

Lecture Series By Henri Darmon: Finiteness Theorems
In Arithmetic Geometry

Seyfi Turkelli

August 10, 2008

INTRODUCTION

These notes were taken in the lecture series given by Henri Darmon during the summer school in Goettingen, Germany between July 24, 2006 and August 5, 2006. The theme of the lecture series is the basic finiteness theorems in arithmetic geometry. Specifically:

Lecture 1: The Arithmetic of Curves: An Overview

Lecture 2: Faltings' Theorem I

Lecture 3: Faltings' Theorem II

Lecture 4: Modular Curves and Mazur's Theorem

Lecture 5: Fermat Curves and Wiles' Theorem

Lecture 6: Elliptic Curves and Modular Forms I

Lecture 7: Elliptic Curves and Modular Forms II

Lecture 8: Kolyvagin's Theorem: An Introduction

Lecture 9: Kolyvagin Cohomology Classes

Lecture 10: Kolyvagin's Proof of BSD

1. The Arithmetic of Curves: An Overview

In this lecture, we are going to introduce fundamental results on arithmetic of curves. Let's start with introducing the notation. Unless stated otherwise, K will denote a number field, S will denote a finite set of primes and $\mathcal{O} = \mathcal{O}_{K,S}$ will stand for the "localization" of the ring of integers \mathcal{O}_K at primes in S (primes in S are inverted!). And, X will denote a curve. Usually, we will assume that X comes equipped with a model \mathcal{X} over $\text{Spec}\mathcal{O}$.

For a given system of equations X , we can ask the following basic questions:

- Is $X(\mathcal{O}_{K,S})$ finite or infinite? If it is infinite, what is the "density" or "proportion" of rational points in $X(\bar{K})$? If it is finite, give upper bounds in terms of X, S, K .

- In case that it is infinite, understand the following counting function:

$$N(X, B) = \{P \in X(\mathcal{O}_{K,S}) \mid h(P) \leq B\}.$$

- If it is finite then understand the $\max h(P)$ where points P are in $X(\mathcal{O}_{K,S})$.

- Find algorithms to compute (or to find a point in) $X(\mathcal{O}_{K,S})$.

1.1. Euler Characteristic and Rational Points

Assume that X is smooth. Then, $X(\mathbb{C}) = S_g \setminus \{P_1, \dots, P_s\}$. One defines its *Euler characteristic* as the number $\chi(X) = 2 - 2g - s$. Euler characteristic determines the "number" of rational points.

Case 1: $\chi(X) > 0$. Then $(g, s) = (0, 0)$ and we have the following theorem:

Theorem 1.1.1. (TFAE)

- i.* $X(K) \neq \emptyset$.
- ii.* $X \cong \mathbb{P}^1$ over K .
- iii.* $X(K_v)$ for all completions K_v of K .

Proof. (i) \Rightarrow (ii) : Riemann-Roch theorem implies that there exists $\phi \in \mathcal{L}(\infty)$ such that $\phi : X \xrightarrow{\sim} \mathbb{P}^1$ where $\infty \in X(K)$.

(ii) \Rightarrow (iii) : Trivial.

(iii) \Rightarrow (i): Hasse-Minkowski theorem. □

Case 2. $\chi(X) = 0$. Then, we have the *affine case* $(g, s) = (0, 2)$ or the *projective case* $(g, s) = (1, 0)$. Assume that $X(\mathcal{O})$ is not empty. Then, X has the structure of a group scheme over \mathcal{O} and we have the following theorem:

Theorem 1.1.2. $X(\mathcal{O})$ is finitely generated.

Affine case is due the Dirichlet's theorem because $X(\mathcal{O}) = \mathcal{O}^*$. And, the projective case is the Mordell-Weil theorem.

Case 3. $\chi(X) < 0$. In this case, we have important results which will occupy some of the proceeding lectures.

Theorem 1.1.3. $X(\mathcal{O})$ is finite.

Affine case is the Siegel's theorem. And, the projective case is the Falting's theorem, which we will talk on in next two lectures. We have an interesting example in the affine case, namely $X := \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Then

$$\mathcal{O}[X] = \mathcal{O}[x, 1/x, 1/(x-1)] \text{ and } X(\mathcal{O}) = \text{Hom}(\mathcal{O}[X], \mathcal{O}).$$

Therefore, $f(x) \in \mathcal{O}^*$ and $1-f(x) \in \mathcal{O}^*$ for all $f \in \text{Hom}(\mathcal{O}[X], \mathcal{O})$. This is the unit equation and we know...

1.2. Case of Dimension 0

We have some finiteness results in case of dimension 0. First, as always, we have some definitions. An \mathcal{O} -algebra R is called *finite* and *flat* (ff) if R is a finitely generated free \mathcal{O} -module. R is called *etale* if R/P is reduced for all $P \in \text{Spec} \mathcal{O}$. And, define

$$\coprod(\mathcal{O}, d) := \{\text{isomorphism classes of ff etale algebras over } \mathcal{O} \text{ of rank } d\}.$$

Theorem 1.2.4. (Hermite) $\coprod(\mathcal{O}, d)$ is finite.

Proof. Given $R \in \coprod(\mathcal{O}, d)$, $L := R \otimes_{\mathcal{O}} K$ is a K -algebra of dimension d unramified outside of S . One can bound the discriminant of L/K . And, one can conclude by using the Hermite's theorem. \square

1.3. Unramified Coverings

If we have an unramified cover $X \rightarrow Y$, we can extract some information on $Y(\mathcal{O})$ from $X(\mathcal{O})$. A finite morphism $\pi : X \rightarrow Y$ over $\text{Spec} \mathcal{O}$ is called unramified if $\pi : X(\mathbb{C}) \rightarrow Y(\mathbb{C})$ is unramified (for some $\mathcal{O} \hookrightarrow \mathbb{C}$).

Lemma 1.3.5. If $\pi : X \rightarrow Y$ is unramified then there exists a finite extension L/K and a finite set $S' \supseteq S$ such that $\pi(X(\mathcal{O}_{L,S'})) \supseteq Y(\mathcal{O})$.

Proof. If $\pi : X \rightarrow Y$ is unramified then there exists a finite set $S' \supseteq S$ such that $\pi : X \rightarrow Y$ over $\mathcal{O}_{K,S'}$ is etale as a covering of schemes. In particular, for all points $P \in Y(\mathcal{O}_{K,S'})$, $\pi^{-1}(P)$ is an etale $\mathcal{O}_{K,S'}$ -algebra, i.e it is in $\coprod(\mathcal{O}_{K,S'}, d)$. By Hermite's theorem (previous one), there exists finitely many such algebras. Then, take $L := \varinjlim(Frac(R))$ where R runs in $\coprod(\mathcal{O}_{K,S'}, d)$. \square

We say that X is *mordellic* if $X(\mathcal{O}_{L,S'})$ for all finite extensions L/K and finite set S of places of L . By using the lemma, we can prove the following corollary (Indeed, this is a very easy exercise.)

Corollary 1.3.6. *If $\pi : X \rightarrow Y$ is unramified then we have:*

X is mordellic if and only if Y is mordellic.

Exercise 1.3.7. Show that Faltings' theorem implies Siegel's theorem. Work out the case when $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Hint: Use covers!

Exercise 1.3.8. If $\chi(X) = 0$ and X is a group scheme over \mathcal{O} then show that $X(\mathcal{O})/nX(\mathcal{O})$ is finitely generated.

Exercise 1.3.9. Let $X : x^7 + y^7 + z^7 = 0$ and $Y = u^3v + v^3w + w^3u = 0$.

- i. Show that $g(X) = 15$ and $g(Y) = 3$.
- ii. Show that $\pi(x, y, z) = (x^3z, xy^3, z^3y)$ is unramified cover of degree 7.
- iii. Show that if $P \in Y(\mathbb{Q})$ then there exists a $\tilde{P} \in X(\mathbb{Q})$ such that $\pi(\tilde{P}) = P$.

2. Faltings' Theorem I

In this lecture we want to prove Faltings' theorem. Recall that S is a finite set of places of K such that X has a model \mathcal{X} over $\mathcal{O} := \mathcal{O}_{K,S}$.

Theorem 2.0.1. (*Faltings*) *Let X/K be a smooth projective curve of $g \leq 2$. Then $X(K)$ is finite.*

(Here, maybe some history.. Who proved what?.....) We will have a series of reductions and will need the following sets:

$\coprod(\mathcal{O}, M_g) :=$ isomorphism classes of smooth curves of genus g over $Spec(\mathcal{O})$.

$\coprod(\mathcal{O}, A_g) :=$ isomorphism classes of abelian varieties of dimension g over $Spec(\mathcal{O})$.

$\coprod(\mathcal{O}, I_g) :=$ k -isogeny classes of abelian varieties of dimension g over $Spec(\mathcal{O})$.

2.1. First Reduction: The Shafarevich Problem

Recall that in the previous lecture, we proved that $\coprod(\mathcal{O}, d)$ is finite (Hermite's theorem). Now, we have:

Conjecture 2.1.2. (Shafarevich) *All the $\coprod(\mathcal{O}, -)$ are finite.*

Theorem 2.1.3. (Kodaira-Parshin) *Shafarevich conjecture for curves implies Faltings' theorem.*

Proof. The idea is the following: for every point $p \in X(K)$, we will construct a curve X_p which is a finite cover of X , $\pi_p : X_p \rightarrow X$, satisfying

- π_p is ramified at only p ,
- $\text{genus}(X_p) > 1$ and depends only on X (not on p),
- X_p is smooth over $\mathcal{O}[1/2]$.

This construction is called $K - P$ construction and gives us a map $X(K) \rightarrow \coprod(\mathcal{O}[1/2], M_{g'})$. So, if we show that this map has finite fibers then we are done. And, the construction is as follows: We have the following commutative diagram of the fiber product

$$\begin{array}{ccc} \tilde{X} & \longrightarrow & \text{Jac}(X) \\ \pi \downarrow & & \downarrow \times 2 \\ X & \longrightarrow & \text{Jac}(X) \end{array}$$

One can see that $\text{deg}(\pi) = 2^{2g}$. Therefore, for $p \in X$, $\pi^{-1}(p) = \tilde{p} + D$ where D is effective of degree $2^{2g} - 1$ and \tilde{p} is the inverse image of identity in $\text{Jac}(X)$. Now, let

$$\begin{aligned} \tilde{J}_D &= \text{generalized Jacobian of } (\tilde{X}, D) \\ &= \{\text{Rational div. of deg 0 on } \tilde{X}\} / \{div(f) \mid f(D') = 1 \text{ for all } D' \text{ supported on } D\}. \end{aligned}$$

And, we have:

$$1 \rightarrow G_m^{2^{2g}-2} \rightarrow \tilde{J}_D \rightarrow \text{Jac}(\tilde{X}) \rightarrow 1$$

Finally, we get our X_p as the fiber product with following commutative diagram:

$$\begin{array}{ccc} X_p & \longrightarrow & \tilde{J}_p \\ \downarrow & & \downarrow \\ \tilde{X} & \longrightarrow & \tilde{J}_D \end{array}$$

So, we get a map:

$$R_1 : X(K) \rightarrow \text{sha}(\mathcal{O}[1/2], M_{g'})$$

defined by

$$p \longmapsto X_p.$$

R_1 has finite fibers; this immediately follows from the following fact:

Theorem 2.1.4. (De Franchis) *Mor*(Y, X) is finite for any curve Y over \mathbb{C} if $g(X) \geq 2$.

This completes the proof. □

2.2. Second Reduction: Curves to Abelian Varieties

We have the following fact:

Theorem 2.2.5. (Torelli) *A curve is determined by its Jacobian with principal polarization.*

Now, consider the map:

$$R_2 : sha(\mathcal{O}, M_{g'}) \rightarrow sha(\mathcal{O}[1/2], A_{g'})$$

defined by

$$X \longmapsto Jac(X).$$

By Torelli, this map has finite fibers because an abelian variety has only finitely many principal polarizations (Explain why? Define polarization!...). This completes the proof of the reduction.

2.3. Third Reduction: Passing to Isogeny Classes

Consider the following natural map:

$$R_3 : sha(\mathcal{O}, A_{g'}) \rightarrow sha(\mathcal{O}, I_{g'}).$$

As in previous cases, we want to say that R_3 has finite fibers. This is the technical part, and also one of the main ingredients, of Faltings' result:

Theorem 2.3.6. (Faltings' finiteness theorem) *Let A be an abelian variety over K . Then, there are only finitely many isomorphism classes of abelian varieties over K that are K -isogenous to A .*

Key ingredient to prove the theorem is the Faltings height of abelian varieties, which is defined using Arakelov intersection theory. Loosely speaking, it has following very important properties (Due to Faltings):

Lemma 2.3.7. *Height does not change "much" under isogeny.*

and

Lemma 2.3.8. *Abelian varieties of bounded height are finite.*

Clearly, the proof follows immediately from these properties. (State these in a formal way. Sketch their proofs. And, of course, define the height or find some references.)

2.4. Fourth Reduction: Isogeny Classes to l -adic Representations

Given an abelian variety of dimension g over K , we have

$$A[l^n] \cong (\mathbb{Z}/l^n\mathbb{Z})^{2g}$$

with the obvious action of G_K where $A[q]$ denotes the group of q -torsion elements of A . We define *Tate module* by

$$T_l(A) := \varprojlim A[l^n] \cong \mathbb{Z}_l^{2g}$$

and \mathbb{Q}_l -vector space by

$$V_l(A) := T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

$V_l(A)$ is a $2g$ -dimensional \mathbb{Q}_l -vector space with commuting actions of G_K and $\text{End}_K(A)$. Now, we define

$$E = \mathbb{Q}_l\text{-algebra generated by } \text{End}_K(A) \hookrightarrow \text{End}_{\mathbb{Q}_l}(V_l(A))$$

and

$$\Pi = \mathbb{Q}_l\text{-algebra generated by } G_K \hookrightarrow \text{End}_{\mathbb{Q}_l}(V_l(A)).$$

Note that $V_l(A)$ as a bi-representation of E and Π depends only on isogeny class of A . We now have the map

$$R_4 = V_l : \text{sha}(\mathcal{O}, I_{g'}) \rightarrow \mathcal{R}$$

where \mathcal{R} is the set of isomorphism classes of $2g'$ -dimensional *semisimple rational l -adic representations* of G_K which are *unramified outside of $S := \{p|l\} \cup \{p \text{ that are invariant in } \mathcal{O}\}$* . This definition is motivated by the following facts about $V_l(A)$:

Fact 2.4.9.

1. $V_l(A)$ is *semisimple* for E -action i.e. *the category of abelian varieties of up to isogeny is semisimple*,
2. (Weil) $V_l(A)$ is unramified outside S where $S = \{p|l\} \cup \{p \text{ that are invariant in } \mathcal{O}\}$,
3. (Weil) V_l is a rational representation, i.e. *given $v \notin S$, Frob_v acting on $V_l(A)$ has a characteristic polynomial in $\mathbb{Z}[t]$ with roots α_i satisfying*

$$|\alpha_i| \leq \sqrt{N(v)} \text{ and } |\text{Trace}(\text{Frob}_v)| \leq 2g' \sqrt{N(v)},$$

4. (Faltings) $V_l(A)$ is semisimple for Π -action. *This a deeper fact which is a part of the proof.*

So, tomorrow (or in the next section), we will prove Π -semisimplicity of $V_l(A)$ and that R_4 has finite fibers, and that R is finite. Hence, we will be "done".

3. Faltings' Theorem II

Let's recall our reductions:

1. (Kodaira-Parshin) $R_1 : X(K) \rightarrow sha(\mathcal{O}, M_{g'}) + \text{De Francis: } Mor(Y, X) < \infty.$
2. (Jacobian) $R_2 : sha(\mathcal{O}, M_{g'}) \rightarrow sha(\mathcal{O}, A_{g'}) + \text{Torelli} + \text{Finite number of polarization.}$
3. (Natural map) $R_3 : sha(\mathcal{O}, A_{g'}) \rightarrow sha(\mathcal{O}, I_{g'}) + \text{Faltings' finiteness theorem.}$
4. $(V_l) R_4 : sha(\mathcal{O}, I_{g'}) \rightarrow \mathcal{R} := Rep_S(G_K, d)$ where $d = 2g'.$

Now, we want to show:

1. $V_l(A)$ is semisimple for Π -action.
2. R_4 is injective (Tate conjectures).
3. $R = Rep_S(G_K, d)$ is finite.

3.1. Step 1: Semisimplicity

Let's start with an exercise to point out the importance of semisimplicity:

Exercise 3.1.1. Show that if we omit the semisimplicity then $Rep_S(G_K, d)$ can be infinite.

We want to prove that any Π -stable subspace W of $V_l(A)$ has a complement. This is equivalent to the existence of an idempotent $u \in \Pi$ with $u(V_l(A)) = W$ (Then take the $ker(u)$ as the complement of W). So, it suffices to prove:

Theorem 3.1.2. *Let $W \subseteq V_l(A)$ be a Π -stable subspace. Then, there exists a $u \in \Pi$ such that $u(V_l(A)) = W$.*

4. Elliptic Curves and Modular Forms I

Until now, we have seen Faltings' theorem, Mazur's theorem and Merel's theorem on modular curves and Fermat's last theorem. From now on, we will focus on elliptic curves over number fields, denote E/K . As we know, Mordell-Weil theorem states

$$E(K) \cong \mathbb{Z}^r \oplus T$$

where T is the torsion part. We have seen that $|T|$ is bounded by a constant $c_{[K:\mathbb{Q}]}$; we know a lot about the torsion part! On the contrary, variation of the rank of elliptic curves is still a mystery.

4.1. Mordell-Weil Theorem

We want to sketch the proof of Mordell-Weil by using descent. Consider the Kummer exact sequence:

$$1 \longrightarrow E[n] \longrightarrow E(\bar{K}) \xrightarrow{n} E(\bar{K}) \longrightarrow 1$$

where $E[n]$ denotes the n -torsion part. Taking G_K -invariants, we get

$$E(K) \xrightarrow{n} E(K) \xrightarrow{\delta} H^1(G_K, E[n]) \longrightarrow H^1(G_K, E)[n] \longrightarrow 0.$$

Locally, we have the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(G_K, E[n]) & \longrightarrow & H^1(G_K, E)[n] \longrightarrow 0. \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & E(K_v)/nE(K_v) & \xrightarrow{\delta_v} & H^1(G_{K_v}, E_v[n]) & \longrightarrow & H^1(G_{K_v}, E_v)[n] \longrightarrow 0 \end{array}$$

Now, we define the n -Selmer group of E (and denote by) to be

$$Sel_n(E/K) = \ker\{H^1(K, E[n]) \rightarrow \bigoplus_v H^1(K_v, E_v)[n]\}.$$

Exercise 4.1.1. (Weak Mordell-Weil Theorem)

- i. Show that $\delta(P)(\sigma) = \tilde{P}^\sigma - \tilde{P}$ for any $P \in E(K)$ and $\sigma \in G_K$ where $\tilde{P} = P/n \in E(\bar{K})$.
- ii. $Sel_n(E/K) \subseteq H_{n\Delta}^1(K, E[n]) :=$ classes unramified outside of $n\Delta$.
- iii. (Hermite) $H_{n\Delta}^1(K, E[n])$ is finite. Hence, conclude that $E(K)/nE(K)$ is finite.

In order to prove Mordell-Weil, we need the height machine. The idea is as follows: We know that $h(nP) = n^2h(P) + O(1)$ where $O(1)$ is a uniform constant (does not depend on points). In other words, $h(P/n) \sim h(P)/n^2$. But, given an elliptic curve, we have a uniform lower bound on the height of points. Therefore, $E(K)$ cannot be n -divisible. This, together with weak Mordell-Weil, gives us the Mordell-Weil theorem.

Another important group is *Tate-Shafarevich group*, which measures the failure in Hasse principle, defined as

$$sha(E/K) = \ker\{H^1(K, E) \rightarrow \bigoplus_v H^1(K_v, E_v)\}.$$

(Q: why is that \bigoplus_v , not \prod_v ?)

4.2. BSD: The Motivation

One of the most important problems is to determine rank of elliptic curves. Although little is known, we have a heuristical approach and a conjecture, *Birch and Swinnerton-Dyer Conjecture*, on the rank.

Assume $K = \mathbb{Q}$; note that this is not a serious assumption (Why?). Let $N_p = |E(\mathbb{F}_p)|$ and $\Delta = \Delta(E)$ be the discriminant. Birch and Swinnerton-Dyer observed heuristically that

$$\prod_{p < x, p \nmid \Delta} \frac{p}{N_p} \sim c_E(\log x)^r.$$

In other words, let's consider the *Hasse-Weil L-function*

$$L(E, s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid \Delta} (1 - a_p p^{-s})^{-1}$$

where $a_p = p + 1 - N_p$ in the first product, and $a_p = 0$ or $= 1$ depending on the case (supersingular?). Formally (not caring about the convergence), we have

$$L(E, 1) = \prod_{p < x, p \nmid \Delta} \frac{p}{N_p} \sim c_E(\log x)^r.$$

On other hand, one can show:

Exercise 4.2.2. $L(E, s)$ converges $\operatorname{Re}(s) > \frac{3}{2}$. Note that $|a_p| < 2\sqrt{p}$.

This motivates our conjecture:

Conjecture 4.2.3. (BSD) $L(E/K, s)$ has an analytic continuation and $\operatorname{ord}_{s=1} L(E/K, s) = \operatorname{rank}(E(K))$.

4.3. BSD: What we know

Basicly, all we know:

Theorem 4.3.4. (Hecke, Wiles, BCDT) $L(E/\mathbb{Q}, s)$ has an analytic continuation.

Theorem 4.3.5. (Gross-Zagier, Kolyvagin) If $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$ then BSD is true.

The key to these theorems lies in the connection to modular forms:

Theorem 4.3.6. (Wiles, BCDT) If E/\mathbb{Q} is an elliptic curve of conductor N , then there exists a normalized eigenform f of weight 2 on $\Gamma_0(N)$ such that E is isogenous to A_f where A_f is a quotient of $J_0(N)$ associated to f by Eichler-Shimura construction.

This has very important consequences. First of all, we have:

$$L(E/\mathbb{Q}, s) = L(A_f, s) = L(f, s) = \sum_{n=1}^{\infty} a_n(f) n^{-s}$$

and, consequently, we have the analytic continuation

$$2\pi\Gamma(s)L(E, s) = \int_0^{i\infty} f(y)\left(\frac{y}{i}\right)^s \frac{dy}{y}.$$

Secondly, there is a morphism

$$\Phi : X_0(N) \rightarrow J_0(N) \rightarrow A_f \rightarrow E$$

which is called the *modular parametrization* attached to E . For simplicity, assume that $A_f = E$ and that N is square-free. We compute Φ as follows: Let w_E be the Neron differential. We know that

$$\Phi^*(w_E) = cw_f = 2\pi i f(z) dz = \sum_{n=1}^{\infty} a_n q^n \frac{dq}{q}$$

where $c = \pm 1$ or ± 2 (??). Thus, we get an analytic formula for $\Phi(\tau)$, $\tau \in \mathcal{H}$ (upper half plane):

$$\int_0^{\Phi(\tau)} w_E = \int_0^{\tau} cw_f = \sum_{n=1}^{\infty} \frac{a_n}{n} q^n$$

(note that we have explicit formulas for a_n). We will find rational points on $X_0(N)$, push them down by Φ and get rational points on E .

4.4. CM Points and Heegner Points

Let $K \subseteq \mathbb{C}$ be an imaginary quadratic field, $K = \mathbb{Q}\sqrt{-D}$ and $D > 0$. We have: $X_0(N) \cong \Gamma_0(N) \backslash \mathcal{H}$. This isomorphism is not algebraic but:

Theorem 4.4.7. *If $\tau \in \mathcal{H} \cap K$ then $\Phi(\tau) \in E(K^{ab})$.*

In the next chapter, we will see systems of CM-points. That is, for certain well-chosen K and τ , we can obtain a point $Q_1 \in X_0(N)(H)$ where H is the Hilbert class field of K . And, $P_K := \text{Tr}_K^H(\Phi(Q_1)) \in E(K)$.

We will also see two important theorems:

Theorem 4.4.8. *(Gross-Zagier) $L'(E/K, s) = c \cdot \hat{h}(P_K)$ where c is some explicit constant and \hat{h} is the Neron-Tate height.*

Theorem 4.4.9. *(Kolyvagin) If P_K has infinite order then $E(K)/\langle P_K \rangle$ is finite.*

5. Elliptic Curves and Modular Forms II

Recall that we have an elliptic curve E/\mathbb{Q} with conductor N and modular representation $\Phi : X_0(N) \rightarrow E$. Today, we will see CM-points on $X_0(N)$ and Heegner points. $K = \mathbb{Q}\sqrt{-D}$ will denote an imaginary quadratic field. We will assume

Heegner hypothesis: all primes $l \mid N$ split in K/\mathbb{Q} .

Let A be an elliptic curve with $\text{End}(A) \cong \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-D}}{2}]$. Heegner hypothesis implies that there exists an ideal $\mathcal{N} \subseteq \mathcal{O}_K$ with $\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

As we have seen, we have a rational point $Q_1(A, A[N]) \in X_0(N)(H)$ with $P_1 = \Phi(Q_1) \in E(H)$ and $P_K = \text{Tr}_K^H(P_1) = \sum_{\sigma \in G(H/K)} P_1^\sigma$ where H is the Hilbert class field of K .