The work of Kolyvagin on the arithmetic of elliptic curves

The main reference is the paper "The work of Kolyvagin on the arithmetic of elliptic curves"(1989) by Karl Rubin.

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N, and fix a modular parametrization

$$\pi : X_0(N) \to E,$$

which we may assume sends the cusp ∞ to 0.

Remark. Here $X_0(N)$ is the usual modular curve over $\mathbb{Q}$ which over $\mathbb{C}$ is obtained by compactifying the quotient $\mathcal{H}/\Gamma_0(N)$ of the complex upper half-plane $\mathcal{H}$ by the group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N|c \right\}.$$

The points of $X_0(N)$ correspond to pairs (A, C) where A is a (generalized) elliptic curve and $\mathbb{Z}/N\mathbb{Z} \cong C \subset A$.

Consider

- an imaginary quadratic field K in which all primes dividing N split,
- an ideal $\mathfrak{a}$ of K such that $\mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$,
- H the Hilbert class field of K,
- $x_H \in X_0(N)(\mathbb{C})$ corresponding to the pair $(\mathbb{C}/\mathcal{O}_K, \mathfrak{a}^{-1}/O_K)$,
- an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$.

Remark.

$$\mathfrak{a}^{-1}/O_K \cong \mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z},$$

which follows from the following

Proposition. Let R be a Dedekind domain. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be non-zero fractional ideals of R with $\mathfrak{a} \supset \mathfrak{b}$. Then there is an isomorphism of R-modules

$$\frac{\mathfrak{a}\mathfrak{c}}{\mathfrak{b}\mathfrak{c}} \cong \frac{\mathfrak{a}}{\mathfrak{b}}.$$

Using the theory of complex multiplication one can show that

$$x_H \in X_0(N)(H).$$

Define

- $y_H = \pi(x_H) \in E(H)$,
- $y_K = \mathrm{tr}_{H/K}(y_H) \in E(K)$,
- $y = y_K - y_K^\tau \in E(K)$,

where τ denotes complex conjugation on K.

Conjecture. $\text{Ш}_{E/\mathbb{Q}}$ is a finite square integer.

Theorem. *(Kolyvagin) Suppose E and y are as above. If y has infinite order in $E(K)$, then $E(\mathbb{Q})$ and $\text{Ш}_{E/\mathbb{Q}}$ are finite.*

Remark. Other versions of this theorem also state that $E(K)$ has rank 1, i.e. the Heegner point $y \in E(K)$ generates a finite-index subgroup in $E(K)$.

Example. Take $E = X_0(11)$ and $K = \mathbb{Q}(\sqrt{-7})$, so $N = 11$, $D = -7$.

```
E = EllipticCurve("11.a2")
K.<a> = QuadraticField(-7)
EK = E.change_ring(K)
E.heegner_point(-7)._trace_numerical_conductor_1()
algdep(E.heegner_point(-7)._trace_numerical_conductor_1()[0],2)
tx = _.roots(K)[0][0]
#tx.parent()
#tx
yk = EK.lift_x(tx);yk;
y=Pk - EK(Pk[0].conjugate(), Pk[1].conjugate()); y;
y.order();
```

We can also use $K = \mathbb{Q}(\sqrt{-35})$.

Theorem. *(Gross and Zagier) With E and y as above, y has infinite order in $E(K)$ if and only if $L(E,1) \neq 0$ and $L'(E,\chi_K,1) \neq 0$, where χ_K is the quadratic character attached to K.*

Remark.

$$L(E,s) = \sum_{n \geq 1} a_n n^{-s}, \quad L(E,s,\chi) = \sum_{n \geq 1} \chi(n) a_n n^{-s}.$$

Definition. (Kronecker symbol) For every quadratic discriminant D one can define the **Kronecker symbol**, denoted by $\chi_D(n)$ or $\left(\frac{D}{n}\right)$. One can define it by requiring:

1. χ_D is completely multiplicative;
2. $\chi_D(0) = 0$ and $\chi_D(1) = 1$;
3. For every odd prime p, $\chi_D(p)$ is equal to the Legendre symbol at p;
4. $$\chi_D(2) = \begin{cases} 0 & \text{if } D \equiv 0 \pmod 2 \\ 1 & \text{if } D \equiv 1 \pmod 8 \\ -1 & \text{if } D \equiv 5 \pmod 8 \end{cases}$$
5. $$\chi_D(-1) = \begin{cases} 1 & \text{if } D > 0 \\ -1 & \text{if } D < 0 \end{cases}$$

Definition. Let K be a quadratic number field of discriminant D. Then we can define χ_D, the **quadratic character attached to** K, using the Kronecker symbol:

$$\chi_K = \chi_D : (\mathbb{Z}/D)^\times \to \{\pm 1\}.$$

Conjecture. (Analytic Conjecture) If E is an elliptic curve and the sign in the functional equation of $L(E,s)$ is $+1$, then there exists at least one imaginary quadratic field K, in which all primes dividing N split, such that $L'(E,\chi_K,1)\neq 0$.

This analytic conjecture, together with the theorems of Kolyvagin and Gross-Zagier, would imply:
For any elliptic curve E, if $L(E,1)\neq 0$ then $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ are finite. (This is known for elliptic curves with CM.)

Notation. For any abelian group A, A_n will denote the n-torsion in A and

$$A_{n^\infty}=\bigcup_i A_{n^i}.$$

We are going to use Galois cohomology. If A is a module for the appropriate Galois group, we will write

- $H^i(L/F,A)$ for $H^i(\mathrm{Gal}(L/F),A)$,
- $H^i(F,A)$ for $H^i(\mathrm{Gal}(\overline{F}/F),A)$,
- $H^i(F,E)$ for $H^i(F,E(\overline{F}))$.

Tools of proof

Fix a prime p and a positive integer n. For any completion $\mathbb{Q}_v$ of $\mathbb{Q}$ we have the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/p^nE(\mathbb{Q}) & \hookrightarrow & H^1(\mathbb{Q},E_{p^n}) & \twoheadrightarrow & H^1(\mathbb{Q},E)_{p^n} & \longrightarrow & 0\\ & & \downarrow & & \downarrow \mathrm{res}_v & & \downarrow \mathrm{res}_v & & \\ 0 & \longrightarrow & E(\mathbb{Q}_v)/p^nE(\mathbb{Q}_v) & \hookrightarrow & H^1(\mathbb{Q}_v,E_{p^n}) & \twoheadrightarrow & H^1(\mathbb{Q}_v,E)_{p^n} & \longrightarrow & 0 \end{array}$$

and we define the Selmer group $S^{(p^n)}$ as

$$S^{(p^n)}=\bigcap_v \mathrm{res}_v^{-1}(\text{image } E(E_v)),$$

while the p^n-torsion in the Tate-Shafarevich group, $Ш_{p^n}$, fits into the short exact sequence

$$0\to E(\mathbb{Q})/p^nE(\mathbb{Q})\hookrightarrow S^{(p^n)}\twoheadrightarrow Ш_{p^n}.$$

To prove that $Ш_{E/\mathbb{Q}}$ is finite, we need to show that

$$Ш_p=0,\quad \text{for almost all primes } p,$$

while for the other primes p we have that

$$Ш_p\subseteq Ш_{p^2}\subseteq Ш_{p^3}\subseteq\cdots$$

stabilizes.
It suffices to prove that

$$S^{(p)} = 0, \quad \text{for almost all primes } p,$$

while for the other primes p we have that

$$S^{(p)} \subseteq S^{(p^2)} \subseteq S^{(p^2)} \subseteq \cdots$$

stabilizes. We show that in this case the group $S^{(p^n)}$ is annihilated by a power of p, which is independent of n.

For $s \in S^{(p^n)}$ write s_v for the inverse image of $\mathrm{res}_v(s)$ in $E(\mathbb{Q}_v)/p^n E(\mathbb{Q}_v)$.

Note that

$$s \in S^{(p^n)} \subset H^1(\mathbb{Q}, E_{p^n}), \quad \mathrm{res}_v(s) \in H^1(\mathbb{Q}_v, E_{p^n}), \quad s_v \in E(\mathbb{Q}_v)/p^n E(\mathbb{Q}_v).$$

Our main ingredient in bounding $\# S^{(p^n)}$ is the following proposition, which is proved using Galois cohomology.

Proposition 1 Suppose ℓ is a prime such that $E(\mathbb{Q}_\ell)_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$, $k \in \mathbb{Z}_{\geq 0}$, and $c_\ell \in H^1(\mathbb{Q}, E)_{p^n}$ satisfies

- $\mathrm{res}_v(c_\ell) = 0, \quad \forall v \neq \ell$
- $\mathrm{res}_\ell(c_\ell)$ has order p^{n-k}.

Then

$$p^k s_\ell = 0, \quad \forall s \in S^{(p^n)}.$$

We have to construct this cohomology class c_ℓ for sufficiently many ℓ, with k bounded and usually equal to 0. Kolyvagin constructs such a c_ℓ using Heegner points.

Notation. Write

- τ for the complex conjugation on $\overline{\mathbb{Q}}$ induced by our embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$
- $[\tau]$ for its conjugacy class in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

If A is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module with $A_2 = A/2A = 0$ (i.e. with trivial 2-torsion and where every element is 2-divisible), the action of τ gives a decomposition

$$A = A^+ \bigoplus A^-.$$

Assume $p \neq 2, 3$ and let D_K be the discriminant of K.

Lemma 2 Suppose the prime ℓ does not divide $pD_K N$, and $r \in \mathbb{Z}_{\geq 0}$, and $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbb{Q}) = [\tau]$ (i.e. Frobenius lifts to conjugation). Let $\tilde{E}$ be the reduction of E modulo ℓ and $a_\ell = \ell + 1 - \#\tilde{E}(\mathbb{F}_\ell)$. Then

(i) $p^r | a_\ell$ and $p^r | \ell + 1$,

(ii) ℓ is inert in K,

(iii)
$$E(\mathbb{Q}_\ell)_{p^r} \cong \tilde{E}(\mathbb{F}_\ell)_{p^r} \cong \mathbb{Z}/p^r\mathbb{Z}, \quad (E(K_\ell)_{p^r})^- \cong (\tilde{E}(\mathbb{F}_{\ell^2})_{p^r})^- \cong \mathbb{Z}/p^r\mathbb{Z}$$

Proof. The characteristic polynomial of Frobenius acting on E_{p^r} is $T^2 - a_\ell T + \ell$, and the characteristic polynomial of τ acting on $E_{p^r} = E(\mathbb{C})_{p^r}$ is $T^2 - 1$. Comparing these polynomials modulo p proves (i). The second assertion holds because $\mathrm{Frob}_\ell(K/\mathbb{Q}) \neq 1$, and the third because

$$E(\mathbb{Q}_l)_{p^r} \cong (E_{p^r})^+ \cong E(\mathbb{R})_{p^r}, \quad \text{and } E(K_\ell)_{p^r} \cong (E_{p^r})^+ \oplus (E_{p^r})^-.$$

□

We need to following setup for John's part of the talk:
Suppose ℓ is a rational prime which remains prime in K and $\ell \nmid N$. Let $\mathcal{O}_\ell$ the the order of conductor ℓ in $\mathcal{O}_K$, and $x_\ell \in X_0(N)(\mathbb{C})$ corresponding to the pair

$$(\mathbb{C}/\mathcal{O}_\ell, (\mathfrak{a} \cap \mathcal{O}_\ell)^{-1}/\mathcal{O}_\ell).$$

The theory of complex multiplication shows that

$$x_\ell \in X_0(N)(K[\ell]),$$

where $K[\ell]$ denotes the ring class field of K modulo ℓ, the abelian extension of K corresponding to the subgroup $K^\times \mathbb{C}^\times \prod_q (\mathcal{O}_\ell \otimes \mathbb{Z}_q)^\times$ of the ideles of K. It follows easily that

- $K[\ell]$ is a cyclic extension of H of degree $(\ell+1)/u_K$, where $u_K = \#(\mathcal{O}_K^\times)/2$,
- $K[\ell]/H$ is totally ramified at ℓ and unramified everywhere else,
- τ acts on $\mathrm{Gal}(K[\ell]/K)$ by -1.

Proposition 3 states what we need to know about Heegner points.