the torsion subgroup of an elliptic curve injects in the reduction of the curve

Canonical name	TheTorsionSubgroupOfAnEllipticCurveInjectsInTheReductionOfTheCurve
Date of creation	2013-03-22 13:55:47
Last modified on	2013-03-22 13:55:47
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	7
Author	alozano (2414)
Entry type	Theorem
Classification	msc 14H52
Related topic	EllipticCurve
Related topic	BadReduction
Related topic	MazursTheoremOnTorsionOfEllipticCurves
Related topic	NagellLutzTheorem
Related topic	ArithmeticOfEllipticCurves

Let E be an elliptic curve defined over $\mathbb{Q}$ and let $p \in \mathbb{Z}$ be a prime. Let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a minimal Weierstrass equation for $E/\mathbb{Q}$, with coefficients $a_i \in \mathbb{Z}$. Let $\widetilde{E}$ be the reduction of E modulo p (see bad reduction) which is a curve defined over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The curve $E/\mathbb{Q}$ can also be considered as a curve over the p-adics, $E/\mathbb{Q}_p$, and, in fact, the group of rational points $E(\mathbb{Q})$ injects into $E(\mathbb{Q}_p)$. Also, the groups $E(\mathbb{Q}_p)$ and $E(\mathbb{F}_p)$ are related via the reduction map:

$$\pi_p \colon E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$$

$$\pi_p(P) = \pi_p([x_0, y_0, z_0]) = [x_0 \bmod p, y_0 \bmod p, z_0 \bmod p] = \widetilde{P}$$

Recall that $\widetilde{E}$ might be a singular curve at some points. We denote $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ the set of non-singular points of $\widetilde{E}$. We also define

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \pi_p(P) = \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)\}$$

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \pi_p(P) = \widetilde{P} = \widetilde{O}\} = \mathrm{Ker}(\pi_p).$$

Proposition 1. *There is an exact sequence of abelian groups*

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p) \longrightarrow \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p) \longrightarrow 0$$

where the right-hand side map is π_p restricted to $E_0(\mathbb{Q}_p)$.

Notation: Given an abelian group G, we denote by $G[m]$ the m-torsion of G, i.e. the points of order m.

Proposition 2. *Let $E/\mathbb{Q}$ be an elliptic curve (as above) and let m be a positive integer such that* $\gcd(p, m) = 1$. *Then:*

1. $$E_1(\mathbb{Q}_p)[m] = \{O\}$$

2. *If $\widetilde{E}(\mathbb{F}_p)$ is a non-singular curve, then the reduction map, restricted to $E(\mathbb{Q}_p)[m]$, is injective. This is*

$$E(\mathbb{Q}_p)[m] \longrightarrow \widetilde{E}(\mathbb{F}_p)$$

is injective.

Remark: Part 2 of the proposition is quite useful when trying to compute the torsion subgroup of $E/\mathbb{Q}$. As we mentioned above, $E(\mathbb{Q})$ injects into $E(\mathbb{Q}_p)$. The proposition can be reworded as follows: for all primes p which do not divide m, $E(\mathbb{Q})[m] \longrightarrow \widetilde{E}(\mathbb{F}_p)$ must be injective and therefore the number of m-torsion points divides the number of points defined over $\mathbb{F}_p$.

Example:

Let $E/\mathbb{Q}$ be given by

$$y^2 = x^3 + 3$$

The discriminant of this curve is $\Delta = -3888 = -2^4 3^5$. Recall that if p is a prime of bad reduction, then $p \mid \Delta$. Thus the only primes of bad reduction are $2, 3$, so $\widetilde{E}$ is non-singular for all $p \geq 5$.

Let $p = 5$ and consider the reduction of E modulo 5, $\widetilde{E}$. Then we have

$$\widetilde{E}(\mathbb{Z}/5\mathbb{Z}) = \{\widetilde{O}, (1,2), (1,3), (2,1), (2,4), (3,0)\}$$

where all the coordinates are to be considered modulo 5 (remember the point at infinity!). Hence $N_5 = \mid \widetilde{E}(\mathbb{Z}/5\mathbb{Z}) \mid = 6$. Similarly, we can prove that $N_7 = 13$.

Now let $q \neq 5, 7$ be a prime number. Then we claim that $E(\mathbb{Q})[q]$ is trivial. Indeed, by the remark above we have

$$\mid E(\mathbb{Q})[q] \mid \text{ divides } N_5 = 6, N_7 = 13$$

so $\mid E(\mathbb{Q})[q] \mid$ must be 1.

For the case $q = 5$ be know that $\mid E(\mathbb{Q})[5] \mid$ divides $N_7 = 13$. But it is easy to see that if $E(\mathbb{Q})[p]$ is non-trivial, then p divides its order. Since 5 does not divide 13, we conclude that $E(\mathbb{Q})[5]$ must be trivial. Similarly $E(\mathbb{Q})[7]$ is trivial as well. Therefore $E(\mathbb{Q})$ has trivial torsion subgroup.

Notice that $(1, 2) \in E(\mathbb{Q})$ is an obvious point in the curve. Since we have proved that there is no non-trivial torsion, this point must be of infinite order! In fact

$$E(\mathbb{Q}) \cong \mathbb{Z}$$

and the group is generated by $(1, 2)$.