MATH 6370, LECTURE 12
ELLIPTIC CURVES II
APRIL 13

GORDAN SAVIN

In this lecture we shall use torsion points on the elliptic curve E given by the equation $2y^2 = x^3 - x$ to construct abelian extension of $\mathbb{Q}(i)$. Given any field extension of K of $\mathbb{Q}$, let $E(K)$ be the set of solutions (x, y) of the cubic such that x and y are in K.

Exercise: Show that $E(K)$ is a subgroup of $E(\mathbb{C})$. This is the group of K-rational points.

Assume not that K is a Galois extension of K of $\mathbb{Q}(i)$. Let G_K be the Galos group of K over $\mathbb{Q}(i)$. Let $\sigma \in G_K$. If $P = (x, y)$ is point in $E(K)$, then $\sigma(P) = (\sigma(x), \sigma(y)) \in E(K)$. Also, since $i \in K$, $i \cdot (x, y) = (-x, iy) \in E(K)$. Since $\sigma(i) = i$ it is clear that σ and complex multiplication commute!. This is the key observation.

Finding torsion points on E amounts to solving equations $mP = O$. For a fixed m, finding coordinates of P amounts to finding roots of rational polynomials. (Rational since, in this particular case, the curve $2y^2 = x^3 - x$ has rational coefficients) Fix a prime p. For every integer $n = 1, 2, \ldots$, let K_n be the Galois extension of $\mathbb{Q}(i)$ obtained by adjoining the coordinates of p^n-torsion points. Then

$$K_1 \subset K_2 \subset \ldots \subset K = \cup_{n=1}^{\infty} K_n$$

is a tower of Galois extensions. The Galois groups G_n of K_n over $\mathbb{Q}(i)$ form an inverse system,

$$G_1 \leftarrow G_2 \leftarrow \ldots.$$

Let G_K be the limit of this inverse system. The action of G_K on the Tate module $\lim_{\leftarrow} E(p^n) \cong \mathbb{Z}_p^2$ gives an injective homomorphism

$$\varphi : G_K \to \mathrm{GL}(\mathbb{Z}_p).$$

Proposition 0.1. *The group G_K is commutative. More precisely, we have an injective homomorphism*

$$\varphi : G_K \to \mathbb{Z}_p[i]^{\times}.$$

Proof. We know that any $\sigma \in G_K$ commutes with the complex multiplication, i.e. the action of i. Thus $\varphi(G_K)$ is contained in the centralizer of i in $\mathrm{GL}_2(\mathbb{Z}_p)$. Recall, from the last lecture, that i is represented by the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

It is an elementary exercise to check that the centralizer of this matrix is the set of all

$$g = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

where $a, b \in \mathbb{Z}_p$ and $\det(g) = a^2 + b^2 \in \mathbb{Z}_p^\times$. Now $g \mapsto a + bi$ is an isomorphism of the centralizer and $\mathbb{Z}_p[i]^\times$. $\square$

This is great, however, more is true, torsion points generate ray class fields. More precisely, let $I \subseteq A$ be a non-zero ideal. The ray class field corresponding to I is generated by squares of x-coordinates of points P annihilated by I. Let's look at an example $p = 2$. Recall that 2 ramifies, $(2) = (\pi)^2$ in $A = \mathbb{Z}[i]$, where

$$\pi = 1 + i.$$

Let K_m be the extension of $\mathbb{Q}(i)$ obtained by adjoining squares of x-coordinates of points P such that $\pi^m \cdot P = O$. Let G_{K_m} be the Galois group of K_m over $\mathbb{Q}(i)$. Then (note $A^+ = \mu_4$)

$$G_{K_m} \cong (A/\pi^m)^\times/\mu_4.$$

Exercise: Show that $(A/\pi^m)^\times/\mu_4$ is trivial for $m = 1, 2, 3$.

To work out some K_m we need to compute $(x', y') = \pi \cdot (x, y) = (x, y) + (-x, iy)$. Let $y = Ax + B$ be the line through (x, y) and $(-x, iy)$. The slope is

$$A = \frac{(1-i)y}{2x}$$

hence

$$x' = 2A^2 = -i\frac{y^2}{x^2} = \frac{1}{2}\left(\frac{x}{i} + \frac{i}{x}\right)$$

and $y' = -(y + A(x - x'))$. Starting with $P_0 = O$, once can find easily a sequence of points P_m such that $\pi \cdot P_m = P_{m-1}$. For $m = 1, 2, 3, 4$ the square of x-coordinate of P_m is $0, 1, -1, 3 + 2\sqrt{2}$. Hence $K_1 = K_2 = K_3 = \mathbb{Q}(i)$, however, $K_4 = \mathbb{Q}(i, \sqrt{2})$ is a proper extension of $\mathbb{Q}(i)$.

Serge Lang's book, *Elliptic functions*, is a nice introduction to elliptic curves and complex multiplication. In particular, the book contains the construction of the ray class fields for quadratic imaginary fields.