# HILBERT'S TENTH PROBLEM OVER RINGS OF INTEGERS OF NUMBER FIELDS

DAVID BROWN

Abstract. This is a term paper for Thomas Scanlon's Math 229, Model Theory, at UC Berkeley, Fall 2006. The goal of this survey is to understand Bjorn Poonen's theorem about elliptic curves and Hilbert's Tenth problem over rings of integers of number fields and to record and exposit a few ideas which may be useful in an attack with Poonen's theorem as a starting point.

## Contents



*Date*: December 17, 2006.

## 1. Introduction

Hilbert's Tenth Problem asks, for a given ring $R$, does there exist an algorithim with input a polynomial $f \in R[x_1, \ldots, x_n]$ and output YES if $f$ has a solution in $R$ and NO otherwise. The answer for $R = \mathbb{Z}$ is a rather famous no, and various progress has been made for other rings (for a nice survey see [?PoonExpo]).

The current plan for this survey is to understand Bjorn Poonen's theorem about elliptic curves and Hilbert's Tenth over rings of integers of number fields, and then to record and exposit many lines of attack with this starting point.

## 2. Elliptic Curves and Hilbert's Tenth Problem

In the Aim workshop Extentions of Hilbert's Tenth problems [?AIM] Bjorn Poonen asks the following

**Question 2.1.** (Poonen) Is it true that for all number fields $K$, there exists a variety (scheme of finite type) over $\mathbb{Z}$ such that

(1) $X(\mathbb{Z})$ is infinite.
(2) $X(\mathcal{O}_K) = X(\mathbb{Z})$.

This question is motivated by results such as the following.

**Theorem 2.2.** *(Poonen)* [?PoonenEllH10] *Let $F \subset K$ be number fields. If there exists an elliptic curve $E$ over $F$ such that* rk $E(K) =$ rk $E(F) = 1$*, then there exists a diophantine definition of $\mathcal{O}_F$ over $\mathcal{O}_K$. (In particular, a negative solution to Hilbert's Tenth problem over $\mathcal{O}_F$ would imply a negative solution over $\mathcal{O}_K$).*

This theorem has since been refined:

**Theorem 2.3.** *(Poonen, Shlapentokh)* [?ellShlap] *Let $F \subset K$ be number fields. If there exists an elliptic curve $E$ over $F$ such that* rk $E(K) =$ rk $E(F) > 0$*, then there exists a diophantine definition of $\mathcal{O}_F$ over $\mathcal{O}_K$.*

Furthermore, a nice alternative is the following

**Theorem 2.4.** *(Cornelissen, Pheidas, Zahidi)* [?DivAmple] *The Diophantine problem for the ring of integers $\mathcal{O}_K$ of a number field $K$ has a negative answer if the following exist:*

(i) *an elliptic curve defined over $K$ of rank one over $K$.*
(ii) *a division-ample set $A \subset \mathcal{O}_K$.*

*Furthermore, condition two is satisfied if Question (2.1) is true for a commutative group variety $G$ over $\mathbb{Z}$ such that $G(\mathcal{O}_K)$ is finitely generated.*

Using $p-$adic $L$-series, it has been shown that the condition of (2.2) has been satisfied for infinitely many $K$ [?PoonExpo] not covered by the above three conditions. However, Karl Rubin noted that, by pairity considerations, there are fields $K$ such that any elliptic curve of rank 1 over $\mathbb{Q}$ has rank even rank over $K$. See (6.4) below for a proof of this.

2.1. **Results.** Let $K$ be one of the following classes of number fields:

- Totally real [?Den]
- Quadratic extension of a totally real field [?DL]
- A field with exactly one pair of complex conjugate embeddings [?Phe], [?Shl2].

Then Hilbert's Tenth problem is undecidable over $\mathcal{O}_K$. In particular, HTP is undecidable over multi-quadratic extension and any abelian extension.

## 3. Lines of Attack

What would it take to prove that Hilbert's Tenth Problem has a negative solution for *all* rings of integers of number fields? Shlapentokh concludes in a talk [?SG2] that it suffices to prove any of the following "SPR (Stable Positive Rank)" conjectures:

(1) For any number field extension $M/K$ there exists an elliptic curve $E$ defined over $K$ such that rank $E(M) =$ rank $E(K) > 0$.
(1') For any number field extension $M/\mathbb{Q}$ there exists an elliptic curve $E$ defined over $\mathbb{Q}$ such that rank $E(M) =$ rank $E(\mathbb{Q}) > 0$.
(2) For any cyclic number field extension $M/K$ there exists an elliptic curve $E$ defined over $K$ such that rank $E(M) =$ rank $E(K) > 0$.
(3) For any Kummer extension of number fields $M/K$ there exists an elliptic curve $E$ defined over $K$ such that rank $E(M) =$ rank $E(K) > 0$.

Of course, we can replace "exists an elliptic curve ..." with any statement equivalent to "HTP is true over $\mathcal{O}_K$ iff HTP is true over $\mathcal{O}_L$".

(1) and (1') are pretty clear. For (2), just note that it suffices to consider $M/Q$ galois in case (1'), and then use a minimality argument. For (3), also note that the degree of $K(\mu_n)$ over $K$ is less than $n$.

## 4. Key Notion: Definability

A negative answer to HTP over $\mathbb{Q}$ would imply a negative answer over $\mathbb{Z}$ (just clear denominators). More work is required to deduce a negative answer to HTP over $\mathbb{Q}$ from one over $\mathbb{Z}$. Here we explore many of the relevant ideas for the opposite deduction.

### 4.1. Diophantine Definablitliy.

**Definition 4.1.** We call a subset $S \subset R^n$ *diophantine* over $R$ if there exists a polynomial $f \in R[x_1, \ldots, x_n, y_1, \ldots, y_n]$ such that $S$ is the projection of the zero set of $f$ onto the first $n$ coordinates. Equivalently, the set of $n$-tuples $\bar{a} = (a_1, \ldots, a_n) \in R^n$ such that $f(\bar{a}, \bar{y}) = 0$ has a solution in $R$ is exactly $S$.

In this definition we could take multiple polynomials as well. The important property is that $S$ is a projection of an algebraic set.

To deduce a negative answer to HTP over $\mathbb{Q}$ is would suffice to have a *diophantine definition* of $\mathbb{Z}$ inside $\mathbb{Q}$. Indeed, suppose we could find a polynomial $f(t, \bar{x}) \in \mathbb{Q}[t, \bar{x}]$ such that $f(a, \bar{b}) = 0$ implies $a \in \mathbb{Z}$. Suppose further that HTP over $\mathbb{Q}$ has a positive solution, i.e.

there is an algorithm to decide if any given polynomial with rational coefficients has a rational solution. Let $g \in \mathbb{Z}[x_1, \ldots, x_r]$. Then we can first decide whether $g$ has a rational solution, and then decide if each rational number if an integer. Specifically, $g$ has an integer solution iff

$$g(x_1, \ldots, x_r)^2 + f(x_1, \bar{y_1})^2 + \ldots + f(x_r, \bar{y_r})^2$$

has a solution.

4.2. **Diophantine Models.** A weaker condition than diophantine definablilty is the following:

**Definition 4.2.** Let $\phi : \mathbb{Z} \to R$ be an injection such that $\phi(\mathbb{Z})$ is diophantine. We say that $\phi$ is a diophantine model of $\mathbb{Z}$ in $R$ if the graphs of addition and multiplication are diophantine over $R$.

*Remark* 4.3. If $R$ has a diophantine model of $\mathbb{Z}$, HTP has a negative solution over $R$

*Remark* 4.4. One can find an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q}) \cong \mathbb{Z}$. This is a good candidate for a diophantine model, since the graph addition on $E$ is diophantine.

*Remark* 4.5. Equivalently, $\phi$ is a diophantine model if it is *recursive* – for any input $a$, the value $\phi(a)$ is computable.

4.3. **Mazur's Conjecture on the Topology of Rational Points.** No one has been able to find a diophantine definition of $\mathbb{Z}$ in $\mathbb{Q}$, and perhaps this is because of the following reasonable

**Conjecture 4.6.** (Mazur [?Maz] [?MazUpdate]) Let $V$ be a variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ has at most finitely many connected components.

Mazur's conjecture has the following

**Corollary 4.7.** *There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.*

*Proof.* The proof can be summarized by this picture:

$$\begin{array}{ccccc} X(\mathbb{Q}) & \subset & \overline{X(\mathbb{Q})} & \subset & \mathbb{R}^n \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z} & = & \overline{\mathbb{Z}} & \subset & \mathbb{R} \end{array}$$

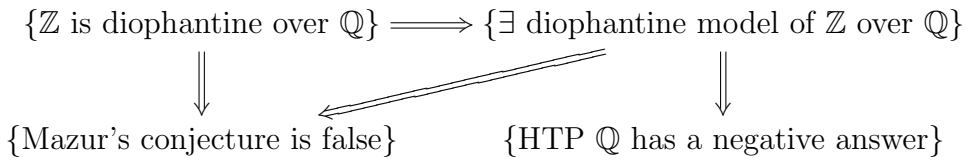
□

A little deeper lies the

**Theorem 4.8.** *(Cornelissen, Zahidi [?CZ]) Mazur's conjecture implies that there is no diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.*

So we might have to try harder. In this paper they also prove that Mazur's conjecture is false for rational function fields over finite fields of constants.

In summary, we borrow the following picture from [?PoonExpo]:




4.4. **Ellitpic Curves and Definability.** The above results (2.1) are proved using Pell's equation (i.e. arithmetic of tori) to explicitly give a diophantine definition of $\mathbb{Z}$ inside of $\mathcal{O}_F$, and there is some hope for using elliptic curves over $\mathbb{Q}$ to give a model of $\mathbb{Z}$ inside of $\mathbb{Q}$. Here we say a few words about the proof of Poonen's theorem (2.2).

*Outline of Proof*: Let $F \subset K$ be a finite extension of number fields.

- Construct a set $S$ diophantine over $\mathcal{O}_K$ such that
$$\{m^2 : m \in \mathbb{Z}_{\geq 1}\} \subset S \subset \mathcal{O}_F \subset \mathcal{O}_K.$$
- Set $S_1 := \{s - s' : s, s' \in S\} \supset \{$ odd integers at least 3 $\}$ (since $(m+1)^2 - m^2 = 2m + 1$).
- $S_2 := S_1 \cup \{4 - s : s \in S\} \supset \{$ all odd integers$\}$.
- $S_3 := S_2 \cup \{s + 1 : s \in S_2\} \supset \mathbb{Z}$.
- $S_4 := \{a_1\beta_1 + \ldots + a_b\beta_b : a_i \in S_3\}$ where $\beta_1, \ldots, \beta_b$ are a $\mathbb{Z}$-basis for $\mathcal{O}_F$. Then $S_4 \supset \mathcal{O}_F$.
- Each $S_i \subset \mathcal{O}_F$, so $S_4 = \mathcal{O}_F$.
- Finally, each $S_i$ is also diophantine over $\mathcal{O}_K$ (it is enought to note that the graphs of the operations used in the definitions are diophantine), and we conclude that $\mathcal{O}_F$ is diophantine over $\mathcal{O}_K$.

The construction of $S$ uses little more than the standard theory of canonical heights and formal groups on elliptic curves. The height $\hat{h}(P)$ of a point roughly measures the extent to which the denominator of a point is divisible by various primes; a key observation is that $\hat{h}(mP) = m^2\hat{h}(P)$.

*Remark* 4.9. By the same trick, to find a diophantine definition of $\mathbb{Z}$ in $\mathbb{Q}$ it would suffice to find a set $S$ diophantine in $\mathbb{Q}$ such that
$$S_0 := \{m^2 : m \in \mathbb{Z}_{\geq 1}\} \subset S \subset \mathbb{Z} \subset \mathbb{Q}.$$

Waring's problem for polynomials (see [?VinoWaring] for example) says that for any integer valued polynomial $f$ with GCD 1 (i.e. no integer $n$ divides $f(m)$ for every $m$), there is a $G(f)$ such that, for every $m$, there exist integers $x_i$ such that
$$m = \sum_{i=0}^{G(f)} f(x_i).$$

It would be enough to have $\{f(m) : m \in \mathbb{Z}\} \subset S$ for any polynomial $f$. Note however that this would still contradict Mazur's conjecture...

## 5. L-Functions

Given an elliptic curve $E/K$, there is an analytic function attatched to $E$, called its *L-function* (see [?RSRanks] for definitions and a nice survey). We have the following

**Conjecture 5.1.** (BSD)

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rk}(E/K).$$

Let $F \subset K$ be a Galois extension with Galois group $G$. Then the L-function of $E/K$ decomposes as

$$L(E/K, s) = \prod_{\chi \in \mathrm{rep}\, G} L(E/F, \chi, s)^d$$

where $\chi$ runs over all the representations of $G$ and $d$ is the dimension of $\chi$. Even more generally, let $F \subset K \subset L$ where $L$ is the Galois closure of $K$, with $G = \mathrm{Gal}(L/F)$. Then $G$ acts on finite set of embeddings of $K$ into an algebraic closure of $F$. Call this representation $\rho$; $\rho$ is also the $\mathrm{Gal}(F^{\mathrm{alg}}/F)$ representation induced by the trivial $\mathrm{Gal}(F^{\mathrm{alg}}/K)$ representaiton (or equivalently the $\mathrm{Gal}(L/F)$ representation induced by the trivial $\mathrm{Gal}(L/K)$ representaiton). Then we have

$$L(E/K, s) = L(E/F, \rho, s).$$

In the case $K = L$, this is just the regular representation of $G$ on itself and we get the first decomposition.

**Example 5.2.** Let $K = \mathbb{Q}(\sqrt{d})$. Then $G = \mathbb{Z}/2\mathbb{Z}$, and

$$L(E/K, s) = L(E \otimes \rho, s) = L(E \otimes tr, s) L(E \otimes \chi, s) = L(E/\mathbb{Q}, s) L(E_d/\mathbb{Q}, s).$$

**Example 5.3.** Let $K = \mathbb{Q}(\sqrt{d_1}, \cdots, \sqrt{d_r})$ (with $r$ chosen minimally). Then $G = (\mathbb{Z}/2\mathbb{Z})^r$. $G$ is abelian, so all representations are 1-dimensional, and here they decompose into quadratic characters.

$$L(E/K, s) = L(E \otimes \rho, s) = \prod_{\chi \in \mathrm{Hom}(G, \mathbb{C}^\times)} L(E \otimes \chi, s) = \prod_d L(E_d/\mathbb{Q}, s)$$

where $d$ runs over all products of distinct $d_i$ (including the empty product).

**Example 5.4.** Let $F \subset K$ with abelian Galois group $G$. Then

$$L(E/K, s) = L(E/F, \rho, s) = \prod_{\chi \in \mathrm{Hom}(G, \mathbb{C}^\times)} L(E/F, \chi, s).$$

If $G$ has prime order (see (3) for relevance), this decomposition is particularly nice, as, for $\chi \neq tr$,

$$L(E/F, \chi, 1) = 0 \Leftrightarrow L(E/F, \chi^n, 1) = 0.$$

Assuming BSD, this says that for the rank of an elliptic curve $E/F$ to not change in a cyclic extension of prime degree $p$, we only need $L(E/F, \chi, 1) \neq 0$ for *one* (non-trivial) $\chi$. Random

matrix theory predicts [?DFK][?DFK2] that if $p \geq 7$ and $F = \mathbb{Q}$, then for a given ellitpic curve only finitely many twisted L-functions $L(E/\mathbb{Q}, \chi, s)$ vanish at $s = 1$. For $p = 3, 5$, the density is expected to be 0 and there are some positive results for $p = 3$. For $p = 2$ this is Goldfeld's conjecture (9.2) and the expected density is 1/2.

*Remark* 5.5. For a general number field $K$, it is unknown what heuristic one gets about the vanishing of $L$-functions by cyclic abelian twists. The problem is that there is no nice expression for the central values for $L$-functions of elliptic curves over larger fields as there is for $\mathbb{Q}$, and without that there is no way to apply the random matrix machine [?Kemail].

*Remark* 5.6. While the connection between L-functions and random matrix theory is still speculative, in the case of elliptic curves over function fields, the connection has been proved [?KS] [?KS2]. What makes the result tenable in this case is that the local zeta functions are polynomials.

*Remark* 5.7. When writing equalities of L-functions we are implicitly assuming (the open conjecture) that these L-functions, which *a priori* converge for $\mathrm{Re}(s) > \frac{3}{2}$, have analytic continuations to the complex plane. Otherwise it doesn't even make sense to talk about the order of vanishing at $s = 1$. By the work on Wiles et all [?BCDT] on the modularity of elliptic curves over $\mathbb{Q}$, when $F = \mathbb{Q}$ and $\chi$ is one dimensional, these L-functions have analytic continuations.

*Remark* 5.8. (Functional Equation) Similarly, it is conjectured that every L-function has a functional equation. For an Artin representation $\rho$ (in particular the representations considered above), letting $\Lambda(s, E/K, \rho) = f(s, E/K, \rho)L(E/K, \rho, s)$, where $f$ is an analyitic "fudge factor", we get a functional equation

$$\Lambda(s, E/K, \rho) = \epsilon(E/K, \rho)\Lambda(2 - s, E/K, \overline{\rho}).$$

So for example, When $\rho$ is trivial we have

$$f = \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Gamma(s)$$

and

$$\Lambda(S, E/K) = w_{E/K}\Lambda(2 - s, E/K).$$

When $\rho = \chi_d$ is a quadratic character and $K = \mathbb{Q}$, we have

$$f = \left(\frac{|d|\sqrt{N_E}}{2\pi}\right)^s \Gamma(s)$$

$$\Lambda(s, E, \chi_d) = w_E\, \chi_d(-N_E)\Lambda(2 - s, E, \chi_d).$$

There are suprisingly complete results such as [?root] for computing epsilon factors, even for non-abelian twists.

## 6. Partial results: Twisting

Maybe if we assume conjectures about L-functions and ellitpic curves we can prove something. A prototype result where we assume a weak form of BSD is the following:

**Proposition 6.1.** *Assume BSD and let $K = Q(\sqrt{d})$. Then there exists an elliptic curve $E/\mathbb{Q}$ with $\mathrm{rk}(E/\mathbb{Q}) = \mathrm{rk}(E/K) > 0$.*

We need the following

**Lemma 6.2.** *Let $N_{E'}$ be the conductor of $E$. Then $N_{E_d}|d^2 N_E$, with equality if $d$ is coprime to $N_E$. Also, $w(E_d) = \chi_d(-N_E)w(E)$ for $d$ coprime to the conductor, and $\chi_d = (\frac{d}{\cdot})$.*

The first part of the lemma follows from considering potential reduction types, and the second from the functional equation (5.8).

*Proof.* Assume $d$ is squarefree, and choose $E/\mathbb{Q}$ such that $E$ has multiplicative reduction at the primes dividing $d$ (easy to do with, say, the family of elliptic curves paramaterized by $X_0(5)$ in [?FisherThesis]). The conductors satisfy $N_{E_d} = d \cdot N_E$ (just check the minimal Weierstrauss equations). We note the following lemma from [?Kisil]:

**Lemma 6.3.** *(Kisilevsky) Let $E$ and $E'$ be elliptic curves over $\mathbb{Q}$. Suppose that for every $d$,*

$$L(E_d, 1) = 0 \Leftrightarrow L(E'_d, 1) = 0.$$

*Then $N_E$ and $N'_E$ differ by a square.*

By Kisilevsky's lemma, there is a $d'$ such that

$$L(E_{d'}, 1) = 0 \text{ and } L(E_{dd'}, 1) \neq 0.$$

By Kolyvagin's theorem [?Koly], we know that $\mathrm{rk}(E_{d'}, \mathbb{Q}) = 0$, and conclude that $\mathrm{rk}(E_{dd'}, \mathbb{Q}) = \mathrm{rk}(E_{dd'}, K)$, and if we assume $BSD$ then, as $L(E_{dd'}, 1) = 0$, then the rank is positive. □

Similarly, assuming BSD we get the following negative result.

**Proposition 6.4.** *There exists a field $K$ such that, for every elliptic curve $E/\mathbb{Q}$ of rank 1, $\mathrm{rk}(E, K) > 1$.*

Thus Poonen's first criterion (2.2) will not always apply. In fact, the proof is little stronger; it says that any elliptic curve of odd rank over $\mathbb{Q}$ will have even rank over $K$.

*Proof.* Suppose $4d$ is prime to $N_E$. Then the root numbers are related by $W_{E_d} = \chi_d(-N_E)W_E$, where $\chi_d = \left(\frac{\Delta(\mathbb{Q}(\sqrt{d}))}{\cdot}\right)$ Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, with $p, q$ primes, and (for good measure) not 2 or 3. Suppose also that $p$ and $q$ are coprime to $N_E$. Then

$$w_{E/K} = w_{E/\mathbb{Q}} w_{E_p/\mathbb{Q}} w_{E_q/\mathbb{Q}} w_{E_{pq}/\mathbb{Q}} = \chi_p(-N_E)\chi_q(-N_E)\chi_{pq}(-N_E)w^4_{E/\mathbb{Q}} = 1$$

and so the rank of $E$ over $K$ is even. The cases where $p$ or $q$ divide $N_E$ are similar but require a more careful analysis of the root numbers and are omitted. □

**Question 6.5.** Given a field $K$, can you always find an elliptic curve $E$ over $K$ with rank 0? It is rumored that if you assume most conjectures in number theory that the answer is yes, but I have yet to confirm this.

## 7. The theory behind Descent on Elliptic Curves

The goal of the remainder of this paper is to record as many situations where there is some hope of control over the rank jump of an elliptic curve over an extension of number fields. Here we review the theory of descent and set notation. In the following section, we will record a few situations where we can explictly write down the Selmer groups for a given family of elliptic curves.

An effective way of understanding the rank is to study the cohomology of the sequence

$$0 \to E(K)[n] \xrightarrow{\times n} E(K) \to E(K) \to 0.$$

Letting $G = \mathrm{Gal}(\bar{K}/K)$, we take $G$ invariants of this sequence to get the long exact sequence of cohomology groups

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

and we shorten this sequence to

$$0 \to E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \to H^1(K, E)[n] \to 0.$$

Knowing the finite group $E(K)/nE(K)$ is really no different than knowing $E(K)$ – indeed, if we know generators for $E(K)/nE(K)$ then the theory of heights allows us to effectively find genrators for $E(K)$. Similarly, if we know $\#E(K)/nE(K)$ and $\#E[n](K)$ (which is easy to compute), then computing $r$ is a quick exercise in group theory. For example, if $E(K)$ is torsion free, or more generally the order of the torsion is prime to $n$, then $n^r = \#E(K)/nE(K)$. Similarly, if say $n = p$ is prime and $E(K)$ has $p-$torsion, then $p^r = \#E(K)/pE(K) - p$ (since the $p$-torsion contributes).

7.1. **Selmer Groups.** Unfortunately, $H^1(K, E[n])$, while often computable, is not finite. The idea now is to use local information to isolate the image of $E(K)/nE(K)$ under the connecting map $\delta$. As we will see the image will live in a finite, computable group.

We proceed as follows. For each prime $\mathfrak{p}$ of $K$ (including the infinite primes), replace $K$ by $K_\mathfrak{p}$ in each of the sequences of the last section. By functorality, we get

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0\ . \\
 & & \downarrow & & \downarrow{\scriptstyle \prod_\mathfrak{p} \mathrm{res}_\mathfrak{p}} & \overset{\alpha}{\searrow} & \downarrow{\scriptstyle \prod_\mathfrak{p} \mathrm{res}_\mathfrak{p}} & & \\
0 & \longrightarrow & \prod_\mathfrak{p} E(K_\mathfrak{p})/nE(K_\mathfrak{p}) & \xrightarrow{\prod_\mathfrak{p} \delta_\mathfrak{p}} & \prod_\mathfrak{p} H^1(K_\mathfrak{p}, E[n]) & \longrightarrow & \prod_\mathfrak{p} H^1(K_\mathfrak{p}, E)[n] & \longrightarrow & 0
\end{array}$$

A trivial observation is that any $K$-rational point of $E$ is also a $K_\mathfrak{p}$-rational point, and so if $\xi \in \mathrm{im}\ \delta$ then $\mathrm{res}(\xi) \in \mathrm{im}\ \delta_\mathfrak{p}$ for every $\mathfrak{p}$. Thus, we define the **n-Selmer Group** as

$$\mathrm{Sel}^{(n)}(E, K) := \{\xi \in H^1(K, E[n]) \big| \mathrm{res}(\xi) \in \mathrm{im}\ \delta_\mathfrak{p} \text{ for every } \mathfrak{p}\} = \ker \alpha.$$

We define another interesting group by

$$Ш(E,K) := \ker\left(H^1(K,E) \to \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}},E)\right).$$

The upshot is that $\mathrm{Sel}^{(n)}(E,K)$ is finite and computable, and as noted above we have an inclusion, which extends to an exact sequence

$$0 \to E(K)/nE(K) \xrightarrow{\delta} \mathrm{Sel}^{(n)}(E,K) \to Ш(E,K)[n] \to 0.$$

7.2. **Descent by Isogeny and Cassel's Formula.** For an isogeny $\phi$ and its dual $\psi$, we get the following formula:

$$\frac{\#\mathrm{Sel}^{(\phi)}}{\#\mathrm{Sel}^{(\psi)}} = \frac{\#E(K)[\phi]\cdot\Omega_{E'}\cdot\prod_q c_{E',q}}{\#E'(K)[\phi]\cdot\Omega_E\cdot\prod_q c_{E,q}},$$

where $c_{E,v} = \#\Phi_v(k_v)$ (the number of components of the reduction mod $v$ of $E$) is the *Tamagawa Number* of $E$ at $v$ and $\Omega_E$ is the real period.

Let $d$ be the degree of $\phi$ and $S$ be the set of places such that $c_v$ is prime to $d$. Then $\mathrm{Sel}^{(\phi)} \subset H^1(K,E[n];S)$; the latter is finite and computable. In our formulas, the latter group will usually be computed in terms of the $S$-unit group and ray-class groups of $K$.

Then we can recover the $p$-Selmer group and a bound on the rank, as

$$\#\mathrm{Sel}^{(p)} \leq \#\mathrm{Sel}^{(\phi)}\cdot\#\mathrm{Sel}^{(\psi)}$$

(with the possibility of a slight improvement). See [?SSpd] for a great survey of explicit descent.

## 8. Descent Formulas

In light of theorem (2.2), we record as many explict formulas for descent on elliptic curves over number fields as possible.

8.1. **Descent Via $n$-Isogeny When $E$ has a n-torsion point.** Tom Fisher works out in his thesis and subsequent papers a crisp theory of 5-descent by isogeny on the family of ellitpic curves with a 5-torsion point parameterized by $X_1(5)$. In the following $p$ will usually denote 5 or 7.

8.1.1. *A Parameter for $X_1(n)$.* Let $\lambda \in K$ and $n = 3, 4, 5$ or 7. Following [?FisherThesis] and [?FisherCTP], we construct the following point on $X_1(n)(K)$:

$$0 \to \mathbb{Z}/n\mathbb{Z} \to D_\lambda \xrightarrow{\psi} C_\lambda \to 0,$$

where $D_\lambda$ has equation

$$\begin{array}{lrcl} n=3 & y^2+xy+y & = & x^3 \\ n=4 & y^2+xy+y & = & x^3+x^2 \\ n=5 & y^2+(1-\lambda)xy-y & = & x^3-x^2 \\ n=7 & y^2+(1+\lambda-\lambda^2)xy+(\lambda^2-\lambda^3)y & = & x^3(\lambda^2-\lambda^3)x^2 \end{array}$$

with $[n](0,0)=\infty$, and $C_\lambda$ has equation

$$\begin{array}{lrcl} n=3 & y^2+xy+\lambda y & = & x^3-5\lambda x-\lambda(7\lambda+1) \\ n=4 & y^2+xy+\lambda y & = & x^3+\lambda x^2-5(\lambda(\lambda+1)x+\lambda(3\lambda^2-12\lambda-1) \\ n=5 & y^2+(1-\lambda)xy-\lambda y & = & x^3-\lambda x^2-5tx-b_2t-7w \\ n=7 & y^2+(1+\lambda-\lambda^2)xy+(\lambda^2-\lambda^3)y & = & x^3+(\lambda^2-\lambda^3)x^2-5tx-b_2t-7w \end{array}$$

where

$$n=5\ \begin{cases} b_2 = \lambda^2-6\lambda+1 \\ t = \lambda(\lambda^2+2\lambda-1) \\ w = \lambda^2(2\lambda^2+\lambda+1) \end{cases}$$

$$n=7\ \begin{cases} b_2 = \lambda^4-6\lambda^3+3\lambda^2+2\lambda+1 \\ t = \lambda(\lambda-1)(\lambda^2-\lambda+1)(\lambda^3+2\lambda^2-5\lambda+1) \\ w = \lambda^2(\lambda-1)^2(2\lambda^6-2\lambda^5+\lambda^4-8\lambda^3+15\lambda^2-9\lambda+2 \end{cases}$$

8.2. **Discriminants and reduction types.** These curves have discriminant

$$\begin{array}{lrcl} p=5 & \Delta(C_\lambda) & = & \lambda(\lambda^2-11\lambda-1)^5 \\ & \Delta(D_\lambda) & = & \lambda^5(\lambda^2-11\lambda-1). \\ p=7 & \Delta(C_\lambda) & = & \lambda(\lambda-1)(\lambda^3-8\lambda^2-5\lambda+1)^7 \\ & \Delta(D_\lambda) & = & \lambda^7(\lambda-1)^7(\lambda^3-8\lambda^2-5\lambda+1) \end{array}$$

For $n=5$ or 7, $D_\lambda$ is semi-stable (at any prime of additive reduction, $E(K_\mathfrak{p})[p])=0$ for $p=5,7$). In Lemma 1.4 of his thesis, Fisher says much more. Let $\beta(\lambda)=\lambda^2-11\lambda-1$ (resp. $\lambda^3-8\lambda^2-5\lambda+1$) for $p=5$ (resp. 7).

**Lemma 8.1.** *Let $K$ be a number field and let $\mathfrak{p}$ be a prime with $\mathfrak{p}\not|n$. Then for $\lambda\in K_\mathfrak{p}$ with $ord_\mathfrak{p}(\lambda)\geq 0$ the Weierstrass equation for $D_\lambda$ is minimal and the reduction types are as follows:*

(i) *If $\lambda=0(mod\ \mathfrak{p})$ (resp. $\lambda(\lambda-1)=0(mod\ \mathfrak{p})$, then $D_\lambda$ has split multiplicative reduction.*

(ii) *If $\beta(\lambda)=0(mod\ \mathfrak{p})$, then $D_\lambda$ has multiplicative reduction, and the reduction is split if and only if $N\mathfrak{p}=1$ mod $n$.*

(iii) *In the remaining cases $D_\lambda$ has good reduction.*

Furthermore, for $\mathfrak{p}|n$, cases $i$ and $iii$ are the same, but in case $ii$ the Weierstrauss equation is no longer minimal and it may not be possible to treat all number fields at once. Also, a quick check shows that $D_\lambda \cong D_{-1/\lambda}$ (resp. $D_{(\lambda-1)/\lambda)}$), so we can always use this lemma to check reduction type at a particular prime.

The upshot of this is that it is easy to calculate root numbers of curves in these families

8.2.1. *Local Images.* Here, for a prime $\mathfrak{p}$, we calculate the image of the local connecting map $\delta_{pp}$. With this data, the Selmer groups become easy to compute.

*$m = 3$.* If $\mathrm{ord}_\mathfrak{p}(\lambda) \geq 0$ then

$$\text{im } \delta_\mathfrak{p} = \begin{cases} K_\mathfrak{p}^*/K_\mathfrak{p}^{*3} & \text{if } \mathrm{ord}_\mathfrak{p}(\lambda) > 0 \\ \mathcal{O}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^{*3} & \text{if } \lambda(27\lambda - 1) \neq 0 (\text{mod } \mathfrak{p}) \\ 1 & \text{if } 27\lambda - 1 = 0 (\text{mod } \mathfrak{p}) \end{cases}$$

If $\mathrm{ord}_\mathfrak{p}(\lambda) < 0$ and $\mathfrak{p} \not| 3$ then

$$\text{im } \delta_\mathfrak{p} = \begin{cases} \mathcal{O}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^{*3} & \text{if } 3|\mathrm{ord}_\mathfrak{p}(\lambda) \\ < \lambda > & \text{otherwise} \end{cases}$$

*$m = 4$.* If $\mathrm{ord}_\mathfrak{p}(\lambda) \geq 0$ then

$$\text{im } \delta_\mathfrak{p} = \begin{cases} K_\mathfrak{p}^*/K_\mathfrak{p}^{*4} & \text{if } \mathrm{ord}_\mathfrak{p}(\lambda) > 0 \\ \mathcal{O}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^{*4} & \text{if } \lambda(16\lambda - 1) \neq 0 (\text{mod } \mathfrak{p}) \\ 1 \text{ or } < -4 > & \text{if } 16\lambda - 1 = 0 (\text{mod } \mathfrak{p}) \end{cases}$$

If $\mathrm{ord}_\mathfrak{p}(\lambda) < 0$ and $\mathfrak{p} \not| 2$ then

$$\text{im } \delta_\mathfrak{p} = \begin{cases} K_\mathfrak{p}^{*2}/K_\mathfrak{p}^{*4} & \text{if } \lambda \in K_\mathfrak{p}^{*2} \\ < \lambda > & \text{if } \mathrm{ord}_\mathfrak{p}(\lambda) \text{ is odd} \\ < \lambda, \mathcal{O}_\mathfrak{p}^{*2} > & \text{otherwise} \end{cases}$$

Moreover, at a real place $v$, im $\delta_v$ is trivial if and only if $16\lambda - 1 > 0$.

*$n = 5, 7$.* If $\mathrm{ord}_\mathfrak{p}(\lambda) \geq 0$ then

$$\text{im } \delta_\mathfrak{p} = \begin{cases} K_\mathfrak{p}^*/K_\mathfrak{p}^{*n} & \text{if } \mathrm{ord}_\mathfrak{p}(\lambda) > 0 \\ \mathcal{O}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^{*n} & \text{if } \lambda\beta(\lambda) \neq 0 (\text{mod } \mathfrak{p}) \\ 1 & \text{if } \beta(\lambda) = 0 (\text{mod } \mathfrak{p}) \text{ and } \mathfrak{p} \not| n. \end{cases}$$

8.2.2. *Selmer Groups.* We write out the computation for $n = 5, 7$ and integral $\lambda$ (the other cases are similar). For the isogeny $\phi : D_\lambda \to C_\lambda$, the Selmer group is

$$\mathrm{Sel}^{(\phi)} = \{\theta \in K^*/K^{*n} : n | v_{\mathfrak{p}}(\theta) \text{ if } v_{\mathfrak{p}}(\lambda) = 0 \text{ and } K_{\mathfrak{p}}^{*n} = K_{\mathfrak{p}}^* \text{ if } v_{\mathfrak{p}}(\beta(\lambda)) > 0\}$$

The last condition is the same as $K(\theta)$ is split at $\mathfrak{p}$. The dual Selmer group can be computed using Tate local duality, but it is easier to use Cassel's formula (7.2) to just get the order.

8.3. **Descent Via p-Isogeny for other p.** $X_0(n)$ has genus 0 iff $n \in \{1, \ldots, 10, 12, 13, 16, 18, 25\}$; $X_1(n)$ has genus 0 iff $n \in \{1, \ldots, 10, 12\}$. It should be interesting to write out the descent formulas for these cases.

## 9. Appendix: Statements of results and conjectures used

Here I record for completeness various results and conjectures from number theory that are used or mentioned.

9.1. **Schinzel's Hypothesis.** Let $f_1(x), \ldots f_r(x) \in \mathbb{Z}[x]$ be irreducible polynomials such that for every prime $p$, there is an $n \in Z$ such that $p \not| \prod_i f_i(n)$. Then Schinzel's Hypothesis [?Sch] is the

**Conjecture 9.1.** There exist infinitely many $n \in \mathbb{Z}$ such that $f_1(n), \ldots, f_r(n)$ are simultaneously prime.

The only known case is when $r = 1$ and $f$ is linear.

9.2. **Goldfeld's Conjecture.** Let $E$ be an ellitpic curve over $\mathbb{Q}$. One would like to study the quadratic twists $E_d$ and make a statement like "the rank of $E_d$ is usually either 0 or 1". Goldfeld made this precise in [?Gold]:

**Conjecture 9.2.**

$$\sum_{|D| \leq X} \mathrm{ord}_{s=1} L_f(1, \chi) \sim \frac{1}{2} X$$

and the slightly stronger conjectures (are they equivalent?):

**Conjecture 9.3.** $\sum_{|D| \leq X} 1 \sim \sum'_{|D| \leq X} 1 \sim \frac{1}{2} X$

Where all sums are taken over $D$ squarefree, the first sum taken over $D$ such that $L(E_D, 1) \neq 0$, the second sum taken over $L(E_D, s)$ has order one at $s = 1$.

9.3. **Finiteness of Sha.** The Birch Swinnerton Dyer conjecture, responsible for fueling much beautiful mathematics, says

**Conjecture 9.4.** (Birch,Swinnerton-Dyer)

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} = \frac{|Ш| \cdot \Omega \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E_{\mathrm{tors}}(\mathbb{Q})|^2}$$

where $r = \mathrm{rk}(E/\mathbb{Q})$.

At various points we want to use the following:

**Conjecture 9.5.** (Pairty) Let $E$ be an elliptic curve over $\mathbb{Q}$, and let $w_{E/\mathbb{Q}} = \pm 1$ be the sign of the functional equation. The Birch-Swinnerton Dyer conjecture predicts that then $\mathrm{rk}(E/\mathbb{Q})$ is even if $w_{E/\mathbb{Q}} = 1$ and odd otherwise.

The assumption $Ш < \infty$ (or the $p$-part of Ш is finite for even one prime) implies the pairty conjecture.


## Acknowledgements



Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
*E-mail address*: browndа@math.berkeley.edu