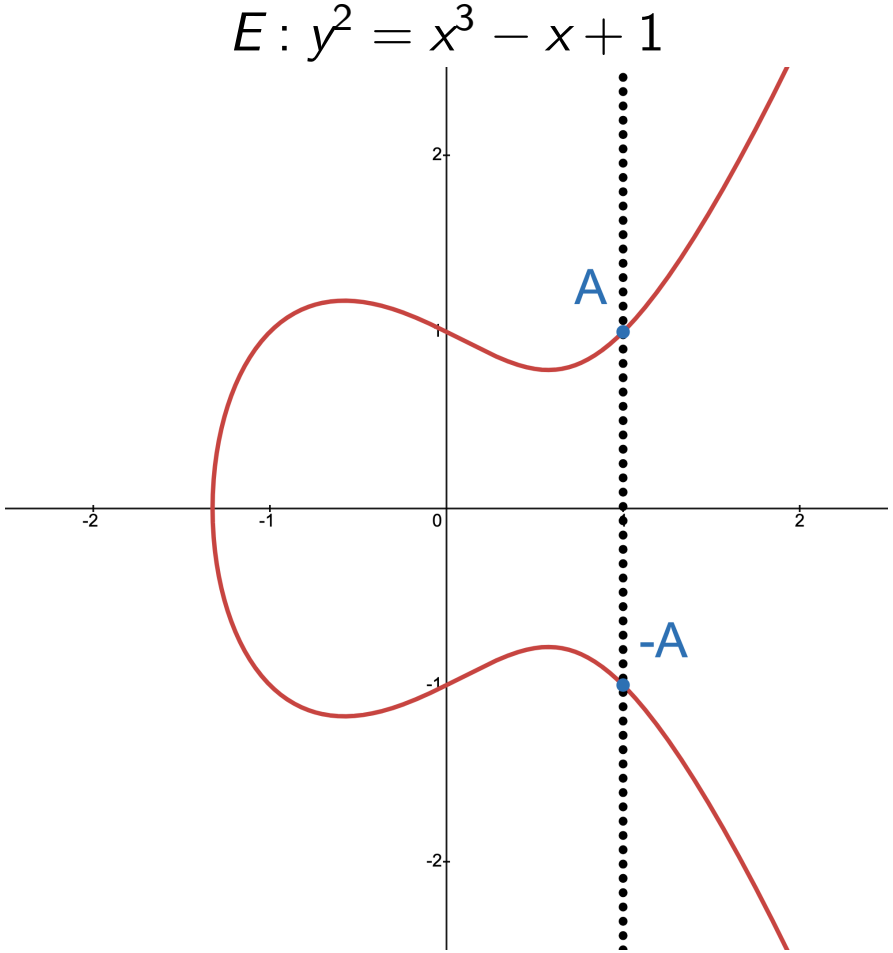
$E : y^2 = x^3 - x + 1$



Notice that

$A + O = A.$

Elliptic Curves over $\mathbb{R}$



Notice that

$$A + O = A.$$

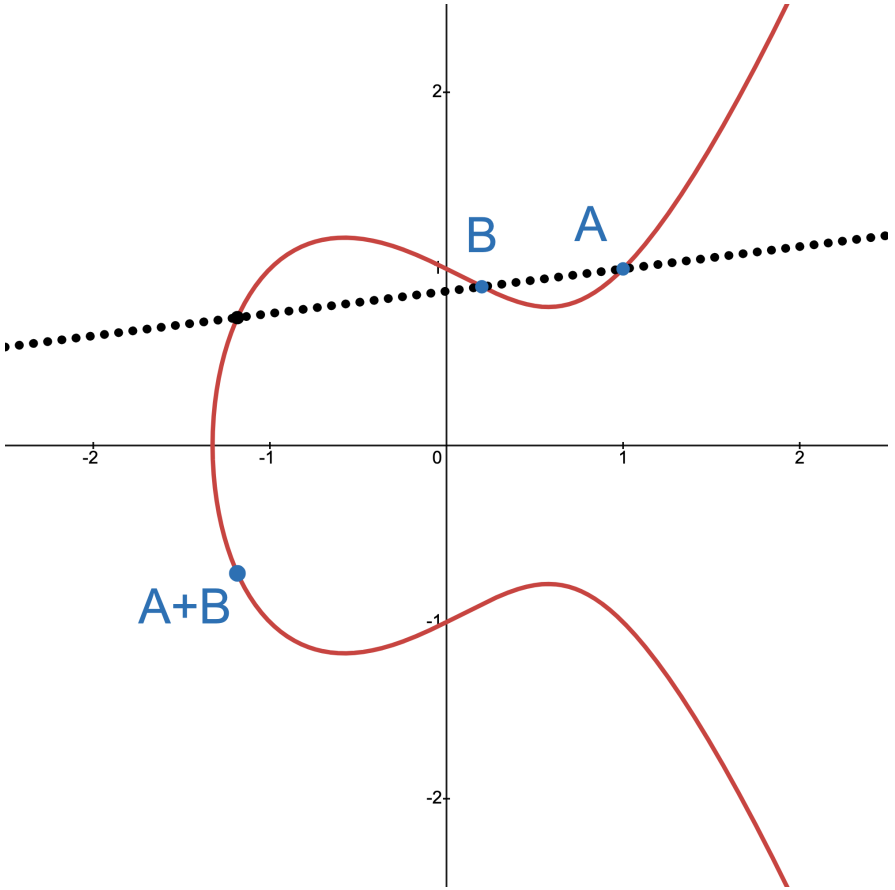
And if we called the reflection of A across the x-axis "$-A$", then as we saw before we get

$$A + (-A) = O.$$

O is acting like the identity for a group!

Elliptic Curves over $\mathbb{R}$

$$E : y^2 = x^3 - x + 1$$



To summarize:

$$A + B \in E,$$

$$A + (B + C) = (A + B) + C,$$

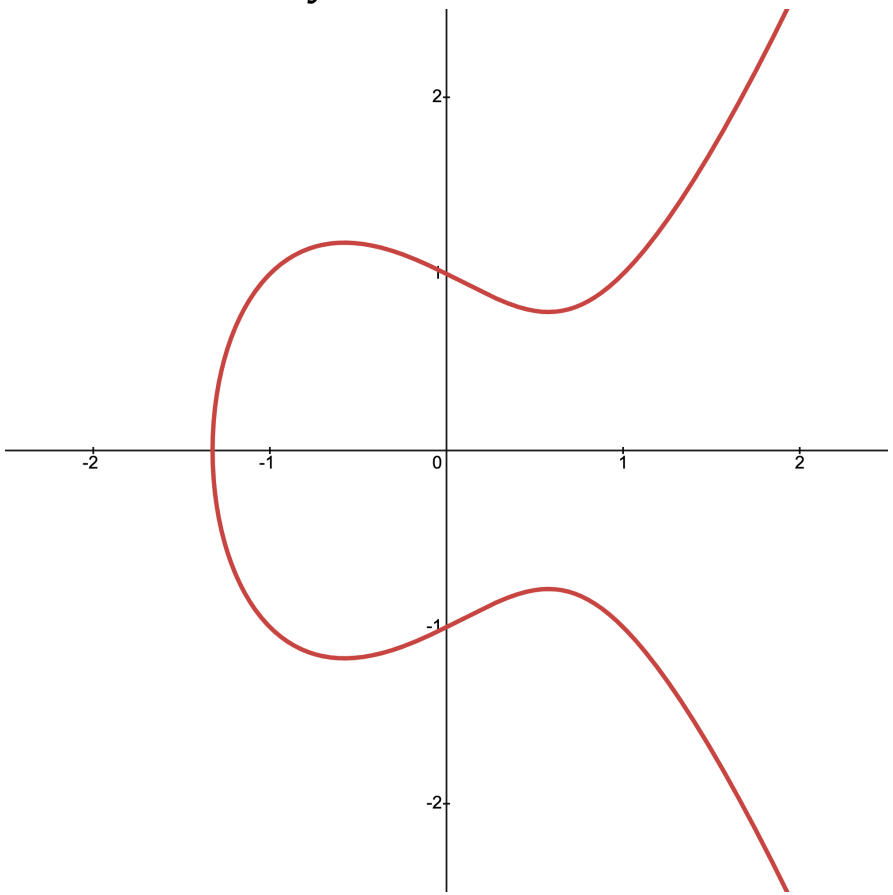
$$A + B = B + A,$$

$$A + O = A,$$

$$A + (-A) = O.$$

Elliptic Curves over $\mathbb{R}$

$$E : y^2 = x^3 - x + 1$$



How many points are on E?

Over $\mathbb{R}$, maybe this isn't too interesting because there are of course an uncountably infinite number of points...

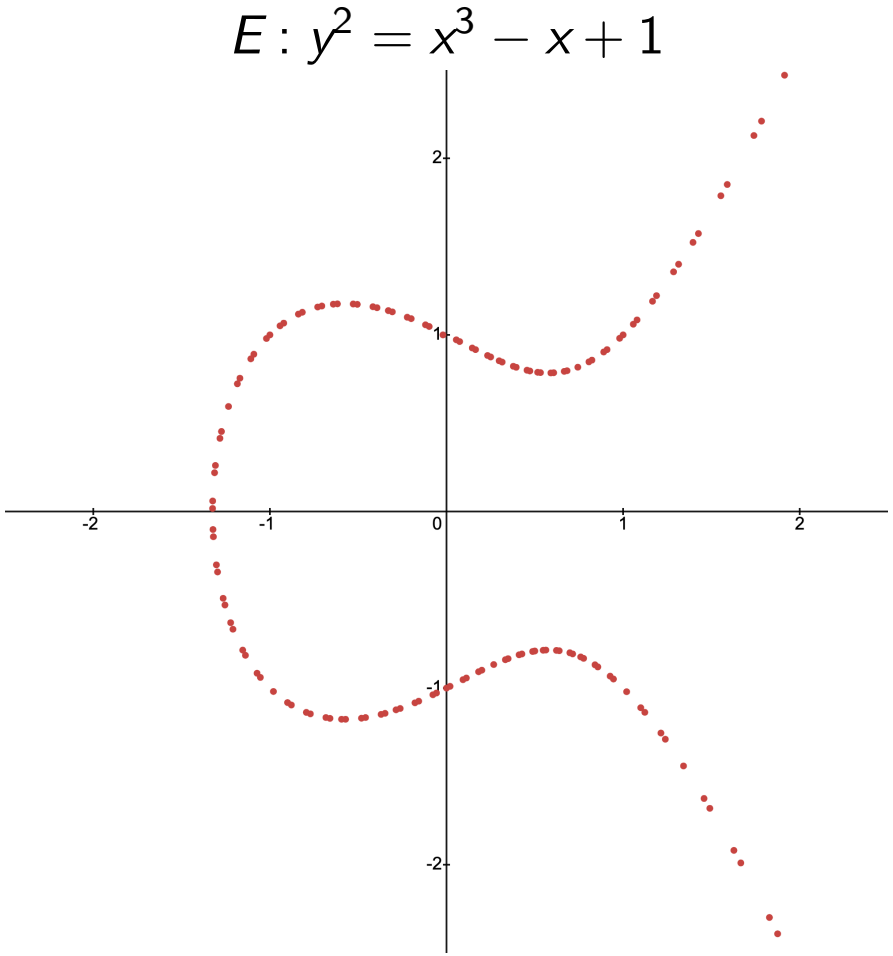
For those interested, in general for any curve E,

$$E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$$

or

$$E(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$$

Elliptic Curves over $\mathbb{Q}$



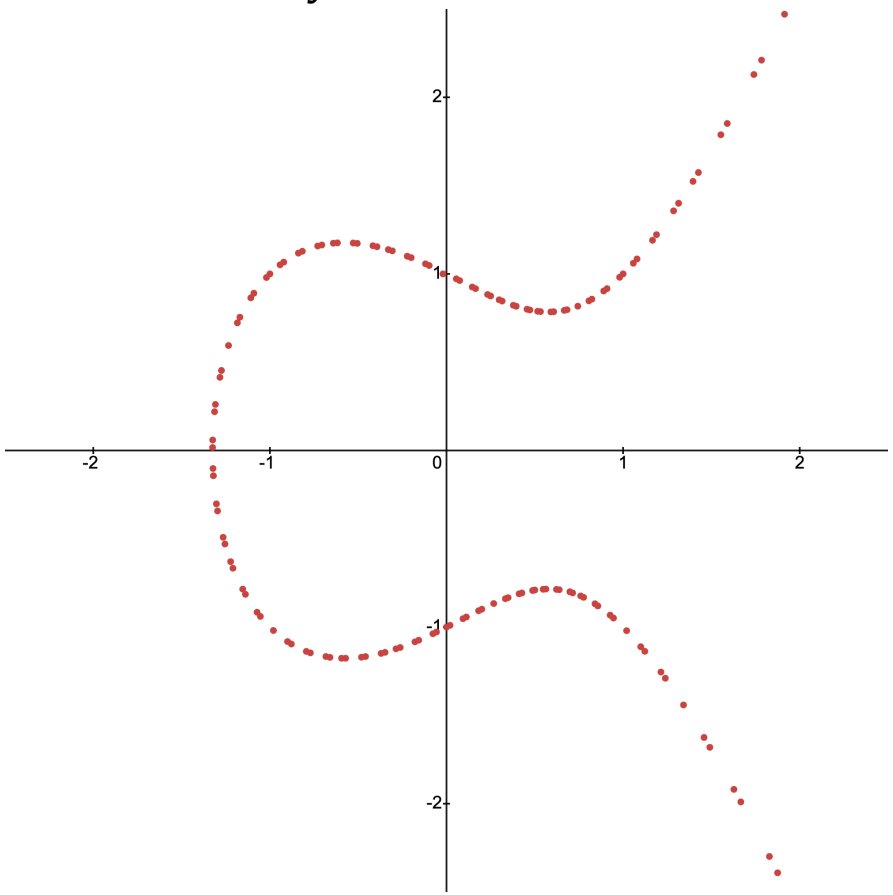
But what about over $\mathbb{Q}$?

These are some of the rational points on this curve (points where both x and y are rational).

Determining the number of points on this isn't so easy anymore...

Elliptic Curves over $\mathbb{Q}$

$$E : y^2 = x^3 - x + 1$$



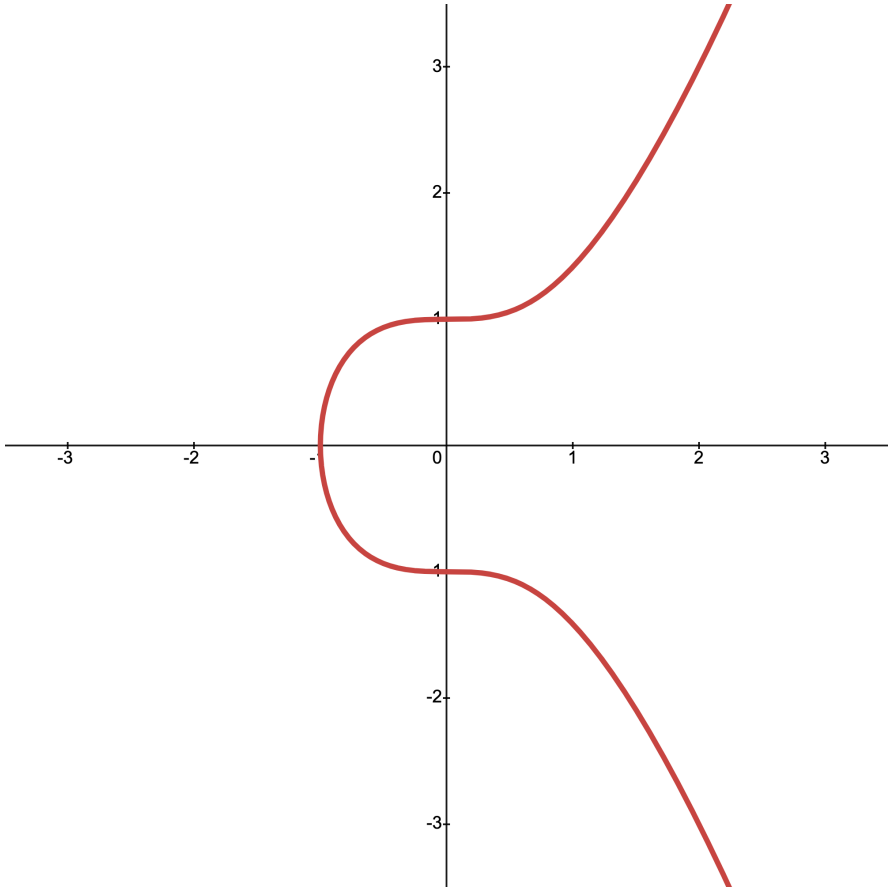
In this particular case, actually there are infinitely many points.

For those interested, in this case

$$E(\mathbb{Q}) \cong \mathbb{Z}.$$

Elliptic Curves over $\mathbb{Q}$

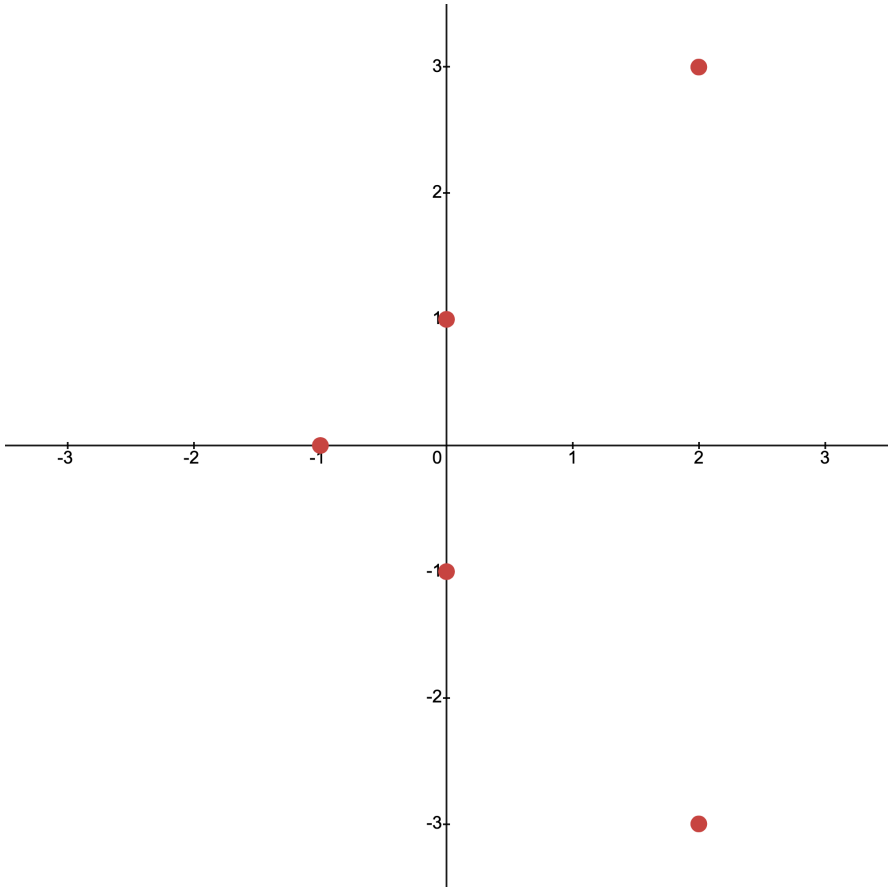
$$E : y^2 = x^3 + 1$$



Let's look at one more example.

Elliptic Curves over $\mathbb{Q}$

$$E : y^2 = x^3 + 1$$



Let's look at one more example.

This curve seemingly has less rational points.

And in fact, these are all of them!

$$E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$$

A Brief Aside: Fermat's Last Theorem

Theorem (Taylor-Wiles (1995))

The equation $a^n + b^n = c^n$ has no non-zero integer solutions if $n \geq 3$.

This was first conjectured by Fermat in 1637, and its proof was certainly one of the greatest achievements in mathematics in the 20th Century.

But what does this have to do with elliptic curves?

A Brief Aside: Fermat's Last Theorem

Suppose we have a non-zero solution (a, b, c) to

$$a^n + b^n = c^n.$$

In his thesis in 1972, Yves Hellegouarch took a look at the elliptic curve

$$E_{a,b,c} : y^2 = x(x - a^n)(x + b^n)$$

At first glance there isn't neccesarily anything wrong with this curve, but it has some strange properties that we typically don't expect.

Mathematicians began to think that maybe a way to prove Fermat's Last Theorem is to show that this curve can't exist.

A Brief Aside: Fermat's Last Theorem

$$E_{a,b,c} : y^2 = x(x - a^n)(x + b^n)$$

Conjecture (Taniyama-Shimura (1955))

Every elliptic curve over $\mathbb{Q}$ is modular.

Theorem (Ribet (1986))

The elliptic curve $E_{a,b,c}$ is NOT modular.

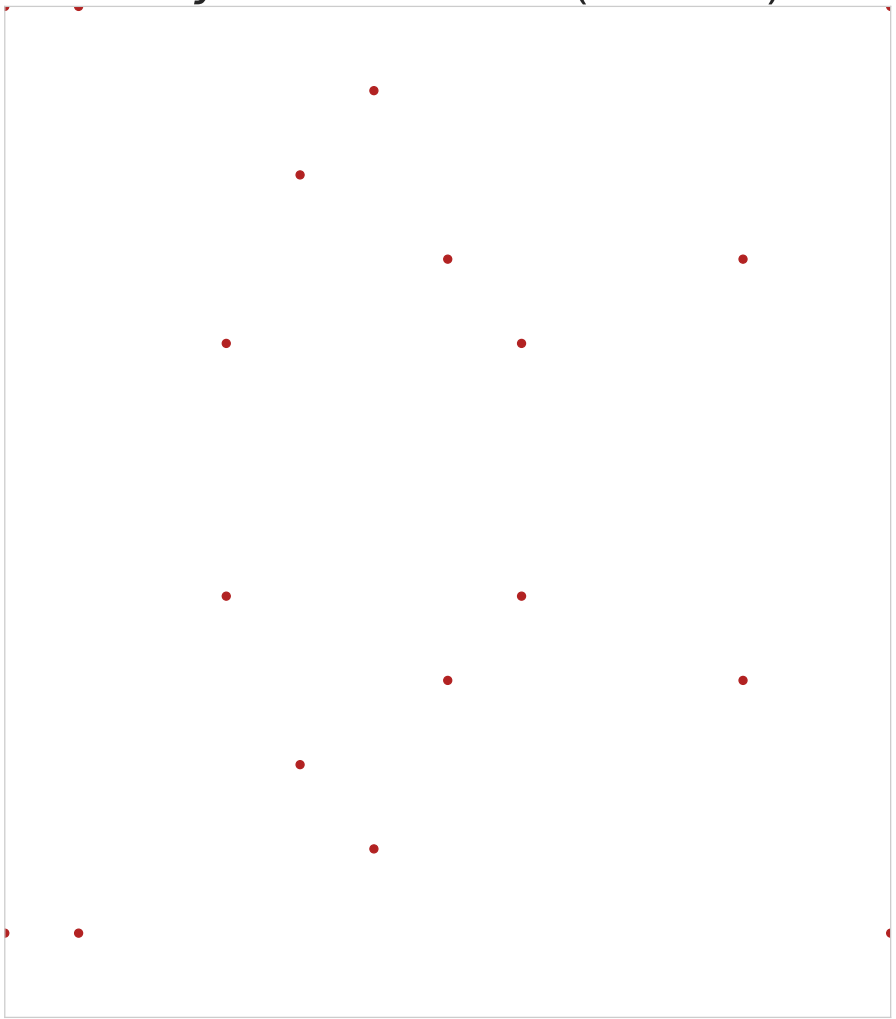
If you prove the Taniyama-Shimura conjecture, then you get Fermat's Last Theorem for free!

Theorem (Taylor-Wiles (1995))

Every (semi-stable) elliptic curve over $\mathbb{Q}$ is modular.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{13}$$



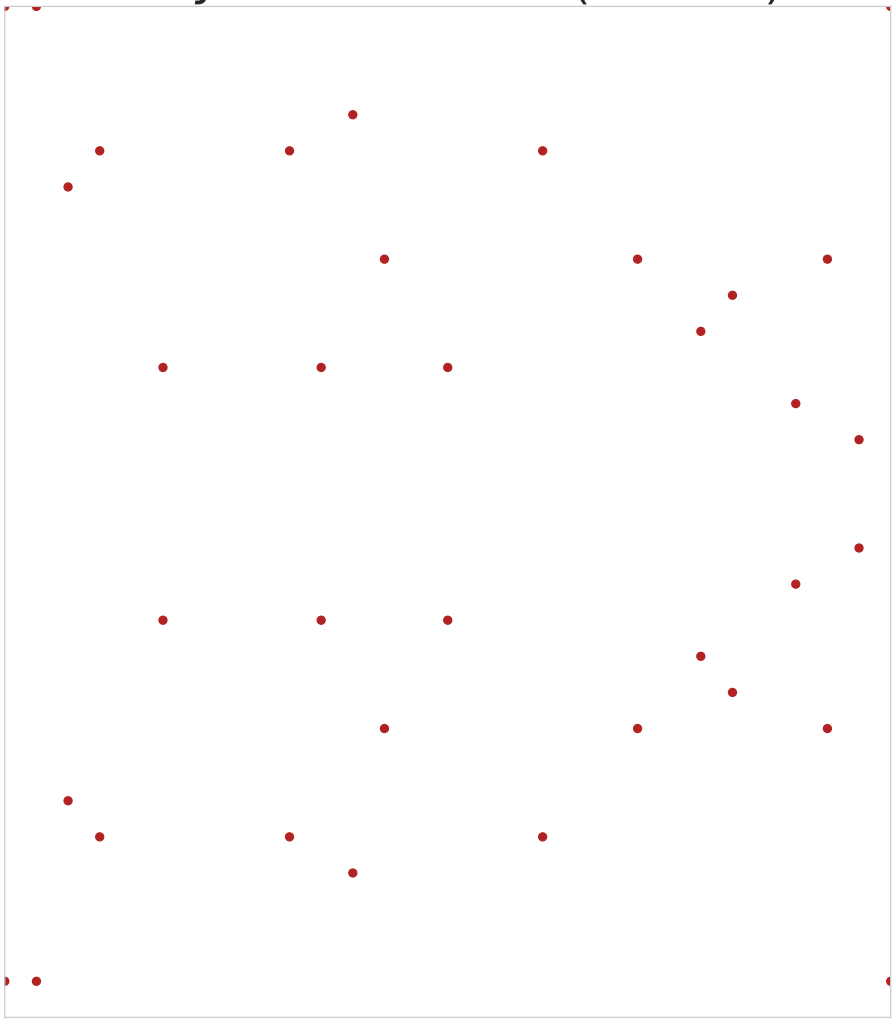
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{29}$$



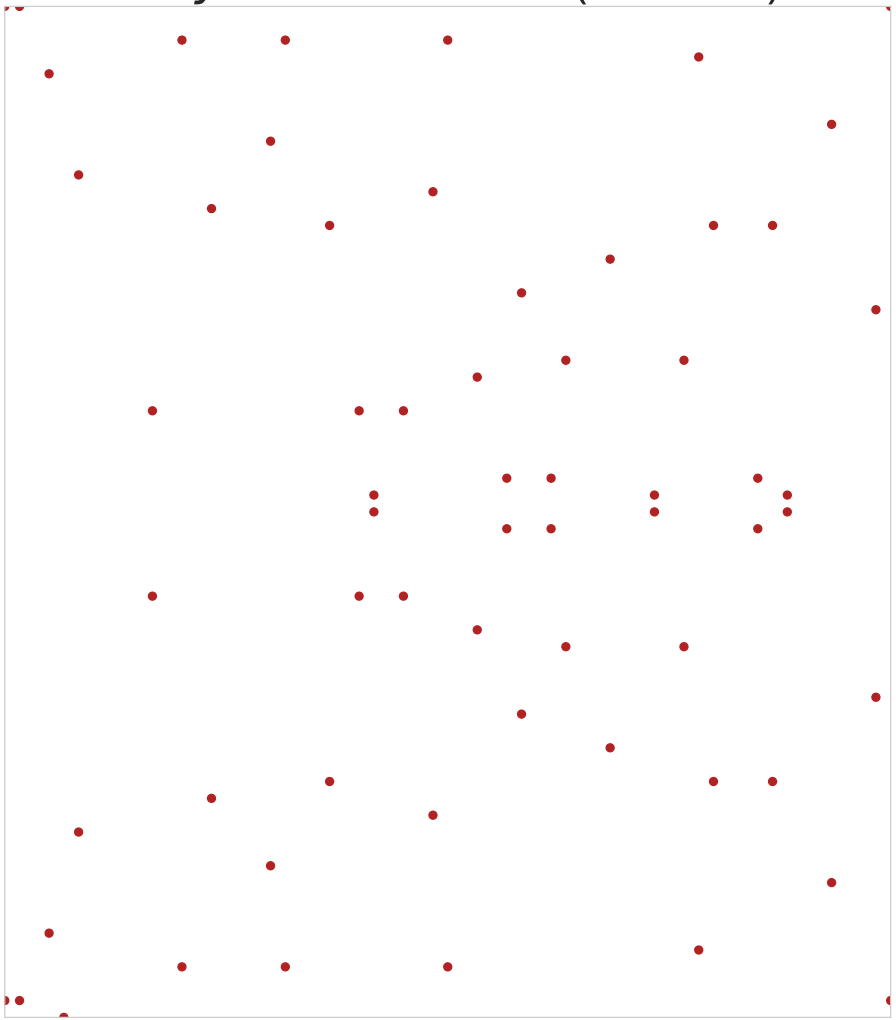
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{61}$$



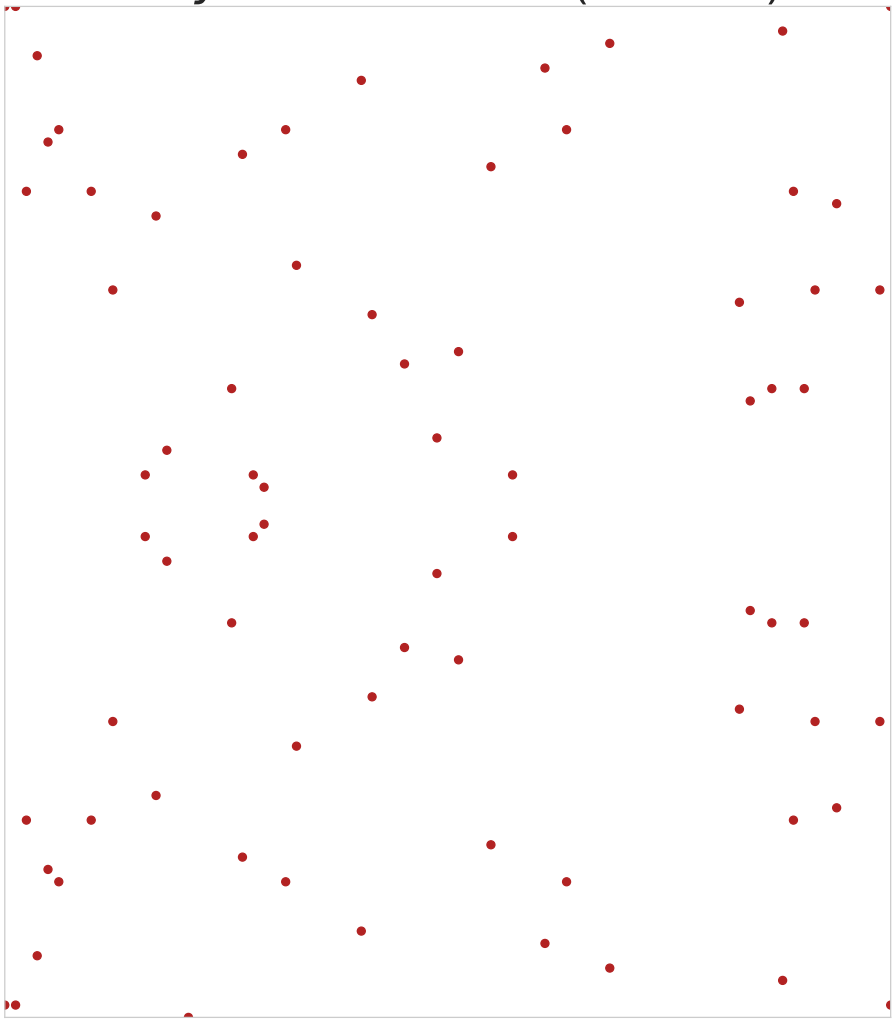
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{83}$$



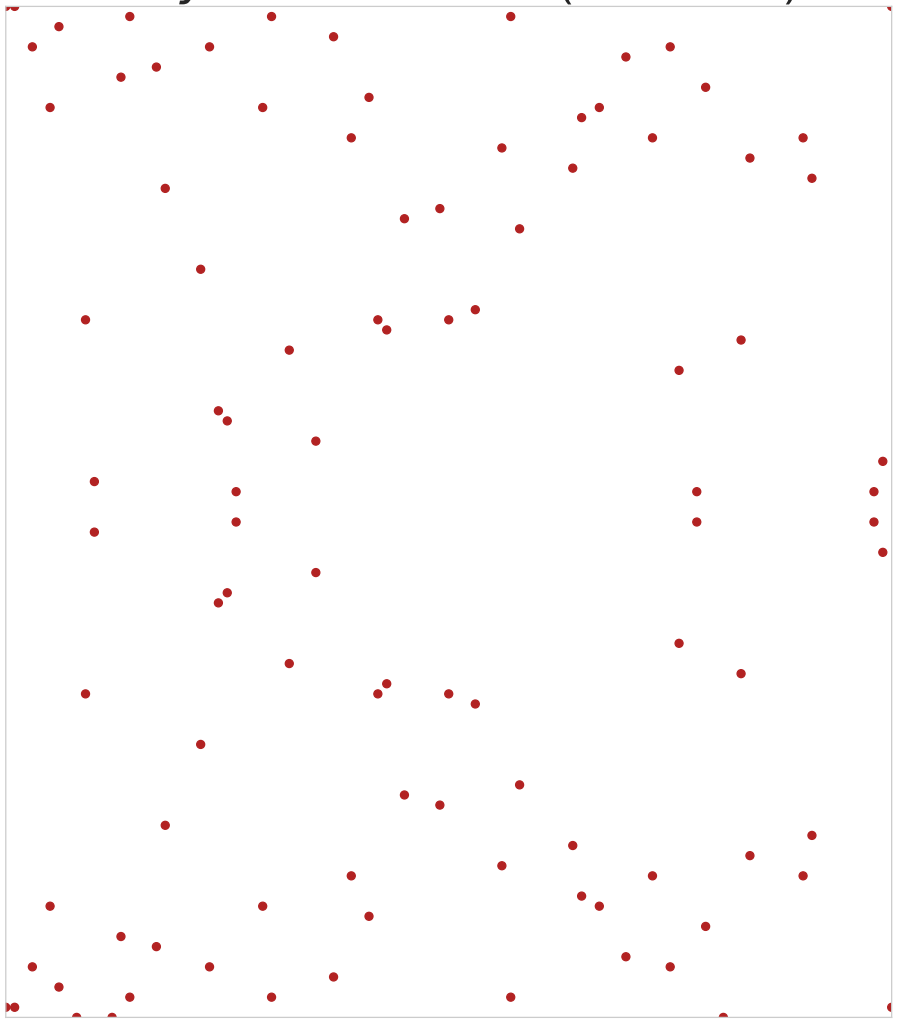
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{101}$$



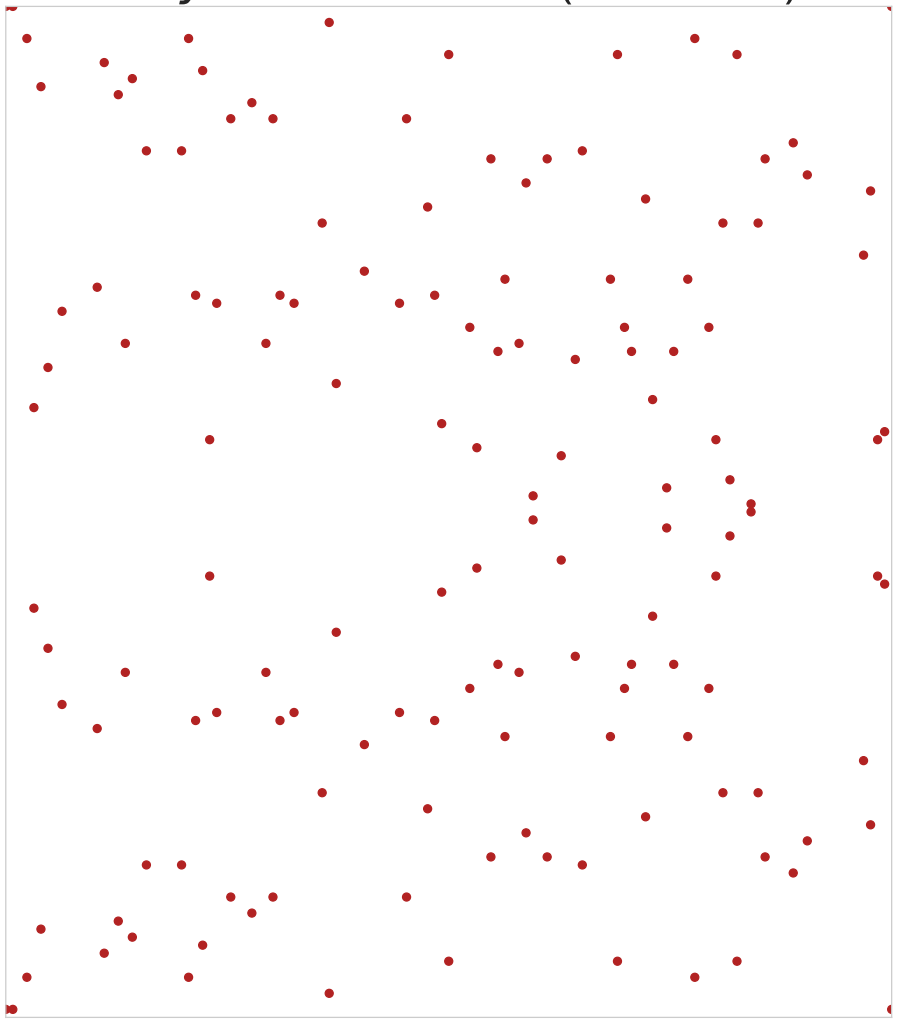
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{127}$$



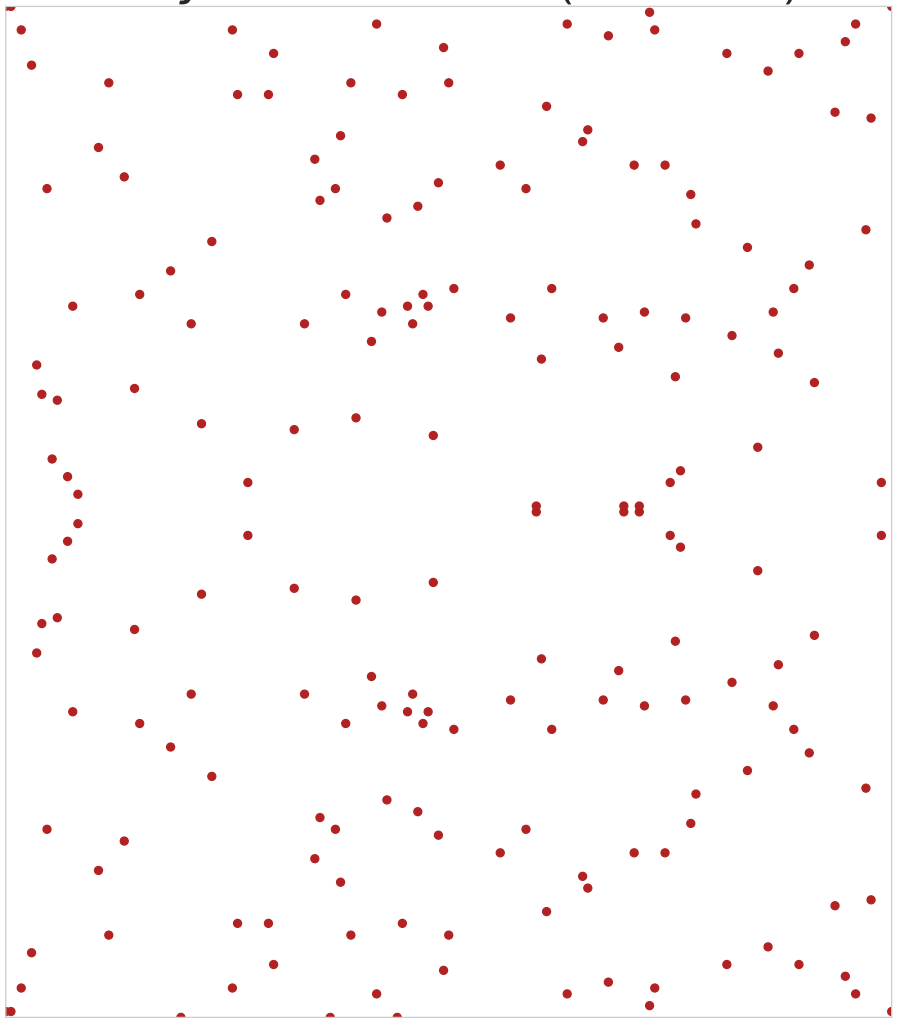
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{173}$$



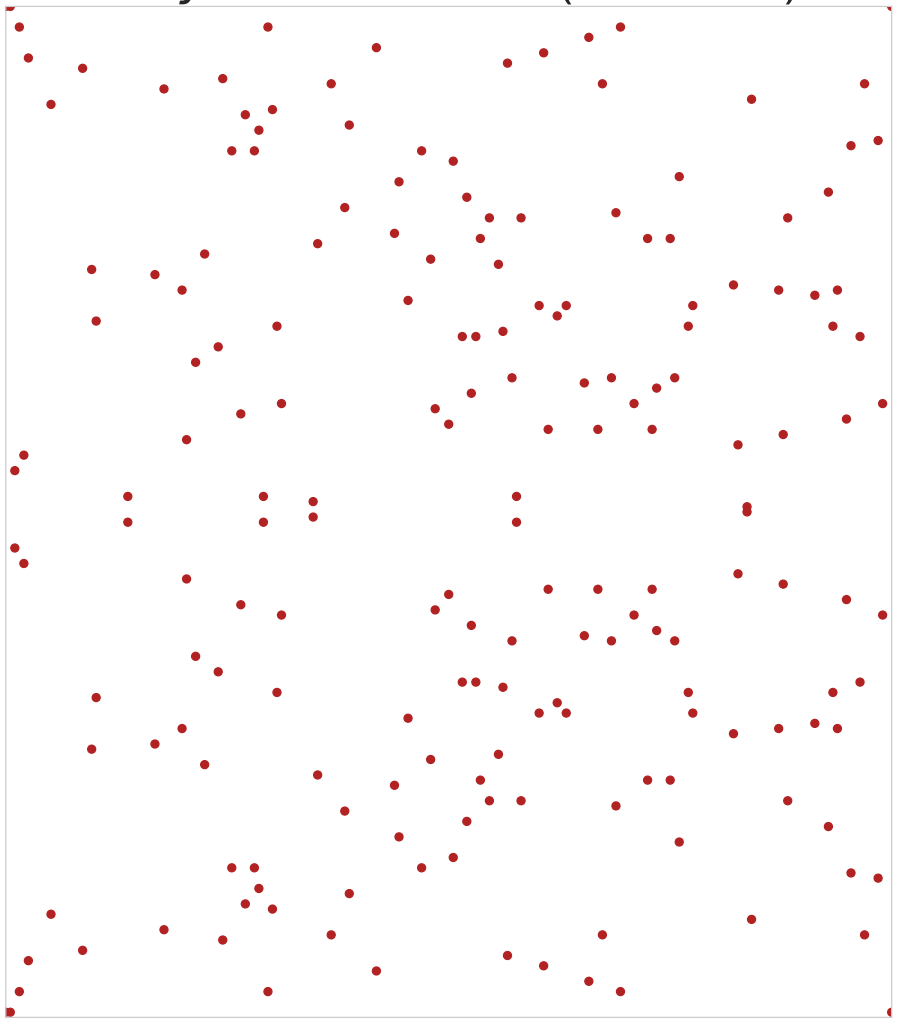
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$E : y^2 \equiv x^3 - x + 1 \pmod{197}$



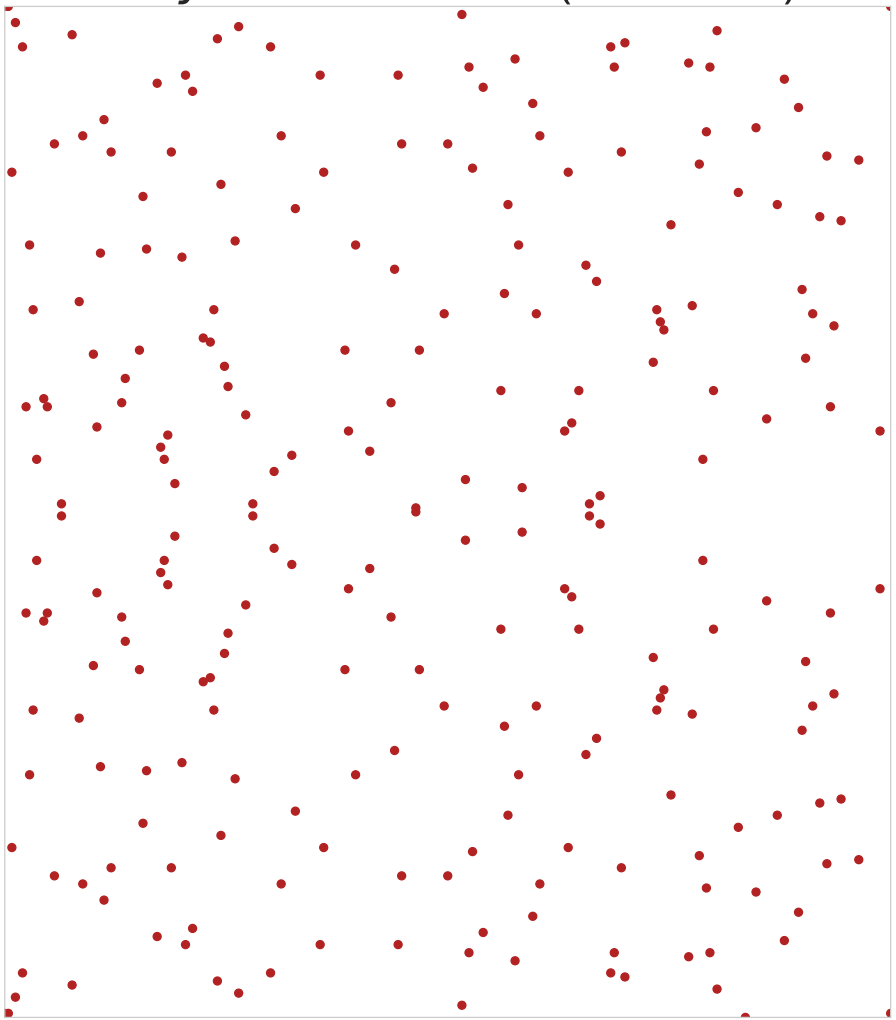
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{251}$$



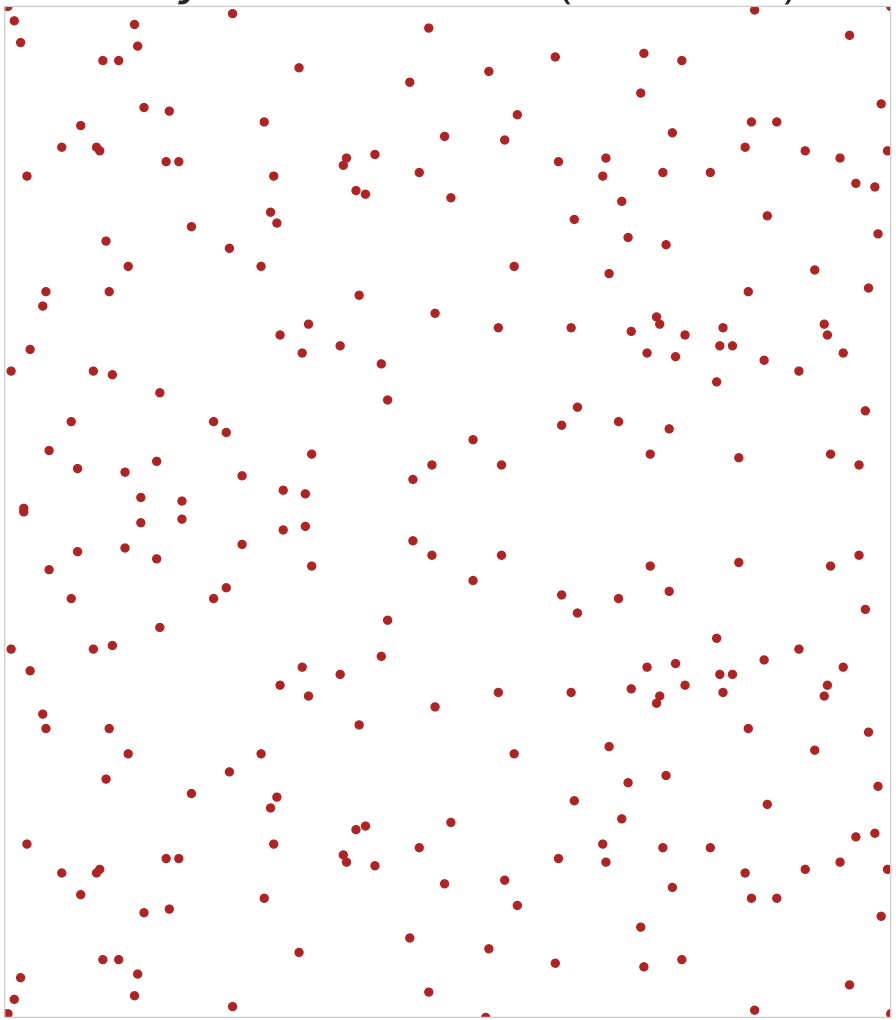
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{281}$$



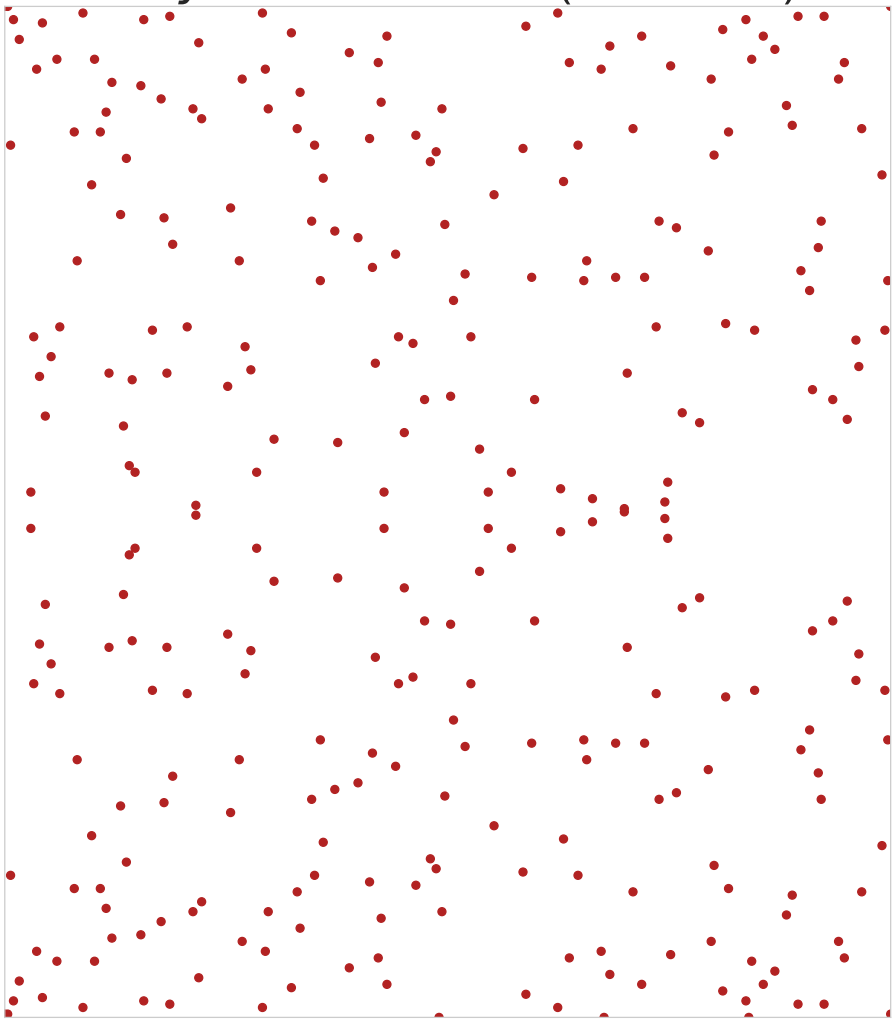
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{307}$$



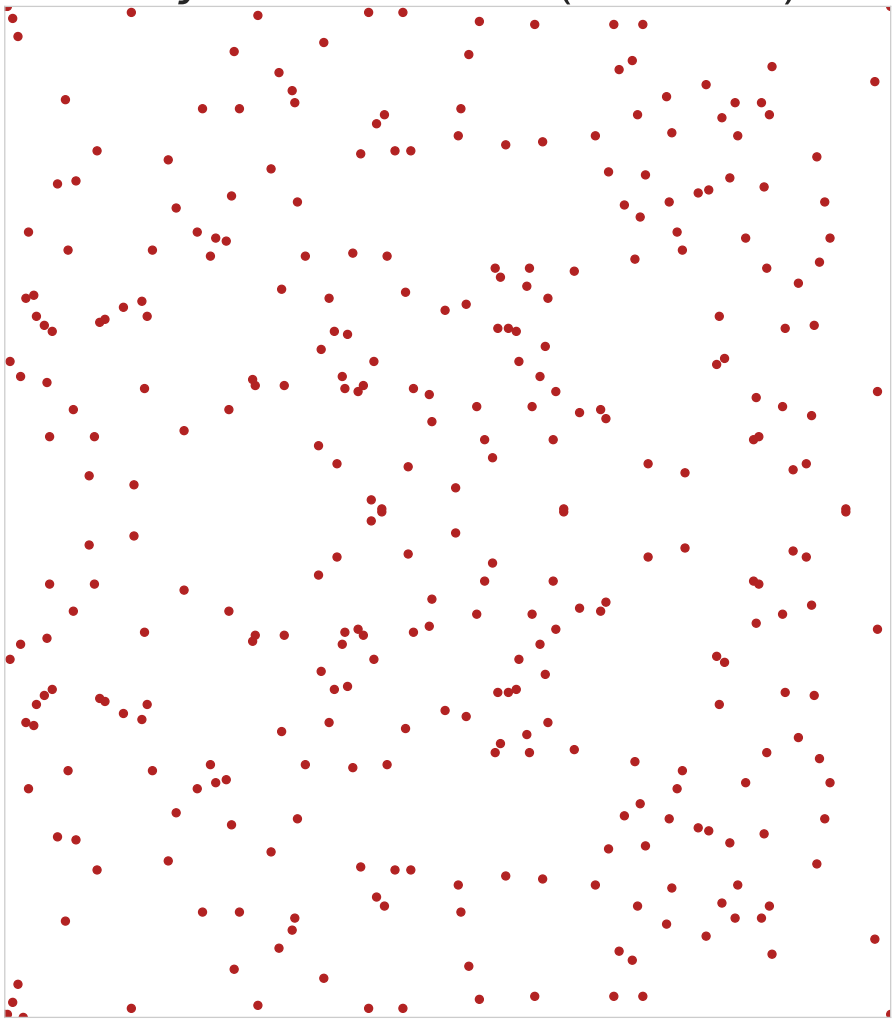
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{337}$$



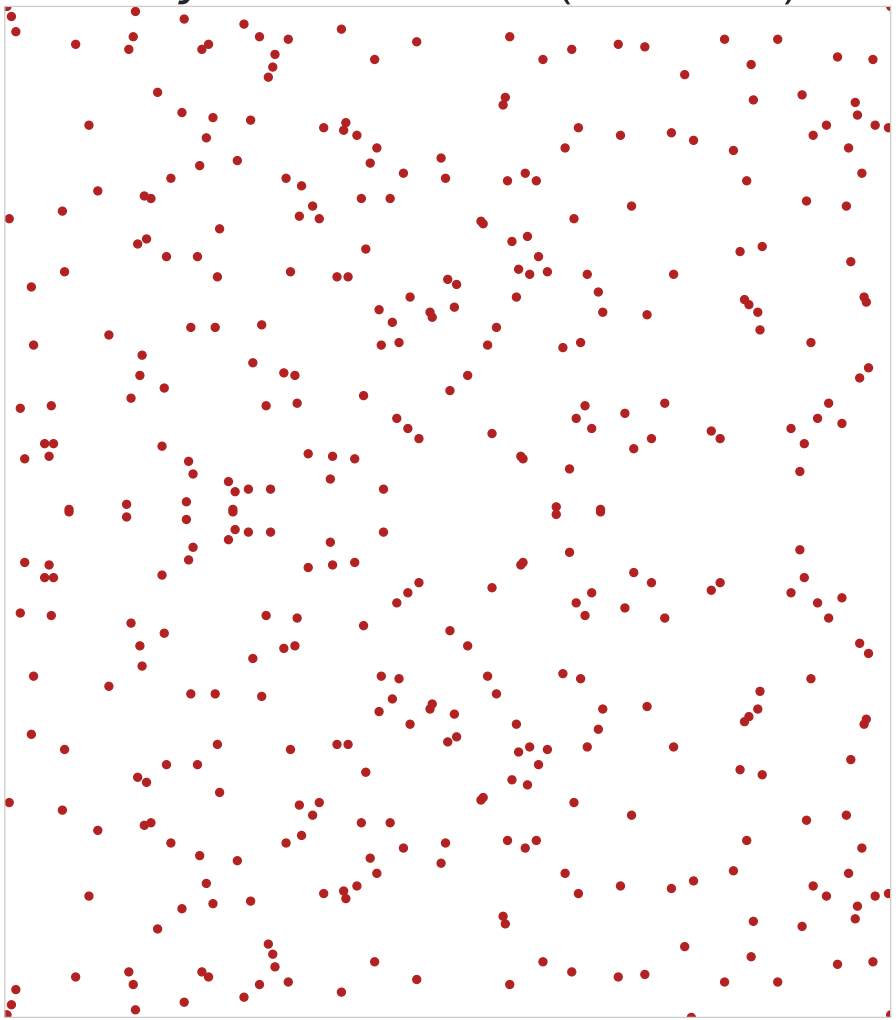
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$E : y^2 \equiv x^3 - x + 1 \pmod{401}$



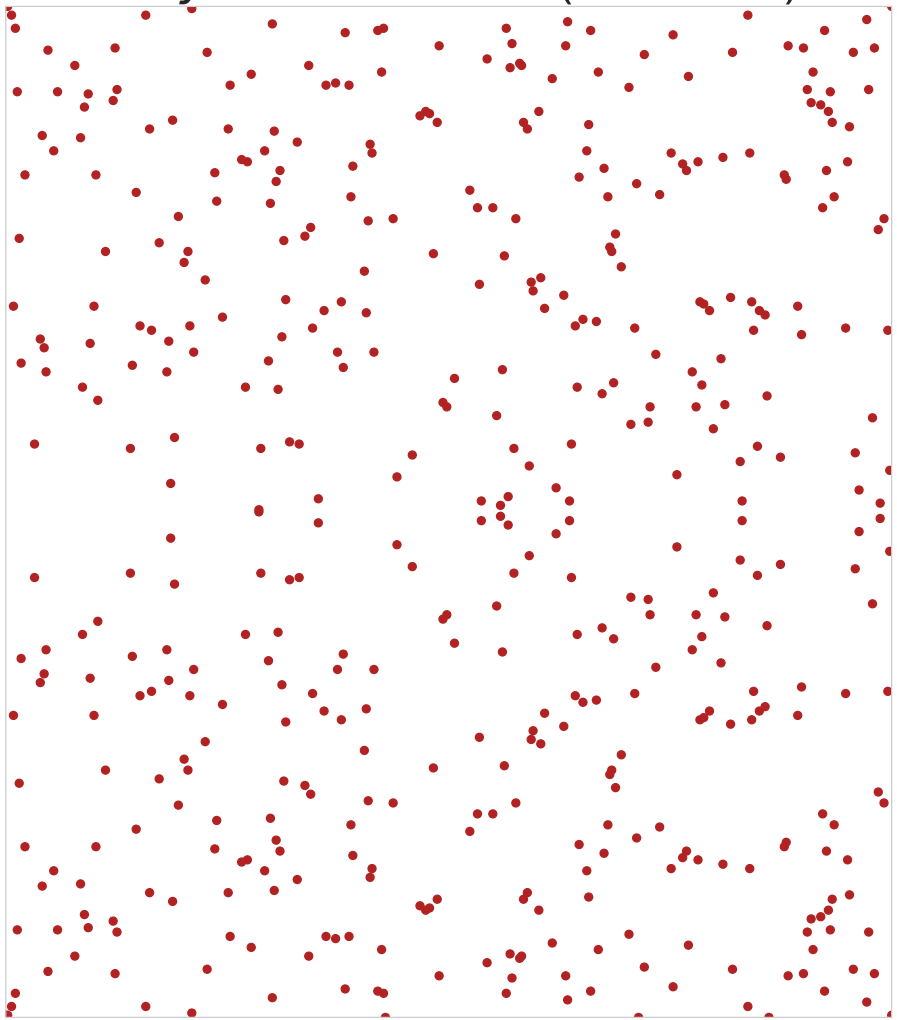
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$



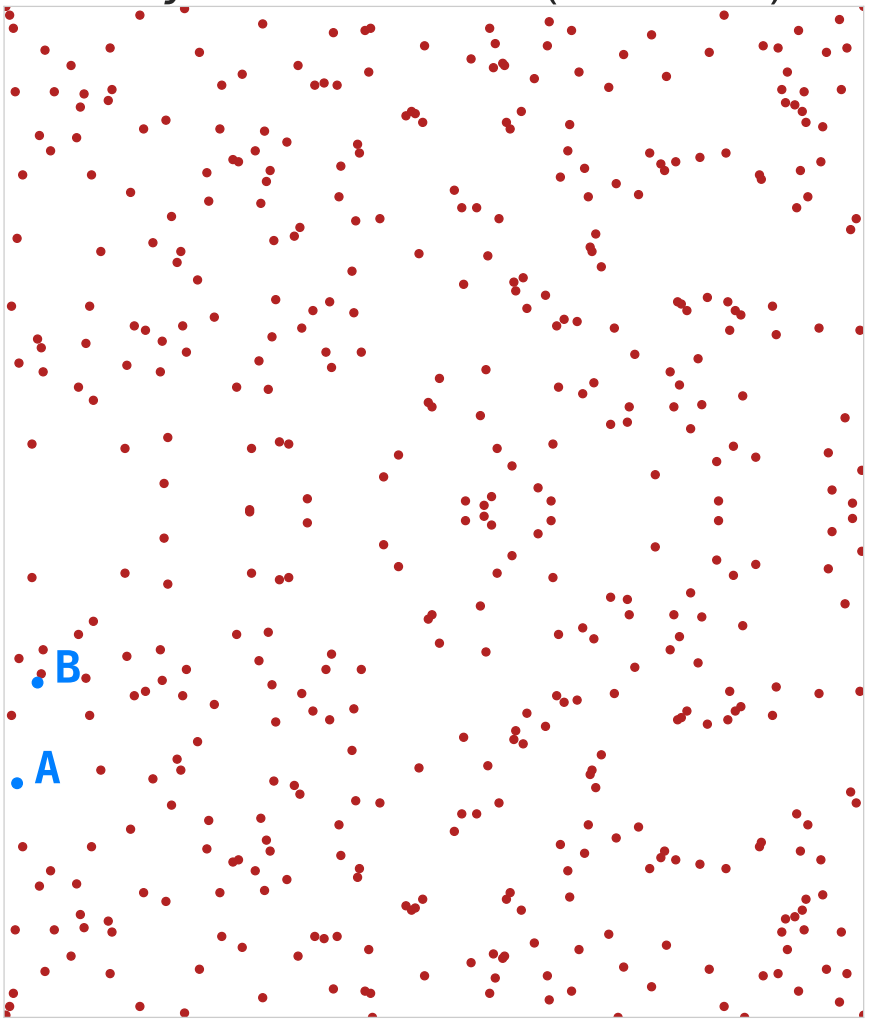
Moving on from looking at these over $\mathbb{Q}$ and $\mathbb{R}$, let's look at them modulo primes.

These curves look quite a bit different.

For small values of p it looks a little boring, but as p increases we get more happening.

Elliptic Curves mod p

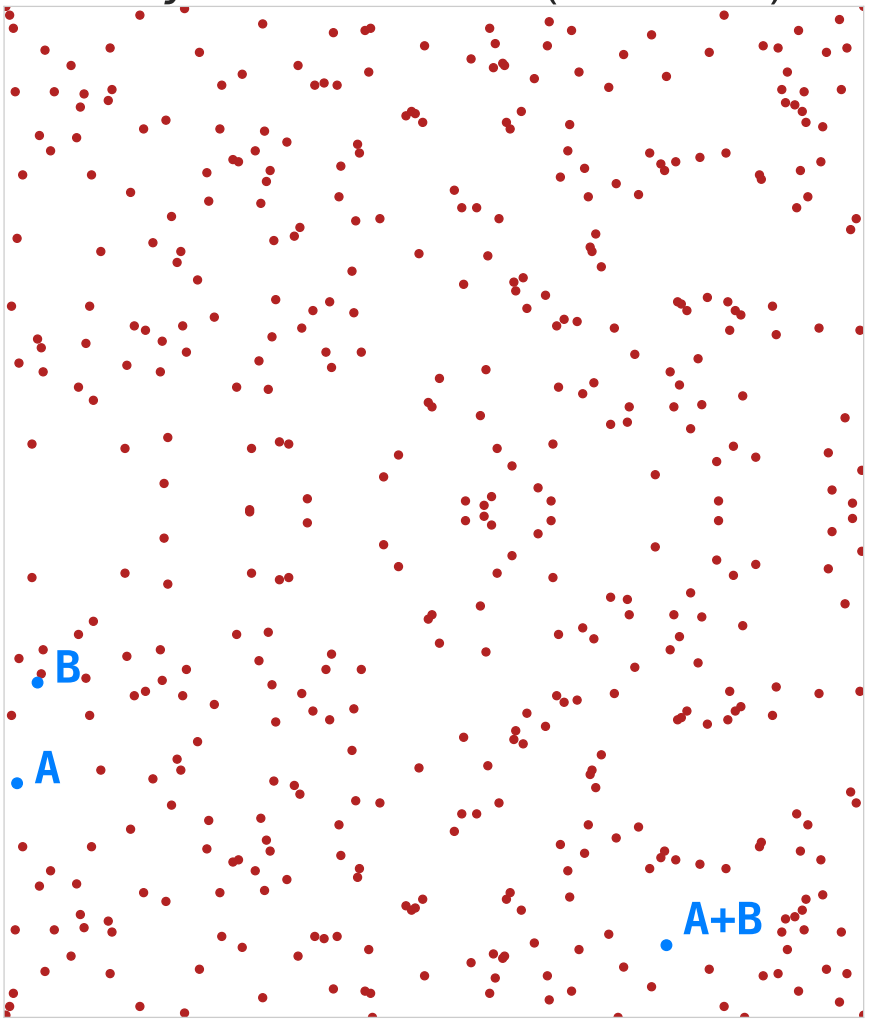
$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$



We can also do point addition, but it looks quite different.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$

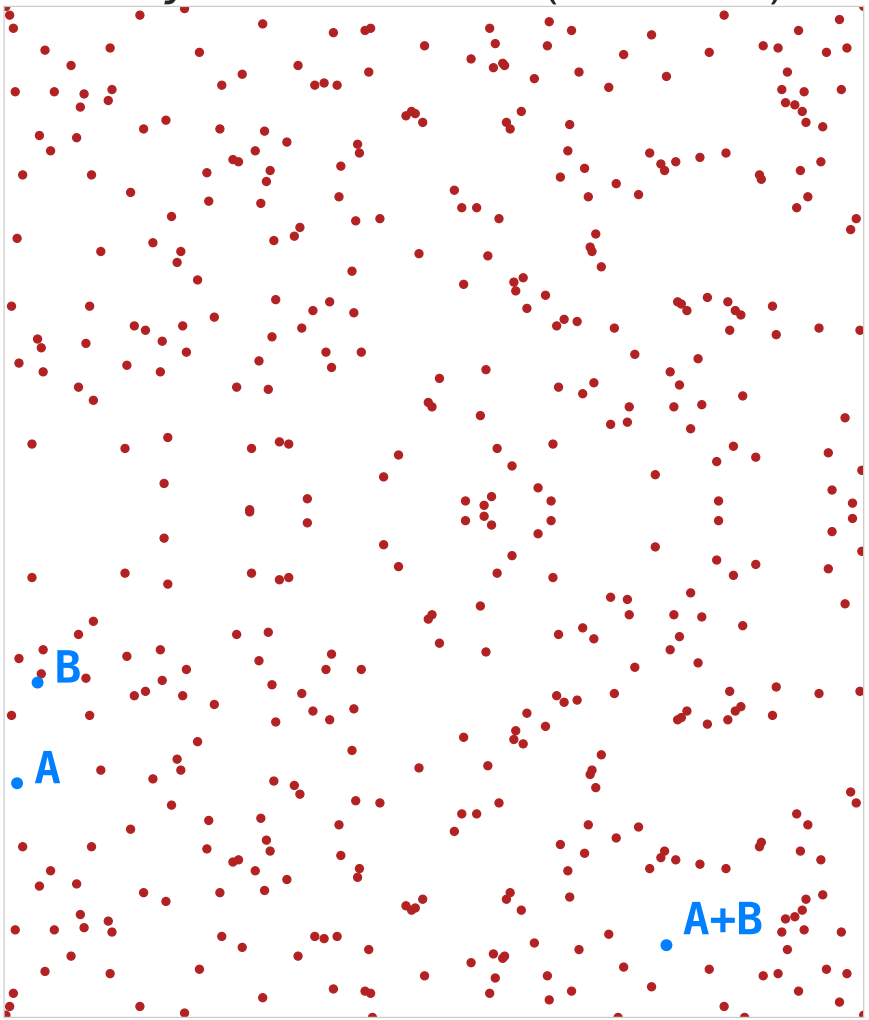


We can also do point addition, but it looks quite different.

There are no longer the same pretty pictures with lines and intersections, but the same formulas apply.

Cryptography

$E : y^2 \equiv x^3 - x + 1 \pmod{463}$



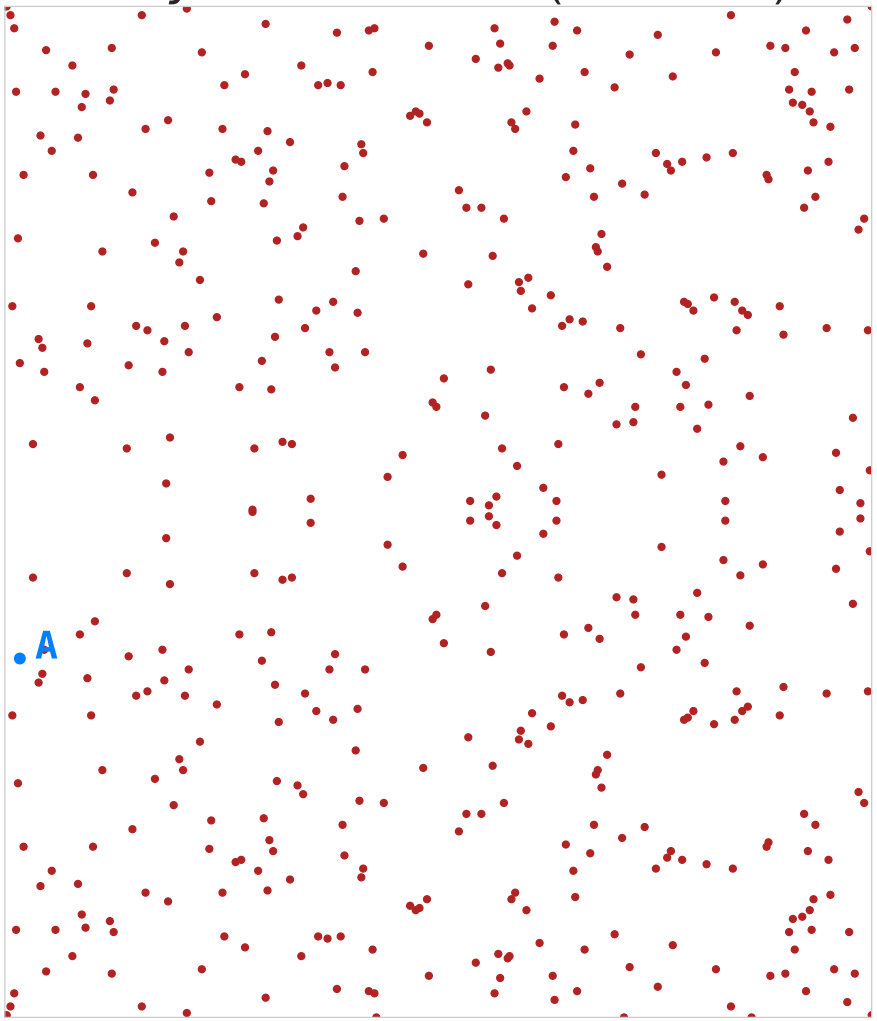
Another brief aside: how does this show up in cryptography?

Public-key systems are generally based on "one-way functions": functions that are easy to compute, but very hard to reverse without specific knowledge (a private key).

Maybe point addition on a curve could be like a one way function!

Cryptography

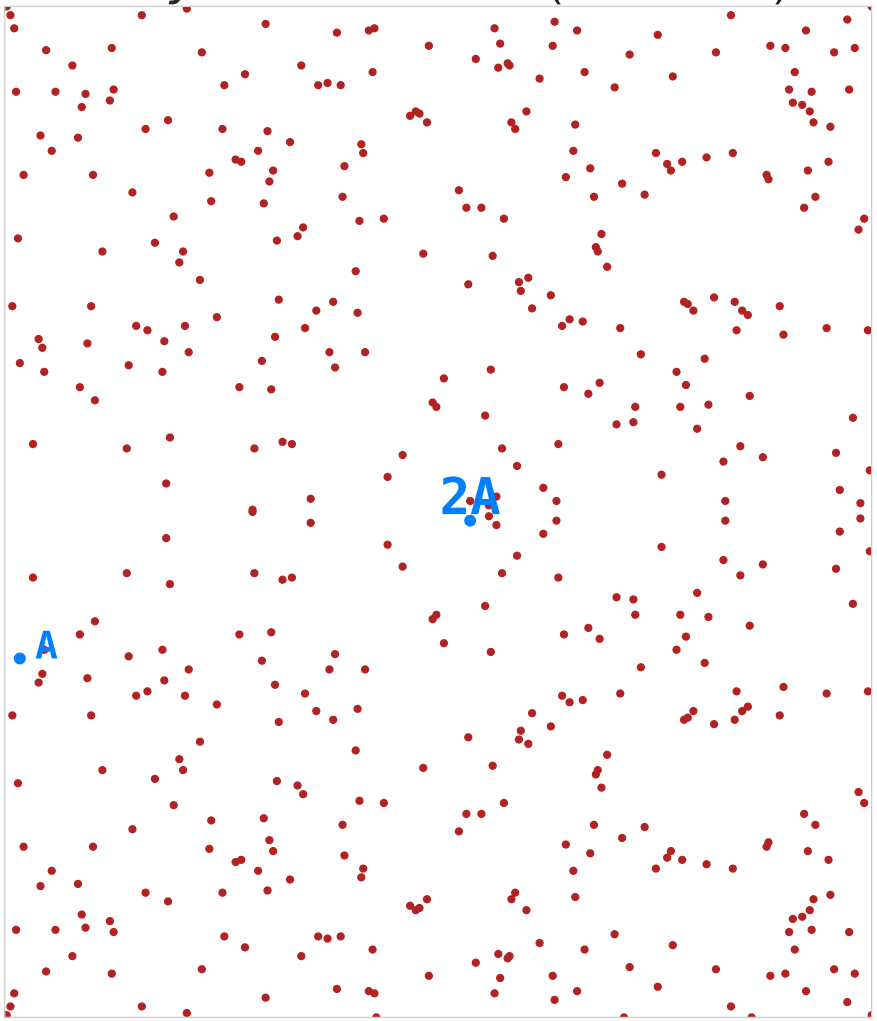
$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$



Suppose I have some point A on the curve, and I start computing multiples of it.

Cryptography

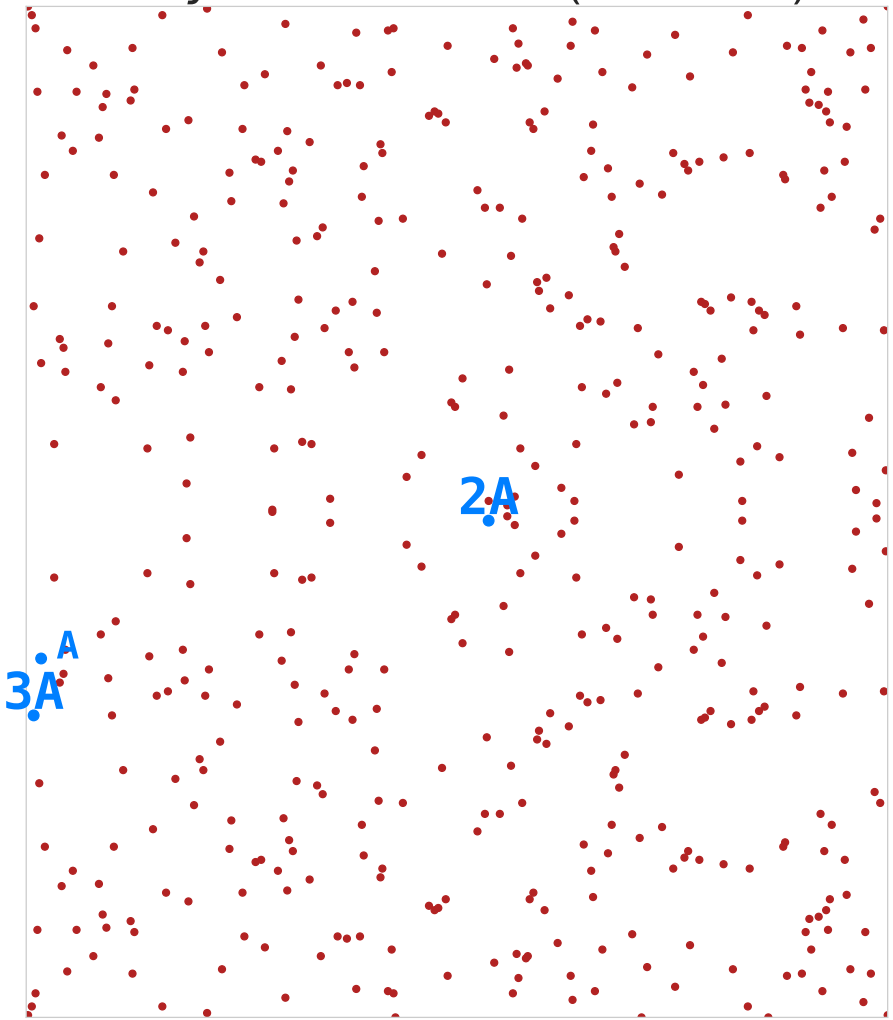
$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$



Suppose I have some point A on the curve, and I start computing multiples of it.

Cryptography

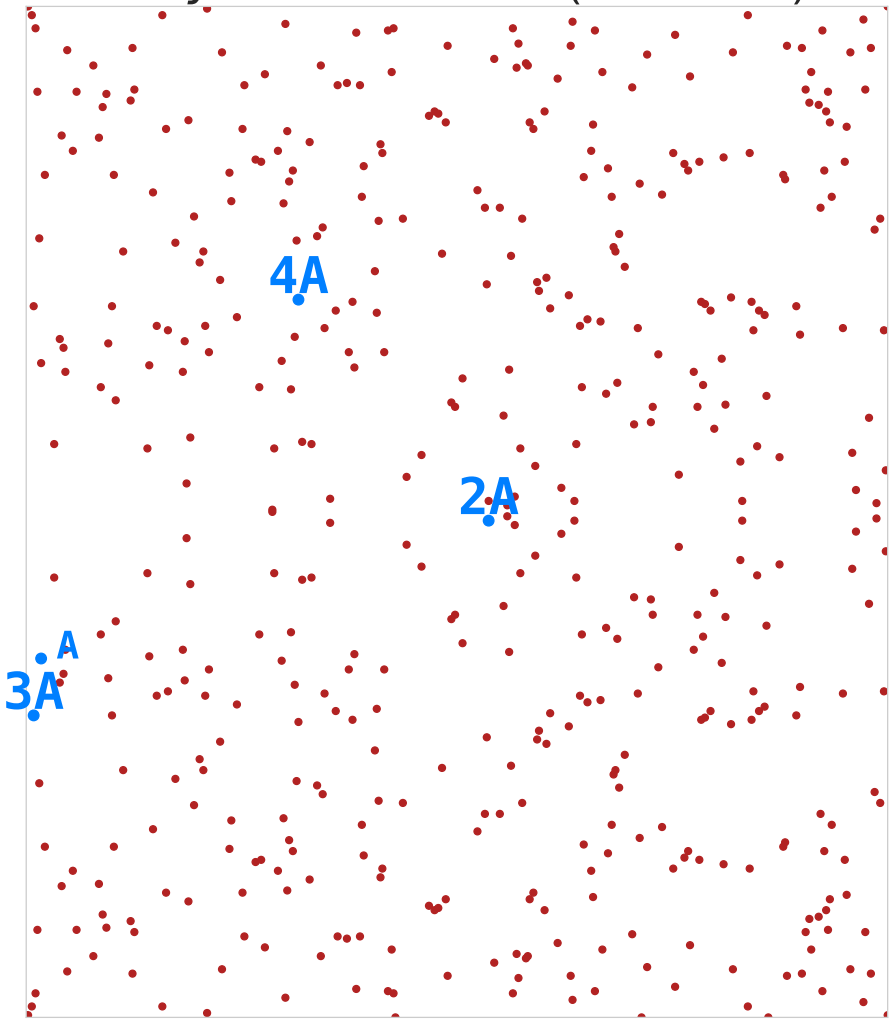
$E : y^2 \equiv x^3 - x + 1 \pmod{463}$



Suppose I have some point A on the curve, and I start computing multiples of it.

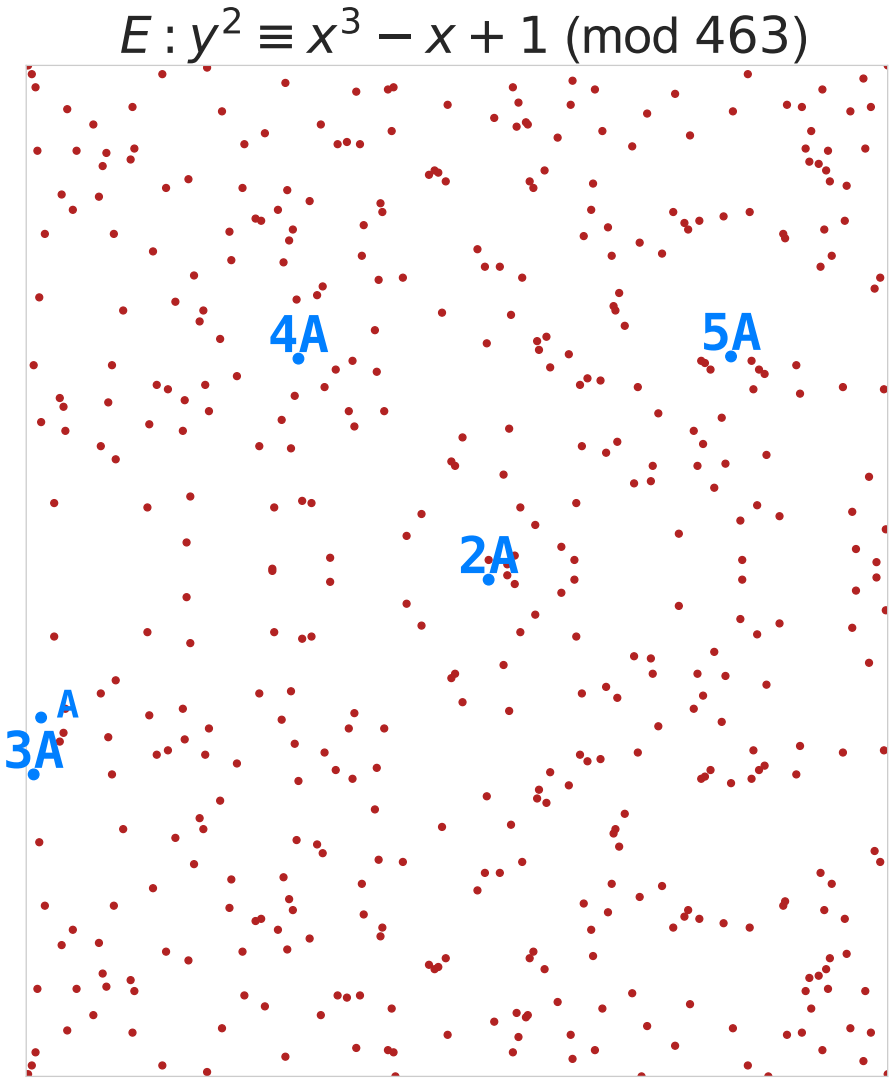
Cryptography

$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$



Suppose I have some point A on the curve, and I start computing multiples of it.

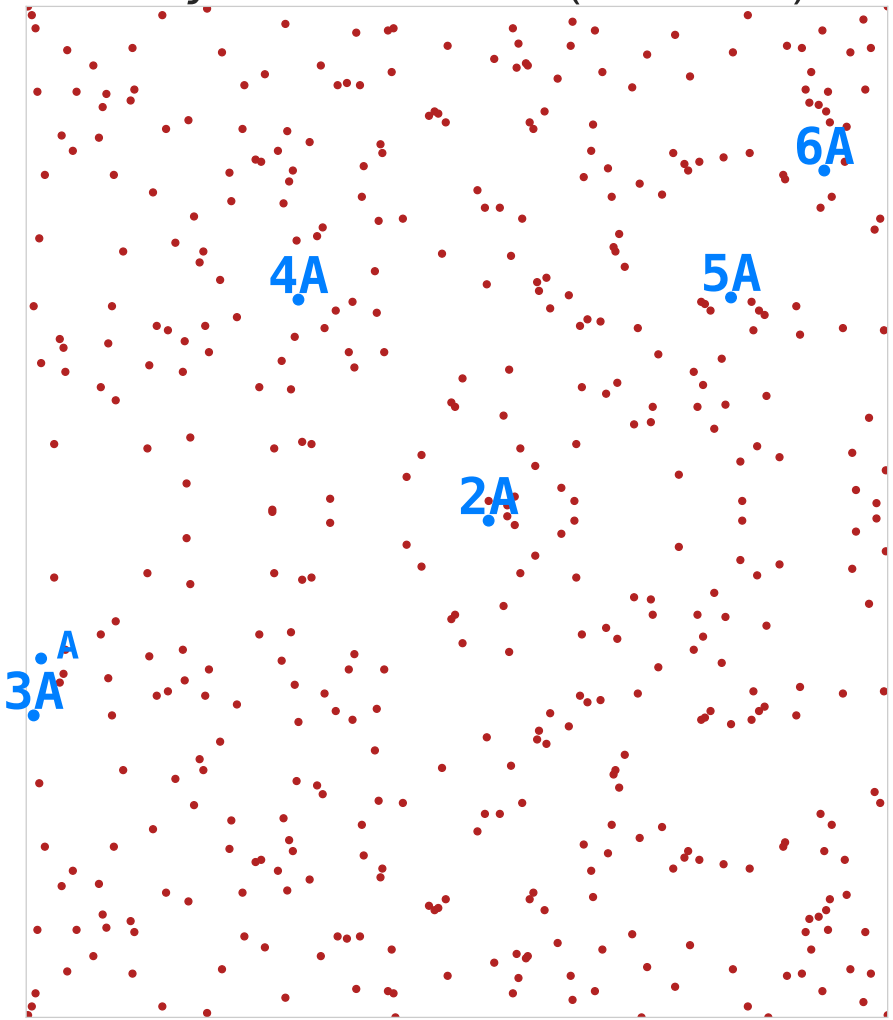
Cryptography



Suppose I have some point A on the curve, and I start computing multiples of it.

Cryptography

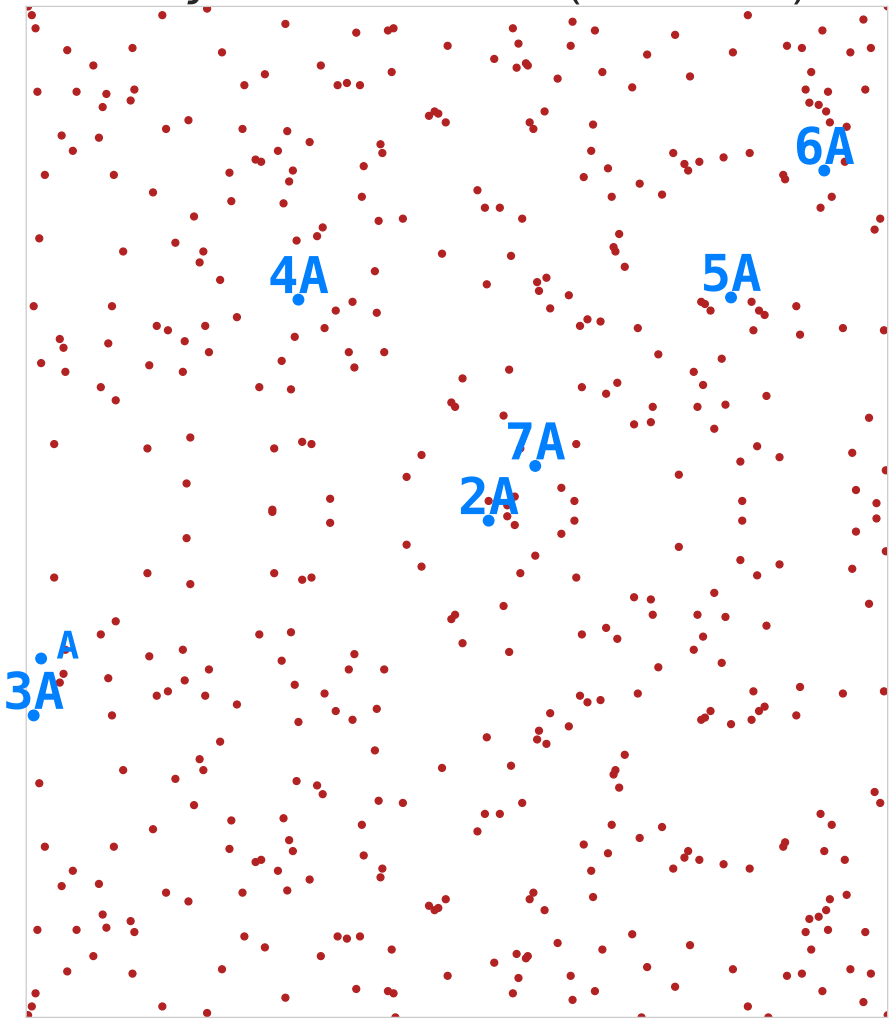
$E : y^2 \equiv x^3 - x + 1 \pmod{463}$



Suppose I have some point A on the curve, and I start computing multiples of it.

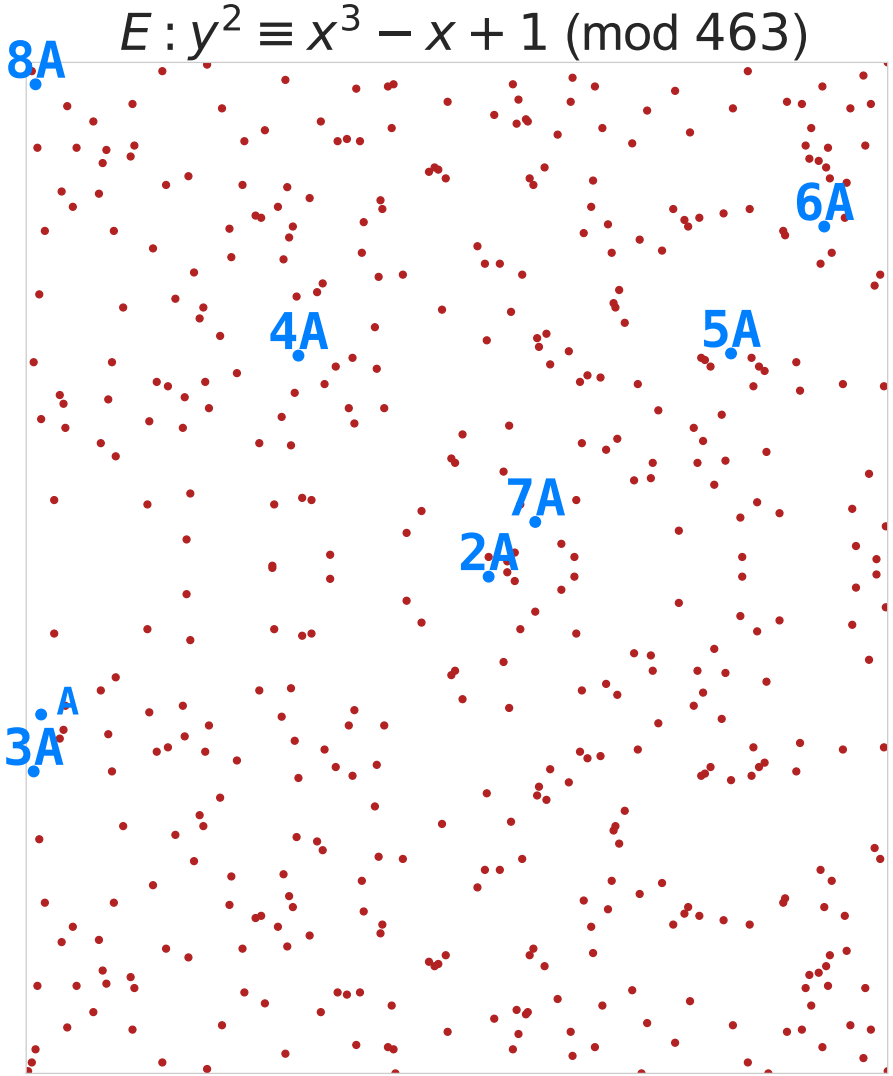
Cryptography

$E : y^2 \equiv x^3 - x + 1 \pmod{463}$



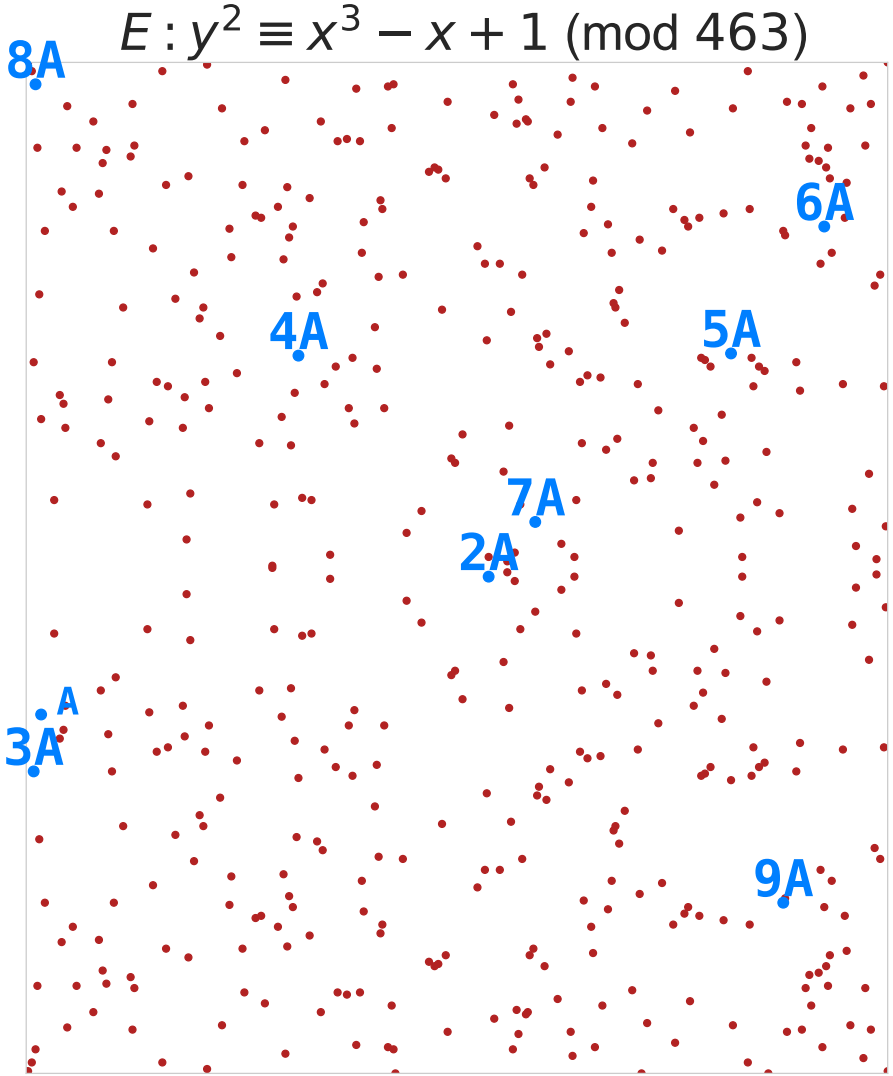
Suppose I have some point A on the curve, and I start computing multiples of it.

Cryptography



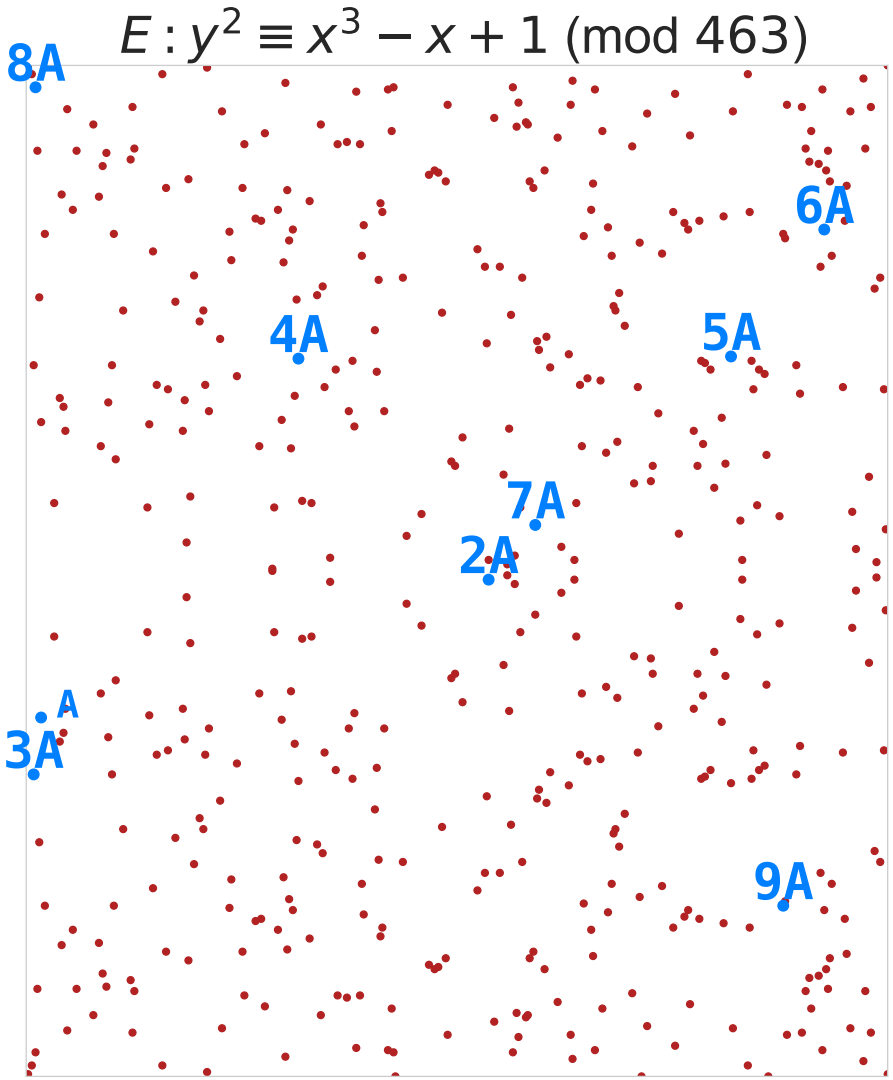
Suppose I have some point A on the curve, and I start computing multiples of it.

Cryptography



Suppose I have some point A on the curve, and I start computing multiples of it.

Cryptography

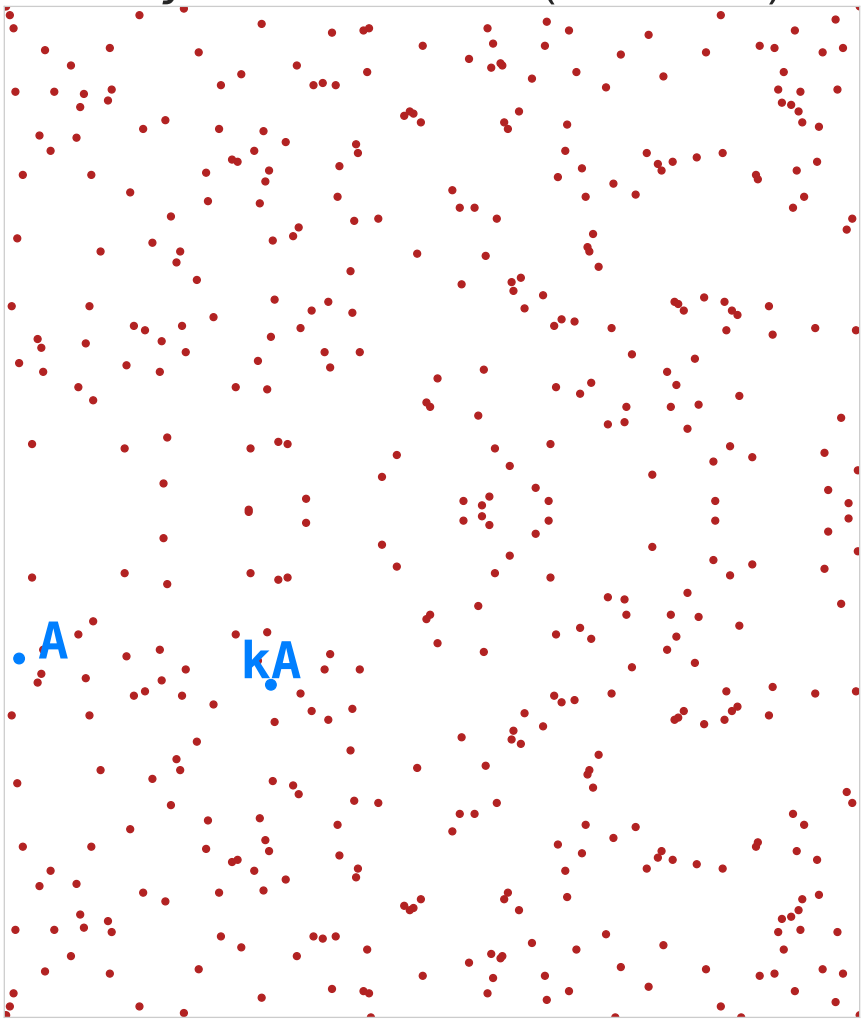


Suppose I have some point A on the curve, and I start computing multiples of it.

This is computationally easy!

Cryptography

$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$



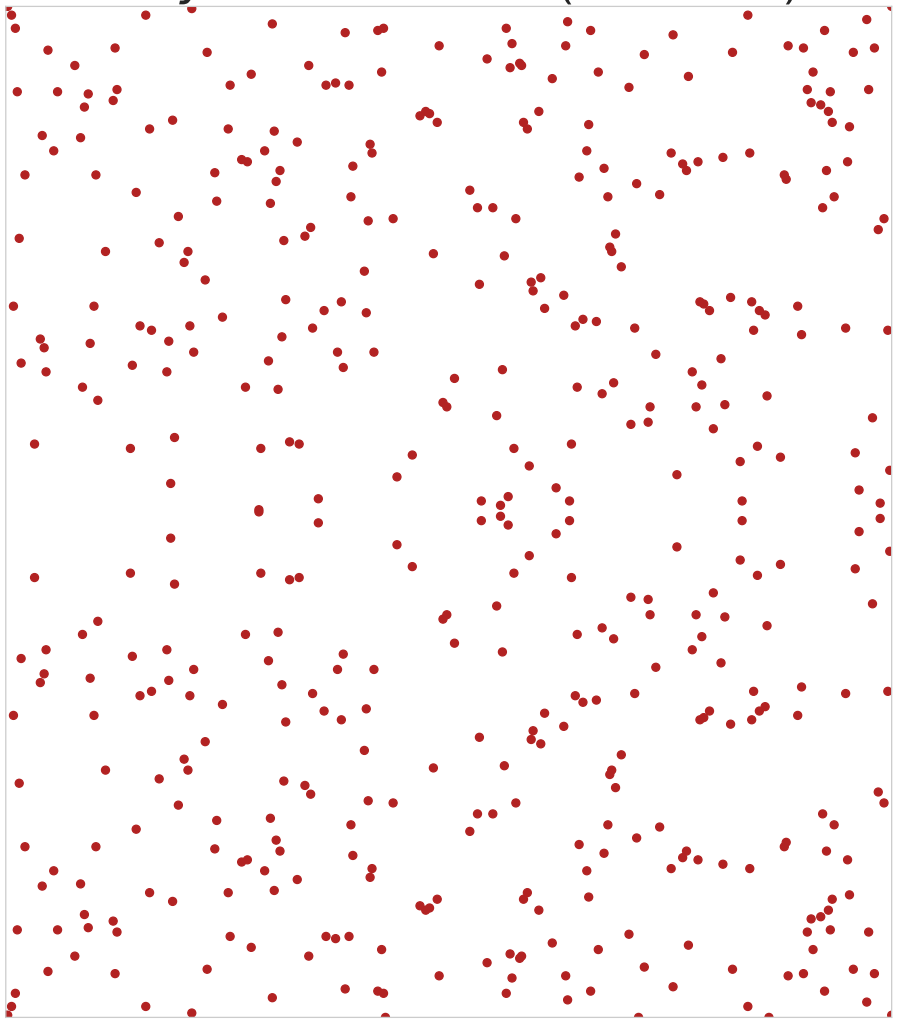
But what if I give you these two points. Can you find k?

If k is really big, this is VERY hard.

The fact that this is hard allows one to build a public-key system.

Elliptic Curves mod p

$$E : y^2 \equiv x^3 - x + 1 \pmod{463}$$



Back to looking at this curve, how many points are there?

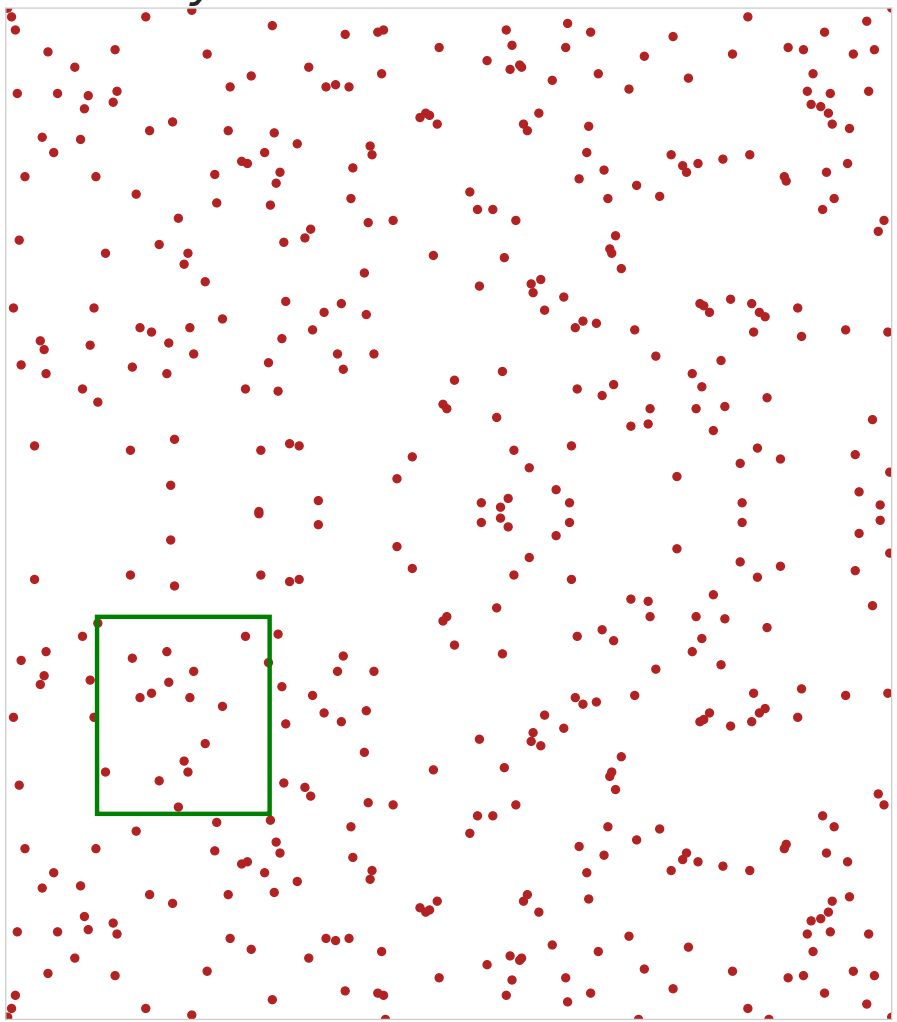
Remember that we also add an extra point "at infinity".

Hasse (1933):

$$\left|\#E(\mathbb{F}_p) - (p+1)\right| \leq 2p^{1/2}.$$

Elliptic Curves mod p

$E : y^2 \equiv x^3 - x + 1 \bmod 463$



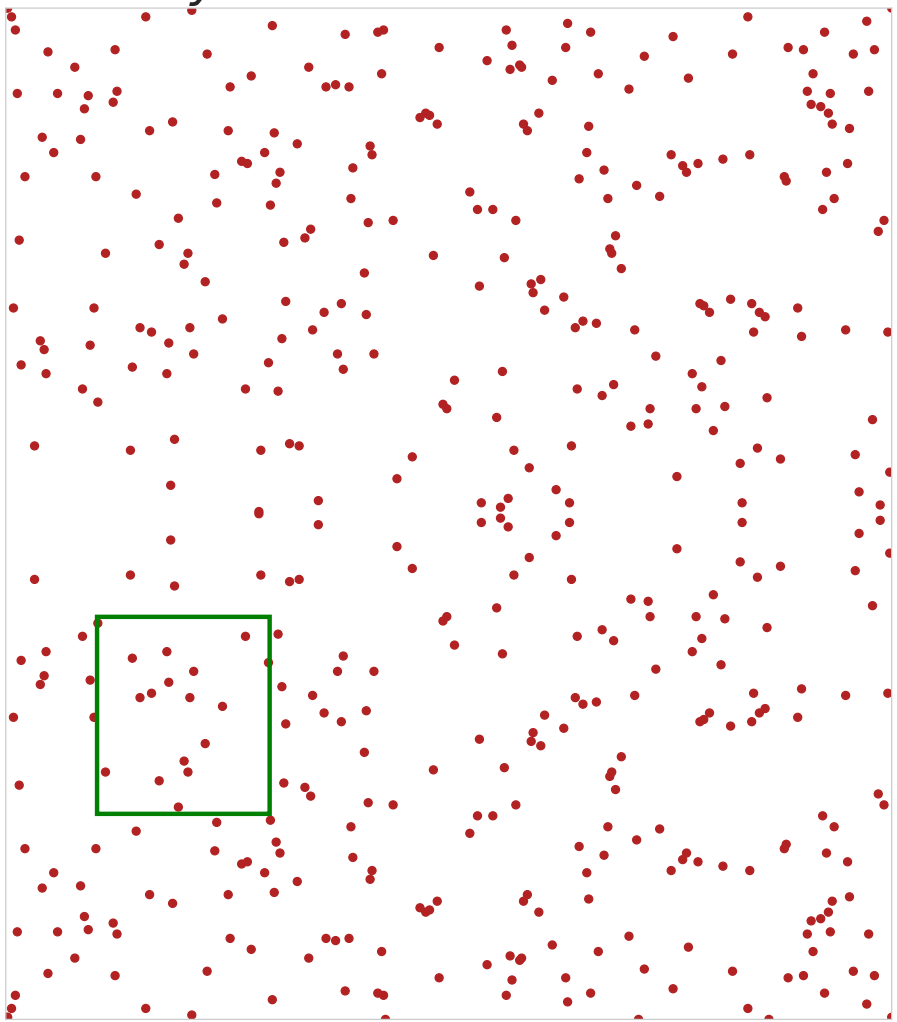
How many points are there in a small box? Can we give an upperbound? We only consider square boxes.

This is fundamentally a different problem, because you lose the group structure when you restrict to a box.

If B is a box let $|B|$ denote its area and $\#E(\mathbb{F}_p, B)$ the number of points on E that lie in B.

Elliptic Curves mod p

$E : y^2 \equiv x^3 - x + 1 \bmod 463$



You can construct examples to show that you cant get an upper bound better than $|B|^{1/6}$.

Kerr and Mohammadi (2021): if $|B| < p^{2/7}$ then $\#E(\mathbb{F}_p, B) \leq |B|^{1/6+o(1)}$.

Generalizing to arbitrary finite fields

Can we generalize this to arbitrary finite fields?

If it has been a minute since you have seen finite fields, don't worry.

A finite field $\mathbb{F}_{p^n}$ has p^n elements in it (a prime power) and is a set with a reasonable notion of addition, subtraction, multiplication and division.

Generalizing to arbitrary finite fields

First, how many points are on an elliptic curve over a finite field $\mathbb{F}_{p^n}$?

That just means the number of solutions to an equation like

$$y^2 = x^3 + Ax + B$$

where $x, y \in \mathbb{F}_{p^n}$.

Theorem (Hasse (1933))

$$|\#E(\mathbb{F}_{p^n}) - (p^n + 1)| \leq 2p^{n/2}.$$

Points in a box?

Counting points in a box? How can we think of a box in a finite field? We no longer have the same geometric intuition...

For those interested: for some $f_0, g_0, F \in \mathbb{F}_p[x]$ with F irreducible of degree n, take $\mathbb{F}_p[x]/\langle F \rangle$ as your finite field $\mathbb{F}_{p^n}$. Then a box is a set like

$$B = \{(f_0, g_0) + (f, g) : \deg f, \deg g < m\}.$$

But for our purposes, just think of a box being elements that are "close together". We will let $|B|$ denote the size of the box and $\#E(\mathbb{F}_{p^n}, B)$ the number of points on the elliptic curve E in the box B.

Points in a box?

Similar to before, in general you can't expect an upper bound for $\#E(\mathbb{F}_{p^n}, B)$ better than $|B|^{1/6}$.

Theorem (Bagshaw and Kerr)

Fix a prime $p > 3$. Let E be an elliptic curve over $\mathbb{F}_{p^n}$ and B a box. If $|B| < p^{2n/7}$ then

$$\#E(\mathbb{F}_{p^n}, B) \leq |B|^{1/6+o(1)}.$$

Going forward?

The requirement that $|B| < p^{2n/7}$ means that the box is very small relative to the whole finite field. Can we relax this condition to allow for larger boxes?

Can we extend these results to other curves?

Thank you!