ON TORSION POINTS OF ELLIPTIC CURVES

Contents

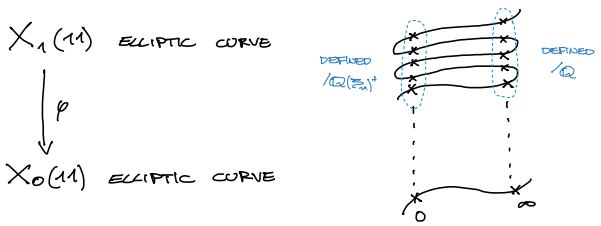
1. Torsion points of order 11

In this section we want to show that there are no elliptic curves with torsion points of order 11. In particular, we want to show that the only rational points on $X_1(11)$ are cuspidal. We will follow the general argument provided by Mazur in his famous paper *Modular Curves and the Eisenstein Ideal*.

First of all recall that $X_1(11)$ and $X_0(11)$ are elliptic curves of conductor 11 and the canonical map

$$\varphi : X_1(11) \to X_0(11)$$

is an isogeny of degree 5. From the modular interpretation, we also know that $X_0(11)$ has two special rational points coming from the cusps $[0], [\infty]$. While $X_1(11)$ has 10 different cusps, 5 defined over $\mathbb{Q}$ and 5 defined over $\mathbb{Q}(\zeta_{11})^+$. We can deduce this looking at the moduli interpretation with generalized elliptic curves and the Néron n-gons.



Consider the Néron models $\mathfrak{X}_1(11)$ and $\mathfrak{X}_0(11)$ defined over $Spec(\mathbb{Z}[1/11])$. We have the exact sequence

$$0 \to \mathbb{Z}/5\mathbb{Z} \to \mathfrak{X}_1(11) \to \mathfrak{X}_0(11) \to 0$$

over $R = Spec(\mathbb{Z})$. The kernel is guaranteed to be $\mathbb{Z}/5\mathbb{Z}$ by a theorem of Oort and Tate. Viewing the schemes as sheaves on the étale site, we can then consider the long exact sequence in cohomology

$$0 \to H^0_{\text{ét}}(R, \mathbb{Z}/5\mathbb{Z}) \to H^0_{\text{ét}}(R, \mathfrak{X}_1(11)) \to H^0_{\text{ét}}(R, \mathfrak{X}_0(11)) \to H^1_{\text{ét}}(R, \mathbb{Z}/5\mathbb{Z}) \to \cdots$$

Recall that by the properties of Néron models, we have $\mathfrak{X}_1(11)(Spec(\mathbb{Z}[1/11])) = X_1(11)(\mathbb{Q})$. The exact sequence then become

$$\frac{X_0(11)(\mathbb{Q})}{\varphi(X_1(11)(\mathbb{Q}))} \hookrightarrow H^1_{\text{ét}}(R, \mathbb{Z}/5\mathbb{Z}).$$

For an affine scheme $R = Spec(\mathbb{Z})$, the étale cohomology over R is equivalent to the Galois cohomology of π_1 groups. Now π_1 acts trivially on $\mathbb{Z}/5\mathbb{Z}$, so the first cohomology group is given by

$$H^1_{\text{ét}}(R, \mathbb{Z}/5\mathbb{Z}) \cong Hom(\pi_1, \mathbb{Z}/5\mathbb{Z}).$$

Since there exists a unique Galois field extension of $\mathbb{Q}$ with cyclic Galois group of order 5 and unramified outside of 11, namely $\mathbb{Q}(\zeta_{11})^+$ we conclude

$$H^1_{\text{ét}}(R, \mathbb{Z}/5\mathbb{Z}) \cong \mathbb{F}_5\,.$$

and then

$$\frac{X_0(11)(\mathbb{Q})}{\varphi(X_1(11)(\mathbb{Q}))} \hookrightarrow \mathbb{F}_5\,.$$

Observe that $X_0(11)$ contains the cusp [0] that has order 5 and it is not contained in the image of the rational points of $X_1(11)$, we conclude

$$\frac{X_0(11)(\mathbb{Q})}{\varphi(X_1(11)(\mathbb{Q}))} \cong \mathbb{F}_5\,.$$

Consider now the dual isogeny $\hat{\varphi} : X_0(11) \to X_1(11)$. Recall that by the Weil pairing we have

$$0 \to \mathbb{Z}/5\mathbb{Z} \to X_0(11)[5] \to \mu_5 \to 0.$$

In this case we obtain by duality

$$0 \to \mu_5 \to X_0(11) \to X_1(11) \to 0.$$

We would like to pass again to a long exact sequence in cohomology. To do this, we cannot use the étale site anymore since μ_5 is not an étale group scheme over $Spec(\mathbb{Z}[1/11])$ because it is not reduced at the fiber at 5. In order to deal with this, we consider instead the flat site obtaining

$$0 \to H^0_{\text{fppf}}(R, \mu_5) \to H^0_{\text{fppf}}(R, \mathfrak{X}_0(11)) \to H^0_{\text{fppf}}(R, \mathfrak{X}_1(11)) \to H^1_{\text{fppf}}(R, \mu_5) \to \cdots$$

and in particular

$$\frac{X_1(11)(\mathbb{Q})}{\widehat{\varphi}(X_1(11)(\mathbb{Q}))} \hookrightarrow H^1_{\text{fppf}}(R, \mu_5).$$

Observe that since μ_5 is not smooth over R, it is not guaranteed that $H^1_{\text{fppf}}(R, \mu_5) \cong H^1_{\text{ét}}(R, \mu_5)$. To compute this cohomology group, consider the Kummer sequence

$$0 \to \mu_5 \to \mathbb{G}_{\text{m}} \xrightarrow{(-)^5} \mathbb{G}_{\text{m}} \to 0$$

that is exact on the fppf site. Passing to the long exact sequence in cohomology we get

$$0 \to H^0_{\text{fppf}}(R, \mu_5) \to H^0_{\text{fppf}}(R, \mathbb{G}_{\text{m}}) \to H^0_{\text{fppf}}(R, \mathbb{G}_{\text{m}}) \to H^1_{\text{fppf}}(R, \mu_5) \to H^0_{\text{fppf}}(R, \mathbb{G}_{\text{m}}) \to \cdots$$

Now we have that the first cohomology group of $\mathbb{G}_{\text{m}}$ for the affine set $Spec(\mathbb{Z}[1/11])$ is the Picard group of $\mathbb{Z}[1/11]$ and in particular it is trivial. We then get

$$1 \to \frac{\mathbb{Z}[1/11]^\times}{(\mathbb{Z}[1/11]^\times)^5} \to H^1_{\text{fppf}}(R, \mu_5) \to 1.$$

Computing the unit groups of $\mathbb{Z}[1/11]$ we obtain

$$\frac{\mathbb{Z}[1/11]^\times}{(\mathbb{Z}[1/11]^\times)^5} \cong \frac{\pm 11^{\mathbb{Z}}}{\pm 11^{5\,\mathbb{Z}}} \cong \mathbb{Z}/5\mathbb{Z}$$

and so we conclude again

$$\frac{X_1(11)(\mathbb{Q})}{\widehat{\varphi}(X_0(11)(\mathbb{Q}))} \hookrightarrow \mathbb{F}_5\,.$$

To conclude that $X_0(11)$ has rank 0 we need a sharper bound on this quotient. To do this, we move our analysis to the prime of bad reduction of our elliptic curve, namely we look closer to the prime

11. In particular, we now look at the curves over $\mathbb{Q}$ and over $\mathbb{Q}_{11}$ the completion at 11. We then obtain the following commutative diagram

$$\begin{array}{ccccc} X_0(11)(\mathbb{Q}) & \longrightarrow & X_1(11)(\mathbb{Q}) & \longrightarrow & H^1_{\text{fppf}}(R,\mu_5) \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle (*)} \\ X_0(11)(\mathbb{Q}_{11}) & \xrightarrow{(**)} & X_0(11)(\mathbb{Q}_{11}) & \longrightarrow & H^1_{\text{fppf}}(\mathbb{Q}_{11},\mu_5). \end{array}$$

We have already previously computed $H^1_{\text{fppf}}(R,\mu_5) \cong \mathbb{F}_5$. Using again the Kummer sequence we obtain

$$\mathbb{Q}_{11}^{\times}/(\mathbb{Q}_{11}^{\times})^5 \cong H^1_{\text{fppf}}(\mathbb{Q}_{11},\mu_5).$$

It is important to remark that μ_5 is contained in $\mathbb{Q}_{11}$ since $\mathbb{Q}_{11}^{\times} \cong \mathbb{Z} \times \mu_{10} \times \mathbb{Z}_{11}$. Using that 5 is invertible in $\mathbb{Z}_{11}$ we obtain that every element in $(1+11\,\mathbb{Z}_{11},\cdot) \cong (\mathbb{Z}_{11},+)$ is a 5th power. We then get

$$(\mathbb{Q}_{11}^{\times})^5 \cong \pm 5\,\mathbb{Z} \times \mathbb{Z}_{11}$$

and then

$$H^1_{\text{fppf}}(\mathbb{Q}_{11},\mu_5) \cong \mathbb{F}_5 \times \mathbb{F}_5\,.$$

Observe that 11 is clearly not a fifth power in $\mathbb{Q}_{11}$, and then the map $(*)$ is injective

$$H^1_{\text{fppf}}(R,\mu_5) \cong 11^{\mathbb{Z}}/11^{5\,\mathbb{Z}} \hookrightarrow H^1_{\text{fppf}}(\mathbb{Q}_{11},\mu_5) \cong \mathbb{Q}_{11}^{\times}/(\mathbb{Q}_{11}^{\times})^5.$$

We want now show that $(**)$ is a surjective map. Using formal groups, we obtain the following commutative diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_{11} & \longrightarrow & X_0(11)(\mathbb{Q}_{11}) & \longrightarrow & \mathfrak{X}_0(11)(\mathbb{F}_{11}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & \mathbb{Z}_{11} & \longrightarrow & X_1(11)(\mathbb{Q}_{11}) & \longrightarrow & \mathfrak{X}_0(11)(\mathbb{F}_{11}) & \longrightarrow & 0. \end{array}$$

Now observe that the composition with $\widehat{\varphi}$ gives a multiplication by 5 map. Since 5 is invertible in $\mathbb{Z}_{11}$ we deduce α is an isomorphism. Furthermore, $\mu_5(\mathbb{Q}_{11}) \cong \mathbb{Z}/5\,\mathbb{Z}$. Using the explicit equation of $X_0(11)$ and $X_1(11)$ we can find that the group structure at $\mathbb{F}_{11}$ is given by

$$\mathfrak{X}_0(11)(\mathbb{F}_{11}) \cong \mathbb{Z}/5\,\mathbb{Z} \times \mathbb{Z}/10\,\mathbb{Z}, \quad \mathfrak{X}_1(11)(\mathbb{F}_{11}) \cong \mathbb{Z}/10\,\mathbb{Z}$$

We then have the following commutative diagram

$$\begin{array}{ccccccccc} & & 0 & & \mathbb{Z}/5\mathbb{Z} & & \ker(\beta) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}_{11} & \longrightarrow & X_0(11)(\mathbb{Q}_{11}) & \longrightarrow & \mathbb{Z}/5\,\mathbb{Z} \times \mathbb{Z}/10\,\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & \mathbb{Z}_{11} & \longrightarrow & X_1(11)(\mathbb{Q}_{11}) & \longrightarrow & \mathbb{Z}/10\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & \operatorname{coker}(\varphi) & & \operatorname{coker}(\beta) & & \end{array}$$

Applying the Snake Lemma we find

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z}/5\mathbb{Z} \longrightarrow \ker(\beta) \longrightarrow 0 \longrightarrow \operatorname{coker}(\varphi) \longrightarrow \operatorname{coker}(\beta) \longrightarrow 0$$

from which we deduce $\ker(\beta) \cong \mathbb{Z}/5\,\mathbb{Z}$ and φ is surjective. In particular, since the map $(**)$ is surjective, the commutative square implies that the following quotient is trivial

$$\frac{X_1(11)(\mathbb{Q})}{\widehat{\varphi}(X_0(11)(\mathbb{Q}))} \cong 0.$$

2. Torsion points of order 19

Consider now the case of the modular curve $X_0(19)$. We will try to apply the same techniques to this curve. $X_0(19)$ is a curve of genus 1 with two rational cusps [0] and $[\infty]$. LMFDB says it is the curve of equation

$$X_0(19) : y^2 + y = x^3 + x^2 - 9x - 15.$$

It is an elliptic curve of conductor 19. Since $3 = Num((19-1)/12)$ we deduce that the cuspidal subgroup of $J_0(9)$ is of order 3. In particular [0] is a point of order 3 on the elliptic curve. In order to determine the rank of $X_0(19)$ we consider the 3-isogeny associated to the subgroup generated by [0] and we try to compute a 3-descent. Consider then

$$\varphi : X_0(9) \to A$$

the 3-isogeny associated. Sage tells us that A is the ellitpic curve of conductor 19 given by the equation

$$y^2 + y = x^3 + x^2 - 769x - 8470.$$

Consider the Néron models $\mathfrak{X}_0(19)$ and $\mathcal{A}$ associated to $X_0(19)$ and A defined over $R = Spec(\mathbb{Z}[1/19])$. Take the short exact sequence of schemes

$$0 \to \mathbb{Z}/3\mathbb{Z} \to \mathfrak{X}_0(19) \xrightarrow{\varphi} \mathcal{A} \to 0.$$

A theorem by Oort and Tate assures us that the kernel of the isogeny is exactly the group scheme $\mathbb{Z}/3\mathbb{Z}$ over R. Viewing the group schemes as sheaves on the étale site, we can consider the long exact sequence in cohomology

$$0 \to H^0_{\text{ét}}(R, \mathbb{Z}/3\mathbb{Z}) \to H^0_{\text{ét}}(R, \mathfrak{X}_0(19)) \to H^0_{\text{ét}}(R, \mathcal{A}) \to H^1_{\text{ét}}(R, \mathbb{Z}/3\mathbb{Z}) \to \cdots$$

The exact sequence then become

$$\frac{A(\mathbb{Q})}{\varphi(X_0(19)(\mathbb{Q}))} \hookrightarrow H^1_{\text{ét}}(R, \mathbb{Z}/3\mathbb{Z}).$$

Observe that we have $H^1_{\text{ét}}(R, \mathbb{Z}/3\mathbb{Z}) = Hom(G^{(19)}, \mathbb{Z}/3\mathbb{Z})$ where $G^{(19)}$ is the absolute galois group unramified everywhere outside of 19. In particular, it factors through $\mathbb{Q}(\zeta_{19})/\mathbb{Q}$ and then we conclude $H^1_{\text{ét}}(R, \mathbb{Z}/3\mathbb{Z}) \cong \mathbb{F}_3$ and

$$\frac{A(\mathbb{Q})}{\varphi(X_0(19)(\mathbb{Q}))} \hookrightarrow \mathbb{Z}/3\mathbb{Z}.$$

Let's take a look at what happen at the prime of bad reduction 19. In particular we look at the completion at 19

$$\begin{array}{ccccc} X_0(19)(\mathbb{Q}) & \longrightarrow & A(\mathbb{Q}) & \longrightarrow & H^1_{\text{ét}}(R, \mathbb{Z}/3\mathbb{Z}) \\ \downarrow & & \downarrow & & \downarrow (*) \\ X_0(19)(\mathbb{Q}_{19}) & \xrightarrow{(**)} & A(\mathbb{Q}_{19}) & \longrightarrow & H^1_{\text{ét}}(\mathbb{Q}_{19}, \mathbb{Z}/3\mathbb{Z}). \end{array}$$

Observe that by Class Field Theory we have that the abelianisation of the absolute Galois group Γ_{19}^{ab} of $\mathbb{Q}_{19}$ is isomorphic to

$$\mathbb{Q}_{19}^{\times} \cong \Gamma_{19}^{ab}.$$

By the usual decomposition of $\mathbb{Q}_{19}^{\times} \cong \mathbb{Z} \times \mu_{18} \times \mathbb{Z}_{19}$ we obtain

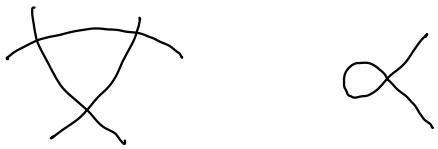
$$H^1_{\text{ét}}(\mathbb{Q}_{19}, \mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

By compatibility of the maps, $(*)$ is an injection. Using formal groups, we obtain the commutative diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_{19} & \longrightarrow & X_0(19)(\mathbb{Q}_{19}) & \longrightarrow & \mathfrak{X}_0(19)(\mathbb{F}_{19}) & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \varphi & & \downarrow \beta & & \\ 0 & \longrightarrow & \mathbb{Z}_{19} & \longrightarrow & A(\mathbb{Q}_{19}) & \longrightarrow & \mathcal{A}(\mathbb{F}_{19}) & \longrightarrow & 0. \end{array}$$

Again, the composition with $\widehat{\varphi}$ gives a multiplication by 3 map. Since 3 is invertible in $\mathbb{Z}_{19}$ we deduce α is an isomorphism. We now need to understand what happens at the Néron models $\mathfrak{X}_0(19)$ and $\mathcal{A}$ at the special fibers. LMFDB tells us that they have respectively Kodaira symbols I_3 and I_1. In particular we then deduce

$$\mathfrak{X}_0(19)(\mathbb{F}_{19}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}, \quad \mathcal{A}(\mathbb{F}_{19}) \cong \mathbb{Z}/18\mathbb{Z}$$



We then have the following commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & \mathbb{Z}/3\mathbb{Z} & & \ker(\beta) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}_{19} & \longrightarrow & X_0(19)(\mathbb{Q}_{19}) & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \beta} & & \\
0 & \longrightarrow & \mathbb{Z}_{19} & \longrightarrow & A(\mathbb{Q}_{19}) & \longrightarrow & \mathbb{Z}/18\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & \operatorname{coker}(\varphi) & & \operatorname{coker}(\beta) & &
\end{array}$$

Applying the Snake Lemma we find

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \ker(\beta) \longrightarrow 0 \longrightarrow \operatorname{coker}(\varphi) \longrightarrow \operatorname{coker}(\beta) \longrightarrow 0$$

from which we deduce $\ker(\beta) \cong \mathbb{Z}/3\mathbb{Z}$, $\operatorname{coker}(\beta) = 0$ and φ is surjective. In particular, since the map $(**)$ is surjective, the commutative square implies that the following quotient is trivial

$$\frac{A(\mathbb{Q})}{\widehat{\varphi}(X_0(19)(\mathbb{Q}))} \cong 1.$$

We now move our attention to the dual isogeny $\widehat{\varphi} : A \to X_0(19)$. By duality we have the short exact sequence

$$0 \to \mu_3 \to A \to X_0(19) \to 0$$

over $\mathbb{Q}$. Taking again the Néron models and applying the result of Oort and Tate we get

$$0 \to \mu_3 \to \mathcal{A} \to \mathfrak{X}_0(19) \to 0$$

over $Spec(\mathbb{Z}[1/19])$. Viewing the schemes as sheaves for the fppf topology, we obtain in a similar fashion as the previous computations

$$\frac{X_0(19)(\mathbb{Q})}{\widehat{\varphi}(A(\mathbb{Q}))} \hookrightarrow H^1_{\text{fppf}}(R, \mu_3).$$

Using the Kummer sequence we obtain

$$H^1_{\text{fppf}}(R, \mu_3) \cong \frac{\pm 19^{\mathbb{Z}}}{(\pm 19^{\mathbb{Z}})^3} \cong \mathbb{Z}/3\mathbb{Z}\,.$$

We conclude $X_0(19)$ has rank 0.

Appendix A. Néron Models

Def 1. *Let R be a Dedekind domain, K its fraction field. Consider E/K an elliptic curve. A* Néron model *for E/K is a smooth group scheme $\mathcal{E}$ defined over $Spec(R)$ whose generic fiber is E/K and which satisfies the following universal property: for $\mathcal{X}/R$ smooth R-scheme with generic fiber X/K, let $\varphi_K : X_{/K} \to E_{/K}$ the rational map defined over K, then there exists a unique R-morphism*

$$\varphi_R : \mathcal{X}_{/R} \to \mathcal{E}_{/R}$$

extending φ_K. The property is called Néron mapping property