Descent and Covering Collections

Michael STOLL
Universität Bayreuth, 95440 Bayreuth, Germany

Abstract. We explain several approaches that allow to prove that a given curve over $\mathbb{Q}$ has no rational points.

Keywords. Rational points, Local solubility, Descent, Selmer set

Introduction

These are notes for the series of three lectures I gave at the NATO Advanced Study Institute on *Arithmetic of Hyperelliptic Curves* that took place in Ohrid, Macedonia, in the summer of 2014.

The main theme of these notes is how one can try to prove that a given curve over $\mathbb{Q}$ does not possess rational points, with a focus on hyperelliptic curves. After introducing hyperelliptic curves and summarizing their most important properties, we study the notion of 'everywhere local solubility'. A curve (or more generally, any variety) over $\mathbb{Q}$ is *everywhere locally soluble* or *ELS*, if it has real points and points over $\mathbb{Q}_p$ for all primes p. We explain that it can be effectively tested whether a curve is ELS or not. Obviously, any curve with rational points is also ELS, so this provides a necessary condition. In most cases of interest (curves of genus zero being the exception), the necessary condition is not sufficient, and indeed a large proportion of curves are ELS, but do not possess rational points. We therefore need more sophisticated ways of proving the non-existence of rational points. One general approach that can be used is *descent*. In its most general version, it uses an unramified and geometrically Galois covering $\pi\colon D \to C$ of the given curve C. Associated to this covering is its *Selmer set* $\mathrm{Sel}(\pi)$. The Selmer set is finite and computable (at least in principle) and receives a map from the set of rational points $C(\mathbb{Q})$. So $\mathrm{Sel}(\pi) = \emptyset$ implies that the curve has no rational points. In the last part of these notes, we explain how a certain Selmer set, the *2-Selmer set*, of a hyperelliptic curve can be computed in practice. We end by mentioning a recent result due to Manjul Bhargava that says that for large g, only a tiny fraction of hyperelliptic curves of genus g can have non-empty 2-Selmer set.

For an overview of the various methods that can be used to determine the set of rational points on a curve, we refer to the survey [1].

Prerequisites

We assume familiarity with algebraic curves, the main results of algebraic number theory and the basic theory of p-adic fields. We give a quick overview of the latter in Section 4.

1. Hyperelliptic Curves

In these notes, a *curve* always means a 'nice' curve, i.e., a smooth, projective and geometrically irreducible curve.

We begin with two definitions of what a hyperelliptic curve is, one more concrete and one more abstract.

Definition 1.1. A *hyperelliptic curve* C over a field k not of characteristic 2 is the (nice) curve associated to an affine plane curve given by an equation of the form

$$y^2 = f(x) = f_n x^n + f_{n-1} x^{n-1} + \ldots + f_1 x + f_0 \,,$$

where f is a squarefree polynomial (equivalently, the discriminant $\mathrm{disc}(f)$ of f is nonzero).

We usually simply write the affine equation

$$C\colon y^2 = f(x)$$

to denote the smooth and projective curve C.

A more abstract definition (that works over any field k) is as follows.

Definition 1.2. A *hyperelliptic curve* over k is a (nice) curve C over k with a morphism $\pi\colon C \to \mathbb{P}^1$ of degree 2, which is defined over k.

Remark 1.3. Some people do not require π to be defined over k. One then obtains a more general notion of 'hyperelliptic', which is sometimes called 'geometrically hyperelliptic' as opposed to 'hyperelliptic over k'. In this more general case, one still has a double cover $\pi\colon C \to Q$ over k, but Q may be a (nice) conic. If Q has k-points, then $Q \cong \mathbb{P}^1_k$ (see below) and we are in the situation of our definition above. Otherwise it follows that C cannot have k-points either, and so these curves are not really interesting for the question we are discussing here.

Writing $k(x)$ for the function field of $\mathbb{P}^1_k$, the function field of C is a quadratic extension of $k(x)$, so if $\mathrm{char}(k) \neq 2$ it is of the form $k(x, \sqrt{f(x)})$ for some squarefree polynomial f. Writing y for $\sqrt{f(x)}$, we obtain the equation $y^2 = f(x)$. Conversely, if $C\colon y^2 = f(x)$ is a hyperelliptic curve according to the first definition, then $C \to \mathbb{P}^1$, $(x, y) \mapsto x$, is a morphism of degree 2 defined over k.

In characteristic 2, one has to consider more general equations of the form

$$y^2 + h(x)y = f(x)\,.$$

If the degree of f is $2g+1$ or $2g+2$, then the curve has genus g. This follows (for example) from the Riemann-Hurwitz formula: the covering π has degree 2 and is ramified at $2g+2$ points (corresponding to the zeros of F (see below) on $\mathbb{P}^1$), so

$$2\,\mathrm{genus}(C) - 2 = 2(-2) + (2g+2) = 2g - 2\,.$$

Usually, one requires f to have degree at least 5. This corresponds to restricting the genus to be ≥ 2. Sometimes, however, it is convenient to also allow 'hyperelliptic' curves of genus 1 or even 0.

We can realize C as a smooth curve in the weighted projective plane $\mathbb{P}_{1,g+1,1}$: Homogenize f to obtain $F(x,z)$ of *even* degree $2g+2$ such that $f(x) = F(x,1)$. Then the equation $y^2 = F(x,z)$ is homogeneous of degree $2g+2$ if we give x and z weight 1 and y weight $g+1$. The projective curve C is covered by the two affine charts $y^2 = f(x) = F(x,1)$ and $v^2 = F(1,u)$.

So the points at infinity on C (which are the points lying above $(1:0) \in \mathbb{P}^1$) are $\infty_s = (1:s:0)$ where $s^2 = F(1,0) = f_{2g+2}$: There is one point $\infty = \infty_0$ when $\deg(f)$ is odd, otherwise there are two (which are k-rational if and only if the leading coefficient of f is a square in k).

Any (nice) curve C of genus 2 over k is hyperelliptic over k: The canonical divisor class has degree 2 and 2-dimensional Riemann-Roch space, so gives rise to a double cover $\pi\colon C \to \mathbb{P}^1$.

In general, for $g \geq 2$, the moduli space of *hyperelliptic* curves of genus g has dimension $2g+3-\dim \mathrm{GL}(2) = 2g-1$, whereas the moduli space of *all* curves of genus g has dimension $3g-3$, so the locus of hyperelliptic curves is of codimension $g-2$.

Since hyperelliptic curves always have the nontrivial automorphism

$$w\colon (x,y) \mapsto (x,-y)$$

(called the *hyperelliptic involution*), there can be curves that are non-isomorphic over k, but become isomorphic over $\bar{k}$: for $d \in k^\times$, the curves $y^2 = f(x)$ and $y^2 = df(x)$ are usually not k-isomorphic if d is not a square in k, but become isomorphic over $k(\sqrt{d})$.

2. Rational Points on Curves

As usual, we write $C(k)$ for the set of k-rational points on C. For a hyperelliptic curve $C\colon y^2 = f(x)$ over k we then have by the above that

$$\begin{aligned}
C(k) &= \{(\xi,\eta) \in k^2 : \eta^2 = f(\xi)\} \cup \{\infty\} && \text{if } 2 \nmid \deg(f);\\
C(k) &= \{(\xi,\eta) \in k^2 : \eta^2 = f(\xi)\} && \text{if } 2 \mid \deg(f) \text{ and } \mathrm{lcf}(f) \neq \square;\\
C(k) &= \{(\xi,\eta) \in k^2 : \eta^2 = f(\xi)\} \cup \{\infty_s, \infty_{-s}\} && \text{if } 2 \mid \deg(f) \text{ and } \mathrm{lcf}(f) = s^2.
\end{aligned}$$

($\mathrm{lcf}(f)$ denotes the leading coefficient of f.)

In the following, we will concentrate on the case $k = \mathbb{Q}$. (More generally, we could consider an algebraic number field k. Essentially everything described here also works in this more general situation, but practical computations tend to become quite a bit more involved.)

The main question will be:

Question 2.1. How can we determine the set $C(\mathbb{Q})$?

In general, the structure of the set $C(\mathbb{Q})$ of rational points on a (nice) curve over $\mathbb{Q}$ depends on the genus g of C.

Theorem 2.2.

If $g = 0$, then $C(\mathbb{Q})$ is either empty, or else $C \cong \mathbb{P}^1$ over $\mathbb{Q}$, so C has infinitely many rational points, which can be given by a 'formula' in terms of a parameter in $\mathbb{P}^1(\mathbb{Q})$.

If $g = 1$, then $C(\mathbb{Q})$ can be empty. Otherwise pick a point $P_0 \in C(\mathbb{Q})$. Then $C(\mathbb{Q})$ has a natural structure of an abelian group with zero P_0; this group is finitely generated (and C is an elliptic curve).

If $g \geq 2$, then $C(\mathbb{Q})$ is finite.

The first result is classical (in parts going back to Diophantus), the second is due to Mordell [2] who (in the same paper) also conjectured the third, which was finally shown some 60 years later by Faltings [3].

Note that this trichotomy is given by the sign (> 0, $= 0$, < 0) of the *Euler characteristic* $2 - 2g$ of C, which is a *topological* invariant of the Riemann surface $C(\mathbb{C})$! This is an instance (one of the rare ones with proof) of the principle that 'Geometry governs Arithmetic'.

We will only consider the case $g \geq 2$. Then $C(\mathbb{Q})$ is finite and so the points can be enumerated in principle. However, none of the known proofs of Faltings' Theorem is *effective:* It is an open problem whether $C(\mathbb{Q})$ is computable in general. For concrete curves C, we may be able to determine $C(\mathbb{Q})$, though.

We split the problem into two parts:

(1) Decide whether $C(\mathbb{Q})$ is empty or not!
(2) If $P_0 \in C(\mathbb{Q})$ is given, determine $C(\mathbb{Q})$!

In these notes, we will mainly focus on the first problem.

Remark 2.3. If $C(\mathbb{Q}) \neq \emptyset$, then one expects C to have a reasonably small rational point, if the genus is ≥ 2. (This would actually follow from Vojta's Conjecture.) As an illustration, consider all genus 2 curves $y^2 = f(x)$ such that f has integral coefficients of absolute value ≤ 3. We measure the 'size' of a point (ξ, η) by the height (i.e., the maximum absolute value of numerator and denominator when written as a fraction in lowest terms) of the x-coordinate ξ. Then of all such curves (up to $\mathbb{Q}$-isomorphism) that possess rational points, one had a smallest point of height ≈ 1500, one of height ≈ 400 and all others (there are roughly 140 000 such isomorphism classes of curves with rational points) have a point of height < 80. See [4] for details.

So if $C(\mathbb{Q}) \neq \emptyset$, then it is easy to prove this fact: just find a point! The hard part is to *prove* that there is no point, when one is unable to find one.

3. Local Solubility

How can we show that $C(\mathbb{Q}) = \emptyset$? One possibility is to look at points on C over larger fields, for which the question is easy to decide. For example, since $\mathbb{Q} \subset \mathbb{R}$, we also have $C(\mathbb{Q}) \subset C(\mathbb{R})$, and we can easily check if $C(\mathbb{R}) = \emptyset$ or not: for a

hyperelliptic curve $C\colon y^2 = f(x)$, we have $C(\mathbb{R}) = \emptyset$ if and only if f has no real roots and $\operatorname{lcf}(f) < 0$.

Example 3.1. Let $C\colon y^2 = -x^6 - 17$, then $C(\mathbb{R}) = \emptyset$, whence $C(\mathbb{Q}) = \emptyset$.

Example 3.2. What about $C\colon y^2 = -x^6 + 3$? We have $C(\mathbb{R}) \neq \emptyset$, but we can still prove that $C(\mathbb{Q}) = \emptyset$, as follows. Let $\xi \in \mathbb{Q}$ (it is clear that there are no rational points at infinity, since the leading coefficient -1 is not a square). We write $v_3(\xi)$ for the 3-adic valuation of ξ.

- If $v_3(\xi) > 0$, then $v_3(-\xi^6 + 3) = 1$, so $-\xi^6 + 3$ cannot be a square;
- if $v_3(\xi) \leq 0$, then $3^{-6v_3(\xi)}(-\xi^6 + 3) \equiv -1 \bmod 3$; again $-\xi^6 + 3 \neq \square$.

Indeed, this even proves that $C(\mathbb{Q}_3) = \emptyset$!

More generally, we can use any field of p-adic numbers $\mathbb{Q}_p$ and ask whether $C(\mathbb{Q}_p)$ is empty or not. Clearly $C(\mathbb{Q}) \neq \emptyset$ implies that $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p. This leads to the following definition.

Definition 3.3. A (nice) curve C over $\mathbb{Q}$ is said to be *everywhere locally soluble* or *ELS*, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Being ELS is a necessary condition for having rational points. This condition is also sufficient for $g = 0$ (and known as the 'Hasse Principle'), but this is false in general.

Question 3.4. Can we decide if a given curve is ELS?

Note that there are two potentially problematic features of the definition. The first is that we have to check the existence of $\mathbb{Q}_p$-points for infinitely many distinct fields $\mathbb{Q}_p$. The second is that each of the fields $\mathbb{Q}_p$ is (as $\mathbb{R}$) uncountable, and it is not obvious how to check if $\mathbb{Q}_p$-points exist. We will deal with these problems below. But before we do that, we recall the basic facts about p-adic numbers.

4. Digression: p-adic Numbers

There are essentially two ways of constructing the field $\mathbb{Q}_p$ of p-adic numbers:

- as a completion of $\mathbb{Q}$ (in analogy with $\mathbb{R}$); or
- as the field of fractions of the projective limit $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

We will review the first construction and sketch how it relates to the second. Define the p-adic absolute value on $\mathbb{Q}$ by

$$|\xi|_p = \begin{cases} 0 & \text{if } \xi = 0; \\ p^{-n} = p^{-v_p(\xi)} & \text{if } \xi = p^n \frac{a}{b} \text{ with } p \nmid ab. \end{cases}$$

Then $|\alpha\beta|_p = |\alpha|_p \cdot |\beta|_p$ and $|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \leq |\alpha|_p + |\beta|_p$, so $|\cdot|_p$ has all the properties of an absolute value, and we can define $\mathbb{Q}_p$ as the completion

of $\mathbb{Q}$ with respect to $|\cdot|_p$. (I.e., we form the ring of Cauchy sequences in $\mathbb{Q}$ with respect to the p-adic absolute value and define $\mathbb{Q}_p$ as the quotient of this ring by the maximal ideal formed by sequences tending to zero. This results in a field that is a complete metric space with respect to the metric induced by the absolute value, which contains $\mathbb{Q}$ as a dense subfield.)

The closed unit ball $\mathbb{Z}_p = \{\xi \in \mathbb{Q}_p : |\xi|_p \leq 1\}$ forms a compact subring; it is the topological closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. It is then easy to check that

$$p^n\mathbb{Z}_p = \{\xi \in \mathbb{Q}_p : |\xi|_p \leq p^{-n}\} \quad \text{and} \quad \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}\,.$$

This leads to the description of the *ring of p-adic integers* as

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}\,,$$

which is more suitable for computations. We then have

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p\left[\tfrac{1}{p}\right],$$

and we can think of elements of $\mathbb{Q}_p$ as 'Laurent series in p'

$$\xi = \sum_{n=n_0}^{\infty} a_n p^n \qquad \text{with } a_n \in \{0, 1, \ldots, p-1\}.$$

It can be shown that $\mathbb{R}$ and the $\mathbb{Q}_p$ for all primes p are all the possible completions of $\mathbb{Q}$. This explains the word 'everywhere' in Definition 3.3; the word 'locally' refers to the fact that all these fields are *local fields:* they are locally compact with respect to their natural topology.

An important tool for working with $\mathbb{Q}_p$ is provided by *Hensel's Lemma:*

Theorem 4.1. *Let $f \in \mathbb{Z}_p[x]$ be monic; write $\bar{f}$ for its image in $\mathbb{F}_p[x]$ (obtained by reducing the coefficients mod p). If there is $a \in \mathbb{F}_p$ such that $\bar{f}(a) = 0$ and $\bar{f}'(a) \neq 0$ (i.e., a is a simple root of $\bar{f}$), then there is a unique $\alpha \in \mathbb{Z}_p$ with $\bar{\alpha} = a$ and $f(\alpha) = 0$.*

Sketch of proof. Take any α_0 with $\bar{\alpha}_0 = a$ and define the sequence (α_n) by Newton iteration: $\alpha_{n+1} = \alpha_n - f(\alpha_n)/f'(\alpha_n)$. It is then fairly easy to show that (α_n) converges to a limit $\alpha \in \mathbb{Z}_p$ that satisfies $f(\alpha) = 0$.

Alternatively, use the Banach Fixed Point Theorem: the 'Newton map' $\alpha \mapsto \alpha - f(\alpha)/f'(\alpha)$ is contracting (one could also use $f'(\alpha_0)$ instead of $f'(\alpha)$ for a fixed α_0) on the set of $\alpha \in \mathbb{Z}_p$ reducing to a. This also shows uniqueness. □

The following is an important consequence.

Corollary 4.2. *Let $\mathcal{C}$ be a curve over $\mathbb{Z}_p$ and let $q \in \mathcal{C}(\mathbb{F}_p)$ be a smooth point on the special fiber $\mathcal{C} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$. Then q lifts to a point $Q \in \mathcal{C}(\mathbb{Q}_p)$ (i.e., $\bar{Q} = q$).*

Proof. We give a proof in the case that $\mathcal{C}$ is a plane curve. We can restrict to a suitable affine chart. So let $\mathcal{C}$ be given by an equation $F(x, y) = 0$, and let $q = (a, b)$. Since q is a smooth point on $\mathcal{C} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ by assumption, at least one of the partial derivatives $\frac{\partial \bar{F}}{\partial x}(a, b)$ and $\frac{\partial \bar{F}}{\partial y}(a, b)$ does not vanish, say the first one. Let $\beta \in \mathbb{Z}_p$ be any lift of b and set $f(x) = F(x, \beta)$. Then $\bar{f}(a) = \bar{F}(a, b) = 0$ and $\bar{f}'(a) = \frac{\partial \bar{F}}{\partial x}(a, b) \neq 0$, so by Theorem 4.1 there is $\alpha \in \mathbb{Z}_p$ lifting a such that $F(\alpha, \beta) = 0$. Then $Q = (\alpha, \beta) \in \mathcal{C}(\mathbb{Q}_p)$. □

5. Checking Local Solubility

We will now show how checking the infinitely many conditions of Definition 3.3 can be reduced to a finite amount of computation. First we reduce to finitely many conditions. For this, we need the following important result due to Weil [5].

Theorem 5.1. *Let C be a (nice) curve of genus g over $\mathbb{F}_p$. Then*

$$p + 1 - 2g\sqrt{p} \leq \#C(\mathbb{F}_p) \leq p + 1 + 2g\sqrt{p}\,.$$

Corollary 5.2. *Let C be a (nice) curve of genus g over $\mathbb{Q}$, and let $p \geq 4g^2$ be a prime of good reduction for C. Then $C(\mathbb{Q}_p) \neq \emptyset$.*

'Good reduction' means that there is a 'model' $\mathcal{C}$ of C over $\mathbb{Z}_p$ (so that the generic fiber $\mathcal{C} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is isomorphic to $C_{\mathbb{Q}_p}$) that has smooth special fiber $\mathcal{C} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$.

Proof. Let $\mathcal{C}$ be a model of C over $\mathbb{Z}_p$ with good reduction. The assumption $p \geq 4g^2$ implies $p \geq 2g\sqrt{p}$, so by Theorem 5.1, $\mathcal{C}(\mathbb{F}_p) \neq \emptyset$. Every point on $\mathcal{C} \otimes \mathbb{F}_p$ is smooth by choice of $\mathcal{C}$, so $C(\mathbb{Q}_p) = \mathcal{C}(\mathbb{Q}_p) \neq \emptyset$ by Theorem 4.1. □

This means that we only have to check for real points and for p-adic points for those primes p that are either 'small' in the sense that $p < 4g^2$ or are of bad reduction for C. For each of these finitely many primes, we can check whether $C(\mathbb{Q}_p)$ is empty or not by the following procedure.

1. Start with some model $\mathcal{C}$ of C over $\mathbb{Z}_p$.
2. If $\mathcal{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$.
3. If $\mathcal{C}(\mathbb{F}_p)$ contains a smooth point, then $C(\mathbb{Q}_p) \neq \emptyset$.
4. Otherwise: for each point $P \in \mathcal{C}(\mathbb{F}_p)$, 'zoom in' at P to get a new model $\mathcal{C}_P$ and repeat.
5. If for some P, $\mathcal{C}_P(\mathbb{Q}_p) \neq \emptyset$, then $C(\mathbb{Q}_p) \neq \emptyset$, else $C(\mathbb{Q}_p) = \emptyset$.

Since we assume that C is smooth, the 'zooming in' will eventually produce models with smooth fiber over $\mathbb{F}_p$. For a hyperelliptic curve, assuming that P has x-coordinate zero, we must have

$$y^2 = f(x) = pa_0 + pa_1x + a_2x^2 + a_3x^3 + \ldots$$

(since the curve mod p is singular at P, $\bar{f}$ must have a multiple root at zero). Any point lifting P must have its x- and y-coordinates divisible by p, so we substitute $x \leftarrow px_1$, $y \leftarrow py_1$. Dividing by p, we obtain

$$py_1^2 = a_0 + pa_1x_1 + pa_2x_1^2 + p^2a_3x_1^3 + \dots .$$

So $\mathcal{C}_P(\mathbb{Q}_p) = \emptyset$ if $p \nmid a_0$. Otherwise write $a_0 = pa_0'$ and divide by p again to obtain the new model

$$y_1^2 = a_0' + a_1x_1 + a_2x_1^2 + pa_3x_1^3 + \ldots = p^{-2}f(px_1)\,.$$

If this process can be repeated indefinitely, then one can construct a convergent sequence (ξ_n) in $\mathbb{Z}_p$, say with limit ξ, such that

$$f(\xi) = \lim_{n\to\infty} f(\xi_n) = 0 \quad \text{and} \quad f'(\xi) = \lim_{n\to\infty} f'(\xi_n) = 0\,,$$

which contradicts the assumption that f has no multiple roots.

We summarize our findings in the following statement.

Corollary 5.3. *Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of genus g such that $f(x) \in \mathbb{Z}[x]$. Then*

(1) $C(\mathbb{Q}_p) \neq \emptyset$ if $p \geq 4g^2$ and $p \nmid \operatorname{disc}(f)$;
(2) we can decide if $C(\mathbb{R}) \neq \emptyset$ or not;
(3) we can decide if $C(\mathbb{Q}_p) \neq \emptyset$ or not for the finitely many primes p not covered by (1).

So we can decide whether C is ELS or not!

To get a feeling how successful this test is for proving that a curve has no rational points, consider hyperelliptic curves of fixed genus g. Order all equations $y^2 = f(x)$ such that f has integral coefficients and is squarefree of degree $2g+1$ or $2g+2$ by increasing height $H(f) = \max_j |f_j|$. Denote that family by $\mathcal{F}_g$.

For a subset $S \subset \mathcal{F}_g$, we define its *density* as the limit

$$\delta(S) = \lim_{X\to\infty} \frac{\#\{C \in S : H(C) \leq X\}}{\#\{C \in \mathcal{F}_g : H(C) \leq X\}}$$

if the limit exists. We similarly define the *upper* and *lower density* $\bar{\delta}(S)$ and $\underline{\delta}(S)$ by replacing the limit with a lim sup or lim inf, respectively.

Conjecture 5.4. *The set of curves in $\mathcal{F}_g$ with rational points has density zero.*

Heuristically, one would expect the fraction of curves with rational points up to height X to decrease like a constant (depending on g) times $X^{-1/2}$.

The best result so far in this direction is due to Bhargava and quite recent.

Theorem 5.5. *The upper density of curves with rational points in $\mathcal{F}_g$ is $o(2^{-g})$.*

We will come back to this at the end of these notes.

Now contrast Conjecture 5.4 with the following result (see [6]).

Proposition 5.6. *The set of ELS curves in $\mathcal{F}_g$ has a density $\delta_g > 0$.*

For example, we have $\delta_2 \approx 0.85$–0.86; as g grows, δ_g gets closer to 1, but $\limsup_{g\to\infty} \delta_g < 1$. The density δ_g can be written as a product $\delta_g = \delta_{g,\infty} \prod_p \delta_{g,p}$ of local densities. Here $\delta_{g,\infty}$ is the measure of the set of coefficient vectors inside the cube $[-\frac{1}{2}, \frac{1}{2}]^{2g+3}$ such that the corresponding polynomial takes a nonnegative value on $\mathbb{R}$, and $\delta_{g,p}$ is the p-adic measure of the set of coefficient vectors in $\mathbb{Z}_p^{2g+3}$ such that the corresponding polynomial takes a square value on $\mathbb{Q}_p$. One can show that $\delta_{g,\infty} \to 1$ as $g \to \infty$, but $\delta_{g,p}$ tends to a limit strictly less than 1 for all primes p.

Conclusion: We need a way of proving $C(\mathbb{Q}) = \emptyset$ even when C is ELS!

6. Descent Theory

6.1. A Double Cover

Before we give a general statement, let us look at a special case of descent. Let $C\colon y^2 = f(x)$ be hyperelliptic over $\mathbb{Q}$ with $f \in \mathbb{Z}[x]$ and assume that $f = f_1 f_2$ in $\mathbb{Z}[x]$ with at least one of $\deg(f_1)$, $\deg(f_2)$ even. Assume that $P = (\xi, \eta) \in C(\mathbb{Q})$ is a rational point, so

$$\eta^2 = f(\xi) = f_1(\xi) f_2(\xi)\,.$$

Then there is a unique squarefree integer d such that $f_1(\xi) = d\eta_1^2$ and $f_2(\xi) = d\eta_2^2$ with $\eta_1, \eta_2 \in \mathbb{Q}$. (Note that at least one of $f_1(\xi)$ and $f_2(\xi)$ is nonzero.)

Define a curve $D_d\colon dy_1^2 = f_1(x), dy_2^2 = f_2(x)$ (as usual, we mean the smooth projective curve associated to this curve in affine 3-space) and the double cover $\pi_d\colon D_d \to C$, $(x, y_1, y_2) \mapsto (x, dy_1y_2)$. The above then says that $P \in \pi_d\big(D_d(\mathbb{Q})\big)$. We have shown:

$$C(\mathbb{Q}) = \bigcup_{d \text{ squarefree}} \pi_d\big(D_d(\mathbb{Q})\big)\,. \tag{1}$$

There are infinitely many squarefree integers, so this statement is not yet very useful. But we will see that we can restrict to a finite union.

To do this, we write everything homogeneously:

$$D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$$

with F_1, F_2 homogeneous of even degree, squarefree and coprime. (This is possible since we assume at least one of f_1 and f_2 to have even degree. If both degrees were odd, then F_1 and F_2 would have the common factor z.)

Now assume that the prime p divides d and that we have a $\mathbb{Q}_p$-rational point on D_d with image $(\xi : \zeta)$ in $\mathbb{P}^1$. We can then assume ξ and ζ to be coprime p-adic integers ('coprime' here just means 'not both divisible by p': p is the only prime in the PID $\mathbb{Z}_p$); then $\eta_1, \eta_2 \in \mathbb{Z}_p$ as well. Modulo p, we then find

$$0 \equiv d\eta_1^2 = F_1(\xi, \zeta) \qquad \text{and} \qquad 0 \equiv d\eta_2^2 = F_2(\xi, \zeta)\,,$$

so $\bar{\zeta}x - \bar{\xi}z$ is a common linear factor of $\bar{F}_1$ and $\bar{F}_2$. This means that p divides the resultant $\mathrm{Res}(F_1, F_2) \in \mathbb{Z}$.

6.2. Digression: The Resultant of Two Binary Forms

Let F and G be two binary forms over a field k:

$$\begin{aligned} F(x,z) &= f_m x^m + f_{m-1}x^{m-1}z + \ldots + f_1 x z^{m-1} + f_0 z^m \\ G(x,z) &= \ g_n x^n \ + \ g_{n-1}x^{n-1}z \ + \ldots + g_1 x z^{n-1} \ + g_0 z^n \end{aligned}$$

Then the $(n+m) \times (n+m)$ determinant

$$\mathrm{Res}(F,G) = \begin{vmatrix} f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 \\ g_n & g_{n-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & g_n & g_{n-1} & \cdots & g_1 & g_0 & 0 \\ 0 & \cdots & 0 & g_n & g_{n-1} & \cdots & g_1 & g_0 \end{vmatrix}$$

is the *Resultant* of F and G.

The resultant has the following properties (exercise!):

1. $\mathrm{Res}(G,F) = (-1)^{(\deg F)(\deg G)}\,\mathrm{Res}(F,G)$.
2. $\mathrm{Res}(F,c) = c^{\deg F}$ if c is constant.
3. $\mathrm{Res}(F, -\beta x + \alpha z) = F(\alpha, \beta)$.
4. $\mathrm{Res}(F, GH) = \mathrm{Res}(F,G)\,\mathrm{Res}(F,H)$.
5. $\mathrm{Res}(F,G) = \mathrm{Res}(F, G+FH)$ if $\deg F + \deg H = \deg G$.
6. $\mathrm{Res}(F\circ\gamma, G\circ\gamma) = \det(\gamma)^{(\deg F)(\deg G)}\,\mathrm{Res}(F,G)$ for $\gamma \in \mathrm{GL}(2,k)$.

The most important property is the following.

7. $\mathrm{Res}(F,G) = 0$ if and only if F and G have a common factor.

By its definition, the resultant is a polynomial with integral coefficients in the coefficients of the two binary forms. In particular, it is compatible with ring homomorphisms. This means that (denoting reduction mod p by a bar)

$$\mathrm{Res}(\bar{F}, \bar{G}) = \overline{\mathrm{Res}(F,G)}\,,$$

so that $\bar{F}$ and $\bar{G}$ have a common factor if and only if p divides $\mathrm{Res}(F,G)$.

6.3. Twists and Selmer Set

Recall the curve

$$D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$$

and that $p \mid d$, $D_d(\mathbb{Q}_p) \neq \emptyset$ together imply $p \mid \mathrm{Res}(F_1,F_2)$. This leads to the following.

Proposition 6.1. *Let $C\colon y^2 = f_1(x)f_2(x)$ be as above and set*

$$S = \left\{ d \in \mathbb{Z} : d \text{ squarefree and } \forall p\colon p \mid d \Rightarrow p \mid \mathrm{Res}(F_1,F_2) \right\}.$$

Then S is finite and

$$C(\mathbb{Q}) = \bigcup_{d\in S} \pi_d\big(D_d(\mathbb{Q})\big)\,.$$

In particular:

$$\forall d \in S\colon D_d \text{ not ELS} \quad \text{implies} \quad C(\mathbb{Q}) = \emptyset\,.$$

Proof. By the considerations above, we have that if $p \mid d$, but $p \nmid \mathrm{Res}(F_1,F_2)$, then D_d is not ELS, so $D_d(\mathbb{Q}) = \emptyset$. This shows that the union in (1) can be restricted to the set S, which is obviously finite (since F_1 and F_2 are coprime, the resultant $\mathrm{Res}(F_1,F_2) \in \mathbb{Z}$ is nonzero and has only finitely many prime divisors). If D_d fails to be ELS for every $d \in S$, then the union is a union of empty sets. □

Example 6.2. Consider

$$C\colon y^2 = (-x^2-x+1)(x^4+x^3+x^2+x+2) = f_1(x)f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0)=2$, $f(1)=-6$, $f(-2)=-12$). We compute $\mathrm{Res}(F_1,F_2) = 19$, so $S = \{1,-1,19,-19\}$. Since $f_2(\xi) > 0$ for all $\xi \in \mathbb{R}$, we have $D_d(\mathbb{R}) = \emptyset$ for $d < 0$.

Also $D_d(\mathbb{F}_3) = \emptyset$ and so $D_d(\mathbb{Q}_3) = \emptyset$ for $d \equiv 1 \bmod 3$ ($\bar{F}_1(1,0) = -1 \neq \square$, $\bar{f}_2(0) = -1$, $\bar{f}_1(1) = -1$, $\bar{f}_2(-1) = -1$).

So for all $d \in S$, we have that D_d is not ELS, therefore $C(\mathbb{Q}) = \emptyset$.

Now we would like to generalize this approach. To do this, we should ask ourselves what were the essential ingredients that made the argument work. It turns out that the relevant condition is that the morphism $\pi\colon D \to C$, $(x,y_1,y_2) \mapsto (x,y_1y_2)$, where

$$D\colon y_1^2 = f_1(x)\,, \quad y_2^2 = f_2(x)\,,$$

is an *unramified* double cover. This is used (in the form '$\mathrm{Res}(F_1,F_2) \neq 0$') for the finiteness statement.

(Note: We need (at least one of) $\deg f_1$ and $\deg f_2$ to be even for the cover to be unramified; otherwise it ramifies above infinity.)

The result extends in fact to general unramified double covers, as follows.

Theorem 6.3. *Let C and D be (nice) curves over $\mathbb{Q}$ such that there is an unramified double cover $\pi\colon D \to C$. Then the set $\mathrm{Sel}(\pi)$ of squarefree $d \in \mathbb{Z}$ such that D_d is ELS, where $\pi_d\colon D_d \to C$ is the corresponding twist of π, is finite and computable, and we have*

$$C(\mathbb{Q}) = \bigcup_{d \in \mathrm{Sel}(\pi)} \pi_d\big(D_d(\mathbb{Q})\big)\,.$$

In particular, if $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

At least locally, the double cover π can be defined by adding an equation $y^2 = f$ to the equations defining C, where f is a suitable rational function on C. The quadratic *twist* corresponding to d is then given by $dy^2 = f$.

Definition 6.4. The set $\mathrm{Sel}(\pi)$ is called the *Selmer set* of π.

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$. However, we can generalize the preceding theorem to more general covers.

Let $\pi\colon D \to C$ be an unramified covering that is in addition *geometrically Galois*. The latter condition means that the extension $\bar{\mathbb{Q}}(C) \subset \bar{\mathbb{Q}}(D)$ of function fields is a Galois extension (which is equivalent to saying that the group of deck transformations of the covering of Riemann surfaces $D(\mathbb{C}) \to C(\mathbb{C})$ has order $\deg \pi$). The word 'geometrically' refers to the fact that we only require the extension of function fields to be Galois after a base-change to $\bar{\mathbb{Q}}$. The group of automorphisms of π defined over $\mathbb{Q}$ may well be smaller. Note that the condition is automatically satisfied when $\deg \pi = 2$, since then there is always the automorphism exchanging the two sheets of the covering.

Definition 6.5. A *twist* of π is a covering $\pi'\colon D' \to C$ over $\mathbb{Q}$ that over $\bar{\mathbb{Q}}$ is isomorphic to π: there is an isomorphism $\phi\colon D_{\bar{\mathbb{Q}}} \to D'_{\bar{\mathbb{Q}}}$ such that $\pi' \circ \phi = \pi$.

Twists of π are classified by the elements of the Galois cohomology set $H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$. If $\mathrm{Aut}(\pi)$ is abelian, then this set is actually a group. For example, $H^1(\mathbb{Q}, \{\pm 1\}) \cong \mathbb{Q}^\times/\text{squares} \mathrel{\hat{=}} \{\text{squarefree integers}\}$. For the following, it is not really necessary to know what this cohomology set is; we use it only to denote a set parametrizing the twists of π. For $\xi \in H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$, we write $\pi_\xi\colon D_\xi \to C$ for the corresponding twist of π.

The Descent Theorem for double covers then generalizes to the following Descent Theorem. A different, but essentially equivalent version is due to Chevalley and Weil [7].

Theorem 6.6. *Let C and D be (nice) curves over $\mathbb{Q}$ such that there is an unramified and geometrically Galois covering $\pi\colon D \to C$. Then the set $\mathrm{Sel}(\pi)$ consisting of those elements $\xi \in H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$ such that D_ξ is ELS is finite and computable, and we have*

$$C(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi\big(D_\xi(\mathbb{Q})\big)\,.$$

In particular, if $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

In the proof, one uses the fact that the covering is geometrically Galois to show that every rational point on C lifts to a rational point on some twist D_ξ (this is analogous to the argument leading to equation (1)). The fact that the covering is unramified is used to show that the set $\mathrm{Sel}(\pi)$ is finite (this is analogous to the proof of Proposition 6.1).

As before, the set $\mathrm{Sel}(\pi)$ is called the *Selmer set* of π.

The computability holds 'in principle'. In the next section, we will see one situation in which it is also practical.

Let us discuss some of the practical and theoretical aspects of descent on curves.

If we can compute $\mathrm{Sel}(\pi)$ for some covering $\pi\colon D \to C$, then:

- If $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.
- Otherwise, we obtain a finite list of curves D_ξ, $\xi \in \mathrm{Sel}(\pi)$, with coverings $\pi_\xi\colon D_\xi \to C$ such that $C(\mathbb{Q}) = \bigcup_{\xi\in\mathrm{Sel}(\pi)} \pi_\xi\big(D_\xi(\mathbb{Q})\big)$.

Definition 6.7. In the latter case, the family $(\pi_\xi)_{\xi\in\mathrm{Sel}(\pi)}$ is a *covering collection* for C.

If we can determine $D_\xi(\mathbb{Q})$ for all $\xi \in \mathrm{Sel}(\pi)$, then we also know $C(\mathbb{Q})$. However, the D_ξ are more complicated than C (for example, the genus is larger). But there may be morphisms $\phi\colon D_\xi \to C'$ to other curves. If we can find $C'(\mathbb{Q})$ and this set is finite, then we can compute $D_\xi(\mathbb{Q})$: for each $P \in C'(\mathbb{Q})$, check the fiber $\phi^{-1}(P)$ for rational points.

An example of this occurs in the situation of the double covers of hyperelliptic curves considered at the beginning of this section. The curve $D_d\colon dy_1^2 = f_1(x)$, $dy_2^2 = f_2(x)$ covers the two hyperelliptic curves $dy_1^2 = f_1(x)$ and $dy_2^2 = f_2(x)$ whose genus is *smaller* than that of C. If, for example, the degree of f_2 is 3 or 4, then the second curve has genus 1. Assuming it has rational points, it will be an elliptic curve, and we may be lucky and can show that it has rank zero. We can then find its finitely many rational points. The rational points on C coming from points on D_d then must have x-coordinates in the set of x-coordinates of the rational points on $dy_2^2 = f_2(x)$.

How can we produce suitable unramified coverings? One possibility is the following (and this in fact produces essentially all the coverings with abelian automorphism groups).

If C possesses a rational divisor class of degree 1, then C can be embedded into its Jacobian variety J. (This is not an essential condition, but it simplifies the explanation.) For each $n \geq 2$, we then obtain an unramified and geometrically Galois covering of C by pulling C back under the multiplication-by-n map of J. We write $\mathrm{Sel}_n(C)$ for the associated Selmer set and call it the *n-Selmer set* of C. The following conjecture is a weak form of the 'Main Conjecture' formulated in [8].

Conjecture 6.8.

$$C(\mathbb{Q}) = \emptyset \iff \exists n\colon \mathrm{Sel}_n(C) = \emptyset\,.$$

In particular, this would imply that the question '$C(\mathbb{Q}) = \emptyset$?' is decidable: Search for points by day and compute $\mathrm{Sel}_n(C)$ for $n = 2, 3, 4, \ldots$ by night. If the conjecture holds, then you will eventually either find a point or find an empty Selmer set.

In the next section, we will consider $\mathrm{Sel}_2(C)$ for C hyperelliptic.

7. Two-Cover Descent on Hyperelliptic Curves

7.1. The $x - T$ Map and the Fake 2-Selmer Set

What can we do if $C\colon y^2 = f(x)$ does not admit an unramified double cover over $\mathbb{Q}$?

The right hand side $f(x)$ may not factor over $\mathbb{Q}$, but it does so over suitable field extensions (for example, over the splitting field of f). The corresponding double covers are permuted by the action of the Galois group, so by combining them, we obtain a covering defined over $\mathbb{Q}$ again, which is not a double cover, but an unramified and geometrically Galois covering with automorphism group $J[2]$, the two-torsion subgroup of the Jacobian J of C. So what we obtain in this way is a *2-covering* of C, which can be obtained by pulling back C via the multiplication-by-2 map on J (assuming we can embed C into J). The corresponding Selmer set is the *2-Selmer set*, $\mathrm{Sel}_2(C)$.

In this situation, a closely related set can be described in an explicit way that is amenable to computation. For this, define $A = \mathbb{Q}[x]/\langle f(x)\rangle$. Since f is squarefree, this is a product of number fields, each generated by a root of an irreducible factor of f. Write T for the image of x in A. For a commutative ring R, denote the subgroup of squares in $R^\times$ by $R^\square$. If $\deg(f)$ is odd, set

$$H = \{\alpha \in A^\times/A^\square : N_{A/\mathbb{Q}}(\alpha) \in \mathrm{lcf}(f)\mathbb{Q}^\square\}\,;$$

if $\deg(f)$ is even, set

$$H = \{\alpha \in A^\times/(\mathbb{Q}^\times A^\square) : N_{A/\mathbb{Q}}(\alpha) \in \mathrm{lcf}(f)\mathbb{Q}^\square\}\,.$$

Here $N_{A/\mathbb{Q}}$ is the group homomorphism induced by the norm map $A \to \mathbb{Q}$. Note that in the even degree case, the norm maps $\mathbb{Q}^\times$ into $\mathbb{Q}^\square$, so we indeed obtain a well-defined homomorphism.

Write $A_v = A \otimes_{\mathbb{Q}} \mathbb{Q}_v$ (for v a prime or ∞) and define H_v accordingly. There is the '$x - T$ map'

$$\delta\colon C(\mathbb{Q}) \longrightarrow H, \qquad P \longmapsto x(P) - T$$

and similarly

$$\delta_v\colon C(\mathbb{Q}_v) \longrightarrow H_v, \qquad P \longmapsto x(P) - T\,;$$

the definition has to be modified for points at infinity (then the image is 1) and for points with vanishing y-coordinate (then $x(P) - T$ is zero in a component $\cong \mathbb{Q}$

or $\mathbb{Q}_v$ of A or A_v; this component has to be replaced by $f'(x(P))$). Of course, instead of $x(P) - T$ we really mean its image in H or H_v. To see that the image of δ (or δ_v) really is contained in specified coset of the kernel of this norm map, observe that (for $x(P) \neq \infty$ and $y(P) \neq 0$)

$$N_{A/\mathbb{Q}}\big(x(P) - T\big) = \operatorname{lcf}(f)^{-1} f\big(x(P)\big) = \operatorname{lcf}(f)\big(y(P)\operatorname{lcf}(f)^{-1}\big)^2 \in \operatorname{lcf}(f)\mathbb{Q}^{\square}\,.$$

There are natural homomorphisms $\rho_v \colon H \to H_v$ induced by the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$. For each place v, we obtain a commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\delta} & H \\ \downarrow & & \downarrow{\scriptstyle \rho_v} \\ C(\mathbb{Q}_v) & \xrightarrow{\delta_v} & H_v \end{array}$$

linking δ with δ_v.

Definition 7.1. The *fake 2-Selmer set* of C is the subset

$$\operatorname{Sel}_2^{\text{fake}}(C) = \{\alpha \in H : \forall v \colon \rho_v(\alpha) \in \operatorname{im}(\delta_v)\}$$

of H.

Since essentially by definition δ restricts to a map $C(\mathbb{Q}) \to \operatorname{Sel}_2^{\text{fake}}(C)$, it follows that $C(\mathbb{Q})$ is empty if $\operatorname{Sel}_2^{\text{fake}}(C) = \emptyset$.

The relation with the 2-Selmer set is as follows.

Proposition 7.2. *There is a natural map* $\operatorname{Sel}_2(C) \to \operatorname{Sel}_2^{\text{fake}}(C)$*, which is either a bijection or (usually) a two-to-one map. We have a bijection if and only if either* f *has an irreducible factor of odd degree (this is always the case when* f *itself has odd degree) or else* f *can be written as a constant times the product of two conjugate polynomials of odd degree with coefficients in a quadratic extension of* $\mathbb{Q}$ *(this implies that* $\deg(f) \equiv 2 \bmod 4$*, so* g *is even). In any case, we have that* $\operatorname{Sel}_2^{\text{fake}}(C) = \emptyset$ *if and only if* $\operatorname{Sel}_2(C) = \emptyset$*.*

There is a geometric interpretation of the map $\operatorname{Sel}_2(C) \to \operatorname{Sel}_2^{\text{fake}}(C)$. Whereas $\operatorname{Sel}_2(C)$ classifies ELS 2-coverings of C up to $\mathbb{Q}$-isomorphism, the fake 2-Selmer set $\operatorname{Sel}_2^{\text{fake}}(C)$ classifies ELS 2-coverings of C up to $\mathbb{Q}$-isomorphism and post-composition with the hyperelliptic involution w. Usually, a 2-covering π and the composition $w \circ \pi$ are non-isomorphic, so the map $\operatorname{Sel}_2(C) \to \operatorname{Sel}_2^{\text{fake}}(C)$ identifies isomorphism classes of 2-coverings in pairs. However, if f factors in the right way, then π and $w \circ \pi$ are always isomorphic, and we obtain a bijection.

7.2. Computing the Fake 2-Selmer Set

We will now explain how the fake 2-Selmer set can be computed. This is very much in parallel to the computation of the (fake) 2-Selmer group of the Jacobian J of C, compare the contribution by Steffen Müller. In fact, assume that f has odd degree and is monic. Then there is a natural embedding $\iota\colon C \to J$ obtained from taking ∞ as a base-point (so $\iota(P) = [P - \infty]$). In this case our H is the same as Müller's H, and $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \mathrm{Sel}_2(C)$ can be identified with a subset of $\mathrm{Sel}_2(J) \subset H$. This subset is cut out by the condition that $\rho_v(\alpha) \in H_v$ must be in the image of $\delta_v = \delta_{J,v} \circ \iota$ (where $\delta_{J,v}$ is the local $x-T$ map on J) instead of just in the image of $\delta_{J,v}$. An element $\alpha \in H$ corresponds to a 2-covering $\pi\colon X \to J$ and gives rise to a 2-covering $\pi\colon D = \pi^{-1}(C) \to C$. The stronger condition for $\mathrm{Sel}_2(C)$ as compared to $\mathrm{Sel}_2(J)$ amounts to requiring D to be ELS instead of just X. Note that our set-up enables us to check the ELS condition on the 2-covering D without actually having to construct D!

For the following, we assume that f has integral coefficients. This can always be achieved by scaling y appropriately. (In the odd degree case, we can in addition achieve f to be monic, by scaling both variables.) Let Σ be $\{\infty, 2\}$ together with all prime divisors of $\mathrm{disc}(f)$ and of $\mathrm{lcf}(f)$. This is a finite set of places, so the subgroup $A(\Sigma, 2) \subset A^\times/A^\square$ of elements 'unramified outside Σ' is finite and computable by standard results of algebraic number theory, giving rise to a finite subset H_Σ of H. (The actual computation of $A(\Sigma, 2)$ and thence of H_Σ requires an explicit knowledge of the ideals class groups and unit groups of the number fields occurring as factors of A.)

In a very similar way as for the Jacobian, one shows that $\mathrm{Sel}_2^{\mathrm{fake}}(C) \subset H_\Sigma$. Roughly speaking, if $p \notin \Sigma$ is a prime, then the whole construction can be done over $\mathbb{F}_p$, which means that the image of δ_p is contained in the part H_p^0 of H_p that comes from $\mathbb{Z}_p[x]/\langle f\rangle$. Since we have

$$H_\Sigma = \{\alpha \in H : \forall p \notin \Sigma\colon \rho_p(\alpha) \in H_p^0\}\,,$$

this leads to

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

The number of elements we have to consider is now finite, but there are still conditions at infinitely many places to check. Note, however, that if $\mathrm{im}(\delta_p) = H_p^0$ for some $p \notin \Sigma$, then the condition is already taken care of by restricting to H_Σ. Since $\rho_p(\alpha) \in \mathrm{im}(\delta_p)$ means $D_\alpha(\mathbb{Q}_p) \neq \emptyset$ (where D_α denotes the corresponding 2-covering curve of C), by Corollary 5.2, we will always have $\mathrm{im}(\delta_p) = H_p^0$ for $p \notin \Sigma$ if $p \geq 4\,\mathrm{genus}(D)^2$. Here we use that for $p \notin \Sigma$ and $\rho_p(\alpha) \in H_p^0$, the curve D_α has good reduction at p. So we finally have the finite description

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v \in \Sigma \cup \{p < 4\,\mathrm{genus}(D)^2\}\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

The degree of the covering $D \to C$ is $\#J[2] = 4^g$, so by the Riemann-Hurwitz formula,we have $\mathrm{genus}(D) = 4^g(g-1)+1$, which means that the bound $4\,\mathrm{genus}(D)^2$ is quite large: already for $g = 2$, we have to consider all primes up to 1153.

Still, these considerations show that we can compute $\mathrm{Sel}_2^{\mathrm{fake}}(C)$, if we can compute the 'local images' $\mathrm{im}(\delta_v) \subset H_v$. That this is possible follows from the fact that δ_v is locally constant: It is a continuous map from the compact space $C(\mathbb{Q}_v)$ (in the v-adic topology) to the discrete space H_v, so $C(\mathbb{Q}_v)$ splits into finitely many closed and open subsets on which δ_v is constant. These subsets can be explicitly described. We conclude:

Theorem 7.3. *There is an algorithm for computing* $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

This algorithm is implemented in Magma [9]. For details, see [10,11].

In practice, we use a subset of the primes we would have to consider. This results in a set S that contains $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

- If $S = \emptyset$, then $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$ as well.
- If we know $X \subset C(\mathbb{Q})$ such that $\delta(X) = S$, then $S = \mathrm{Sel}_2^{\mathrm{fake}}(C)$.

In many applications, one of these cases occurs.

The main computational bottleneck is the computation of $A(\Sigma, 2)$, which involves computing ideal class groups and unit groups of the number fields corresponding to the irreducible factors of f. However, for moderate degrees of the irreducible factors and moderate size of the coefficients, this part of the computation is feasible (if the degrees and/or coefficients get larger, one might have to assume the Generalized Riemann Hypothesis to make it feasible).

7.3. Examples

For many curves of genus 2 with small coefficients that are ELS, but seem to have no (reasonably small) rational points, the fake 2-Selmer set turns out to be empty, and we obtain a computational proof that these curves have no rational points.

To make this more concrete, we summarize the results of [4]. There we considered all curves of genus 2 of height ≤ 3.

- There are 196 171 isomorphism classes over $\mathbb{Q}$ of such curves.
- On 137 490 of these curves, one finds a (small) rational point.
- Of the remaining 58 681 curves, 29 403 are not ELS.
- Of the remaining 29 278 ELS curves C, 27 786 have $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$.
- For the last 1 492 curves C, we could show that $C(\mathbb{Q}) = \emptyset$ using the Mordell-Weil sieve (see Samir Siksek's contribution). (For 42 of these curves, we had to assume the Birch and Swinnerton-Dyer conjecture for the Jacobian or the Generalized Riemann Hypothesis.)

So among the ELS curves without rational points in our sample, the 2-Selmer set computation had a success rate of about 95%!

7.4. A Recent Result

That this high success rate is no accident is supported by the following recent result by the 2014 Fields Medalist Manjul Bhargava [12].

Theorem 7.4. *As $g \to \infty$, the (fake) 2-Selmer set is empty for a set of hyperelliptic curves of genus g (in the family $\mathcal{F}_g$) of lower density $1 - o(2^{-g})$.*

In fact, Bhargava shows that the average size of $\mathrm{Sel}_2^{\mathrm{fake}}(C)$ is $o(2^{-g})$, which implies the above result. The lower density is positive for all $g \geq 1$ and exceeds 50% for $g \geq 2$.

Bhargava's result has the following obvious consequence.

Corollary 7.5. *As $g \to \infty$, the set of curves in $\mathcal{F}_g$ that do not have a rational point has lower density $1 - o(2^{-g})$.*

This is the best approximation so far to the expected true density of 1, compare Conjecture 5.4.

References

[1] Michael Stoll: *Rational points on curves*, J. Théor. Nombres Bordeaux **23**, 257–277 (2011).

[2] Louis J. Mordell: *On the rational solutions of the indeterminate equation of the third and fourth degrees*, Proc. Cambridge Philos. Soc. **21**, 179–192 (1922).

[3] Gerd Faltings: *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73**:3, 349–366 (1983).

[4] Nils Bruin and Michael Stoll: *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17**, 181–189 (2008).

[5] André Weil: *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. **1041** = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948. iv+85 pp.

[6] Bjorn Poonen and Michael Stoll: *A local-global principle for densities.* In: Scott D. Ahlgren (ed.) et al.: *Topics in number theory.* In honor of B. Gordon and S. Chowla. Kluwer Academic Publishers, Dordrecht. Math. Appl., Dordr. **467**, 241–244 (1999).

[7] Claude Chevalley and André Weil: *Un théorème d'arithmétique sur les courbes algébriques*, C. R. Acad. Sci. Paris **195**, 570–572 (1932).

[8] Michael Stoll: *Finite descent obstructions and rational points on curves*, Algebra & Number Theory **1**, 349–391 (2007).

[9] Wieb Bosma, John Cannon and Catherine Playoust: *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24**, 235–265 (1997).

[10] Michael Stoll: *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98**, 245–277 (2001).

[11] Nils Bruin and Michael Stoll: *Two-cover descent on hyperelliptic curves*, Math. Comp. **78**, 2347–2370 (2009).

[12] Manjul Bhargava: *Most hyperelliptic curves over $\mathbb{Q}$ have no rational points*, Preprint (2013). arXiv:1308.0395