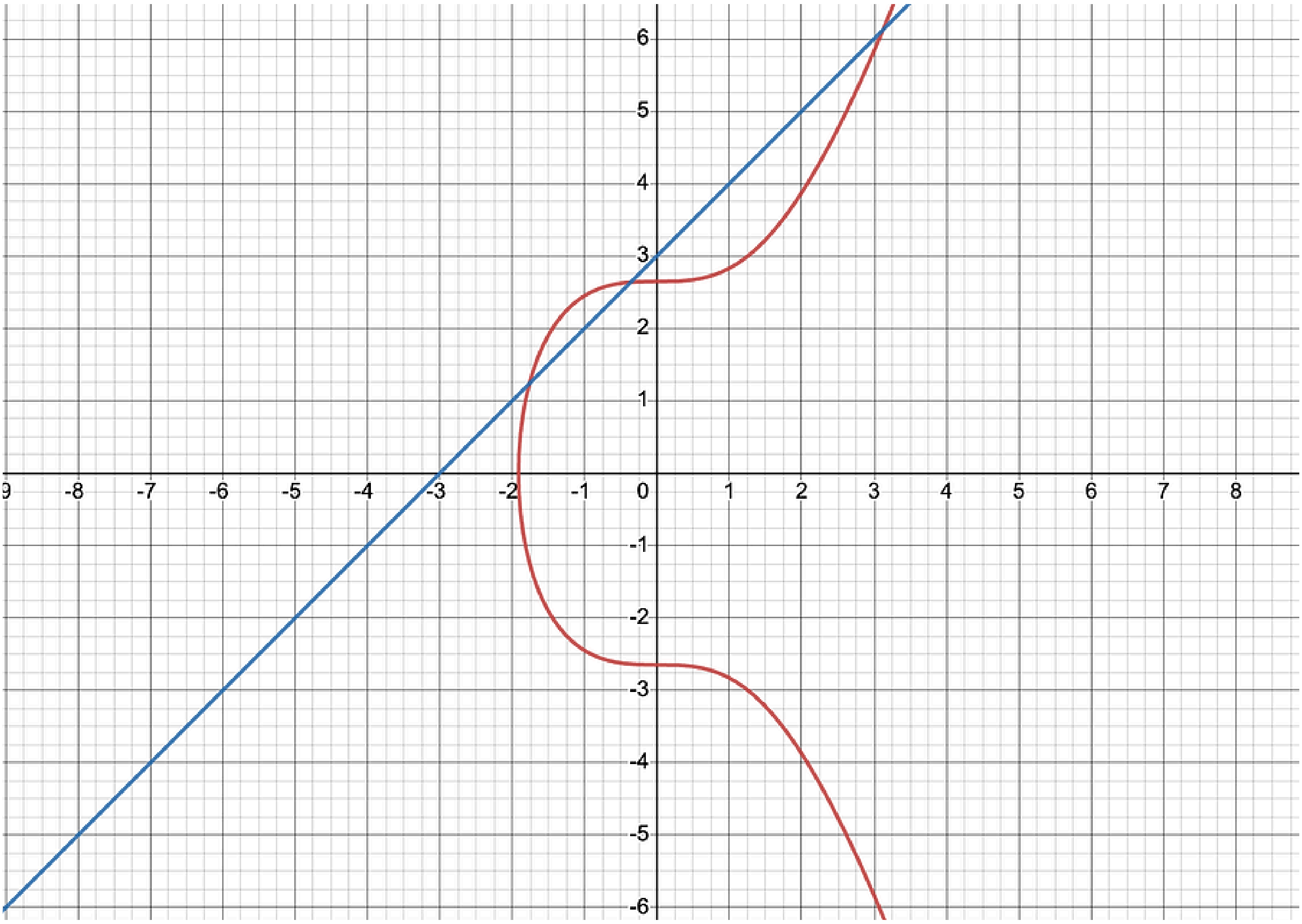
Jul 22, 2023 3 min read

Why elliptic curve point addition in prime finite fields always lands on integers



One thing that seems incredibly remarkable about elliptic curve addition (in the context of cryptography), is that when a line is drawn between two points, where the x and y values are integers, the output will have integer value.

Under purely random chance, this seems like it should be impossible: connect two points in a euclidean space and pick another integer x for the intersection point, the chances are overwhelming that the corresponding y value will not be an integer.
So how does this work?

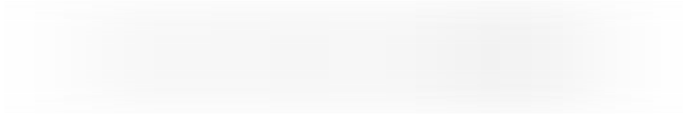
Elliptic Curve Point Addition

In summary: if we do elliptic curve addition in a *prime integer finite field* (that is important!), then all the binary operators used to calculate the third point will be the addition and multiplication in that prime field. Both those operators are closed by definition, therefore the result of the operation is in the prime finite field, i.e. an integer.

The formula for point addition

Using Wikipedia's notation for elliptic curve point addition (and explicitly adding the mod p), we have

in the curve



Elliptic curve addition is

Although it looks like we are doing subtraction and division, remember, subtraction is just addition with an element's inverse, and division is multiplication with the denominator's inverse. In a field, all elements have an inverse (except the identity under multiplication, i.e. dividing by zero), so we aren't using any binary operators that will take us out of integer land when computing lambda.

When computing x_r, λ^2 is really just shorthand field multiplication of two elements. The rest of the operators should obviously be members of the field, and hence the entire operation is closed.

There is no spooky moon math here that causes a line drawn between two points on $y^2 = x^3 + ax + b$ (mod p) to land on another integer. We could try to write a proof for that, but that would be nightmare to construct.

If instead we use the axioms of elementary group theory, then the proof is intuitive and obvious.

Exercise for the reader

Demonstrate that point doubling for elliptic curves (adding a point with itself) in a prime finite field is closed under the definition of a group, i.e. the result will be a pair of integers in the prime finite field. Decompose the operation into the group's two binary operators and use inverses where appropriate. The formula again is taken from the same Wikipedia page:

What if we were not doing this in a prime finite field?

If we were not doing this modulo p, then clearly we cannot expect to land on an integer most of the time. This should be obvious. We are working in a field of real numbers, not integers, so the binary operators in a field will generally produce real numbers, not integers. The “moon math magic” is entirely reliant on us doing all the arithmetic modulo p.

What about associativity?

To be a group, the binary operator of addition must be associative, i.e. A + (B + C) = (A + B) + C. It is not immediately obvious this is true when we zip around an elliptic curve in this manner. However, this can verified algebraically (using primary school algebra) if we write out the formula for the addition of three points using different parenthesis ordering, then demonstrate the two equations are equal. We can also demonstrate elliptic curves are an abelian group doing using this method.

Learn more with RareSkills

This material is taken from our Zero Knowledge Proofs Course.