Chabauty and the Mordell–Weil Sieve

Samir SIKSEK [1],
Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
e-mail: samir.siksek@gmail.com

Abstract. These notes are based on lectures given at the "Arithmetic of Hyperelliptic Curves" workshop, Ohrid, Macedonia, 28 August–5 September 2014. They offer a brief (if somewhat imprecise) sketch of various methods for computing the set of rational points on a curve, focusing on Chabauty and the Mordell–Weil sieve.

Keywords. curves, rational points, Chabauty, Coleman, Mordell–Weil sieve

1. 💣 Warning

These notes are intended to give the reader with only modest knowledge of algebraic geometry a feel for some methods for computing the set of rational points on a curve of genus ≥ 2, especially Chabauty and the Mordell–Weil sieve. As we are trying to do this assuming as little background as possible, **some of the mathematics will be only approximately correct**. We will often avoid giving precise definitions and omit all proofs. Instead we offer examples that should guide the reader's intuition.

Acknowledgment. I would like to thank the workshop organizers for their wonderful hospitality, which made our stay in Ohrid particularly enjoyable and productive.

2. A review of some basic algebraic geometry I

I heartily recommend the first three chapters of Silverman's book [21] as an introduction to basic algebraic geometry with a view to arithmetic. In what follows we introduce some basic notions that the reader will find in a more organized and thorough fashion in Silverman's book.

We think of varieties as defined by systems of polynomial equations in affine or projective space. An **affine variety** $V \subset \mathbb{A}^n$ defined over a field k is given by a system of polynomial equations

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \quad \vdots \qquad\qquad\qquad f_i \in k[x_1, \ldots, x_n]. \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

[1]The author is supported by an EPSRC Leadership Fellowship EP/G007268/1, and EPSRC *LMF: L-Functions and Modular Forms* Programme Grant EP/K034383/1.

For $L \supseteq k$, the set of L-points of V is

$$V(L) = \{(a_1, \ldots, a_n) \in L^n \,:\, f_i(a_1, \ldots, a_n) = 0 \text{ for } i = 1, \ldots, m\}.$$

A **projective variety** $V \subseteq \mathbb{P}^n$ defined over k is given by a system of polynomial equations

$$V : \begin{cases} f_1(x_0, \ldots, x_n) = 0, \\ \qquad \vdots \\ f_m(x_0, \ldots, x_n) = 0, \end{cases} \qquad f_i \in k[x_0, \ldots, x_n] \text{ are homogeneous.}$$

For $L \supseteq k$, the set of L-points of V is

$$V(L) = \{(a_0, \ldots, a_n) \in L^{n+1} \setminus \{0\} \,:\, f_i(a_0, \ldots, a_n) = 0 \text{ for } i = 1, \ldots, m\} / \sim,$$

where $(a_0, \ldots, a_n) \sim (b_0, \ldots, a_n)$ if there is some $\lambda \in L^*$ such that $\lambda a_i = b_i$ for $i = 0, \ldots, n$. A variety $V \subset \mathbb{P}^n$ is covered by $n+1$ **affine patches**:

$$V \cap \{x_i = 1\} \qquad i = 0, 1, \ldots, n.$$

3. Local Methods

We're interested in understanding $V(\mathbb{Q})$ for varieties defined over $\mathbb{Q}$. More generally, if k is a number field, we're interested in $V(k)$ for varieties defined over k.

Local methods make use of the fact that $\mathbb{Q} \subset \mathbb{R}$ and $\mathbb{Q} \subset \mathbb{Q}_p$ for all primes p. It is convenient to write $\mathbb{R} = \mathbb{Q}_\infty$. Then $V(\mathbb{Q}) \subseteq V(\mathbb{Q}_p)$ for all p (including ∞). So,

$$V(\mathbb{Q}_p) = \emptyset \implies V(\mathbb{Q}) = \emptyset.$$

Example 3.1

$$V : x^2 + y^2 + z^2 = 0, \qquad V \subset \mathbb{P}^2. \tag{1}$$

Note $V(\mathbb{R}) = \emptyset$, so $V(\mathbb{Q}) = \emptyset$. But also, $V(\mathbb{Q}_2) = \emptyset$.

Let V be a variety defined over $\mathbb{Q}$. We say that V **has points everywhere locally** if $V(\mathbb{Q}_p) \neq \emptyset$ for all p (including ∞). We make the following trivial observation:

$$V(\mathbb{Q}) \neq \emptyset \implies V \text{ has points everywhere locally.}$$

It is interesting to ask if the converse of this statement is true. The following theorem says that this is true for quadrics. A *quadric* in $\mathbb{P}^n$ is a variety that is defined by a single homogeneous quadratic equation. For example, (1) is a quadratic in $\mathbb{P}^2$.

Theorem 1 (Hasse–Minkowski) *Let $V \subset \mathbb{P}^n$ be a quadric ($n \geq 3$), defined over $\mathbb{Q}$. Then the following are equivalent:*

- *V has points everywhere locally;*
- *$V(\mathbb{Q}) \neq \emptyset$ (V has global points).*

We say, quadrics **satisfy the Hasse principle**.

Fact 3.2 *For varieties V defined over $\mathbb{Q}$ (or a number field), there is an algorithm to decide if V has points everywhere locally.*

For more on local methods, see Stoll's lectures.

4. A review of some basic algebraic geometry II

4.1. Dimension

We classify varieties by **dimension**, a non-negative integer: $0, 1, 2, \ldots$.

Fact 4.1 *A variety $V \subset \mathbb{A}^n$ or $\mathbb{P}^n$, defined by a single polynomial equation $V : f = 0$, where f is a non-constant polynomial, has dimension $n-1$.*

Example 4.2

$$V_1 \subset \mathbb{A}^1, \qquad V_1 : x^3 + x + 1 = 0 \quad \textit{has dimension } 0.$$

$$V_2 \subset \mathbb{A}^2, \qquad V_2 : y^2 = x^6 + 1, \quad \textit{has dimension } 1.$$

$$V_3 \subset \mathbb{P}^2, \qquad V_3 : x^3 + y^3 + z^3 = 0, \quad \textit{has dimension } 1.$$

$$V_4 \subset \mathbb{P}^3, \qquad V_4 : x^3 + y^3 + z^3 + w^3 = 0, \qquad \textit{has dimension } 2.$$

Varieties of dimension $1, 2, 3, \ldots$ are called **curves, surfaces, threefolds,** etc.

4.2. Smoothness

Let V be an affine variety $V \subset \mathbb{A}^n$ of dimension d, defined over a field k, and given by a system of polynomial equations

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \qquad \vdots \qquad\qquad\qquad f_i \in k[x_1, \ldots, x_n]. \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

We say that $P \in V(\overline{k})$ is **smooth** if

$$\operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i=1,\ldots,m,\ j=1,\ldots,n} = n - d,$$

otherwise we say that P is **singular**. We say that V is **smooth** or **non-singular** if it is smooth at all points $P \in V(\overline{k})$.

If $V \subset \mathbb{P}^n$, we say that V is **smooth** if all the affine patches $V \cap \{x_i = 1\}$ are smooth.

Example 4.3 *Let $C \subset \mathbb{A}^2$ be given by*

$$C : y^2 = f(x)$$

where f is a non-constant polynomial. Then $P = (a,b) \in C$ is singular iff the 1×2 matrix $(2a \quad -f'(b))$ is zero. So

$$2a = 0, \qquad a^2 = f(b), \qquad f'(b) = 0.$$

If $\mathrm{char}(k) \neq 2$, then $f(b) = f'(b) = 0$. Such $b \in \overline{k}$ exists if and only if f is not squarefree, or equivalently if $\mathrm{disc}(f) = 0$ where $\mathrm{disc}(f)$ is the discriminant of f. Thus C has a singular point if and only if $\mathrm{disc}(f) = 0$, and C is smooth iff $\mathrm{disc}(f) \neq 0$.

*A smooth curve of the form $y^2 = f(x)$ with $\deg(f) \geq 5$ is called a **hyperelliptic curve**.*

Example 4.4 *Let $V \subset \mathbb{P}^n$ (defined over k) be given by*

$$V : f(x_0, \ldots, x_n) = 0,$$

*where $f \neq 0$ is homogeneous. Then V is **singular** if and only if there is $P \in V(\overline{k})$ such that*

$$\frac{\partial f}{\partial x_1}(P) = \cdots = \frac{\partial f}{\partial x_n}(P) = 0.$$

4.3. Curves

We will restrict our attention to curves.

Definition 4.5 *By a **curve** C over a field k, we mean a smooth, projective, absolutely irreducible (or geometrically irreducible), 1-dimensional k-variety.*

Given a curve $C/\mathbb{Q}$, our goal is to understand $C(\mathbb{Q})$.

Example 4.6 *The following example illustrates the notion of **reducibility**. Consider the variety $V \subset \mathbb{A}^2$ over $\mathbb{Q}$ given by the equation*

$$V : x^6 - 1 = y^2 + 2y.$$

Can rewrite as

$$V : (y + 1 - x^3)(y + 1 + x^3) = 0.$$

So

$$V = V_1 \cup V_2$$

where

$$V_1 : y + 1 - x^3 = 0, \qquad V_2 : y + 1 + x^3 = 0.$$

Note V is reducible *(we can write it as the union of two proper subvarieties), but V_1 and V_2 are* irreducible. *To understand $V(\mathbb{Q})$ enough to understand $V_1(\mathbb{Q})$ and $V_2(\mathbb{Q})$.*

Example 4.7 *The following example illustrates the notion of* ***absolute reducibility****. Consider the variety $V \subset \mathbb{A}^2$ over $\mathbb{Q}$ given by the equation*

$$V : 2x^6 - 1 = y^2 + 2y.$$

V is irreducible, but absolutely reducible *(can be written as a union of proper subvarieties defined over a field extension) since*

$$V_{\overline{\mathbb{Q}}} = \{y + 1 + \sqrt{2}x^3 = 0\} \cup \{y + 1 - \sqrt{2}x^3 = 0\}.$$

If $(x, y) \in V(\mathbb{Q})$ then

$$y + 1 + \sqrt{2}x^3 = y + 1 - \sqrt{2}x^3 = 0.$$

In other words

$$y = -1, \qquad x = 0.$$

So $V(\mathbb{Q}) = \{(0, -1)\}$.

Moral: To understand rational points on varieties, it is enough to understand rational on absolutely irreducible varieties.

4.4. Function Fields

Let $V \subset \mathbb{A}^n$ be an absolutely irreducible affine variety defined over k by the equations

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases} \qquad f_i \in k[x_1, \ldots, x_n].$$

The **affine coordinate ring** of V is given by

$$k[V] = k[x_1, \ldots, x_n]/(f_1, \ldots, f_m).$$

The **function field** $k(V)$ of V is the field of fractions of $k[V]$. If $V \subset \mathbb{P}^n$ then its function field is the function field of any affine patch (the function fields of any two affine patches will be isomorphic).

Example 4.8

$$k[\mathbb{A}^n] = k[x_1, \ldots, x_n], \qquad k(\mathbb{A}^n) = k(x_1, \ldots, x_n),$$

$$k(\mathbb{P}^n) = k(\mathbb{P}^n \cap \{x_0 = 1\}) = k(x_1, \ldots, x_n).$$

Example 4.9 *It is easy to calculate the function field of a hyperelliptic curve.*

$$C : y^2 = f(x) \qquad f \in k[x] \backslash k, \qquad \operatorname{disc}(f) \neq 0.$$

Namely

$$k[C] = k[x, y]/(y^2 - f(x)), \qquad k(C) = k(x)\left(\sqrt{f(x)}\right).$$

Example 4.10 *This very basic example illustrates the problems we can have with reducible varieties. Let*

$$V \subset \mathbb{A}^2, \qquad V : x_1 x_2 = 0,$$

defined over a field k. The affine coordinate ring of V is $k[V] = k[x_1, x_2]/(x_1 x_2)$. Note that x_1, x_2 are zero divisors in $k[V]$ so it isn't an integral domain. It does not have a field of fractions and so there is no function field. In the definition of function field above we restricted ourself to absolutely irreducible varieties, so we will not run into this problem, even if we extend our base field k.

4.5. Genus

We classify curves by **genus**. This is a geometric invariant that is a non-negative integer: $0, 1, 2, \ldots$.

Example 4.11 *If*

$$C/k : F(x, y, z) = 0, \qquad C \subset \mathbb{P}^2$$

is smooth, where $F \in k[x, y, z]$ is homogeneous of degree n, then C has genus $(n-1)(n-2)/2$.

Example 4.12 *Let*

$$C/k : y^2 = f(x), \qquad C \subset \mathbb{A}^2 \qquad (f \in k[x] \text{ non-constant}).$$

If C is smooth (by Example 4.3 this is equivalent to $\operatorname{disc}(f) \neq 0$) and $\deg(f) = d$ then

$$\text{genus}(C) = \begin{cases} (d-1)/2 & d \text{ odd} \\ (d-2)/2 & d \text{ even.} \end{cases}$$

Recall we defined a hyperelliptic curve to be of the form $y^2 = f(x)$ where $\operatorname{disc}(f) \neq 0$ and $d \geq 5$. Thus the genus of a hyperelliptic curve is ≥ 2.

5. Curves of Genus 0

The following theorem is a standard consequence of the Riemann–Roch Theorem.

Theorem 2 *Let C be a curve of genus 0 defined over k. Then C is isomorphic (over k) to a smooth plane curve of degree 2 (i.e. a conic). Moreover, if $C(k) \neq \emptyset$ then C is isomorphic over k to $\mathbb{P}^1$.*

A conic is just a quadric in $\mathbb{P}^2$. Thus the Hasse–Minkowski Theorem (Theorem 1) is applicable to curves of genus 0, and give us the following.

Theorem 3 (The Hasse Principle) *Let $C/\mathbb{Q}$ be a curve of genus 0. The following are equivalent:*

(a) $C(\mathbb{Q}) \neq \emptyset$;
(b) $C(\mathbb{R}) \neq \emptyset$ *and* $C(\mathbb{Q}_p) \neq \emptyset$ *for all primes* p.

Note that condition (b) says that C has points everywhere locally. It appears that to check (b) we need to check infinitely many conditions. However we stated previously that there is an algorithm for checking if a variety has points everywhere locally. This is illustrated by the following strengthening of Theorem 3.

Theorem 4 (Legendre, Hasse) *Let*

$$C : ax^2 + by^2 + cz^2 = 0, \qquad a, b, c \text{ non-zero, squarefree integers.} \tag{2}$$

This is a smooth curve of genus 0. The following are equivalent:

(a) $C(\mathbb{Q}) \neq \emptyset$;
(b) $C(\mathbb{R}) \neq \emptyset$ *and* $C(\mathbb{Q}_p) \neq \emptyset$ *for all primes* p.
(c) $C(\mathbb{R}) \neq \emptyset$ *and* $C(\mathbb{Q}_p) \neq \emptyset$ *for all primes* $p \mid 2abc$.

Any conic in $\mathbb{P}^2$ defined over $\mathbb{Q}$ can be written in the form (2) by completing squares, and appropriately scaling the equation and unknowns. Note that to test that C has points everywhere locally (condition (b)), we need only check the existence of local points for a certain finite set of primes (condition (c)).

6. Curves of Genus 1

This section is included for completeness. For more details on curves of genus 1 see the lectures by Jan-Steffen Müller and by Michael Stoll in the same volume.

Theorem 5 *If C is a curve of genus 1 over a field k and $P_0 \in C(k)$, then C is isomorphic over k to a Weierstrass elliptic curve*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad \subset \mathbb{P}^2,$$

where the isomorphism sends P_0 to $(0:1:0)$.

Theorem 6 (The Mordell–Weil Theorem) *If $k = \mathbb{Q}$ or a number field, then $C(k)$ is a finitely generated abelian group with P_0 as the zero element.*

Currently, for curves $C/\mathbb{Q}$ of genus 1,

(i) there is no known algorithm for deciding if $C(\mathbb{Q}) \neq \emptyset$;
(ii) there is no known algorithm for computing a Mordell–Weil basis for $C(\mathbb{Q})$ if it is non-empty.

But there is a descent strategy that often succeeds with (i) and (ii).

6.1. Failure of the Hasse Principle in Genus 1

Example 6.1 *The following example is due to Selmer. Let $C \subset \mathbb{P}^2$ be given by*

$$C : 3x^3 + 4y^3 + 5z^3 = 0.$$

This is a curve of genus 1 *defined over $\mathbb{Q}$. Then*

1. *$C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ (C has points everywhere locally);*
2. *$C(\mathbb{Q}) = \emptyset$ (C has no global points).*

In other words, C is a counterexample to the Hasse principle.

Exercise 6.2 *Show that $X^4 - 17 = 2Y^2$ (also a curve of genus* 1*) is a counterexample to the Hasse principle.*

7. Genus ≥ 2

The most important theorem in the subject is the following.

Theorem 7 (Faltings, 1983) *Let C be a curve of genus ≥ 2 over $\mathbb{Q}$. Then $C(\mathbb{Q})$ is finite.*

Whilst the statement of Faltings' Theorem is simple and elegant, the only known proofs are deep (probably the easiest to read is the one found in the book of Hindry and Silverman [14]). The known proofs are ineffective: they do not give an algorithm for computing the rational points. Currently, for curves $C/\mathbb{Q}$ of genus ≥ 2,

1. There is no known algorithm for computing $C(\mathbb{Q})$.
2. There is no known algorithm for deciding if $C(\mathbb{Q}) \neq \emptyset$.

But there is a bag of tricks that can be used to show that $C(\mathbb{Q})$ is empty, or determine $C(\mathbb{Q})$ if it is non-empty. These include:

(i) Local Methods.
(ii) Quotients.
(iii) Descent.
(iv) Chabauty.
(v) Mordell–Weil sieve.

The purpose of these lectures is to get a feel for each of these methods and see it applied to a particular example. We've already talked about local methods in Section 3. Quotients and descent are dealt with in detail in Stoll's lectures. but for completeness we will go through them quickly, before covering Chabauty and the Mordell–Weil sieve.

8. Quotients

Let C be a curve over a field k. A quotient is curve D/k with a non-constant morphism

$$\phi : C \to D$$

also defined over k.

Lemma 8.1 (Trivial Observation) *$\phi(C(k)) \subseteq D(k)$. If we know $D(k)$ and it is finite, we can compute $C(k)$.*

Example 8.2 *Let*

$$C : Y^2 = AX^6 + BX^4 + CX^2 + D, \qquad A, B, C, D \in \mathbb{Z},$$

and suppose $\operatorname{disc}(AX^6 + BX^4 + CX^2 + D) \neq 0$*, so C has genus* 2*. Let*

$$E_1 : y^2 = Ax^3 + Bx^2 + Cx + D, \qquad E_2 : y^2 = Dx^3 + Cx^2 + Bx + A.$$

Then E_1, E_2 are elliptic curves over $\mathbb{Q}$. We have non-constant morphisms

$$\phi_1 : C \to E_1, \qquad (X, Y) \mapsto (X^2, Y),$$

and

$$\phi_2 : C \to E_2, \qquad (X, Y) \mapsto \left(\frac{1}{X^2}, \frac{Y}{X^3}\right).$$

If the ranks of either E_i is 0 *we can determine $E_i(\mathbb{Q})$ (which is finite) and so can determine $C(\mathbb{Q})$.*

As a special case, consider the genus 2 *curve $C/\mathbb{Q}$ given by*

$$C : Y^2 = 13X^6 - 1.$$

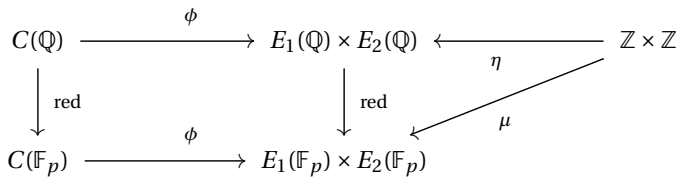
It is easy to show that C has points everywhere locally. Take $E : y^2 = x^3 + 13$ and $\phi : C \to E$ to be given by $(X, Y) \mapsto (-1/X^2, Y/X^3)$. Now $E(\mathbb{Q}) = \{\infty\}$. So $C(\mathbb{Q}) \subseteq \phi^{-1}(\infty) = \{(0, i), (0, -i)\}$. Thus $C(\mathbb{Q}) = \emptyset$.

Example 8.3 *The following example will help prepare the reader for introduction of the Mordell–Weil sieve. Let*

$$C/\mathbb{Q} : Y^2 = 11X^6 - 19.$$

Again, C has points everywhere locally. In the notation of Example 8.2, $E_1(\mathbb{Q}) \cong \mathbb{Z}$ and $E_2(\mathbb{Q}) \cong \mathbb{Z}$.

Let p be a prime of good reduction for C. Note the commutative diagram:



Here $\phi = (\phi_1, \phi_2)$ where the ϕ_i are as in Example 8.2; red *denotes reduction modulo p; η is given by $\eta(m,n) = (mP_1, nP_2)$ where P_1, P_2 are generators for $E_1(\mathbb{Q})$, $E_2(\mathbb{Q})$ respectively; and finally $\mu = \text{red} \circ \eta$. Observe that*

$$(\text{red} \circ \phi)(C(\mathbb{Q})) \subset \phi(C(\mathbb{F}_p)) \cap \mu(\mathbb{Z} \times \mathbb{Z}).$$

Exercise: *Use this with $p = 7$ to show that $C(\mathbb{Q}) = \emptyset$.*

9. Descent

Let's dive straight into an example of descent.

Example 9.1 *We will study the rational points on the genus 2 curve.*

$$C : Y^2 = (X^2 + X + 1)(X^4 + 7), \tag{3}$$

which has no obvious quotients. Write

$$X = \frac{x}{z}, \qquad Y = \frac{y}{z^3}, \qquad x, y, z \in \mathbb{Z}, \qquad \gcd(x,z) = 1.$$

So

$$y^2 = (x^2 + xz + z^2)(x^4 + 7z^4). \tag{4}$$

Note we have 2 extra points on this model $(x : y : z) = (1 : \pm 1 : 0)$ which we think of as points are infinity on (3). We think of (4) as an equation for C in $\mathbb{P}(1,3,1)$. Does C have any other rational points?

We will return to Example 9.1 soon. We need the following elementary lemma.

Lemma 9.2 *If x, y are coprime non-zero integers and $xy = z^n$ where z is also an integer, $n \geq 1$, then there exists x_1, $y_1 \in \mathbb{Z}$ such that $x = \pm x_1^n$ and $y = \pm y_1^n$.*

The proof is an easy exercise using unique factorization; the same is true of the following generalization.

Lemma 9.3 *Let S be a set of primes. Let x, y are non-zero integers such that $xy = z^n$ where z is also an integer and $n \geq 1$. If x, y are coprime outside S then there exists x_1, $y_1 \in \mathbb{Z}$ such that $x = ax_1^n$ and $y = by_1^n$, where all the prime factors of a, b belong to S.*

9.1. Resultants

A good reference on resultants is [9, Chapter 16].

Lemma 9.4 *Let $f, g \in \mathbb{Z}[x]$, coprime. Then there exists $R = R(f,g) \in \mathbb{Z}$, $R \neq 0$ (R is called the **resultant**), and polynomials $a, b \in \mathbb{Z}[x]$ such that*

$$a(x)f(x) + b(x)g(x) = R.$$

In particular, if $\alpha \in \mathbb{Z}$, then $\gcd(f(\alpha), g(\alpha)) \mid R$.

It is easy to compute the resultant R; it is just a determinant involving the coefficients of f and g (see [9]).

Lemma 9.5 *Let $F(x,y)$, $G(x,y)$ be coprime homogeneous polynomials $\in \mathbb{Z}[x,y]$. Let $f = F(x,1)$ and $g = G(x,1)$, and define $R = R(F,G) = R(f,g)$ (the resultant of F and G). If α, $\beta \in \mathbb{Z}$ are coprime, then*

$$\gcd(F(\alpha,\beta), G(\alpha,\beta)) \mid R.$$

Proof: We know that $a(x)f(x) + b(x)g(x) = R$. Substitute $x = \alpha/\beta$ and homogenize, to obtain

$$A(\alpha,\beta)F(\alpha,\beta) + B(\alpha,\beta)G(\alpha,\beta) = R\beta^m$$

for some m. It turns out that also,

$$A'(\alpha,\beta)F(\alpha,\beta) + B'(\alpha,\beta)G(\alpha,\beta) = R\alpha^n.$$

So

$$\gcd(F(\alpha,\beta), G(\alpha,\beta)) \mid \gcd(R\beta^m, R\alpha^n) = R.$$

□

Example 9.6 *We return to Example 9.1. The resultant of the two factors on the right hand-side of* (4) *is* 43, *so*

$$\gcd(x^2 + xz + z^2, x^4 + 7z^4) = 1 \text{ or } 43.$$

In particular, the two factors are coprime outside $S = \{43\}$. Hence

$$x^2 + xz + z^2 = ay_1^2, \qquad x^4 + 7z^4 = ay_2^2 \qquad \text{where } a = \pm 1 \text{ or } a = \pm 43.$$

So we obtain four curves

$$D_a : \begin{cases} X^2 + X + 1 = aY_1^2, \\ X^4 + 7 = aY_2^2 \end{cases}$$

with $a = \pm 1, \pm 43$. Let $\phi_a : D_a \to C$ be given by $\phi_a(X, Y_1, Y_2) = (X, aY_1Y_2)$. From the above argument,

$$C(\mathbb{Q}) = \bigcup_{a \in \{\pm 1, \pm 43\}} \phi_a\left(D_a(\mathbb{Q})\right).$$

Vague Definition: Given a curve C over a number field k, a **descent** is some process which yields a finite family $\phi_a : D_a \to C$ of **covers** such that

$$C(k) = \bigcup_a \phi_a\left(D_a(k)\right). \tag{5}$$

Example 9.7 *We continue Example 9.1. Observe that*

- $D_{-1}(\mathbb{R}) = \emptyset$, *so* $D_{-1}(\mathbb{Q}) = \emptyset$.
- $D_{-43}(\mathbb{R}) = \emptyset$, *so* $D_{-43}(\mathbb{Q}) = \emptyset$.
- $D_{43}(\mathbb{Q}_2) = \emptyset$, *so* $D_{43}(\mathbb{Q}) = \emptyset$.

Thus after descent and local solvability checking, we have

$$C(\mathbb{Q}) = \phi(D(\mathbb{Q}))$$

where

$$D = D_1 : \begin{cases} X^2 + X + 1 = Y_1^2, \\ X^4 + 7 = Y_2^2, \end{cases} \qquad \phi(X, Y_1, Y_2) = (X, Y_1Y_2).$$

In fact D_1 has four rational points are infinity. So $D_1(\mathbb{Q}) \neq \emptyset$.

We have reduced finding all rational points on C (which has genus 2) to finding all rational points on D (which has genus 3). The curve D has a genus 1 quotient: $X^4 + 7 = Y_2^2$. In fact, we have $\psi : D \to E$, where

$$E : y^2 = x(x^2 + 7), \qquad (X, Y_1, Y_2) \mapsto (X^2, XY_2).$$

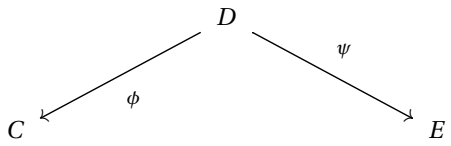
But $E(\mathbb{Q}) = \{(0,0), \infty\}$ so

$$D(\mathbb{Q}) = \{(1 : \pm 1 : \pm 1 : 0)\}.$$

Hence

$$C(\mathbb{Q}) = \{(1 : \pm 1 : 0)\}.$$

Note the following diagram



To find the rational points on C we constructed a cover D and used its quotient E.

Example 9.8 *The curve*

$$C : X^4 - 17 = 2Y^2$$

has points everywhere locally. We will use descent to show that $C(\mathbb{Q}) = \emptyset$. Write

$$X = \frac{x}{z}, \qquad Y = \frac{y}{z^2}, \qquad x, y, z \in \mathbb{Z}, \qquad \gcd(x, z) = 1.$$

so

$$x^4 - 17z^4 = 2y^2.$$

Note y is even: write $y = 2y_1$. So

$$x^4 - 17z^4 = 8y_1^2.$$

Obtain

$$(x^2 + z^2\sqrt{17})(x^2 - z^2\sqrt{17}) = 8y_1^2. \tag{6}$$

Let $K = \mathbb{Q}(\sqrt{17})$, and $\mathcal{O}$ its ring of integers:

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\frac{(1 + \sqrt{17})}{2}.$$

The ring of integers $\mathcal{O}$ has class number 1 (thus it is a UFD). We rewrite (6) as

$$\left(\frac{x^2 + z^2\sqrt{17}}{2}\right)\left(\frac{x^2 - z^2\sqrt{17}}{2}\right) = 2y_1^2;$$

The two factors on the left belong to $\mathcal{O}$, and their gcd divides divides x^2 and $\sqrt{17}z^2$, so divides $\sqrt{17}$. But $17 \nmid y$. So the two factors are coprime. Moreover the unit group of $\mathcal{O}$ is

$$\mathcal{O}^\times = \{\pm(4 + \sqrt{17})^n : n \in \mathbb{Z}\},$$

and 2 factors in $\mathcal{O}$ as

$$2 = \left(\frac{5+\sqrt{17}}{2}\right)\left(\frac{5-\sqrt{17}}{2}\right).$$

So

$$\frac{x^2+z^2\sqrt{17}}{2} = \alpha\mu^2, \qquad \frac{x^2-z^2\sqrt{17}}{2} = \bar{\alpha}\bar{\mu}^2, \qquad \mu \in \mathcal{O}$$

and

$$\alpha = \pm\left(\frac{5\pm\sqrt{17}}{2}\right), \qquad \text{or} \qquad \alpha = \pm\left(\frac{5\pm\sqrt{17}}{2}\right)(4+\sqrt{17}).$$

Since $\alpha\bar{\alpha} = 2$, *and* $\alpha > 0$ *we have*

$$\alpha = \left(\frac{5\pm\sqrt{17}}{2}\right).$$

So

$$\frac{x^2+z^2\sqrt{17}}{2} = \left(\frac{5\pm\sqrt{17}}{2}\right)(u+v\sqrt{17})^2 \qquad u, v \in \mathbb{Q}.$$

Expanding

$$x^2+z^2\sqrt{17} = \left(5u^2+85v^2\pm 34uv\right) + \left(\pm(u^2+17v^2)+10uv\right)\sqrt{17},$$

and equating coefficients of $1, \sqrt{17}$ *gives*

$$\begin{cases} 5u^2+85v^2\pm 34uv = x^2 \\ \pm(u^2+17v^2)+10uv = z^2. \end{cases}$$

The important point is that, for each $a = \pm 1$, *these two equations define a curve* D_a *over* $\mathbb{Q}$, *and* $C(\mathbb{Q}) = \cup\phi_a(D_a(\mathbb{Q}))$, *even though the descent argument used factorization over an extension.*

Finally, it is possible to check that $D_a(\mathbb{Q}_{17}) = \emptyset$. *Thus* $C(\mathbb{Q}) = \emptyset$.

9.2. A more general example: descent of hyperelliptic curves

Suppose that

$$C : y^2 = f(x),$$

where $f \in \mathbb{Z}[x]$ is irreducible with even degree n. Homogenizing we have

$$Y^2 = F(X,Z)$$

where F is homogeneous and $F(x,1) = f(x)$. Let θ be a root of f and $K = \mathbb{Q}(\theta)$. Then we can factor

$$Y^2 = (X - \theta Z)G(X,Z)$$

Using algebraic number theory

$$X - \theta Z = \alpha \cdot \mu^2$$

where $\alpha = a_0 + a_1\theta + \cdots a_{n-1}\theta^{n-1}$ belongs to a finite computable set, and $\mu \in K$. Write $\mu = u_0 + u_1\theta + \cdots + u_{n-1}\theta^{n-1}$. Expanding we obtain

$$X - \theta Z = Q_1^\alpha(u_0,\ldots,u_n) + Q_2^\alpha(u_0,\ldots,u_n)\theta + \cdots + Q_n^\alpha(u_0,\ldots,u_n)\theta^{n-1}.$$

where the Q_i^α are homogeneous quadratic forms with coefficients in $\mathbb{Q}$. Comparing coefficients we have obtain covers

$$D_\alpha : \begin{cases} Q_3^\alpha(u_0,\ldots,u_n) = 0 \\ \vdots \\ Q_n^\alpha(u_0,\ldots,u_n) = 0, \end{cases}$$

These covers satisfy

$$C(\mathbb{Q}) = \bigcup_\alpha \phi_a\left(D_\alpha(\mathbb{Q})\right). \tag{7}$$

One can probably obtain information about the rational points on $C(\mathbb{Q})$ by studying the local solubility of the D_α, their rational points and the rational points of their quotients.

The strategy explained above is a crude approximation to 2-**cover descent** on hyperelliptic curves. For more on that see Stoll's lectures and also the papers [4], [5] of Bruin and Stoll. A generalization of 2-**cover descent** is given in [20].

10. Divisors

Let C be a curve over k. A divisor D on C is a formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in C(\overline{k}).$$

We define the **degree** of D to be $\sum a_i$. We say that D is **rational** if it is invariant under $\mathrm{Gal}(\overline{k}/k)$.

Example 10.1 *Let*

$$C : y^2 = x(x^2+1)(x^3+1).$$

This is a genus 2 *curve defined over* $\mathbb{Q}$. *Let*

$$D_1 = 2\cdot(0,0) + (1,2), \quad D_2 = (i,0) - (-i,0), \quad D_3 = (i,0) + (-i,0) - 2\cdot(1,2).$$

These are divisors and their degrees are

$$\deg(D_1) = 3, \qquad \deg(D_2) = 0, \qquad \deg(D_3) = 0.$$

Observe that any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *sends* i *to itself (e.g.* σ *is the identity) or changes its sign (e.g.* σ *is complex conjugation). Thus* D_1 *is rational,* D_3 *is rational, but* D_2 *is* ***not*** *rational, since complex conjugation negates it.*

The **divisor group** of C/k, denoted by $\mathrm{Div}(C/k)$ is the set of rational divisors of C/k. This is obviously an abelian group with addition defined in the obvious formal way. The **degree** 0 **subgroup of the divisor group** is the subgroup

$$\mathrm{Div}^0(C/k) := \{D \in \mathrm{Div}(C/k) \,:\, \deg(D) = 0\}.$$

This is an abelian group.

Example 10.2 *We continue Example 10.1. In the example* $D_3 \in \mathrm{Div}^0(C/\mathbb{Q})$*, but* $D_1, D_2 \notin \mathrm{Div}^0(C/\mathbb{Q})$.

11. Principal Divisors

Let C be a curve defined over a field k. Let $k(C)$ be the function field of C, and let $f \in k(C)^*$. If $P \in C(\overline{k})$ then there is $v_P(f) \in \mathbb{Z}$ which measures the **order of vanishing** of f at P. Define

$$\mathrm{div}(f) = \sum_{P \in C(\overline{k})} v_P(f) \cdot P.$$

A divisor of the form $\mathrm{div}(f)$ is called a **principal divisor**.

Fact 11.1 *If* $f \in k(C)^*$ *then* $\mathrm{div}(f) \in \mathrm{Div}^0(C/k)$.

Example 11.2 *Let* $f = \frac{x^2-7}{x^3}$ *on* $\mathbb{P}^1/\mathbb{Q}$*. Then*

$$\mathrm{div}(f) = -3 \cdot (0) + (\sqrt{7}) + (-\sqrt{7}) + \infty.$$

Intuitively, if x *is large, then* $f \sim 1/x$ *which explains why it vanishes to order* 1 *at* ∞*. Observe that* $\mathrm{div}(f) \in \mathrm{Div}^0(\mathbb{P}^1/\mathbb{Q})$.

12. The Picard Group

It follows from Fact 11.1 that

$$\mathrm{Princ}(C/k) := \{\mathrm{div}(f) : f \in k(C)^*\}$$

is contained in $\mathrm{Div}^0(C/k)$. This is called the **subgroup of principal divisors**. It is easy to show that it is a subgroup using the properties

$$\operatorname{div}(1) = 0, \qquad \operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g), \qquad \operatorname{div}(1/f) = -\operatorname{div}(f),$$

that follow from the definition of div. We define the **Picard group** of C/k as

$$\operatorname{Pic}^0(C/k) := \frac{\operatorname{Div}^0(C/k)}{\operatorname{Princ}(C/k)}.$$

The following two theorems are standard consequences of the Riemann–Roch Theorem (See [21, Chapters II and III]).

Theorem 8

$$\operatorname{Pic}^0(\mathbb{P}^1/k) = 0.$$

Theorem 9 *Let*

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in k, \quad 4A^3 + 27B^2 \neq 0.$$

be an elliptic curve over k. Then

$$E(k) \cong \operatorname{Pic}^0(E/k), \qquad P \mapsto [P - \infty]. \tag{8}$$

In (8), the group operation on $E(k)$ is the usual one defined by secants and tangents.

If C is a curve that isn't an elliptic curve, what is the correct object to replace $E(k)$ in the isomorphism (8)?

13. Jacobians

Let C/k be a curve of genus g. We don't define the **Jacobian** J_C of C, but mention that it is a g-dimensional abelian variety defined over k that is 'functorially associated' to C. An elliptic curve E is its own Jacobian $J_E = E$.

Theorem 10 *(Mordell–Weil Theorem) If k is a number field then $J_C(k)$ is a finitely generated abelian group.*

The proof uses descent and heights and is similar to the proof of the Mordell–Weil Theorem for elliptic curves. We can often compute $J_C(k)$ in practice, but there is no algorithm guaranteed to work. For more on this see the lectures by Müller and by Balakrishnan.

Theorem 11 *Let C be a curve with $C(k) \neq \emptyset$. Then*

$$J_C(k) \cong \operatorname{Pic}^0(C/k).$$

For more on this theorem see [16, Section 3]. We usually use elements of $\operatorname{Pic}^0(C/k)$ to represent elements of $J_C(k)$.

Example 13.1 *We continue Example 10.1. Let*

$$C : y^2 = x(x^2+1)(x^2+3).$$

This is a curve of genus 2 *defined over* $\mathbb{Q}$*. It has one rational point at infinity which we denote by* ∞ *(and which we see on a smooth model in a projective plane with appropriate weights). The curve* C *has genus* 2*. Using descent it is possible to show that*

$$J_C(\mathbb{Q}) = \frac{\mathbb{Z}}{2\mathbb{Z}} \cdot [(0,0) - \infty] \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \cdot [(i,0) + (-i,0) - 2\infty].$$

It is easy to check that

$$[(0,0) - \infty] + [(i,0) + (-i,0) - 2\infty] = [(\sqrt{-3},0) + (-\sqrt{-3},0) - 2\infty];$$

to check this the reader should write down a function on C *whose divisor is*

$$(0,0) + (i,0) + (-i,0) - (\sqrt{-3},0) - (-\sqrt{-3},0) - \infty.$$

Definition 13.2 *Let* C/k *be a curve of genus* ≥ 1*. Let* $P_0 \in C(k)$*. The* ***Abel–Jacobi*** *map associated to* P_0 *is the embedding*

$$\iota : C \hookrightarrow J_C, \qquad P \to [P - P_0].$$

Lemma 13.3 *If* C *has genus* ≥ 1 *and* $P_0 \in C(k)$ *then* $\iota(C(k)) \subseteq J_C(k)$*. If moreover* $J_C(k)$ *is finite (and we know it) we can compute* $C(k)$*.*

Example 13.4 *We continue Example 13.1.*

$$J_C(\mathbb{Q}) = \left\{0,\ [(0,0) - \infty],\ [(i,0) + (-i,0) - 2\infty],\ [(\sqrt{-3},0) + (-\sqrt{-3},0) - 2\infty]\right\}.$$

We can take $\iota : C \hookrightarrow J_C$*,* $P \mapsto [P - \infty]$*, and using this we find that*

$$C(\mathbb{Q}) = \{\infty, (0,0)\}.$$

Question: If $J_C(\mathbb{Q})$ is infinite, but we knew a Mordell–Weil basis, can we still recover $C(\mathbb{Q})$?

The quick answer is that sometimes we can using Chabauty and the Mordell–Weil sieve.

14. Chabauty's Theorem

Let $C/\mathbb{Q}$ be a curve of genus ≥ 2. We shall henceforth write $J = J_C$. Write

$$g = \text{genus}(C), \qquad r = \text{rank}(J(\mathbb{Q})).$$

Theorem 12 (Chabauty, 1941) *If $r \leq g-1$ then $C(\mathbb{Q})$ is finite.*

This theorem is superceded by Faltings' Theorem, which asserts finiteness of $C(\mathbb{Q})$ with no condition on r. However as we shall see, the proof strategy often allows us to compute $C(\mathbb{Q})$ provided the condition $r \leq g-1$ is satisfied. Coleman [11] proved the following stronger theorem.

Theorem 13 (Coleman, 1995) *Let p be a prime of good reduction for C and suppose $p > 2g$. If $r \leq g-1$ then*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

The method of **Chabauty (or Chabauty–Coleman)** is based on the proof of Coleman's Theorem.

15. Chabauty's Method

15.1. Differentials

Let C be a curve of a field k with $g = \text{genus}(C)$. Write Ω_C for the **space of regular differentials**. This is a k-vector space of dimension g.

Example 15.1 *Let $f \in k[x]$ satisfy $\text{disc}(f) \neq 0$. Suppose $\text{char}(k) \neq 2$. Let*

$$C : y^2 = f(x).$$

We know

$$g = \begin{cases} (d-2)/2 & d \text{ even} \\ (d-1)/2 & d \text{ odd} \end{cases} \qquad d = \deg(f).$$

Then a k-basis for Ω_C is

$$\frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y}.$$

15.2. A Pairing

Let C be a curve over $\mathbb{Q}_p$ (p is a finite prime). Then there is a pairing

$$\langle , \rangle : \Omega_C \times J(\mathbb{Q}_p) \to \mathbb{Q}_p,$$

which is defined by

$$\langle \omega, [\sum P_i - Q_i] \rangle = \sum \int_{Q_i}^{P_i} \omega.$$

The pairing has the following properties:

1. it is $\mathbb{Q}_p$-linear on the left;
2. it is $\mathbb{Z}$-linear on the right;
3. the kernel on the right is $J(\mathbb{Q}_p)_{\text{tors}}$ (the torsion subgroup of $J(\mathbb{Q}_p)$.

Example 15.2 *Here we follow the expository article of McCallum and Poonen, "The Method of Chabauty and Coleman" [15], to compute an integral on a curve. Let*

$$C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

This is a curve of genus 2 *with two points at infinity (defined over* $\mathbb{Q}$*). We work over* $\mathbb{Q}_3$*.*

$$\begin{aligned}
\int_{(0,1)}^{(-3,1)} \frac{dx}{y} &= \int_{(0,1)}^{(-3,1)} (1 + 6x + 5x^2 + 22x^3 + 22x^4 + 8x^5 + x^6)^{-1/2} dx \\
&= \int_{(0,1)}^{(-3,1)} (1 - 3x + 11x^2 - 56x^3 + \cdots) dx \\
&= \int_0^{-3} (1 - 3x + 11x^2 - 56x^3 + \cdots) dx \\
&= \left[x - \frac{3x^2}{2} + \frac{11x^3}{3} - \frac{56x^4}{4} + \cdots \right]_{x=0}^{x=-3} \\
&= (-3) - \frac{3 \cdot (-3)^2}{2} + \frac{11 \cdot (-3)^3}{3} - \frac{56(-3)^4}{4} + \cdots \\
&\equiv 87 \pmod{3^5}.
\end{aligned}$$

The integral above is called 'a tiny integral', where the two end points are sufficiently p-adically close to ensure p-adic convergence when evaluating the p-power series.

If $D \in J(\mathbb{Q}_p)$ then there exists a computable $n > 0$ such that

$$nD = \sum [P_i - Q_i]$$

where P_i are p-adically close to the Q_i. If $\omega \in \Omega_C$ then

$$\langle \omega, D \rangle = \frac{1}{n} \langle \omega, nD \rangle = \frac{1}{n} \sum \int_{Q_i}^{P_i} \omega.$$

The integrals are all tiny and so can be evaluated as in the above example.

Example 15.3 *We continue Example 15.2. Want to approximate* $\int_{\infty_-}^{\infty_+} dx/y$*. One can show that*

$$9[\infty_+ - \infty_-] = [(-3,1) - (0,1)].$$

Thus

$$\int_{\infty_-}^{\infty_+} \frac{dx}{y} = \frac{1}{9} \int_{(0,1)}^{(-3,1)} \frac{dx}{y} = \frac{1}{9}(87 + O(3^5)) = \frac{29}{3} + O(3^3).$$

Likewise

$$\begin{aligned}\int_{\infty_-}^{\infty_+} \frac{x\,dx}{y} &= \frac{1}{9}\int_{(0,1)}^{(-3,1)} \frac{x\,dx}{y} \\ &= \frac{1}{9}(72 + O(3^5)) \\ &= 8 + O(3^3).\end{aligned}$$

Lemma 15.4 *Let C be a curve over $\mathbb{Q}$ of genus g. Write r for the rank of $J(\mathbb{Q})$. Suppose $r \leq g-1$. Let p be a prime. Then there is some non-zero $\omega \in \Omega_{C/\mathbb{Q}_p}$ such that*

$$\langle \omega, D \rangle = 0 \text{ for all } D \in J(\mathbb{Q}).$$

Proof: The proof follows trivially from the properties of the integration pairing $\langle\ ,\ \rangle$, the fact that $\dim(\Omega_{C/\mathbb{Q}_p}) = g$, and basic linear algebra. Convince yourself that this is true. □

We call an ω as in Lemma 15.4 an **annihilating differential**.

Example 15.5 *We continue Example 15.2. A basis for $\Omega_{C/\mathbb{Q}_3}$ is dx/y, $x\,dx/y$. Using descent it is possible to show that*

$$J(\mathbb{Q}) \cong \mathbb{Z} \cdot [\infty_+ - \infty_-].$$

We want $\omega = \epsilon\,dx/y + x\,dx/y$ such that $\langle \omega, [\infty_+ - \infty_-] \rangle = 0$. But

$$\langle \frac{dx}{y}, [\infty_+ - \infty_-] \rangle = \frac{29}{3} + O(3^3), \qquad \langle \frac{x\,dx}{y}, [\infty_+ - \infty_-] \rangle = 8 + O(3^3).$$

So we take

$$\epsilon = \frac{-8 + O(3^3)}{29/3 + O(3^3)} = 69 + O(3^4).$$

We focus on finding rational points $P \in C(\mathbb{Q})$ such that $P = (t,s) \equiv (0,1) \pmod 3$. Suppose P is such a point. Now $[P - (0,1)] \in J(\mathbb{Q})$ thus

$$\int_{(0,1)}^{(t,s)} \omega = 0$$

where $\omega = \epsilon\,dx/y + x\,dx/y$ is the annihilating differential. Note that this is a tiny integral:

$$\begin{aligned}\int_{(0,1)}^{(t,s)} \omega &= \int_{(0,1)}^{(t,s)} (\epsilon + x)\frac{dx}{y} \\ &= \int_0^t (\epsilon + x)(1 - 3x + 11x^2 - 56x^3 + \cdots)\,dx \\ &= \epsilon t + \frac{-3\epsilon + 1}{2} t^2 + \frac{11\epsilon - 3}{3} t^3 + \cdots.\end{aligned}$$

Note $t \equiv 0 \pmod 3$. *So* $t = 3z$ *where* $z \in \mathbb{Z}_3$. *So*

$$(-4\cdot 3^2 + O(3^5))z + (-103\cdot 3^2 + O(3^7))z^2 + (3^5 + O(3^6))z^3 + \sum_{j\geq 4} O(3^4)z^j = 0.$$

We need the following theorem of Strassmann; for a proof see the book of Cassels on local fields [8].

Theorem 14 (Strassmann) *Let* $f = \sum_{i\geq 0} a_i z^i$ *be a powerseries with* $a_i \in \mathbb{Z}_p$, *such that* $\lim a_i = 0$. *Let* $k = \min v_p(a_i)$, *and let*

$$N = \max\{j : v_p(a_j) = k\}.$$

Then the number of zeros of f *in* $\mathbb{Z}_p$ *is* $\leq N$.

Example 15.6 *Back to the example. For the powerseries*

$$(-4\cdot 3^2 + O(3^5))z + (-103\cdot 3^2 + O(3^7))z^2 + (3^5 + O(3^6))z^3 + \sum_{j\geq 4} O(3^4)z^j = 0.$$

we have $k = 2$, *and*

$$N = \max\{1, 2\} = 2.$$

So the equation in z *has at most two solutions. There are at most two rational points* $P \in C(\mathbb{Q})$ *such that* $P = (t, s) \equiv (0, 1) \pmod 3$. *But we know two such points:* $(0, 1)$ *and* $(-3, 1)$. *So there are no others. Now check for yourself that*

$$C(\mathbb{F}_3) = \{\overline{\infty_+},\ \overline{\infty_-},\ (\overline{0}, \overline{1}),\ (\overline{0}, \overline{2})\}.$$

By searching for rational points on C *we find*

$$\infty_+,\ \infty_-,\ (0, 1),\ (0, -1),\ (-3, 1),\ (-3, -1).$$

Are they all? From the points of $C(\mathbb{F}_3)$, *we know that every* $P \in C(\mathbb{Q})$ *must satisfy* $P \equiv P_0 \pmod 3$ *where* P_0 *is one of the following* ***rational points****:*

$$\infty_+,\ \infty_-,\ (0, 1),\ (0, -1).$$

Using Chabauty (i.e. the strategy above) we obtain a bound on the number of points congruent to P_0 *for each one of these four points:*

P_0	*bound on number of rational* $P \equiv P_0 \pmod 3$	*known rational* $P \equiv P_0 \pmod 3$
∞_+	1	∞_+
∞_-	1	∞_-
$(0, 1)$	2	$(0, 1)$, $(-3, 1)$
$(0, -1)$	2	$(0, -1)$, $(-3, -1)$

We conclude that

$$C(\mathbb{Q}) = \{\infty_+,\ \infty_-,\ (0, 1),\ (0, -1),\ (-3, 1),\ (-3, -1)\}.$$

Note for Chabauty to succeed in finding $C(\mathbb{Q})$:

1. we require $r \leq g-1$;
2. we need explicit generators for $J(\mathbb{Q})$ (or some subgroup of $J(\mathbb{Q})$ of finite index);
3. we want some prime p of good reduction so that the known rational points surject onto the residue classes mod p;
4. in each residue class we want to find enough rational points to match the Chabauty bound!

Even if we have (1) and (2), we find in most examples that (3) and (4) fail. The **Mordell–Weil** sieve often allows us to fix that. Before going on to the Mordell–Weil sieve, I would like to recommend the expository article of McCallum and Poonen [15] as well as Wetherell's thesis [23] as great introductions to the method of Chabauty. For an approach that uses formal groups instead of differentials, see Flynn's article [12] or the book of Cassels and Flynn [10]. The method of Chabauty has been extended in several ways. The most important of these is 'elliptic curve Chabauty'. For this I recommend Bruin's thesis [1] and Bruin's paper [2] for an introduction and for applications to the generalized Fermat equation, and the paper of Flynn and Wetherell [13] for a beautiful Diophantine application. Other extensions of Chabauty's method can be found in [18] and [19].

No account of the method of Chabauty (however brief) would be complete without mentioning the beautiful paper of Poonen and Stoll [17], where they apply Chabauty to hyperelliptic curves $y^2 = f(x)$ where f is a squarefree polynomial of degree $2g+1$. They show for $g \geq 3$ that a positive proportion of these curves have exactly one rational point, and that this proportion converges to 1 as $g \to \infty$. The reader will see shortly how hard we have to work to compute the rational points on one curve—Poonen and Stoll compute the points for 'most' odd degree hyperelliptic curves!

16. The Mordell–Weil Sieve

Let $C/\mathbb{Q}$ be a curve, J its Jacobian, and

$$\iota : C \hookrightarrow J$$

an Abel–Jacobi map. We assume that we know $J(\mathbb{Q})$ (in other words, we know a basis for $J(\mathbb{Q})$). The **Mordell–Weil Sieve** is a strategy for producing a 'small' finite set $W \subset J(\mathbb{Q})$, and a subgroup $L \subset J(\mathbb{Q})$ of 'huge' index such that

$$\iota(C(\mathbb{Q})) = \bigcup_{D \in W} D + L.$$

If $P \in C(\mathbb{Q}_p)$ we define the **residue disk of** P as

$$B_p(P) = \{Q \in C(\mathbb{Q}_p) : Q \equiv P \pmod{p}\}.$$

The number of residue disks is $\#C(\mathbb{F}_p)$.

Suppose $r < g-1$. Let ω be an annihilating differential, and $P \in C(\mathbb{Q})$. Chabauty's method gives a bound $\mathrm{Chab}_p(P)$ for the number of points of rational points in the residue disc of P:

$$\#C(\mathbb{Q}) \cap B_p(P) \leq \mathrm{Chab}_p(P).$$

Let $\mathscr{K}$ be the **known** rational points. If $\#\mathscr{K} \cap B_p(P) = \mathrm{Chab}_p(P)$ then

$$C(\mathbb{Q}) \cap B_p(P) = \mathscr{K} \cap B_p(P).$$

I.e. we know all of the rational points in the residue disc of P.

16.1. An Extended Example

We illustrate the need for the Mordell–Weil sieve with a particular example. Let

$$C : y^2 = 2x^6 - 3x^2 - 2x + 1;$$

this is a curve of genus 2 defined over $\mathbb{Q}$. The Mordell–Weil group is

$$J(\mathbb{Q}) = \mathbb{Z} \cdot [(-2,-11) - (0,1)].$$

Thus J has rank 1 and C satisfies the Chabauty bound $r \leq g-1$. A short search reveals the following four points:

$$\mathscr{K} = \{(0,1),\ (0,-1),\ (-2,11),\ (-2,-11)\}.$$

An annihilating differential for $p = 3$ is

$$\omega = (66 + O(3^5))\frac{dx}{y} + \frac{x\,dx}{y}.$$

Applying Chabauty with $p = 3$ gives

P	$\mathrm{Chab}_3(P)$	$\mathscr{K} \cap B_3(P)$
$(0,1)$	2	$\{(0,1)\}$
$(0,-1)$	2	$\{(0,-1)\}$
$(-2,11)$	1	$\{(-2,11)\}$
$(-2,-11)$	1	$\{(-2,-11)\}$

For $P = (-2,-11)$ and $(-2,11)$ there are no other rational points in the same residue disc. For $P = (0,1)$ and $P = (0,-1)$ we don't know.

Let

$$B_9(P) = \{Q \in C(\mathbb{Q}_3) : Q \equiv P \pmod 9\}.$$

We can use Chabauty to determine upper bounds for the number of rational points in this smaller residue disc:

P	$\mathrm{Chab}_9(P)$	$\mathscr{K} \cap B_9(P)$
$(0,1)$	1	$\{(0,1)\}$
$(0,-1)$	1	$\{(0,-1)\}$

For $P = (0,1)$ and $(0,-1)$ there are no other rational points in the smaller residue disc $B_9(P)$. We deduce the following:

Lemma 16.1 *The only rational points in*

$$B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11), \tag{9}$$

belong to $\mathscr{K} = \{(0,1),(0,-1),(-2,11),(-2,-11)\}$.

Note

$$C(\mathbb{F}_3) = \{(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{1}),(\bar{1},\bar{2}).\}$$

It follows that

$$C(\mathbb{Q}_3) = B_3(0,1) \cup B_3(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11).$$

Thus (9) does not fill up all of $C(\mathbb{Q}_3)$. To show that $\mathscr{K} = \{(0,1),(0,-1),(-2,11),(-2,-11)\}$ is all of the rational points, we need to show that every rational point belongs to (9). This is what the **Mordell–Weil** sieve will achieve.

Let $P_0 = (0,1)$. Let

$$\iota : C \hookrightarrow J, \qquad Q \mapsto [Q - P_0]$$

be the associated Abel-Jacobi map. Recall

$$J(\mathbb{Q}) = \mathbb{Z} \cdot D, \qquad D = [(-2,-11) - (0,1)].$$

Note that

$$\iota(0,1) = 0, \quad \iota(0,-1) = -2D, \quad \iota(-2,11) = -3D, \quad \iota(-2,-11) = D.$$

Suppose $Q \in C(\mathbb{Q})$. Then $\iota(Q) = nD$ with $n \in \mathbb{Z}$. We will use reduction mod p for lots of primes p to 'predict' n modulo certain integers N_p. Let p be a prime of of good reduction. Let

$$N_p = \text{order of } \bar{D} \in J(\mathbb{F}_p).$$

Consider the commutative diagram

$$\begin{array}{ccccc}
C(\mathbb{Q}) & \xrightarrow{\iota} & J(\mathbb{Q}) & \xleftarrow[\eta]{} & \mathbb{Z} \\
\downarrow{\scriptstyle \text{red}} & & \downarrow{\scriptstyle \text{red}} & & \downarrow \\
C(\mathbb{F}_p) & \xrightarrow{\iota} & J(\mathbb{F}_p) & \xleftarrow[\eta]{} & \mathbb{Z}/N_p\mathbb{Z}
\end{array}$$

Here $\eta(m) = mD$. Define

$$W_p = \{m \in \mathbb{Z}/N_p\mathbb{Z} : m \cdot \overline{D} \in \iota(C(\mathbb{F}_p))\}.$$

By diagram chasing, if $Q \in C(\mathbb{Q})$ and $n \in \mathbb{Z}$ satisfies $nD = \iota(Q)$ then $n \pmod{N_p} \in W_p$.

To summarize, for every prime p of good reduction, the Mordell–Weil sieve gives an integer N_p and a set W_p such that $n \bmod N_p \in W_p$. In the following table, we give for some small primes p, the integers N_p and sets W_p.

p	N_p	W_p
3	13	$\{0,1,10,11\}$
5	21	$\{0,1,18,19\}$
7	65	$\{0,1,13,19,27,36,44,50,62,63\}$
23	16	$\{0,1,7,13,14\}$
61	208	$\{0,1,24,53,153,182,205,206\}$

The integers N_p in the table are not pairwise coprime. We shall use this to eliminate some of the possibilities in the table. Note that $16 \mid 208$. Observe that if $n \equiv 24 \pmod{208}$ then $n \equiv 8 \pmod{16}$. However, looking at the 4-th row of the table we realize that this is impossible. We can therefore delete the entry 24 from W_{61} in the 5-th row. The same is true for the entries 53, 153, 182. Also $13 \mid 65$. We can use this fact, to delete the entries 19 and 44 for W_7. This is what the table now looks like.

p	N_p	W_p
3	13	$\{0,1,10,11\}$
5	21	$\{0,1,18,19\}$
7	65	$\{0,1,13,\cancel{19},27,36,\cancel{44},50,62,63\}$
23	16	$\{0,1,7,13,14\}$
61	208	$\{0,1,\cancel{24},\cancel{53},\cancel{153},\cancel{182},205,206\}$

We need more data. We shall add the information corresponding to the primes $p = 17$, 19.

p	N_p	W_p
3	13	$\{0,1,10,11\}$
5	21	$\{0,1,18,19\}$
7	65	$\{0,1,13,\cancel{19},27,36,\cancel{44},50,62,63\}$
17	39	$\{0,1,36,37\}$
19	234	$\{0,1,42,67,72,82,100,132,150,160,165,190,231,232\}$
23	16	$\{0,1,7,13,14\}$
61	208	$\{0,1,\cancel{24},\cancel{53},\cancel{153},\cancel{182},205,206\}$

Note that $39 \mid 234$. This allows us to delete all but four entries in W_{19}:

p	N_p	W_p
3	13	$\{0,1,10,11\}$
5	21	$\{0,1,18,19\}$
7	65	$\{0,1,13,\cancel{19},27,36,\cancel{44},50,62,63\}$
17	39	$\{0,1,36,37\}$
19	234	$\{0,1,\cancel{42},\cancel{67},\cancel{72},\cancel{82},\cancel{100},\cancel{132},\cancel{150},\cancel{160},\cancel{165},\cancel{190},231,232\}$
23	16	$\{0,1,7,13,14\}$
61	208	$\{0,1,\cancel{24},\cancel{53},\cancel{153},\cancel{182},205,206\}$

From the row corresponding to $p = 19$, we now observe the following: if $Q \in C(\mathbb{Q})$ then $\iota(Q) = nD$ where $n \equiv 0, 1, -3, -2 \pmod{234}$. But

$$\iota(0,1) = 0, \quad \iota(0,-1) = -2D, \quad \iota(-2,11) = -3D, \quad \iota(-2,-11) = D.$$

Take $n \equiv -3 \pmod{234}$. So $n = -3 + 234m$. Then

$$\begin{aligned}[Q - P_0] = \iota(Q) &= nD \\ &= -3D + m(234 \cdot D) \\ &= \iota(-2,11) + m(234 \cdot D) \\ &= [(-2,11) - P_0] + m(234 \cdot D).\end{aligned}$$

Hence $[Q - (-2,11)] = m(234 \cdot D)$. We can repeat this argument with $n \equiv 0,\ 1,\ -2 \pmod{234}$ to reach the following conclusion.

Lemma 16.2 *If $Q \in C(\mathbb{Q})$ then there exists $P \in \mathscr{K}$ such that*

$$[Q - P] \in \mathbb{Z} \cdot (234 \cdot D).$$

It turns out that Lemmas 16.1 and 16.2 are enough to show that $C(\mathbb{Q}) = \mathscr{K}$. To see this we need a short digression on p-adic filtrations.

16.2. p-adic Filtration

We briefly return to generality with C a curve over $\mathbb{Q}$ of genus ≥ 1 and J its Jacobian. Let p be a prime of good reduction. Let

$$J^m(\mathbb{Q}_p) = \{D \in J(\mathbb{Q}_p) : D \equiv 0 \pmod{p^m}\}.$$

We have

$$J(\mathbb{Q}_p) \supset J^1(\mathbb{Q}_p) \supset J^2(\mathbb{Q}_p) \supset J^3(\mathbb{Q}_p) \supset \cdots$$

is a system of decreasing neighbourhoods of the origin. Also

$$J(\mathbb{Q}_p)/J^1(\mathbb{Q}_p) \cong J(\mathbb{F}_p), \qquad J^m(\mathbb{Q}_p)/J^{m+1}(\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^g \text{ for } m \geq 1. \tag{10}$$

16.3. Continuation of the Extended Example

We return to our extended example of Subsection 16.1. It turns out that

$$\#J(\mathbb{F}_3) = 13, \qquad 234 = 2 \cdot 3^2 \cdot 13.$$

By (10) we have $234D \in J^3(\mathbb{Q}_3)$; that is $234D \equiv 0 \pmod{3^3}$. We have two important pieces of information given by Lemma 16.1 and the above computation.

1. If $Q \in C(\mathbb{Q})$ then there is some $P \in \mathscr{K}$ such that

$$[Q-P] \in \mathbb{Z} \cdot (234 \cdot D).$$

2. $234D \equiv 0 \pmod{3^3}$.

Thus

$$Q \equiv P \pmod{3^3}, \qquad P \in \mathscr{K} = \{(0,1),(0,-1),(-2,11),(-2,-11)\}.$$

So Q belongs to

$$B_{27}(0,1) \cup B_{27}(0,-1) \cup B_{27}(-2,11) \cup B_{27}(-2,-11)$$
$$\subset B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11).$$

Now applying Lemma 16.1 we have

$$C(\mathbb{Q}) = \{(0,1),\ (0,-1),\ (-2,11),\ (-2,-11)\}.$$

The reader will note that for this example we needed both Chabauty and the Mordell–Weil sieve to compute the rational points on C.

16.4. The Mordell–Weil Sieve: More Conceptually

Let $C/\mathbb{Q}$ be a curve, J its Jacobian. Fix $P_0 \in J(\mathbb{Q})$. Let

$$\iota : C \hookrightarrow J, \qquad P \mapsto [P - P_0]$$

be the Abel–Jacobi map. We assume that we know $J(\mathbb{Q})$ (in other words, we know a basis for $J(\mathbb{Q})$). As we said previously, the Mordell–Weil Sieve is a strategy for producing a 'small' finite set $W \subset J(\mathbb{Q})$, and a subgroup $L \subset J(\mathbb{Q})$ of 'huge' index such that

$$\iota(C(\mathbb{Q})) = \bigcup_{D \in W} D + L =: W + L.$$

We define inductively subgroups of finite index $L_i \subset J(\mathbb{Q})$, and finite subsets $W_i \subset J(\mathbb{Q})$, such that

$$L_0 \supseteq L_1 \supseteq L_2 \supseteq L_3 \supset \cdots$$

and

$$\iota(C(\mathbb{Q})) \subset W_i + L_i.$$

Start: let

$$L_0 := J(\mathbb{Q}), \qquad W_0 := 0.$$

Inductive Step: choose a prime p of good reduction. Consider the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\iota} & W_i + L_i \subseteq J(\mathbb{Q}) \\ \downarrow \text{red} & & \downarrow \text{red} \\ C(\mathbb{F}_p) & \xrightarrow{\iota} & J(\mathbb{F}_p) \end{array}$$

Let

$$L_{i+1} = \mathrm{Ker}\left(L_i \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p)\right).$$

Let

$$W'_{i+1} = W_i + (L_i / L_{i+1}).$$

Here by L_i/L_{i+1} we really mean a choice of representatives for the cosets of L_{i+1} in L_i. Clearly $W'_{i+1} + L_{i+1} = W_i + L_i$. So $\iota(C(\mathbb{Q})) \subset W'_{i+1} + L_{i+1}$. The vertical arrow on the right-hand side of the above diagram now factors through W'_{i+1}:

$$\begin{array}{ccccc} C(\mathbb{Q}) & \xrightarrow{\iota} & W'_{i+1} + L_{i+1} & & \\ \downarrow \text{red} & & \downarrow \text{red} & \searrow & \\ C(\mathbb{F}_p) & \xrightarrow{\iota} & J(\mathbb{F}_p) & \xleftarrow[\text{red}]{} & W'_{i+1} \end{array}$$

Let

$$W_{i+1} = \{w \in W'_{i+1} \,:\, \mathrm{red}(w) \in \iota(C(\mathbb{F}_p))\}.$$

Then $\iota(C(\mathbb{Q})) \subset W_{i+1} + L_{i+1}$. This completes the inductive step of the definition.

In practice, if the primes p are chosen randomly then the method quickly leads to a combinatorial explosion: the set W_i would grow very very quickly. Roughly speaking, a good choice of p would have

- $[L_i : L_{i+1}]$ is small;
- $\#J(\mathbb{F}_p)$ is smooth.

The first assumption means that W'_{i+1} is not too big compared to W_i, so that it is feasible to compute W_{i+1}. The second assumption is more subtle. To understand it the reader should go back to the example and recall that what made the Mordell–Weil sieve work there was the fact that the numbers N_p have common factors, and so information modulo one N_p has a good chance of contradicting information modulo another N_p.

In practice, **with a good strategy for choosing the** p, we usually find that

$$W_i = \iota(\mathscr{K}) \qquad (\mathscr{K} \subset C(\mathbb{Q}) \text{ are the known points})$$

for large i, and the index $[J(\mathbb{Q}) : L_i]$ is growing (albeit slowly). The L_i are decreasing neighbourhoods of the origin in the profinite topology. When the Mordell–Weil sieve works, it tells us that every rational point on C is close, in the profinite topology on $J(\mathbb{Q})$, to one of the known ones. For more on the right strategy for the Mordell–Weil sieve I refer the reader to [6] and to [7].

16.5. Integral Points on a Genus 2 *Curve*

Let's see one more example of the Mordell–Weil sieve given in [7]. Let

$$C : y^2 - y = x^5 - x, \qquad \iota : C \hookrightarrow J,\ P \mapsto [P - \infty].$$

The Mordell–Weil group is

$$J(\mathbb{Q}) = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z} \cdot D_2 \oplus \mathbb{Z} \cdot D_3,$$

where

$$D_1 = [(0,1) - \infty], \qquad D_2 = [(1,1) - \infty], \qquad D_3 = [(-1,1) - \infty].$$

The rank exceeds the genus and so the method of Chabauty is inapplicable. This does not however stop us from applying the Mordell–Weil sieve. The known rational points are

$$\begin{aligned}\mathscr{K} = \{&\infty,\ (-1,0),\ (-1,1),\ (0,0),\ (0,1),\ (1,0),\ (1,1),\ (2,-5),\\ &(2,6),\ (3,-15),\ (3,16),\ (30,-4929),\ (30,4930),\ (1/4,15/32),\\ &(1/4,17/32),\ (-15/16,-185/1024),\ (-15/16,1209/1024)\}.\end{aligned}$$

Using 922 prime $p < 10^6$ it can be shown that

$$\iota(C(\mathbb{Q})) \subset \iota(\mathscr{K}) + L$$

where

$$[J(\mathbb{Q}) : L] \sim 3.32 \times 10^{3240}.$$

The shortest non-zero vector in L has length $\sim 1.156 \times 10^{1080}$. From the theory of heights it follows that if $P \in C(\mathbb{Q}) \setminus \mathscr{K}$ then

$$H(P) \geq \exp(10^{2160}).$$

Here $H(P)$ is the naive height: if $P = (X/Z^2, Y/Z^5)$ with X, Y, Z integers and $\gcd(X,Y) = 1$ then $H(P) = \max\{X, Z^2\}$. Baker's theory [7] tells us that if P is an **integral point** on C then

$$H(P) \leq \exp(10^{565}).$$

So we know all the integral points:

$$C(\mathbb{Z}) = \{(-1,0),\ (-1,1),\ (0,0),\ (0,1),\ (1,0),\ (1,1),\ (2,-5),$$
$$(2,6),\ (3,-15),\ (3,16),\ (30,-4929),\ (30,4930)\}.$$

We end with the following challenge: How do you find the rational points on C?

References

[1] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, Dissertation, University of Leiden, Leiden, 1999.

[2] N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27–49.

[3] N. Bruin and N. D. Elkies, *Trinomials ax^7+bx+c and ax^8+bx+c with Galois groups of order* 168 *and* 8·168, pp. 172–188 of C. Fieker and D. R. Kohel (Eds.), **Algorithmic Number Theory**, 5th International Symposium, ANTS-V, Lecture Notes in Computer Science 2369, Springer-Verlag, 2002.

[4] N. Bruin and M. Stoll, *Deciding existence of rational points on curves: an experiment*, Experimental Mathematics **17** (2008), 181–189.

[5] N. Bruin and M. Stoll, *Two-cover descent on hyperelliptic curves*, Mathematics of Computations **78** (2009), 2347–2370.

[6] N. Bruin and M. Stoll, *The Mordell-Weil sieve: proving the non-existence of rational points on curves*, LMS Journal of Computing Mathematics **13** (2010), 272–306.

[7] Y. Bugeaud, M. Mignotte, M. Stoll, S. Siksek and Sz. Tengely, *Integral Points on Hyperelliptic Curves*, Algebra & Number Theory **2** (2008), No. 8, 859–885.

[8] J. W. S. Cassels, *Local Fields*, LMS Student Texts **3**, Cambridge University Press, 1986.

[9] J. W. S. Cassels, *Lectures of Elliptic Curves*, LMS Student Texts **24**, Cambridge University Press, 1991.

[10] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Mathematical Society Lecture Note Series **230**, Cambridge University Press, 1996.

[11] R. F. Coleman, *Effective Chabauty*, Duke Mathematical Journal **52** (1985), No. 3, 765–770.

[12] E. V. Flynn, *A Flexible Method for Applying Chabauty's Theorem*, Compositio Math. **105** (1997), 79–94.

[13] E. V. Flynn and J. L. Wetherell, *Covering Collections and a Challenge Problem of Serre*, Acta Arithmetica **XCVIII.2** (2001), 197–205.

[14] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, GTM **201**, Springer, 2000.

[15] W. McCallum and B. Poonen, *The Method of Chabauty and Coleman*, in "Explicit Methods in Number Theory: Rational Points and Diophantine Equations", eds K. Belabas et al., Panoramas et synthèses **36** (2012).

[16] B. Poonen and E. F. Schaefer, *Explicit descent on cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188.

[17] B. Poonen and M. Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Annals of Mathematics **180** (2014), No. 3, 1137–1166.

[18] S. Siksek, *Chabauty for symmetric powers of curves*, Algebra & Number Theory **3** (2009), no. 2, 209–236.

[19] S. Siksek, *Explicit Chabauty over number fields*, Algebra & Number Theory **7** (2013), no. 4, 765–793.

[20] S. Siksek and M. Stoll, *Partial descent on hyperelliptic curves and the generalized Fermat equation* $x^3+y^4+z^5=0$, Bulletin of the LMS **44** (2012) 151–166.

[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer, 1986.

[22] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM **151**, Springer, 1994.

[23] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. dissertation, University of California at Berkeley, 1997.