Elliptic Curves - Assignment 3

Matteo Durante, s2303760, Leiden University

12th March 2019

Exercise 3

(a) To do this, it is sufficient to assign integer values between 0 and 6 to X and find the square roots of X^3+2 modulo 7. We will then have to add the point at infinity, i.e. the one satisfying $Y^2Z = X^3 + 2Z^3$ with $Z = 0$ and s.t. at least one between X and Y is $\neq 0$.

X	0	1	2	3	4	5	6
Y	3,4	-	-	1,6	-	1,6	1,6

It follows that the complete list of points of the elliptic curve E given by the affine equation considered is $(0:3:1)$, $(0:4:1)$, $(3:1:1)$, $(3:6:1)$, $(5:1:1)$, $(5:6:1)$, $(6:1:1)$, $(6:6:1)$, $(0:1:0)$. We will omit the last coordinate and denote the point at infinity by O.

(b) Since $E(\mathbb{F}_7)$ has 9 elements, every element will have an order dividing 9.

We know that $a_1 = a_2 = a_3 = a_4 = 0$, $a_6 = 2$, hence $b_2 = b_4 = b_8 = 0$, $b_6 = 8 \equiv 1$ in $\mathbb{F}_7$ [1, p. III.1]. By [1, prop. 2.3], for every point $P \in E(\mathbb{F}_7)$ we get the following:

$$x([2]P) = \frac{x_P^4 + 5x_P}{4x_P^3 + 1}, \quad -(x_P, y_P) = (x_P, -y_P).$$

Thanks to this we get that, for every point $P \in E$, $x_P = x_{[2]P}$, thus either $[2]P = P$ or $[2]P = -P$. It follows that every point has order 1 or 3 and, since there is no element of order 9, $E(\mathbb{F}_7)$ is not cyclic.

Exercise 6

Proof. (a) Let $E/\mathbb{K}$ be an elliptic curve defined over $\mathbb{K}$ s.t. $P = (0,0) \in E$ is a point of order ≥ 4. We know that it is given by a Weierstrass equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{K}$ for every i.

Since P lies on it, $a_6 = 0$.

Let $g(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x$.

Since P does not have order 2, we know that the line tangent to E at P is not vertical. Also, since $\nabla(g) = (-a_4, a_3)$, it has equation $a_3y = a_4x$ and by the previous observation $a_3 \neq 0$. We can therefore do the substitution $y = y' + \frac{a_4}{a_3}x$, which turns our Weirstrass equation into $y^2 + b_1xy + b_3y = x^3 + b_2x^2$, $b_3 = a_3 \neq 0$, and changes the equation of the previously mentioned tangent line to $y = 0$. Notice that it has not moved P.

If the line tangent to E at P didn't meet any other point, then the third point on E met by it would be P itself. Let Q be the third point on E and the line passing through O and P. We have that $[2]P = Q \neq O$. We want to determine $P + Q$, but this is obvious because the line passing through P and Q is again the one through O and P, hence $[3]P = O$, which is absurd because it has order ≥ 4 by assumption.

We have shown that this tangent meets another point, $Q \neq O, P$. Since it has equation $y = 0$, this means that $x^3 + b_2x^2$ has a root $-b_2 \neq 0$.

We can then do another change of variables, $y = (\frac{b_3}{b_2})^3 y'$, $x = (\frac{b_3}{b_2})^2 x'$. Dividing then the equation we now have by $(\frac{b_3}{b_2})^6$, we get the following:

$$y^2 + \frac{b_1 b_2}{b_3} xy + \frac{b_2^3}{b_3^2} y = x^3 + \frac{b_2^3}{b_3^2} x^2$$

Setting $u = \frac{b_1 b_2}{b_3}, v = \frac{b_2^3}{b_3^2}$, we finally get the equation $y^2 + uxy + vy = x^3 + vx^2$. $\square$

(b) Let's look again at the previous setting and suppose that P has order 5. Remember that, up to isomorphism, our curve can be described by $y^2 + uxy + vy = x^3 + vx^2$.

We have that $u \neq 1$, for otherwise P would have order 4.

The tangent line at $-2P = (-v, 0)$ can be described by the equation $y = \frac{v}{1-u}(x + v)$ and, substituting this in the equation of E, we get an equation of degree 3 for the coordinate x of $4P = -2(-2P)$. By solving it, we get that this coordinate is given by $\frac{v^2+uv-v}{u^2-2u+1}$. Since P has order 5 by assumption, we have $4P = -P = (0, -v)$, thus $\frac{v^2+uv-v}{u^2-2u+1} = 0$.

It follows that $v(v - u + 1) = 0$ and, since $v \neq 0$, for otherwise $P = -P$, we have that $u = 1 + v$. Substituting this into the equation of E, we get that $y^2 + (1 + v)xy + vy = x^3 + vx^2$, which gives us a one-parameter family of elliptic curves with a rational point of order 5.

References

[1] Silverman James Harris. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.