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)
```

$\left(-\frac{1677023}{60279696} : \frac{1406201395535}{468011559744} : 1\right)$

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?

Armin Straub
straub@southalabama.edu