

Elliptic curve cryptography

The idea of Diffie–Hellman (used, for instance, in DH key exchange, ElGamal or DSA) can be carried over to algebraic structures different from multiplication modulo p .

Recall that the key idea is, starting from individual secrets x, y , to share g^x, g^y modulo p in order to arrive at the joint secret $g^{xy} \pmod{p}$. That's using multiplication modulo p .

One important example of other such algebraic structures, for which the analog of the discrete logarithm problem is believed to be difficult, are elliptic curves.

https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

Comment. The main reason (apart from, say, diversification) is that this leads to a significant saving in key size and speed. Whereas, in practice, about 2048bit primes are needed for Diffie–Hellman, comparable security using elliptic curves is believed to only require about 256bits.

For a beautiful introduction by Dan Boneh, check out the presentation:

https://www.youtube.com/watch?v=4M8_0o71piA

Points on elliptic curves

An **elliptic curve** is a (nice) cubic curve that can (typically) be written in the form

$$y^2 = x^3 + ax + b.$$

A point (x, y) is on the elliptic curve if it satisfies this equation. Each elliptic curve also contains the special point O (“the point at ∞ ”). [O will act as the neutral element when “adding points”.]

Advanced comment. Sometimes it is useful (or necessary) to consider elliptic curves defined by more general cubic equations such as $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (however, in most cases, a linear change of variables can transform this equation into the simpler form $y^2 = x^3 + ax + b$ mentioned above).

Example 216. Determine some points (x, y) on the elliptic curve E , described by

$$y^2 = x^3 - x + 9.$$

Solution. We can try some small values for x (say, $x=0, x=1, x=2, \dots$) and see what y needs to be in order to get a point on the elliptic curve. For instance, for $x=1$, we get $x^3 - x + 9 = 9$ which implies that $(1, \pm 3)$ are points on the elliptic curve.

Doing so, we find the integral points $(0, \pm 3), (\pm 1, \pm 3)$.

On the other hand, for $x=2$, we get $x^3 - x + 9 = 15$ which implies that $(2, \pm\sqrt{15})$ are points on the elliptic curve. Depending on the application, we are often not interested in such irrational points.

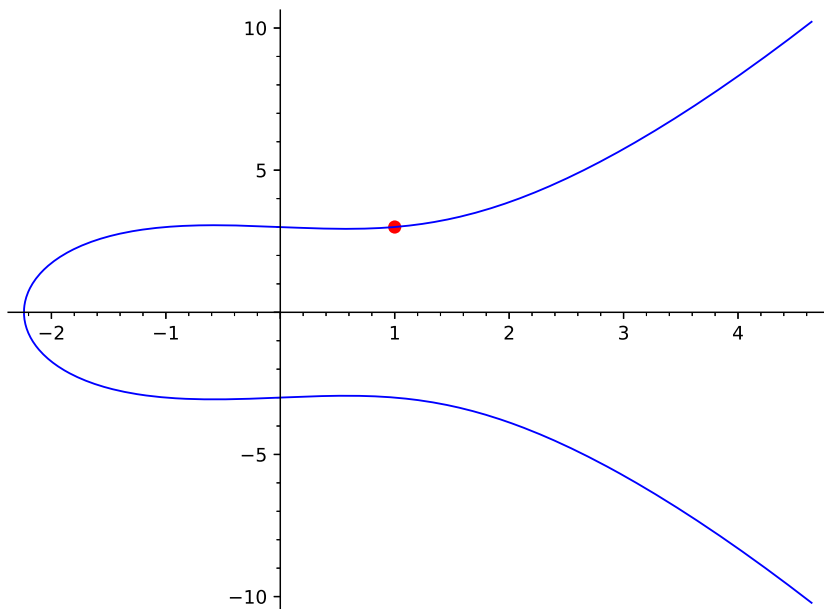
Much less obvious rational points include $(35, 207)$ or $(\frac{1}{36}, \frac{647}{216})$ (see Example 218).

Comment. In general, it is a very difficult problem to determine all rational points on an elliptic curve, and lots of challenges remain open in that arena.

Example 217. Plot the elliptic curve E , described by $y^2 = x^3 - x + 9$ and mark the point $(1, 3)$.

Solution. We let Sage do the work for us:

```
>>> E = EllipticCurve([-1,9])
>>> E.plot() + E(1,3).plot(pointsize=50, rgbcolor=(1,0,0))
```



Adding points on elliptic curves

Note. Simply adding the coordinates of two points P and Q on an elliptic curve will (almost always) not result in a third point on the elliptic curve. However, we will define a more fancy “addition” of points, which we will denote $P \boxplus Q$, such that the $P \boxplus Q$ is on the elliptic curve as well.

Given a point $P = (x, y)$ on E , we define $-P = (x, -y)$ which is another point on E .

Let us introduce an operation \boxplus in the following geometric fashion: given two points P, Q , the line through these two points intersects the curve in a third point R .

We then define $P \boxplus Q = -R$.

We remark that $P \boxplus (-P)$ is the point O “at ∞ ”. That’s the neutral (zero) element for \boxplus .

How does one define $P \boxplus P$? (Tangent line!)

Comment. Are you able to explain why, if P and Q have rational coordinates, the same is true for R ?

Remarkably, the “addition” $P \boxplus Q$ is associative. (This is not obvious from the definition.)

Using \boxplus , we can construct new points: for instance, $(0, 3) \boxplus (1, -3) = (35, 207)$ as we will verify in the next example using Sage.

Easier to verify (but not producing anything new) is $(0, 3) \boxplus (1, 3) = (-1, -3)$.

Example 218. Consider again the elliptic curve E , described by $y^2 = x^3 - x + 9$.

- (a) Determine $(0, 3) \boxplus (1, 3)$.
- (b) Determine $(0, 3) \boxplus (1, -3)$.
- (c) Determine $4(0, 3)$, which is short for $(0, 3) \boxplus (0, 3) \boxplus (0, 3) \boxplus (0, 3)$.

Solution. We let Sage do the work for us:

```
>>> E = EllipticCurve([-1,9])
```

```
>>> E(0,3) + E(1,3)
```

```
(-1: -3: 1)
```

```
>>> E(0,3) + E(1,-3)
```

```
(35: 207: 1)
```

```
>>> 4*E(0,3)
```

```
(-1677023/60279696, 1406201395535/468011559744, 1)
```

We conclude that $(0, 3) \boxplus (1, 3) = (-1, -3)$ and $(0, 3) \boxplus (1, -3) = (35, 207)$ (one of the points mentioned in Example 216), while

$$4(0, 3) = \left(-\frac{1677023}{60279696}, \frac{1406201395535}{468011559744} \right).$$

Comment. Note how Sage represents the point (x, y) as $(x: y: 1)$. These are **projective coordinates** which make it easier to incorporate the special point O which is represented by $(0: 1: 0)$.

https://en.wikipedia.org/wiki/Projective_coordinates

The following computation demonstrates that adding O doesn't do anything:

```
>>> E(0)
```

```
(0: 1: 0)
```

```
>>> E(0,3) + E(0)
```

```
(0: 3: 1)
```

Comment. Note that, starting with a single point such as $(0, -3)$, we can generate other points such as $2(0, -3) = \left(\frac{1}{36}, \frac{647}{216} \right)$ (one of the points mentioned in Example 216). If the initial point is rational then so are the points generated from it.

Advanced comment. If you want to dig deeper, you can try to translate the geometric description of the addition $P \boxplus Q$ into algebra by deriving equations for the coordinates of $P \boxplus Q = (x_r, y_r)$ in terms of the coordinates of $P = (x_p, y_p)$ and $Q = (x_q, y_q)$. For instance, for the elliptic curve $y^2 = x^3 + ax + b$, one finds that

$$\begin{aligned} x_r &= \lambda^2 - x_p - x_q, \\ y_r &= \lambda(x_p - x_r) - y_p, \end{aligned}$$

where $\lambda = (y_q - y_p) / (x_q - x_p)$ is the slope of the line connecting P and Q . If P and Q are the same point, then this line becomes the tangent line and the slope becomes $\lambda = (3x_p^2 + a) / (2y_p)$ instead. For more details:

https://en.wikipedia.org/wiki/Elliptic_curve

From these formulas, can you reproduce the computations we did in Sage?