RATIONAL POINTS ON ELLIPTIC CURVES AND THE p-ADIC GEOMETRY OF SHIMURA CURVES

CHAO LI

Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$. The abelian group $E(\mathbb{Q})$ is finitely generated due to the theorem of Mordell-Weil. All the 15 possibilities of its torsion part are determined by Mazur but its rank $r(E/\mathbb{Q})$ is far from being completely understood. Our first goal is to try to understand the rank $r(E/\mathbb{Q})$ for certain elliptic curves $E/\mathbb{Q}$ satisfying the following three conditions. (I could pretend to be clever and mystify these conditions by writing down them right away. But I shouldn't. So how about introducing them only when we need them?)

1. 2-descent

A key pole played in the proof of Mordell-Weil theorem is the method of descent. Let $n \geq 2$ be an integer. Associated to the exact sequence

$$0 \to E[n] \to E \to E \to 0,$$

we have an exact sequence in Galois cohomology

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbb{Q})/nE(\mathbb{Q}) \arrow[r, "\delta"] \arrow[d] & H^1(\mathbb{Q}, E[n]) \arrow[r] \arrow[d] & H^1(\mathbb{Q}, E)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v E(\mathbb{Q}_v)/nE(\mathbb{Q}_v) \arrow[r, "\prod_v \delta_v"] & \prod_v H^1(\mathbb{Q}_v, E[n]) \arrow[r] & \prod_v H^1(\mathbb{Q}_v, E)[n] \arrow[r] & 0
\end{tikzcd}$$

Understanding the Kummer map δ helps us to understand $E(\mathbb{Q})$. Though the group $H^1(\mathbb{Q}, E[n])$ is an enormous infinite group, one can cut out a finite group $\mathrm{Sel}_n(E/\mathbb{Q})$, the *$n$-Selmer group*, using the local conditions defined by the local Kummer maps δ_v. One then has an exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \mathrm{Sel}_n(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0.$$

Computing $\mathrm{Sel}_n(E/\mathbb{Q})$ bounds $r(E/\mathbb{Q})$ from above. Such a procedure is called an *n-descent*, though it is not so easy to compute for general n.

Now we are going to describe an explicit 2-descent (which by definition is a 2-descent that is very explicit). In fact, the Galois module $E[2]$ can be easily described and allows us to identify the Kummer maps.

Proposition 1.1. *Let $L = \mathbb{Q}[t]/f(t)$. Then $H^1(\mathbb{Q}, E[2]) \cong (L^\times/(L^\times)^2)_{\mathbb{N}=\square}$ and*

$$\delta : E(\mathbb{Q})/2E(\mathbb{Q}) \to (L^\times/(L^\times)^2)_{\mathbb{N}=\square}$$

is explicitly given by $P \mapsto x(P) - t$. The similar description holds for local Kummer maps δ_v.

Now we assume

a) $f(x) \in \mathbb{Z}[x]$ is a monic *irreducible* polynomial of *squarefree* and *negative* discriminant $\mathrm{disc}(f) = -D$ (so $D \equiv 3 \pmod 4$).

This implies that

1. $E[2](\mathbb{Q}) = 0$.
2. L is an imaginary cubic field. Let A be the ring of integers of L. Then $A^\times \cong \mathbb{Z} \times \{\pm 1\}$.

(3) $\Delta(E) = -16D$. The equation is minimal. E has multiplicative reduction at $p \mid D$, additive reduction at 2 and good reduction elsewhere.

The multiplicative reduction condition and the negative discriminant pins down all the local conditions at $p \neq 2$ (the image of δ_v are the units) and ∞ (trivial image), allowing one to compute $\mathrm{Sel}_2(E/\mathbb{Q})$ explicitly up to only uncertainty caused by the local condition at $p = 2$.

Theorem 1.2. *Assume a). Then* $\mathrm{rank}_2 \mathrm{Sel}_2(E/\mathbb{Q}) = \mathrm{rank}_2 \mathrm{Pic}(A)$ *or* $\mathrm{rank}_2 \mathrm{Pic}(A) + 1$.

2. Root numbers

The 2-Selmer rank is determined once we know its parity. The famous conjecture of Birch and Swinnerton-Dyer asserts that

$$r(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s),$$

where $L(E/\mathbb{Q}, s)$ is the L-function of $E/\mathbb{Q}$. It implies the special case concerning the parity of both sides, the parity conjecture: $(-1)^{r(E/\mathbb{Q})} = \varepsilon(E/\mathbb{Q})$, where $\varepsilon(E/\mathbb{Q})$ is the sign of the functional equation of $L(E/\mathbb{Q}, s)$, called the *root number* of $E/\mathbb{Q}$. Since our E has no 2-torsion, according to a theorem of Monsky,

$$(-1)^{\mathrm{rank}_2 \mathrm{Sel}_2(E/\mathbb{Q})} = \varepsilon(E/\mathbb{Q}).$$

So it suffices to pin down the root number $\varepsilon(E/\mathbb{Q})$.

The nice thing about the root number is that is admits a factorization into local terms. However it could tricky since the split (resp. nonsplit) multiplicative reduction has root -1 (resp. $+1$) . We do a trick by going to a quadratic extension $\mathbb{Q}(i)$. Then $\varepsilon(E/\mathbb{Q}(i)) = \varepsilon_2(E/\mathbb{Q}(i))$. If we assume

b) E has Kodaira type IV over $\mathbb{Q}_2$.

Then we can pin down $\varepsilon_2(E/\mathbb{Q}) = \varepsilon_2(E/\mathbb{Q}(i)) = -1$ and the conductor $N(E/\mathbb{Q}) = 4D$. In particular,

Proposition 2.1. *Assume a), b). Then* $\varepsilon(E/\mathbb{Q}(i)) = -1$.

Let $E^* : -y^2 = f(x)$ be the (-1)-quadratic twist of E. Then because

$$\varepsilon(E/\mathbb{Q}(i)) = \varepsilon(E/\mathbb{Q})\varepsilon(E^*/\mathbb{Q}),$$

we know that one of E, E^* has root number $+1$ and another has root number -1. We write them as $E^{\pm}$ according to the sign. It follows that

Proposition 2.2. *Assume a), b). Then* $\mathrm{rank}_2 \mathrm{Sel}_2(E^+/\mathbb{Q})$ *is even;* $\mathrm{rank}_2 \mathrm{Sel}_2(E^-/\mathbb{Q})$ *is odd.*

If we further assume

c) $\mathrm{Pic}(A)$ has odd order.

Proposition 2.3. *Assume a), b), c). Then* $\mathrm{rank}_2 \mathrm{Sel}_2(E^+/\mathbb{Q}) = 0$*;* $\mathrm{rank}_2 \mathrm{Sel}_2(E^-/\mathbb{Q}) = 1$.

In particular, $r(E^+/\mathbb{Q}) = 0$ and $r(E^-/\mathbb{Q}) \leq 1$. BSD predicts $r(E^-/\mathbb{Q}) = 1$ and thus $r(E/\mathbb{Q}(i)) = 1$. Notice one expects that the condition a), b), c) should define a positive portion among all elliptic curves (though I don't know how to prove it). Gross-Zagier and Kolyvagin says that if $\mathrm{ord}_{s=1} L(E/\mathbb{Q}(i), s) = 1$, then $r(E/\mathbb{Q}(i)) = 1$ and a point of infinite order is supplied by a Heegner point. We don't know that the order of vanishing is exactly one, but BSD predicts it should. So let us look at the Heegner point and see what we can say about it.

3. Heegner points on Shimura curves

The Heegner points over $\mathbb{Q}(i)$ are coming from a Shimura curve associated to then quaternion algebra

$$B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = -1, j^2 = D, ij = -ji.$$

It is ramified at $p = 2$ and $p \equiv 3 \pmod 4, p \mid D$. Let $R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij \subseteq B$ (an order of reduced discriminant $4D$). Then the Shimura curve has complex uniformization

$$X = X_R = B^\times(\mathbb{Q})\backslash\mathcal{H}^\pm \times B^\times(\mathbb{A}_f)/\hat{R}^\times = R^\times\backslash\mathcal{H}^\pm.$$

Shimura showed that X has a canonical model over $\mathbb{Q}$ and classifies abelian surfaces with endomorphisms by R. The Heegner points correspond to embeddings $\mathbb{Z}[i] \hookrightarrow R$ and are defined over $\mathbb{Q}(i)$.

Let σ be the cuspidal automorphic representation on $GL_2(\mathbb{A})$ associated to E and let π be the automorphic representation on $B(\mathbb{A})$ via the Jacquet-Langlands correspondence. Then $\mathrm{Hom}^0_{\mathbb{Q}}(J, E) \cong \pi^{\hat{R}^\times}$, where $J = \mathrm{Jac}(X)$.

1. For $p \mid D$ or $p \equiv 1 \pmod 4$, $\pi_p \cong \sigma_p$.
2. For $p \mid D$ and $p \equiv 3 \pmod 4$, π_p is trivial on $R_p^\times$, since $R_p \subseteq B_p$ is the maximal order. So it is the trivial or sign representation of $B_p^\times/R_p^\times\mathbb{Q}_p^\times \cong \mathbb{Z}/2$.
3. For $p = 2$, π_p is trivial on $R_p^\times$ since $R_p^\times = 1 + \varpi\mathcal{O}_p \subseteq B_p^\times$ consists of the one units. So it is the unique 2-dimensional representation of $B_p^\times/R_p^\times\mathbb{Q}_p^\times \cong S_3$.

Proposition 3.1. $\mathrm{Hom}^0_{\mathbb{Q}}(J, E)$ *has dimension 2.*

Now let P_0 be the Heegner point corresponding to the natural embedding $\mathbb{Z}[i] \to R$. The group $B_p^\times/R_p^\times\mathbb{Q}_p^\times \cong S_3$ acts on X and $S_3 \cdot x_0$ consists of three points $\{P_0, P_1, P_2\}$. So $D^0 = \mathrm{Div}^0(P_0, P_1, P_2)$ is the A_2 lattice as a S_3-module. S_3 also acts on J, hence on $\mathrm{Hom}^0_{\mathbb{Q}}(J, E)$. Therefore $\mathrm{Hom}_{\mathbb{Q}}(J, E)$ is either the A_2 lattice or its dual. In either case,

Proposition 3.2. $\mathrm{Hom}_{\mathbb{Q}}(J, E) \otimes_{\mathbb{Z}[S_3]} D^0 \cong \mathbb{Z}$ *and its image* P *lies in* $E^-(\mathbb{Q}) \subseteq E(\mathbb{Q}(i))$.

So we constructed a candidate for a point of infinite order on $E^-(\mathbb{Q})$.

Example 3.3. Consider the case $D = 11$. The Shimura curve X has genus 2 and is given by the equation $-y^2 = x^6 - 7x^4 + 59x^2 + 11$. The three elliptic points are ∞, $(1, 8i)$ and $(-1, 8i)$. The Jacobian J is $(2, 2)$-isogenous to $E \times F$, where

$$E = 44A1 : y^2 = x^3 + 7x^2 + 59x - 11, \quad F = 44A2 : y^2 = x^3 - 59x^2 - 77x - 121$$

are 3-isogenous to each other. Therefore $\mathrm{Hom}^0_{\mathbb{Q}}(J, E)$ is indeed 2-dimensional. Moreover, the point $(-1, 8)$ is a point of infinite order on the (-1)-twist of E.

In order to prove P has infinite order, one hopes for the best that P is not divisible by 2 in $E(\mathbb{Q}(i))$. If one believes it, then at least the divisor $P_0 - P_1 \in J(\mathbb{Q}(i))$ cannot be divisible by 2. This is a question only involving the Shimura curve X and can be investigated by studying the reduction of J mod 2. Our next goal is to compute the reduction of J mod 2 using the theory of p-adic uniformization.

4. p-adic uniformization and reduction of Jacobian of Shimura curves

Now we turn to a slightly more general situation. Let $B/\mathbb{Q}$ be a quaternion algebra ramified at p and possibly other places (we will specialize to the case $p = 2$ in the end). Let $S \subseteq B$ be an order such that S_p is an maximal order $\mathcal{O}_p$ of B_p. Let $R \subseteq S$ be an index p sub-order such that

$$R_p = \{x \in \mathcal{O}_p : x \bmod \varpi \in \mathbb{F}_p \subseteq \mathbb{F}_{p^2} \cong \mathcal{O}_p/\varpi\}.$$

Then $R_p^\times$ has index $p+1$ in $S_p^\times$. Let X (resp. Y) be the Shimura curve associated to R (resp. S). Then $X \to Y$ is a degree $p+1$ covering map. By the complex uniformization, either of X and Y is a union of projective curves of the form $\Gamma\backslash\mathcal{H}^\pm$, where Γ is a discrete subgroup of $PGL_2(\mathbb{R})$. Interestingly, by a deep theorem of Cerednik-Drinfeld, these Shimura curves also admit p-adic uniformization. Let $\Omega = \mathbb{C}_p - \mathbb{Q}_p$ be the p-adic half plane, then $Y(\mathbb{C}_p)$ (as a rigid analytic space) is a union of Mumford curves of the form $\Gamma\backslash\Omega$, where Γ is a discrete subgroup of $PGL_2(\mathbb{Q}_p)$. Even better, Ω has an integral model over $\mathbb{Z}_p$, whose special fiber consists of $\mathbb{P}^1$'s with intersection graph an infinite $(p+1)$-valent tree T. When Γ acts freely on the tree T, the Shimura curve Y has a regular stable model over $\mathbb{Z}_p$ whose special fiber consists of $\mathbb{P}^1$ with intersection graph $\Gamma\backslash T$. So one can describe the reduction mod p of the Shimura curve Y (whose level at p is maximal) in terms of the quotient graph $\Gamma\backslash T$.

What about the Shimura curve X with non-maximal level at p? The miracle is that the p-adic half plane Ω is far from "simply-connected": it admits a tower of etale covers (known as the *Drinfeld tower*)

$$\cdots\Omega_n \to \cdots \to \Omega_2 \to \Omega_1 \to \Omega_0 = \Omega,$$

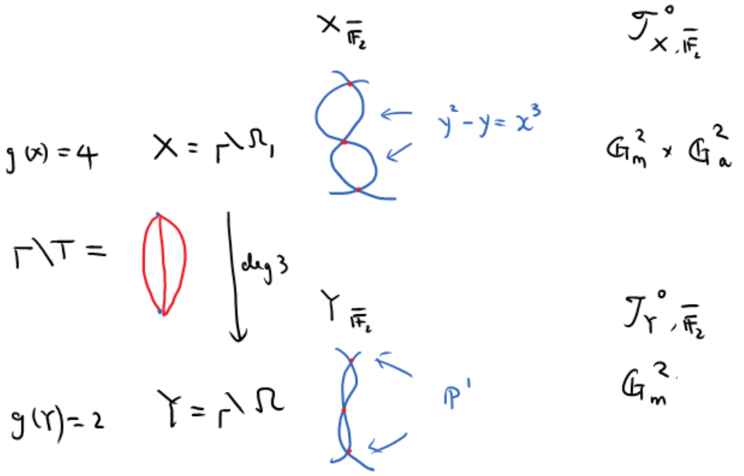
where the covering group for $\Omega_n \to \Omega$ is $(\mathcal{O}_p/\varpi^n)^\times$. The n-th cover Ω_n can be used to uniformize the Shimura curve with level $1+\varpi^n\mathcal{O}_p$ at p. Therefore our Shimura curve X is uniformized by the first (tame) Drinfeld cover Ω_1. Using Teitelbaum's geometric description of Ω_1 and Edixhoven's theorem on the Neron models under tamely ramified extensions, we are able to compute the reduction mod p of the Jacobians J_X and J_Y.

Theorem 4.1. *Let $\mathcal{J}_X$ (resp. $\mathcal{J}_Y$) be the Neron model of J_X (resp. J_Y) over $W = W(\overline{\mathbb{F}_p})$. Suppose the level away from p is small enough. Then the connected component of the special fiber of the Neron models are given by*

$$\mathcal{J}^0_{Y,\overline{\mathbb{F}_p}} \cong \mathbb{G}_m^{g(Y)}, \quad \mathcal{J}^0_{X,\overline{\mathbb{F}_p}} \cong \mathbb{G}_m^{g(Y)} \times \mathbb{G}_a^{g(X)-g(Y)},$$

where $g(\cdot)$ denotes the genus.

Example 4.2. Consider the case $p = 2$.



$X_{\overline{\mathbb{F}}_2}$
$\mathcal{J}^\circ_{X,\overline{\mathbb{F}}_2}$
$g(X)=4$
$X = \Gamma\backslash\Omega_1$
$y^2-y=x^3$
$\mathbb{G}_m^2 \times \mathbb{G}_a^2$
$\Gamma\backslash T =$
deg 3
$Y_{\overline{\mathbb{F}}_2}$
$\mathcal{J}^\circ_{Y,\overline{\mathbb{F}}_2}$
$\mathbb{G}_m^2$
$\mathbb{P}^1$
$g(Y)=2$
$Y = \Gamma\backslash\Omega$

Remark 4.3. Come back to our original situation ($p = 2$). Since $\mathbb{G}_a$ is killed by 2, if the reduction of $P_0 - P_1 \in J(\mathbb{Q}(i))$ projects to a *nonzero* element in $\mathbb{G}_a^{g(X)-g(Y)}$, then $P_0 - P_1$ cannot be divisible by 2. Whether $P_0 - P_1$ maps to a nonzero element in $\mathbb{G}_a^{g(X)-g(Y)}$ seems to be more subtle: it can be checked by constructing a regular model of X over $\mathbb{Z}_2[i]$, but the special fiber of such a regular model is often *nonreduced* and complicates the computation.