Rank of Elliptic Curves

The goal of this paper is to present how can be determined the rank of an elliptic curve and also to give an introduction to the machinery of Selmer and Tate-Shafarevich groups.

1 Notation

- K will always denote a number field even though for some of the results I will mention we only need K to be a perfect field
- $\overline{K}$ is the algebraic closure of K and $G_{\overline{K}/K}$ denotes the Galois group of $\overline{K}/K$
- K_v is the completion of K at a valuation v
- M_K^0 denotes the set of non-archimedean valuations of K while M_K^∞ denotes the set of archimedean valuations of K
- $M_K = M_K^0 \cup M_K^\infty$
- For an elliptic curve E defined over the field K and for any subfield L , between K and $\overline{K}$, $E(L)$ denotes the group of $L-rational$ points of E. If it's not specified E denotes $E\left(\overline{K}\right)$
- For an integer $m \geq 2$ μ_m represents the group of $m^{th} - roots$ of unity
- For an integer m $E[m]$ represents the group of $m-torsion$ points of E. In general for an isogeny $\phi : E \rightarrow E'$, $E[\phi] = Ker\phi$
- Always the notation $[m]P$ means $P + P + \ldots P$ added m times in E
- O will always denote the origin of the elliptic curve , i.e. the point at infinity for E
- For an integer $m \geq 2$, $e_m : E[m] \times E[m] \rightarrow \mu_m$ denotes the classical Weil pairing which is surjective
- Also , for a valuation v on a field K_v we denote by R_v the ring of integers and M_v the maximal ideal ; thus $k_v = R_v/M_v$
- When we reduce the elliptic curve defined over a local field K_v modulo M_v we obtain a curve $\tilde{E}(k_v)$ whose nonsingular points form a group $\tilde{E_{ns}}(k_v)$
- $Isom(C) = \{\phi : C \rightarrow C|\ \phi\ isomorphism\}$, $\forall C$ projective smooth curve , which will always be our assumption about a curve
- For every curve C , $K(C)$ denotes its function field
- In general , for an elliptic curve and a point P on it τ_P is the morphism given by translation by P

- We say that a cocycle $\xi \in H^1(G,M)$ is unramified at a subgroup H of G if its restriction to $H^1(H,M)$ is trivial. Moreover , in the usual notation $\xi in H^1(G_{\overline{K}/K},M)$ we say that ξ is unramified at a place $v \in M_K$ if ξ is unramified at I_v.

2 Mordell-Weil group

For this section we take E/K be an elliptic curve , $m \geq 2$ an integer and we assume that $E[m] \subset E(K)$. We have the Kummer pairing :

$$\kappa : E(K) \times G_{\overline{K}/K} \to E[m]$$

which is defined as follows : for $P \in E(K)$ and $\sigma \in G_{\overline{K}/K}$, take $Q \in E$ s.t. $[m]Q = P$ and then define $\kappa(P,\sigma) = Q^\sigma - Q$.

We can verify imediately that κ is well defined (for this we use $E[m] \subset E(K)$). It's also easy to see that the kernel on the left of the pairing is $mE(K)$ while on the right is $G_{\overline{K}/L}$, where

$$L = K([m]^{-1}E(K))$$

the field obtained by adjoining to K all the coordinates of points on E that multiplied by m , in the additive group of E , land in $E(K)$. So , we can see κ as giving a morphism :

$$\delta_E : E(K)/mE(K) \to Hom(G_{\overline{K}/K}, E[m])$$

by : $\delta_E(P)(\sigma) = \kappa(P,\sigma)$, $\forall\ P \in E(K)$ and $\forall \sigma \in G_{\overline{K}/K}$.

We also have the short exact sequence : $0 \to E[m] \to E \to E \to 0$ where the second nontrivial map is multiplication by m .

Each of the groups in the sequence has a $G_{\overline{K}/K} - action$ on it and so , we can form the long exact sequence in cohomology :

$$0 \to E[m] \to E(K) \to E(k) \to H^1(G_{\overline{K}/K}, E[m]) \to \dots$$

Because $G_{\overline{K}/K}$ acts trivially on $E[m]$ and from basic chase on the diagram we see that δ_E is actually the above connecting morphism from the long exact sequence between $E(K)/mE(K)$ and $H^1(G_{\overline{K}/K}, E[m])$.

Using Hilbert's Thorem 90 , we have an isomorphism :

$$\delta_K : K^*/K^{*m} \to Hom(G_{\overline{K}/K}, \mu_m)$$

, given by : $\delta_K(b)(\sigma) = \frac{\beta^\sigma}{\beta}$, where $\beta \in \overline{K^*}$ satisfies : $\beta^m = b$.

Theorem 1 (a) There exists a bilinear pairing $b : E(K)/mE(k) \times E[m] \to K^*/K^{*m}$ s.t. $e_m(\delta_E(P),T) = \delta_K(b(P,T))$.

(b) The pairing b is nondegenerate on the left.

(c) Let $S \subset M_K$ be the set of archimedean valuations rogether with the finite primes at which E has bad reduction and the primes dividing m . Then the image of b lies in the subgroup of K^*/K^{*m} given by :

$$K(S,m) = \{d \in K^*/K^{*m} \mid ord_v(d) \equiv 0(mod\ m)\ for\ all\ v\ not\ in\ S\}$$

.

(d)The pairing b may be computed as follows : for each $T \in E[v]$ choose functions $f_T, g_T \in K(E)$ s.t. $div(f_T) = m(T) - m(O)$ and $f_T \circ [m] = g_T^m$.

Then for $P \neq T$, $b(P,T) \equiv f_T(P)(mod\ K^{*m})$. Then by linearity : $b(T,T) = f_T(P+T)f_T(P)^{-1}$ for any $P \neq T$.

Proof See Chapter X in silverman's book : Arithmetic of Elliptic Curves [AEC].

I'll use Theorem 1 to do :

Theorem 2 (Complete 2-descent) Let E/K be an elliptic curve given by a Weierstrass equation :

$$y^2 = (x-e_1)(x-e_2)(x-e_3)$$

with $e_i \in K\ \forall\ i \in \overline{1,3}$.

Let $S \subset M_K$, containing all archimedean places , all places dividing m and all places at which E has bad reduction. There is an injective morphism : $E(K)/2E(K) \to K(S,2) \times K(S,2)$ defined by :

$$P = (x,y) \to \{ \begin{array}{l} (x-e_1, x-e_2)\ ,\ if x \neq e_1\ ,\ e_2 \\ (\frac{e_1-e_3}{e_1-e_2}, e_1-e_2)\ ,\ if\ x = e_1 \\ (e_2-e_1, \frac{e_2-e_3}{e_2-e_1})\ ,\ if\ x = e_2 \\ (1,1)\ ,\ if\ P = O \end{array}$$

Moreover , let $(b_1, b_2) \in K(S,2) \times K(S,2)$ be a pair that in not the image of one of the three points : O , $(e_1, 0)$, $(e_2, 0)$. Then (b_1, b_2) is the image of a point $P = (x,y) \in E(K)/2E(K)$ iff the equations :

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1$$

have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K^*$. If such a solution exists , then one can take :

$$P = (x,y) = (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3)$$

.

Proof In the setting of Theorem 1 , for $m = 2$, we take O , $T_1 = (e_1, 0)$, $T_2 = (e_2, 0)$ and $T_3 = (e_3, 0)$ and because of the non-degeneracy of b on the left we can construct an injective morphism : $E(K)/2E(K) \to K(S,2) \times K(S,2)$ (our desired map) by mapping $P \in E(K)$ (modulo $2E(K)$) into $(b(P,T_1), b(P,T_2))$. We got the actual expression of the map .

Now , for $(b_1, b_2) \in K(S,2) \times K(S,2)$, to determine if it is in the image of b , we need to exist

$$(x, y, z_1, z_2) \in K^* \times K^* \times K^* \times K^*$$

s.t. $y^2 = (x - e_1)x - e_2)(x - e_3)$ and $x - e_i = b_i z_i^2$ for all $i \in \overline{1,2}$.

This gives the existence of $z_3 \in K$ s.t. $b_1 b_2 z_3^2 = x - e_3$ and eliminating x we get the exact two equations from the statement of the theorem and moreover

$$x = b_1 z_1^2 + e_1$$

$$y = b_1 b_2 z_1 z_2 z_3$$

as desired.

3 General theory of twisting

Definition A twist of C/K is another smooth curve C'/K which is isomorphic with C over $\overline{K}$. The set of twists modulo $K-isomorphisms$ is denoted $Twist(C/K)$.

We also define $\xi : G_{\overline{K}/K} \to Isom(C)$, by $\xi_\sigma = \phi^\sigma \phi^{-1}$ for some fixed $\phi : C' \to C$, giving a twist of C.

Theorem 3 Let C/K be a smooth curve . For each twist C'/K of C/K , choose an isomorphism $\phi : C' \to C$ and define the map ξ_σ as above.

(a) ξ is a $1-cocycle$ in $H^1(G_{\overline{K}/K}, Isom(C))$

(b) The cohomology class $\{\xi\}$ is determined by the $K-isomorphism$ class of C' , not by the choice of ϕ . We thus obtain the map :

$$Twist(C/K) \to H^1(G_{\overline{K}/K}, Isom(C))$$

(c) The map from (b) is a bijection.

Proof The proof of all of the above statements is straightforward with the exception of the surjectivity of the map from (b). So I'll do only this part.

We take $\{\xi\} \in H^1(G_{\overline{K}/K}, Isom(C))$ and we need to construct a curve C'/K and a morphism $\phi : C' \to C$ s.t. $\phi^\sigma \phi^{-1} = \xi_\sigma$, $\forall\ \sigma \in G_{\overline{K}/K}$.

We construct $K(C')$ which is $\overline{K}-isomorphic$ to $K(C)$ by an isomorphism Z.

We want $G_{\overline{K}/K}$ to act on $\overline{K}(C)$ as follows :

for $f \in \overline{k}(C)$ and $\sigma \in G_{\overline{K}/K}$:

$$Z(f)^\sigma = Z(f^\sigma \xi_\sigma)$$

where by $f^\sigma \xi_\sigma$ I mean $\xi_\sigma^*(f^\sigma)$ (ξ_σ^* is the induced map on function fields , from $\overline{K}(C)$ into itself , corresponding to the morphism $\xi_\sigma : C \to C$).

So we had $Z : \overline{K}(C) \to \overline{K}(C)$ automorphism s.t. $Z(K(C) = K(C')$. Because $G_{\overline{K}/K}$ acts differently on $\overline{K}(C)$, the fixed subfield of $\overline{K}(C)$ is going to be (possibly) different than $K(C)$ and we'll prove that this field , call it L , is the function field we're looking for. By construction : $L = Z(K(C)$, both being the $G_{\overline{K}/K}-invariants$ of $\overline{K}(C)$ with respect to the corresponding $G_{\overline{K}/K}-actions$. So , L has transcendence degree 1 over K . (It is clear that $L \cap \overline{K} = K$ because if $Z(f) \in L \cap \overline{K}$ for some $f \in K(C)$, because $Z|_{\overline{K}} = id_{\overline{K}}$, it means that $f \in \overline{K}$ and $K(C) \cap \overline{K} = K$ and so $L \cap \overline{K} = K$.)

Thus there exists a smooth curve C'/K s.t. $L = K(C')$ and so C' and C are isomorphic over $\overline{K}$.

So , after proving that C' is a twist of C , it only remains to show that the isomorphism $\phi : C' \to C$ obtained above , generates $\{\xi\}$.

So : $\phi^* = Z|_{K(C)}$, which means that : $\forall\ f \in K(C)$, $\forall \sigma \in G_{\overline{K}/K}$:

$\phi^*(f)^\sigma = \phi^*(f^\sigma \xi_\sigma) \Rightarrow (f\phi)^\sigma = f^\sigma \xi_\sigma \phi \Rightarrow \phi^\sigma \phi^{-1} = (f^\sigma)^{-1} f^\sigma \xi_\sigma \Rightarrow \phi^\sigma \phi^{-1} = \xi_\sigma$, as desired .

If we work with an elliptic curve instead of a general smooth curve we can describe better the twisting process.

Theorem 4 The map $E \times Aut(E) \to Isom(E)$ given by :

$$(P, \alpha) \to \tau_P \circ \alpha$$

is a bijection of sets.

Proof Straightforward.

Theorem 5 Let E/K be an elliptic curve .

(a) the natural inclusion $Aut(E) \to Isom(E)$ induces an inclusion

$$H^1(G_{\overline{K}/K}, Aut(E) \subset H^1(G_{\overline{K}/K}, Isom(E))$$

We'll denote $Twist((E,O)/K)$ the first set.

(b) Let $C/K \in Twist((E,O)/K)$. Then $C(K) \neq \emptyset$ and so C/K is an elliptic curve over K.

(c) If E'/K is an elliptic curve which is isomorphic to E over $\overline{K}$, then $E'/K \in Twist((E,O)/K)$ via the association between the isomorphisms of E and elements of $H^1(G_{\overline{K}/K}, Isom(E))$, given by theorem 3.

Proof Straightforward.

Theorem 6 Assume that $char K \neq 2, 3$ and let $n = |Aut(E)|$. then $Twist((E,O)/K) \cong K^*/K^{*n}$. More precisely , choose a Weierstrass equation

$$E: \ y^2 = x^3 + Ax + B$$

for E/K and choose some $D \in K^*/K^{*n}$. Then the elliptic curve corresponding to D is $E_D \in Twist((E,O)/K)$ and has the Weierstrass equation :

$$E_D \ : \ y^2 = x^3 + D^2Ax + D^3B \ , \ if \ j(E) \neq 0, 1728$$

$$E_D \ : \ y^2 = x^3 + DAx \ , \ if \ j(E) = 1728$$

$$E_D \ : \ y^2 = x^3 + DB \ , \ if \ j(E) = 0$$

Moreover , if we define an equivalence $\sim$ on the set $K \times K^*$, by :

$(j,D) \sim (j',D')$ if $j = j'$ and $\frac{D}{D'} \in K^{*n(j)}$ (n9j) is the order of the automorphism group of the elliptic curve represented by invariant j) , then the $K - isomorphism$ classes of elliptic curves E/K are in $one - to - one$ correspondence with elements of the quotient : $K \times K^{*}/\sim$.

Proof It's a classical result for elliptic curves $Aut(E) \cong \mu_n$ as $G_{\overline{K}/K} - modules$. This gives :

$Twist((E,O)/K) \cong H^1(G_{\overline{K}/K}, Aut(E)) \cong H^1(G_{\overline{K}/K}, \mu_n) \cong K^*/K^{*n}$

I'll do here the explicit computation of E_D only for the case $j(E) \neq 0, 1728$; the other two cases are similar.

So , we take $D \in K^*$ and let $\delta \in \overline{K}$ s.t. $\delta^2 = D$; we may choose to write $\delta = \sqrt{D}$

We define $\xi : G_{\overline{K}/K} \to \mu_2$, by $\xi_\sigma = \frac{\sqrt{D}^\sigma}{\sqrt{D}}$.

We also have the canonical isomorphism : $[]$: $\mu_2 \to Aut(E)$, given by $[s](x,y) = (x, sy)$.

Now , if we comeback to the proof of Theorem 3 , the construction of the function field from (c) , we see that on $K(E_D)$ we have the following relations :

$x^\sigma = x$ and $y^\sigma = \xi_\sigma y$

So we see that x and $\frac{y}{\sqrt{D}}$ are $G_{\overline{K}/K} - invariants$,meaning they are both in $K(E_D)$.

Because : $y^2 = x^3 + Ax + B$, we see that x and $\frac{y}{\sqrt{D}}$satisfy the equation :

$$D(\frac{y}{\sqrt{D}})^2 = x^3 + Ax + B$$

We redenote by x and y the former x and $\frac{y}{\sqrt{D}}$ and then after a rescaling by D we get the desired equation of E_D.

4 Homogeneous spaces

This was defined in the lectures , so I'm going to use that definition and the properties established in class.

Theorem 7 Let E/K be an elliptic curve and C/K be a homogeneous space for E/K. Fix a point $p_0 \in C$ and define a map : $\theta : E \to C$, by $\theta(P) = P_0 + P$.

(a) θ is an isomorphism defined over $K(P_0)$. In particular , C/K is a twist of E/K. (In our definition of a homogeneous space C/K is assumed to be a smooth curve , so it makes sense to say that θ ,from above, is a morphism of curves and it's clearly defined over $K(P_0)$.)

(b) $\forall\, p,q \in C\ :\ q - p = \theta^{-1}(q) - \theta^{-1}(p)$. (This is the defining property of a homogeneous space over an elliptic curve or any other group variety.)

(c) The subtraction map $\nu\ :\ C \times C \to E$,given by $\nu(q,p) = q - p$ is a morphism defined over K.

Definition Two homogeneous spaces C/K and C'/K for E/K are equivalent if there is an isomorphism $\theta\ :\ C \to C'$ defined over K which is compatible with the action of E on C and C' , i.e.

$$\forall\ p \in C\ and\ P \in E\ :\ \theta(p+P) = \theta(p) + P$$

. The equivalence class containing E , acting on itself by translations , is called the trivial class. The collection of equivalence classes of homogeneous spaces for E/K is called the Weil-Chatelet group , denoted $WC(E/K)$.

Theorem 8 Let C/K be a homogeneous space for E/K. Then C/K is the trivial class iff $C(K)$ is not empty.

Proof If $C(K) \neq \emptyset$, take $P_0 \in C(K)$ and then $\theta : E \to C$ given by $\theta(P) = P_0 + P$ is a $K-morphism$ because $K(P_0) = K$ and so by definition of a homogeneous space we see that E and C are $K-isomorphic$, i.e. C is in the trivial class.

Conversely , if C is in the trivial class , then there exists a $K-isomorphism$, $\theta : E \to C$ s.t.

$$\forall\ P \in E(K)\ :\ \theta(P) = \theta(O) + P$$

and

$$\forall\ \sigma \in G_{\overline{K}/K}\ :\ \theta(P)^\sigma \theta(O)^\sigma + P^\sigma\ iff\ \theta(P^\sigma) = \theta(O)^\sigma + P$$

Because $P^\sigma = P$ ($P \in E(K)$) we see that $\theta(O) = \theta(O)^\sigma$ for all $\sigma \in G_{overlineK/K}$. Thus : $\theta(O) \in C(K)$, as desired.

Theorem 9 Let E/K be an elliptic curve . There is a natural bijection between $WC(E/K)$ and $H^1(G_{\overline{K}/K}, E)$ defined as follows :

for C/K a homogeneous space take $p_0 \in C$; then $\{C/K\} \to \{\sigma \to p_0^\sigma - p_0\}$.

So , because $H^1(G_{\overline{K}/K}, E)$ is a group , the above bijection induces a group structure on $WC(E/K)$.

Proof All of the above statements are clear except the surjectivity of the above map - so this is what I'm going to prove now.

Let $\xi : G_{\overline{K}/K} \to E$ be a $1-cocycle$. We can embed E in $Isom(E)$ through the translations si we may view $\xi \in H^1(G_{\overline{K}/K}, Isom(E))$ which we showed that it corresponds to a twist of E/K.

Thus , exists a curve C/K and a $\overline{K} - isomorphism\ \phi : C \to E$ s.t. $\tau_{-\xi_\sigma} = \phi^\sigma \phi^{-1}$ for all $\sigma \in G_{\overline{K}/K}$, where by $\tau_{-\xi_\sigma}$ I mean translation by $-\xi_\sigma \in E$.

We define a map : $\mu : C \times E \to C$ given by : $\mu(p, P) = \phi^{-1}(\phi(p) + P)$ for all $(p, P) \in C \times E$. I claim that μ gives a structure of homogeneous space on C and the cocycle associated to C in Theorem 9 is $\{\xi\}$.

Indeed , $\forall\ p_1, p_2 \in C\ :\ \mu(p_1, \phi(p_2) - \phi(p_1)) = p_2$, which shows that μ acts simply transitive on C.

To see that μ is well-defined over K : $\forall \sigma \in G_{\overline{K}/K}$ we have : $\mu(p, P)^\sigma = (\phi^\sigma)^{-1}(\phi^\sigma(p^\sigma + P^\sigma)$ while $\mu(p^\sigma, P^\sigma) = \phi^{-1}(\phi(p^\sigma + P^\sigma)$.

The two expressions are equal iff :

$$(\phi^\sigma \phi^{-1})(\phi(p^\sigma + P^\sigma)) = \phi^\sigma(p^\sigma + P^\sigma)$$

This is equivalent with :

$$\tau_{-\xi_\sigma}(\phi(p^\sigma + P^\sigma)) = \phi^\sigma(p^\sigma + P^\sigma)$$

Again this is equivalent with :

$$\phi(p^\sigma + P^\sigma) - \xi_\sigma = \phi^\sigma(p^\sigma) + P^\sigma$$

Then the desired claim follows from :

$$\phi^\sigma(p^\sigma) = (\phi^\sigma\phi^{-1})\phi(p^\sigma) = \phi(p^\sigma) - \xi_\sigma$$

Finally , knowing that C/K is a homogeneous space for E/K it's imediate to see that the associated cocycle is $\{\xi\}$. (Just take $p_0 = \phi^{-1}(O)$.)

5 The Selmer and Tate-Shafarevich groups

For a nonzero isogeny $\phi : E \to E'$ defined over K , we have the short exact sequence :

$$0 \to E[\phi] \to E \to E' \to 0$$

which gives us the long exact sequence :

$$0 \to E(K)[\phi] \to E(K) \to E'(K) \to H^1(G_{\overline{K}/K}, E[\phi]) \to H^1(G_{\overline{K}/K}, E) \to H^1(G_{\overline{K}/K}, E') \to \dots$$

from which we extract the short exact sequence

$$0 \to E'(K)/\phi(E(K)) \to H^1(G_{\overline{K}/K}, E[\phi]) \to H^1(G_{\overline{K}/K}, E)[\phi] \to 0$$

For each $v \in M_K$ we take its extension to $\overline{K}$ and a decomposition group $G_v \subset G_{\overline{K}/K}$. Then we also get :

$$0 \to E'(K_v)/\phi(E(K_v)) \to H^1(G_v, E[\phi]) \to H^1(G_v, E)[\phi] \to 0$$

Remembering that $H^1(G_{\overline{K}/K}, E) = WC(E/K)$ and that G_v can be seen both as $G_{\overline{K_v}/K_v}$ and as a subgroup of $G_{\overline{K}/K}$, we have the two exact sequences bellow for which there are natural maps from each group of the first sequence to the corresponding group of the second sequence :

$$0 \to E'(K)/\phi(E(K)) \to H^1(G_{\overline{K}/K}, E[\phi]) \to WC(E/K)[\phi] \to 0$$

$$0 \to \prod_{v\in M_K} E'(K_v)/\phi(E(K_v)) \to \prod_{v\in M_K} H^1(G_v, E[\phi]) \to \prod_{v\in M_K} WC(E/K_v)[\phi] \to 0$$

We want to compute the kernel of the map : $H^1(G_{\overline{K}/K}, E[\phi]) \to WC(E/K)[\phi]$

Definition With the above notations the $\phi - Selmer$ group of E/K is :

$$S^\phi(E/K) = Ker\{H^1(G_{\overline{K}/K}, E[\phi]) \to \prod_{v\in M_K} (E/K_v)\}$$

The Shafarevich-Tate group is :

$$\Xi(E/K) = Ker\{WC(E/K) \to \prod_{v\in M_K} WC(E/K_v)\}$$

Note that both groups are kernels of maps obtained from considering the above two short exact sequences , more exactly they both refer to

$$WC(E/K)[\phi] \to \prod_{v \in M_K} WC(E/K_v)[\phi]$$

In general , an element of $WC(e/K)$ becomes trivial in $\prod_{v \in M_K} WC(E/K_v)$ if the associated curve , which is defined over K , has a $K_v - rational$ point for every $v \in M_K$.

Theorem 10 Let $\phi : E/K \to E'/K$ be an isogeny .

(a) there is an exact sequence :

$$0 \to E'(K)/\phi(E(K)) \to S^\phi(E/K) \to \Xi(E/K)[\phi] \to 0$$

(b) the Selmer group $S^\phi(E/K)$ is finite.

Proof (a) Straightforward from the definitions.

(b) Let S be the set of infinite places of K together with the finite places that divide $m = deg(\phi)$ and with the finiteley many places at which E has bad reduction. From now on this set S wherever called will denote exactly the above set of places.

I claim that $\xi \in S^\phi(E/K)$ is unramified outside S. So take v not in S and because $\xi \in S^\phi(E/K)$, ξ is tgrivial in $WC(E/K_v)$. Thus there exists $P \in E(\overline{K_v})$ s.t.

$$\xi_\sigma = P^\sigma - P \in E[\phi], \forall \sigma \in G_{\overline{K_v}/K_v} = G_v$$

If we take in the above equality $\sigma \in I_v$ and then take the $v - reduction$ we see that

$$\tilde{\xi_\sigma} = \tilde{P}^\sigma - \tilde{P} = \tilde{O}$$

So $\xi_\sigma \in E[\phi] \subset E[m]$ and the reduced in κ_v is $\tilde{O}$. Because of our choice of v we know that $E[m]$ injects into $E(\kappa_v)$. thus : $P^\sigma = P$, i.e. $\xi\sigma = O, \forall\ \sigma \in I_v$.

So ξ is unramified at v. Now , the result of the problem follows imediately after a classical result of homological algebra which says that if M is a finite abelian $G_{\overline{K}/K} - module$ and $S \subset M_K$ is a finite set of places , then the set :

$$H^1(G_{\overline{K}/K}, M; S) = \{\xi \in H^1(G_{\overline{K}/K}, M) | \xi\ is\ unramified\ outside\ S\}$$

is finite. (We saw that $S^\phi(E/K) \subset H^1(G_{\overline{K}/K}, E[\phi]; S)$.)

So , now after we finished the proof of Theorem 10 , we see that to identify an element of $H^1(G_{\overline{K}/K}, E[\phi]; S)$ as being from $S^\phi(E/K)$ we only need to verify if $C(K_v) \neq \emptyset$ for each of the finitely many $v \in S$ where C is the corresponding homogeneous space $\{C/K\} \in WC(E/K)$.

Moreover , if $E[m] \subset E(K)$ then $H^1(G_{\overline{K}/K}, E[m]; S) \cong K(S, m) \times K(S, m)$.

Indeed in this case : $H^1(G_{\overline{K}/K}, E[m]) = Hom(G_{\overline{K}/K}, E[m])$ and then if we take L the maximal abelian extension of K having exponent m which is unramified outside S we get $Hom(G_{L/K}, E[m]) \cong Hom(G_{\overline{K}/K}, E[m]; S)$.

But by construction : $G_{L/K}$ is a radical extension because we only adjoin $m^{th} - roots$ of elements from K and so , identifying $E[m]$ with $\mu_m \times \mu_m$ we get :

$$Hom(G_{L/K}, E[m]) = Hom(G_{L/K}, \mu_m) \times Hom(G_{L/K}, \mu_m)$$

and by the long exact sequence derived from the short exact sequence :

$$1 \to \mu_m \to L^* \to L^{*m} \to 1$$

we get that $K(S, m) \cong Hom(G_{L/K}, \mu_m)$ and so the claimed result is true.

Then for example , for $m = 2$, the homogeneous space associated to a pair $(b_1, b_2) \in K(S, 2) \times K(S, 2)$ is the curve C in $\mathbf{P^3}$ given by the homogenized version of the equations from theorem 2 :

$$b_1 z_1^2 - b_2 z_2^2 = (e_2 - e_1) z_0^2$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = (e_3 - e_1) z_0^2$$

Then , for any such pair (b_1, b_2) we only need to check if the curve C has a point in K_v for every $v \in S$.

Now , we have the exact sequence :

$$E(K) \to S^{[m]}(E/K) \to \Xi(E/K)[m] \to 0$$

and we want to know which elements of $S^{[m]}(E/K)$ correspond to rational points of E. For this we have a procedure that works in case $\Xi(E/K)[m]$ is finite (which may not be the case !).

We can take the 2 exact sequences bellow that have natural maps between the corresponding terms from the first sequence to the second sequence : the identity map between $E(K) \to E(K)$ and the multiplication bt $m^{n-1} - map$ between the Tate-shafarevich groups while the map between the Selmer groups is the induced map from multiplication by $m^{n-1} - map$ between $E[m^n]$ and $[m]$.

$$E(K) \to S^{[m^n]}(E/K) \to \Xi(E/K)[m^n] \to 0$$

$$E(K) \to S^{[m]}(E/K) \to \Xi(E/K)[m] \to 0$$

Then if we denote by $S^{(m,n)}(E/K)$ the image of $S^{[m^n]}(E/K)$ in $S^{[m]}(E/K)$ we get an exact sequence :

$$0 \to E(K)/mE(K) \to S^{(m,n)}(E/K) \to m^{n-1}\Xi(E/K)[m^n] \to 0$$

Now , the procedure is as follows:

Compute $S^{(m,n)}(E/K)$ for sufficiently large n and also compute $T_{(m,n')}(E/K)$ for sufficiently large n' , where $T_{(m,n')}(E/K)$ is the subgroup of $S^{[m]}$ generated by $\{P \in E(K) | h_x(P) \leq n\}$ ($h_x(P)$ represents the logarithmic height of P with respect to function x.)

If $S^{(m,n)}(E/K) = T_{(m,n')}(E/K)$ for some n and n' then our problem is solved because then $m^{n-1}\Xi(E/K)[m^n] = 0$ and because of the exact sequence (clear from the definitions)

$$0 \to E(K)/mE(K) \to S^{(m,n)}(E/K) \to m^{n-1}\Xi(E/K)[m^n] \to 0$$

We see that then $E(K)/mE(K)$ is generated by points of height $h_x(P) \leq n'$. then we can find generators for the Mordell-Weil group.

In the remaining of this section I'll present how can the above theory be applied to the $2-isogenies$. Thus , let $\phi : E \to E'$ be such an isogeny with kernel $\{O,T\}$ defined over K. Because $T \in E[2]$ we may take $T=(0,0)$ and the Weierstrass form of E/K to be : $y^2 = x^3+ax^2+bx$. We identify once again $E[\phi]$ with μ_2 and so : $K^*/K^{*2} \cong H^1(G_{\overline{K}/K}, E[\phi])$

Thus : $H^1(G_{\overline{K}/K}, E[\phi]; S) \cong K(S,2)$

So , for $d \in K(S,2)$, the corresponding cocycle is :

$$\sigma \to \{ \begin{array}{l} O \ , \ if \ \sqrt{d}^{\sigma} = \sqrt{d} \\ (0,0) \ , \ if \ \sqrt{d}^{\sigma} = -\sqrt{d} \end{array}$$

Again , we have to look in $\overline{K}(E)$ to the fixed field with respect to the following $G_{\overline{K}/K} - action$:

$$\sqrt{d}^{\sigma} = \xi_{\sigma}\sqrt{d}$$

$$x^{\sigma} = \{ \begin{array}{l} x \ , \ if \ \sqrt{d}^{\sigma} = \sqrt{d} \\ \frac{b}{x} \ , \ if \ \sqrt{d}^{\sigma} = -\sqrt{d} \end{array}$$

$$y^{\sigma} = \{ \begin{array}{l} y \ , \ if \ \sqrt{d}^{\sigma} = \sqrt{d} \\ -\frac{by}{x^2} \ , \ if \ \sqrt{d}^{\sigma} = -\sqrt{d} \end{array}$$

These expressions come from the proof of Theorem 9 plus the fact that the translations by $\xi_{\sigma} = -\xi_{\sigma}$ have simple formulas : for one point is the identity map while for the other we use the basic formulas for addition on an elliptic curve : $(x,y)+(0,0) = (\frac{b}{x}, -\frac{by}{x^2})$

It's not difficult to determine the invariant function under the above maps and so we see that they are generated by $\frac{\sqrt{d}x}{y}$ and $\sqrt{d}(x-\frac{b}{x})$. Using the Weierstrass equation for the elliptic curve we see that the twisted curve satisfies the equation

$$dw^2 = d^2 - 2adz^2 + (a^2-4ab)z^4$$

where $z = \frac{\sqrt{d}x}{y}$ and $w = \sqrt{d}(x-\frac{b}{x})(\frac{x}{y})^2$. The above curve in $/bfA^2$ is part of a smooth projective curve from $\mathbf{P^3}$, call it C_d that is described by the homogeneous equations :

$$x_3x_0 = x_1^2$$

$$x_2^2 - \frac{a^2-4ab}{d}x_3^2 + 2ax_0x_3 - dx_0^2 = 0$$

then , from a previous remark , in order to compute the Selmer group associated to ϕ for E/K we only need to check if $C_d(K_v) \neq \emptyset$ for each $d \in K(S,2)$ and each $v \in S$.

The isogeny is given by : $(x,y) \to (\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2})$ and so E' has the Weierstrass equation : $y^2 = x^3 - 2ax^2 + (a^2-4ab)x$. Finally , as in Theorem 2 , we can compute the connecting morphism :

$$\delta : E'(K) \to H^1(G_{\overline{K}/K}, E[\phi]) \cong K^*/K^{*2}$$

which is now given by

$$\delta(O) = 1 \ , \ \delta((0,0)) = a^2 - 4ab \ and \ \delta((x,y)) = x(mod\ K^{*2}) \ if \ x \neq O, (0,0)$$

6 A family of curves

I'll determine next the Selmer groups and a bound for the rank over $\mathbf{Q}$ of the elliptic curves from the family : $y^2 = x^3 + 2px$, where p denotes as usually an odd prime.

First I'll prove that $E_{p_{tors}}(\mathbf{Q}) = \mathbf{Z/2Z}$, where by E_p I denote the elliptic curve from the above family corresponding to prime p.

Indeed , it's clear that O and $(0,0)$ are $2-torsion$ rational points and because $\sqrt{-2p}$ is not rational we see that the curve has no more rational $2-torsion$ points.Now , for any prime q different than p , E_p has good reduction at q and so $E_{p_{tors}}(\mathbf{Q})$ injects into $\tilde{E_p}(\mathbf{F_q})$ (this result is assured if we choose q s.t. E_p doesn't have $q-torsion$ points - for example if $q \geq 11$ from Mazur's theorem.

Then if we also pick $q \equiv 3(mod\ 4)$ then we know that $\tilde{E_p}(\mathbf{F_q})$ is supersingular. this follows from basic criterion for supersingular curves that have the form of E_p that if the coefficient of x^{q-1} in $(x^3+2px)^{\frac{q-1}{2}}$ is 0 then the curve is supersingular and so $\#\tilde{E_p}(\mathbf{F_q}) = \mathbf{q+1}$ because supersingular curve satify also : $\#\tilde{E_p}(\mathbf{F_q}) \equiv \mathbf{1(mod\ 4)}$ but also we have the general result of Weil that $|\#\tilde{E_p}(\mathbf{F_q}) - \mathbf{q} - \mathbf{1}| \leq \mathbf{2\sqrt{q}}$.

So , $\#E_{p_{tors}}(\mathbf{Q})|\mathbf{q+1}$ for all primes q with the general conditions from above. So imediately we see that it must be that $\#E_{p_{tors}}(\mathbf{Q})|\mathbf{4}$ and from the analysis of the $2-torsion$ points we see that indeed only 2 torsion points are over $\mathbf{Q}$. but then we may apply the previous section machinery and do a $2-isogeny$.

We'll consider the isogenuous elliptic curve to E_p through the mentioned map :

$$E'_p \ : \ y^2 = x^3 - 8px$$

while the map between the two elliptic curves is ϕ defined by :

$$\phi(x,y) = (\frac{y^2}{x^2}, \frac{y(2p-x^2)}{x^2})$$

The set $S \subset M_{\mathbf{Q}}$ is $\{\infty, 2, p\}$ and so $\mathbf{Q(S,2)} = \{\pm\mathbf{1}, \pm\mathbf{2}, \pm\mathbf{p}, \pm\mathbf{2p}\}$ and for each $d \in \mathbf{Q(S,2)}$ $C_d/\mathbf{Q} \in \mathbf{WC(E/Q)}$ is given by : $dw^2 = d^2 - 8pz^4$.

Similarly , working with the dual isogeny : $\hat{\phi} : E'_p \to E_p$ we get the equations of the twists of E'_p :

$$C'_d \ : \ dw^2 = d^2 + 2pz^4$$

where d belongs to the same set from above . (This wouldn't be true in general but in this case $2p$ and $8p$ have the same set of prime divisors.)

It's straightforward from the definition of the dual isogeny that we have the following exact sequence :

$$0 \to \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[m])} \to \frac{E'(K)}{\phi(E(K))} \to \frac{E(K)}{mE(K)} \to \frac{E(K)}{\hat{\phi}(E'(K))} \to 0$$

where $m = deg(\phi)$ and the middle map from above is $\hat{\phi}$.

I'll use this claim in the previous setting and derive :

$$dim_{\mathbf{F_2}} \frac{E_p(\mathbf{Q})}{2E_p(\mathbf{Q})} = dim_{\mathbf{F_2}} \frac{E'_p(\mathbf{Q})}{\phi(E_p(\mathbf{Q}))} + dim_{\mathbf{F_2}} \frac{E_p(\mathbf{Q})}{\hat{\phi}(E'_p(\mathbf{Q}))} - dim_{\mathbf{F_2}} \frac{E'_p(\mathbf{Q})[\hat{\phi}]}{\phi(E_p(\mathbf{Q})[\mathbf{2}])}$$

But we know that $\phi(E_p(\mathbf{Q}[\mathbf{2}]) = \{\mathbf{O}'\}$ (the origin on E'_p) and also from the formula of $\hat{\phi}$ we also see that $E'_p(\mathbf{Q})[\hat{\phi}] = \{\mathbf{O}', (\mathbf{0}, \mathbf{0}\}$, which gives us

$$rank\ E_p(\mathbf{Q}) = \mathbf{-2} + \mathbf{dim}_{\mathbf{F_2}} \frac{\mathbf{E'_p(Q)}}{\phi(\mathbf{E_p(Q)})} + \mathbf{dim}_{\mathbf{F_2}} \frac{\mathbf{E_p(Q)}}{\hat{\phi}(\mathbf{E'_p(Q)})}$$

Now come the Selmer and Tate-Shafarevich groups into action :

$$0 \to \frac{E'_p(\mathbf{Q})}{\phi(E_p(\mathbf{Q}))} \to S^{\phi}(E_p/(\mathbf{Q}) \to \mathbf{\Xi(E_p/Q)}[\phi] \to \mathbf{0}$$

$$0 \to \frac{E_p(\mathbf{Q})}{\hat{\phi}(E'_p(\mathbf{Q}))} \to S^{\hat{\phi}}(E'_p/\mathbf{Q}) \to \mathbf{\Xi(E'_p/Q)}[\hat{\phi}] \to \mathbf{0}$$

We'll determine $S^{\phi}(E_p/\mathbf{Q})$ and $S^{\hat{\phi}}(E'_p/\mathbf{Q})$. We have to check if $C_d(\mathbf{Q_v}) \neq \emptyset$ for each $v \in \{\infty, 2, p\}$ and for each $d \in \mathbf{Q(S, 2)}$ and then do the same thing for $C'_d(\mathbf{Q_v})$.

First we see that) and $(0,0)$ have image 1 and $-8p = -2p$ in the Selmer group by construction of the δ map. So it's enough to check $d \in \{-1, 2, -2\}$. All the cases are dealt using only Hensel's lemma ; so I'll omit the arguments and state only the results.

$d = -1$ is impossible in $\mathbf{Q_2}$, i.e. : $-w^2 = 1 - 8pz^4$ has no solutions in Q_2.

$d = 2$ has solution in $\mathbf{Q_p}$ iff $(\frac{2}{p}) = 1$ iff $p \equiv 1$ *or* $7(mod\ 8)$. In $\mathbf{Q_2}$ there exists solution iff $p \equiv -1(mod\ 8)$. Thus C_2 has a point iff $p \equiv -1(mod\ 8)$.

$d = -2$ has solution in $\mathbf{Q_p}$ iff $p \equiv 1$, $3(mod\ 8)$. in $\mathbf{Q_2}$ it has a solution iff $p \equiv 1(mod\ 8)$. thus C_{-2} gives us a point iff $p \equiv 1(mod\ 8)$.

So , we conclude that $S^{\phi}(E_p/\mathbf{Q})$ has 4 elements if $p \equiv \pm 1\ mod(\ 8)$ and has 2 elements if $p \equiv \pm 3\ (mod\ 8)$.

Similarly we'll do the analysis for $S^{\hat{\phi}}(E'_p/\mathbf{Q})$. Following the same steps as above we find out that $S^{\hat{\phi}}(E'_p/\mathbf{Q})$ has 4 elements if $p \equiv \pm 1\ (mod\ 8)$ and has 2 elements if $p \equiv \pm 3\ (mod\ 8)$.

Then using the above two exact sequences linking the Selmer and Tate-Shafarevich groups to the rank of the elliptic curve we conclude that :

- if $p \equiv \pm 3\ (mod\ 8)$ then $rank\ E_p(\mathbf{Q}) = \mathbf{0} = \mathbf{\Xi(E_p/Q)}[\phi] = \mathbf{\Xi(E'_p/Q)}[\hat{\phi}]$
- if $p \equiv \pm 1\ (mod\ 8)$ then

$$rank\ E_p(\mathbf{Q}) + \mathbf{dim}_{\mathbf{F_2}}\mathbf{\Xi(E_p/Q)}[\phi] + \mathbf{dim}_{\mathbf{F_2}}\mathbf{\Xi(E'_p/Q)}[\hat{\phi}] = \mathbf{2}$$