RATIONAL POINTS ON CURVES

J. STEFFEN MÜLLER

Abstract. These are notes for the first three lectures of a course at the Summer School Computational Methods in Number Theory in July 2019 in Bristol. Please let me know about typos or mathematical errors (unfortunately, there will be no extra credit). Some exercises and many useful comments were provided by Stevan Gajovic.

Contents

1. First lecture

1.1. Introduction.

Throughout these notes $X/\mathbb{Q}$ denotes a nice curve, where *nice* means smooth, projective and geometrically integral. We denote its genus by g.

The main objective of these notes is to discuss various attempts to solve

Problem 1.1. *Compute* $X(\mathbb{Q})$.

Date: June 27, 2019.

We will focus on computational methods. Many of these are implemented in the computer algebra system `Magma` [5] and we briefly indicate the relevant `Magma`-commands in the notes. If you don't have access to `Magma`, you can use the online calculator at http://magma.maths.usyd.edu.au/calc/.

Much of the functionality for genus 0 and 1 is also implemented in `Sage` [50] and in `Pari/Gp` [58]. I encourage the reader to experiment with all of these!

We will assume throughout that X is given by explicit equations with integral coefficients. To make Problem 1.1 well-defined, we first need to examine the structure of $X(\mathbb{Q})$. We either have $X(\mathbb{Q}) = \varnothing$, which is possible for every g, or we are in one of the following situations:

$g = 0$: There is an isomorphism $X \cong_{\mathbb{Q}} \mathbb{P}^1_{\mathbb{Q}}$.
$g = 1$: By Mordell's theorem, fixing any $P_0 \in X(\mathbb{Q})$, we can endow $X(\mathbb{Q})$ with the structure of a finitely generated abelian group with unit element P_0.
$g \geq 2$: By Faltings' Theorem, $X(\mathbb{Q})$ is finite.

Therefore, *computing* $X(\mathbb{Q})$ means

(I) deciding whether $X(\mathbb{Q})$ is empty;
(II) if $X(\mathbb{Q}) \neq \varnothing$,
  $g = 0$: parametrizing $X(\mathbb{Q})$,
  $g = 1$: finding generators of $X(\mathbb{Q})$,
  $g \geq 2$: enumerating $X(\mathbb{Q})$.

Today, we are mostly concerned with (I). More precisely, we will discuss methods to show that $X(\mathbb{Q}) = \varnothing$ – provided that this is indeed the case.

We start with a trivial, yet quite useful observation: If $X(K) = \varnothing$ for some field extension $K \supset \mathbb{Q}$, then $X(\mathbb{Q}) = \varnothing$. For instance, we can consider completions K of $\mathbb{Q}$.

Definition 1.2. We call X *everywhere locally soluble* (or *ELS*) if $X(\mathbb{R}) \neq \varnothing$ and if $X(\mathbb{Q}_p) \neq \varnothing$ for all prime numbers p.

It is obvious that $X(\mathbb{Q})$ can only be non-empty if X is ELS.

1.2. **Checking local solubility.**

We now discuss how to test whether X is ELS. Checking whether $X(\mathbb{R})$ is empty is not difficult. But since there are infinitely many prime numbers p, we must first show that checking local solubility everywhere is a finite problem. For a prime number p, the idea is to first check whether $\bar{X}(\mathbb{F}_p) = \varnothing$, where we write $\bar{X}$ for the reduction of X modulo p. If this is the case, then of course $X(\mathbb{Q}_p)$ is also empty. If not, then we try to lift points from $\bar{X}(\mathbb{F}_p)$ to $X(\mathbb{Q}_p)$.

Lemma 1.3. *Let $\bar{P} \in \bar{X}(\mathbb{F}_p)$ be a smooth point. Then $\bar{P}$ lifts to a point $P \in X(\mathbb{Q}_p)$.*

Proof. See the corresponding exercise in John Cremona's course. □

Hence X has p-adic points for every p such that $\bar{X}$ has smooth $\mathbb{F}_p$-points. Combining this observation with the Hasse-Weil inequality

$$|\#\bar{X}(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}$$

for primes p of good reduction for X, we deduce that we only need to check finitely many primes.

Corollary 1.4. *Let $p > 4g^2$ be a prime of good reduction for X. Then $X(\mathbb{Q}_p) \neq \varnothing$.*

It remains to deal with primes not covered by the above. First suppose that $g = 0$. Via a Riemann-Roch computation, we can assume that X is a conic, given by a ternary quadratic form $Q \in \mathbb{Z}[x, y, z]$ with discriminant $\mathrm{disc}(Q) \neq 0$.

Exercise 1.1. In this exercise we prove a criterion to check whether X is ELS.

(a) Show that we may assume $Q = ax^2 + by^2 + cz^2$ with a, b, c pairwise coprime, squarefree integers such that $a, b > 0$, $c < 0$.
(b) Show that $X(\mathbb{Q}_p) \neq \varnothing$ for $p \nmid abc$.
(c) Show that X is ELS if and only if the system

$$x_1^2 \equiv -bc \pmod{a}, \quad x_2^2 \equiv -ac \pmod{b}, \quad x_3^2 \equiv -ab \pmod{c}$$

has a solution $(x_1, x_2, x_3) \neq 0$. (Hint: Consider odd finite primes $p \mid abc$. Then use the product formula for the Hilbert symbol.)

Now suppose that $g \geq 1$ and that p is a prime number not covered by Lemma 1.3. This means that $\bar{X}(\mathbb{F}_p)$ is nonempty, but only consists of singular points. Roughly speaking, we can proceed as follows: We first choose a model $\mathcal{X}/\mathbb{Z}_p$ of $X_{\mathbb{Q}_p}$; let $\mathcal{X}_p$ denote its special fiber. Then, for all $\bar{P} \in \mathcal{X}_p(\mathbb{F}_p)$, we "zoom in" at $\bar{P}$ and replace $\mathcal{X}$ by the resulting new model (for instance, we can blow up $\mathcal{X}$ in $\bar{P}$). We then check if this new $\mathcal{X}$ satisfies $\mathcal{X}(\mathbb{Z}_p) = \varnothing$. If we can show this, then we get that $X(\mathbb{Q}_p) = \mathcal{X}(\mathbb{Z}_p) = \varnothing$. If not, we repeat until we find a model such that either $\mathcal{X}(\mathbb{Z}_p) = \varnothing$ or $\mathcal{X}_p(\mathbb{F}_p)$ contains smooth points. One can show that this process has to lead to a regular model $\mathcal{X}$ after finitely many steps, so we can decide whether $X(\mathbb{Q}_p) = \varnothing$ after finitely many steps. See Exercise 1.3 for the case where X is hyperelliptic and $p \neq 2$.

Therefore there is an effective algorithm to check whether any nice $X/\mathbb{Q}$ is ELS, and this also turns out to be very efficient in practice. In `Magma`, one can check local solubility at a prime p via `IsLocallySolvable(X, p)`. If X has an affine equation $y^n = f(x)$, then one can use `HasPointsEverywhereLocally(f,n)` to check whether X is ELS. If X is a conic or a model of a genus 1 curve, then there is the command `IsLocallySolvable(X)`.

Now it is natural to wonder whether checking ELS always suffices in order to show that a curve has no rational points.

Definition 1.5. We say that a class of nice curves satisfies the *Hasse principle* (or *local-to-global principle*), if every curve in this class has a rational point if and only if it is ELS.

Theorem 1.6. *(Legendre) Curves of genus 0 satisfy the Hasse principle.*

But as you saw in Céline Maistret's lectures, the class of curves of genus 1 does not satisfy the Hasse principle. For instance, if $E/\mathbb{Q}$ is an elliptic curve such that $Ш(E/\mathbb{Q})$ is nontrivial, then E has twists $X/\mathbb{Q}$ which do not satisfy the Hasse principle.

In fact, one expects that most nice curves of a fixed positive genus are ELS, yet have no rational points. One can make this precise in terms of densities, see John Cremona's lectures. For instance, one expects the density of nice curves of fixed genus g without a rational point to approach 1 as g increases, but the density of nice curves of fixed genus g which are ELS is always positive (it is about 0.85 for $g = 2$). Hence we need to look for other methods to show that a curve has no rational points.

1.3. **Descent and covering collections.**

The idea of descent is, roughly speaking, to compute the rational points on coverings of X, rather than on X itself. We assume throughout that $g > 0$, and we start with an instructive

Example 1.7. Suppose that X is hyperelliptic, given by a model $X\colon y^2 = f(x)$, where f factors as $f = f_1 f_2$, with $f_1, f_2 \in \mathbb{Z}[x]$ coprime, not constant and not both of odd degree. Consider the curve $Y/\mathbb{Q}$ defined in $\mathbb{P}^3$ by

$$Y\colon y_1^2 = f_1(x),\ y_2^2 = f_2(x).$$

Then the map sending $(x, y_1, y_2) \in Y$ to $(x, y_1 y_2) \in X$ defines an unramified covering $\pi\colon Y \to X$. Of course, not every rational point on X might lift to a rational point on Y. However, every rational point lifts to a rational point on one of finitely many twists of Y! More precisely, for a squarefree integer d the curve

$$Y_d\colon dy_1^2 = f_1(x),\ dy_2^2 = f_2(x)$$

defines a covering $\pi_d\colon Y_d \to X$, given by

$$(x, y_1, y_2) \mapsto (x, dy_1 y_2).$$

Lemma 1.8. *There is a finite and explicitly computable set S of squarefree integers such that*

$$X(\mathbb{Q}) = \bigcup_{d \in S} \pi_d(Y_d(\mathbb{Q})).$$

Proof. We only consider affine points $(x, y) \in X(\mathbb{Q})$. There is a unique squarefree $d \in \mathbb{Z}$ such that $f_1(x) = dy_1^2$ and $f_2(x) = dy_2^2$, with y_1 and y_2 rational numbers. The result follows from the following exercise. □

Exercise 1.2. Let d be a squarefree integer and let $p \mid d$ be a prime number. Show that if $Y_d(\mathbb{Q}_p) \neq \varnothing$, then p divides the resultant of f_1 and f_2 or, in case one of the f_i has odd degree, say f_1, p divides the leading coefficient of f_2.

Definition 1.9. The *Selmer set* of the covering $\pi\colon Y \to X$ is defined by

$$\mathrm{Sel}(\pi) := \{d \in \mathbb{Z} \text{ squarefree } :\ Y_d \text{ is ELS}\}.$$

Then $\mathrm{Sel}(\pi) \subset S$ is finite and explicitly computable and we have $X(\mathbb{Q}) = \varnothing$ if $\mathrm{Sel}(\pi)$ is empty.

We can generalize the previous example to nice curves $X/\mathbb{Q}$. The idea is to cover X by finitely many twists of a fixed covering such that every rational point on X comes from a rational points on one of these coverings. If we can show that the latter have no rational points, then we have shown $X(\mathbb{Q}) = \varnothing$.

Theorem 1.10. *Let $\pi\colon Y \to X$ be an unramified and geometrically Galois covering, which is given explicitly. Then there is a finite and explicitly computable subset $\mathrm{Sel}(\pi) \subset H^1(G_\mathbb{Q}, \mathrm{Aut}(\pi))$ such that we have*

$$X(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi(Y_\xi(\mathbb{Q})).$$

This is essentially the theorem of Chevalley-Weil [14]. Here a twist $Y \to X$ is *geometrically Galois* if $\bar{\mathbb{Q}}(Y)/\bar{\mathbb{Q}}(X)$ is Galois. The twists of $\pi\colon Y \to X$ as in the theorem are parametrized by $H^1(G_\mathbb{Q}, \mathrm{Aut}(\pi))$. For any $\xi \in H^1(G_\mathbb{Q}, \mathrm{Aut}(\pi))$ we have a commutative diagram

$$\begin{array}{ccc} Y_\xi & \xrightarrow{\cong_{\bar{\mathbb{Q}}}} & Y \\ {\scriptstyle \pi_\xi}\downarrow & & \downarrow{\scriptstyle \pi} \\ X & \xrightarrow[=]{} & X \end{array}$$

We call the collection $(Y_\xi)_{\xi \in \mathrm{Sel}(\pi)}$ as in the theorem a *covering collection* of X.

Remark 1.11. The covering π in Example 1.7 has $\mathrm{Aut}(\pi) \cong \mathbb{Z}/2\mathbb{Z}$, and the set of square-free integers forms a system of representatives of $\mathrm{H}^1(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

The correspondence between twists of coverings and Galois cohomology is similar to the correspondence between twists of an elliptic curve $E/\mathbb{Q}$ and the Galois cohomology set $H^1(G_{\mathbb{Q}}, \mathrm{Isom}(E))$ discussed in Céline Maistret's lectures. There, a special kind of twist was discussed; namely, a principal homogeneous space Y_ξ for $\xi \in H^1(G_{\mathbb{Q}}, E[n])$, where $n \geq 2$. We call such a twist $\pi_\xi \colon Y_\xi \to X$ an *n-covering* of E. More generally, for a nice curve $X/\mathbb{Q}$ of genus 1 which is a principal homogeneous space for E, we define an *n-covering of X* to be a covering $\pi \colon Y \to X$ which gives rise to a commutative diagram

$$\begin{array}{ccc} \mathrm{Jac}(X) & \xrightarrow[\cong_{\bar{\mathbb{Q}}}]{} & E \\ {\scriptstyle \pi^*}\downarrow & & \downarrow{\scriptstyle [n]} \\ \mathrm{Jac}(Y) & \xrightarrow[\cong_{\bar{\mathbb{Q}}}]{} & E. \end{array}$$

We define the *n-Selmer set* of X as the set $\mathrm{Sel}^n(X)$ of all n-coverings of X that are ELS.

It is often possible to compute $\mathrm{Sel}^n(X)$ in practice. For instance, when X arises via an m-descent on its Jacobian E, i.e. as an element of $\mathrm{Sel}^m(E/\mathbb{Q})$ for some $m \geq 2$, this is essentially equivalent to a second descent on E. In this case there are practical algorithms to compute $\mathrm{Sel}^n(X)$ when

- $m = n = 2$ (Cassels [12], Merriman-Siksek-Smart [39], Womack [62])
- $m = n = 3$ (Creutz [26])
- $m = 4, n = 2$ (Stamminger [49])
- $mn = 6, 12$ (Fisher [27])

All of these algorithms (and others) are implemented in `Magma`. They can be accessed via `*Descent`, where $* \in \{$`Two,Three,Four,Five,Six,Eight,Nine,Twelve`$\}$. See [20, 21, 22] for further information about descent on elliptic curves.

The construction above extends to general $g \geq 1$ in the following way. Letting $J/\mathbb{Q}$ denote the Jacobian variety of X, an *n-covering of J* is a covering $V \to J$ which is isomorphic to the multiplication-by-n map $[n] \colon J \to J$ over $\bar{\mathbb{Q}}$. Fix an embedding $\iota \colon X \to J$ defined over $\mathbb{Q}$, via a rational divisor class on X of degree 1. Then we define an *n-covering* $\pi \colon Y \to X$ to be the pullback via ι of an n-covering $V \to J$, making the diagram

$$\begin{array}{ccccc} Y & \longrightarrow & V & \xrightarrow{\cong_{\bar{\mathbb{Q}}}} & J \\ {\scriptstyle \pi}\downarrow & & \downarrow & \swarrow{\scriptstyle [n]} & \\ X & \xrightarrow[\iota]{} & J & & \end{array}$$

commute. As above, the *n-Selmer set* $\mathrm{Sel}^n(X)$ is defined as the set of ELS n-coverings of X.

Theorem 1.12. *Let $g \geq 1$ and $n \geq 2$, and suppose that we have explicit equations of J. Then $\mathrm{Sel}^n(X)$ is finite and explicitly computable, and we have*

$$X(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}^n(X)} \pi_\xi(Y_\xi(\mathbb{Q})).$$

An efficient algorithm for computing $\mathrm{Sel}^n(X)$ for curves of genus > 1 is only known for hyperelliptic curves and $n = 2$, see [9]. The idea is to not compute a covering collection

directly, but to replace $\mathrm{Sel}^2(X)$ with a related set, the *fake 2-Selmer set*, which can be computed via algebraic number theory and local computations. The `Magma`-command for this is `TwoCoverDescent(X)`.

Remark 1.13. One can show that all geometrically Galois unramified coverings with abelian Galois group extend to n-coverings.

Remark 1.14. We can also use covering collections to compute $X(\mathbb{Q})$ when there are rational points. See Exercise 1.5 below.

1.4. **Further exercises.**

Exercise 1.3. (Formulated by Stevan Gajovic) Let $X\colon y^2 = f(x)$ be a nice hyperelliptic curve, with $f \in \mathbb{Z}[x]$. We want to describe an algorithm that checks whether $X(\mathbb{Q}_p) = \emptyset$ for $p \neq 2$, a prime number. Recall that we may suppose that $\bar{X}(\mathbb{F}_p) \neq \varnothing$ and that all points in $\bar{X}(\mathbb{F}_p)$ are singular.

(a) Conclude that such a point is of the form $\bar{P} = (x_0, 0)$, for some $x_0 \in \{0, 1, \ldots, p-1\}$. Therefore $p \mid f(x_0)$ and $p \mid f'(x_0)$.
(b) If $p^2 \nmid f(x_0)$, prove that the point $\bar{P}$ does not lift to a point in $X(\mathbb{Q}_p)$.
(c) Now suppose that $p^2 \mid f(x_0)$. Prove that

$$f_1(x) := \frac{f(x_0 + px)}{p^2} \in \mathbb{Z}[x].$$

(d) Let X_1 be the hyperelliptic curve defined by $y^2 = f_1(x)$. Prove that the lifts of $\bar{P}$ are in bijective correspondence with points in $X_1(\mathbb{Q}_p)$.
(e) We continue with X_1. As before, if $\bar{X}_1(\mathbb{F}_p) = \emptyset$ or $\bar{X}_1(\mathbb{F}_p)$ contains a smooth point, then we are done. The remaining case is again when there is a singular point $P_1 = (x_1, 0) \in \bar{X}_1(\mathbb{F}_p)$. Imitate the steps (a)-(c). Conclude that either we can decide in finitely many steps whether $\bar{P}$ lifts to a point in $X(\mathbb{Q}_p)$ or we can construct an infinite sequence of curves $X_n\colon y^2 = f_n(x)$, where

$$f_n(x) := \frac{f_{n-1}(x_{n-1} + px)}{p^2} \in \mathbb{Z}[x]$$

with singular points $P_{n-1} = (x_{n-1}, 0) \in \bar{X}_{n-1}(\mathbb{F}_p)$.
(f) Show that if the process does not terminate, then the resulting infinite sequence of curves leads to a singular point $P \in X(\mathbb{Q}_p)$ (Hint: Guess the coordinates of P! Find the sequence (obviously) converging to $x(P)$ and use this to prove that P is singular).
(g) Conclude that the above leads to an algorithm which is guaranteed to decide whether $X(\mathbb{Q}_p) = \varnothing$ in finitely many steps.

Exercise 1.4. Show that the hyperelliptic curves given by the following affine equations have no rational points.

(a) $y^2 = -x^6 - 3x^5 + 4x^4 + 2x^3 + 4x^2 - 3x - 1$
(b) $y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2)$. Also show that this curve is ELS.

Exercise 1.5. Let $X\colon y^2 = (x^2 + 1)(x^4 + 1)$.

(a) Show that $\mathrm{Sel}(\pi) \subset \{1, 2\}$, where π is as in Example 1.7.
(b) For squarefree $d \in \mathbb{Z}$, let C_d be the hyperelliptic curve defined by $dy^2 = x^4 + 1$. Show that for both $d = 1$ and $d = 2$, there are at least four rational points on C_d. In fact there are exactly four rational points on both C_1 and C_2 – you may assume this (or try to verify it, for instance, using `Magma`).
(c) Use (b) to compute $Y_d(\mathbb{Q})$ for $d = 1, 2$ and to compute $X(\mathbb{Q})$.

2. Second Lecture

Now suppose that $X/\mathbb{Q}$ is a nice curve which has a rational point.

2.1. Curves of genus 0.

Suppose that $g = 0$. As discussed in the first lecture, we may assume that $X\colon Q = 0$ is a smooth conic with integral ternary quadric Q. If we know a rational point $P_0 \in X(\mathbb{Q})$, then we can explicitly construct an isomorphism $X \cong \mathbb{P}^1$ defined over $\mathbb{Q}$ by projecting from P_0. This solves problem (II) from the first lecture for X.

Example 2.1. Consider the unit circle $X\colon x^2+y^2 = 1$ and the point $P_0 = (-1, 0) \in X(\mathbb{Q})$. A non-vertical line through P_0 with rational slope t intersects X in exactly one additional point $P^t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \in X(\mathbb{Q})$. Also taking the vertical line through P_0 into account, we obtain a parametrization of $X(\mathbb{Q})$.

There are various methods to find a rational point P_0. The basic idea of most of them is to repeatedly replace Q by a "simpler" quadric Q' such that Q has a nontrivial zero if and only if Q' does. The most efficient algorithm (to my knowledge) is due to Simon [48]; the idea (for diagonal quadrics) goes back to Gauss.

(i) (Minimization) For a prime $p \mid \operatorname{disc}(Q)$, replace Q by a quadric whose discriminant is not divisible by p. Repeat prime-by-prime until $|\operatorname{disc}(Q)| = 1$.
(ii) (Reduction) Reduce the coefficients of Q until we get a Q for which we can easily read off a solution (e.g. the one in Example 2.1).

For the second step, Simon uses a version of the LLL-algorithm for indefinite quadratic form. It turns out that in practice the passage to a diagonal form, which you applied in Exercise 1.1, can have disastrous effects on the size of the discriminant (which we have to factor), so it is to be avoided if possible.

Simon's algorithm is implemented in `Magma`. You can turn a nice curve $X/\mathbb{Q}$ of genus 0 into a conic using `Conic(X)`. If $X/\mathbb{Q}$ is a smooth conic, use `HasRationalPoint(X)` to find a rational point (if there is one) and `Parametrization(X)` to write down an isomorphism to $\mathbb{P}^1$ defined over $\mathbb{Q}$.

The paper [24] by Cremona and Rusin contains alternative efficient methods.

2.2. From curves of genus 1 to elliptic curves.

Let $X/\mathbb{Q}$ be a nice curve of genus 1. The given model of X could, for instance, be one of the following:

(i) $X\colon y^2 = f(x)$, where f has degree 4 and is squarefree
(ii) a plane cubic in $\mathbb{P}^2$
(iii) $X\colon S_1 \cap S_2$, where S_1 and S_2 are quadric surfaces in $\mathbb{P}^3$.

Such models arise from n-descent ($n = 2, 3, 4$) on the Jacobian E of X, which is an elliptic curve. Note that writing down the model (i) in the 2-descent process (as described, for instance, in [18]) requires the parametrization of conics.

We first need to find a rational point. For models (i) we can use a quadratic sieve strategy as implemented in Stoll's program `j-points`. Note that instead of searching on X itself, we can also search on coverings $\pi\colon Y \to X$ as discussed in §1.3. This can be advantageous, because the map π increases the "size" of a rational point.

Once we have found a rational point $P_0 \in X(\mathbb{Q})$, we can use Riemann-Roch to construct an isomorphism $\psi\colon X \to E$ over $\mathbb{Q}$, where E is the Jacobian of X and is given by

an integral Weierstrass equation, and such that ψ maps P_0 to $O := (0 : 1 : 0) \in X(\mathbb{Q})$. In `Magma`, use `EllipticCurve(X)` (which only works for special configurations) or `EllipticCurve(X,P0)`.

Now the abelian groups $(X(\mathbb{Q}), P_0)$ and $(E(\mathbb{Q}), O)$ are isomorphic and solving Problem (II) from the first lecture for X reduces to computing generators of the finitely generated abelian group

$$(E(\mathbb{Q}), O) \cong \mathbb{Z}^r \oplus T\,, \quad r \geq 0,\ \#T < \infty.$$

The computation of generators of the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}} \cong T$ is usually not difficult. We get an upper bound coming from applying the following observation with several primes.

Lemma 2.2. *Let p be a prime of good reduction for E. Then there is an injection*

$$E(\mathbb{Q}_p)_{\mathrm{tors}} \hookrightarrow \bar{E}(\mathbb{F}_p).$$

To complement this, we can simply search for torsion points. Alternatively (or in addition), we can use the theorem of Nagell and Lutz, which says that an affine torsion point $(x, y) \in E(\mathbb{Q})$ of order $\neq 2$ satisfies $x, y \in \mathbb{Z}$ and $y^2 \mid \Delta_E$. Use `TorsionSubgroup(E)` in `Magma`.

Recall from Céline Maistret's lectures that no effective algorithm is known for the computation of the Mordell-Weil rank r. In practice, we can use descent on E (e.g an n-descent or a descent by isogeny) to compute a Selmer group, leading to an upper bound on r. But we have to complement this with a lower bound, which we find by searching for points on E or on suitable coverings (e.g. from the descent we used for the upper bound). We can show that points in $E(\mathbb{Q})$ are independent modulo torsion using reduction modulo suitable primes of good reduction, see [19] (use `IsLinearlyIndependent(S)` to check independence for a (`Magma`-) sequence S of points in $E(\mathbb{Q})$). Alternatively, we can use the theory of heights discussed below. Note that even for elliptic curves with fairly small coefficients, the "smallest" nontorsion point can be very large.

Remark 2.3. When the analytic rank of $E/\mathbb{Q}$ is ≤ 1, then it is equal to r by the work of Gross-Zagier [29] and Kolyvagin [36], and so we can show this via an L-function computation. For $r = 1$, we can construct a nontorsion point in $E(\mathbb{Q})$ from a Heegner point [29].

In `Magma`, you can try to compute the rank using `Rank(E)`. If this doesn't seem to work, use `RankBounds(E)` or apply one of the descent implementations mentioned above directly.

It remains to solve the following:

Problem 2.4. *Suppose we are given $Q_1, \ldots, Q_r \in E(\mathbb{Q})$ which are independent modulo torsion. Find $P_1, \ldots, P_r \in E(\mathbb{Q})$ such their classes in $\Lambda := E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ are generators.*

In the remainder of today's lecture, we will discuss this in detail.

2.3. **Heights.**

We mentioned the "size" of the coordinates of a rational point on a genus 1 curve above. The notion of size can be made precise using height functions.

Definition 2.5. Let $N \geq 1$ and $P = (x_0 : \ldots : x_N) \in \mathbb{P}^N(\mathbb{Q})$ such that $x_0, \ldots, x_N \in \mathbb{Z}$ and $\gcd_{i=0,\ldots,N}(x_i) = 1$. Then the *height* of P is defined by

$$h(P) := \log \max_i \{|x_i|\}.$$

Note that the height of a rational point essentially measures the number of digits it takes to write down the point. We now define a height function on our elliptic curve $E/\mathbb{Q}$.

Definition 2.6. The *naive height* of an affine point $P = (x, y) \in E(\mathbb{Q})$ is $h(P) := h(x)$. We also set $h(O) := 0$.

Theorem 2.7. *The naive height has the following properties:*

(1) $\{P \in E(\mathbb{Q}) : h(P) \leq B\}$ *is finite for all* $B \in \mathbb{R}_{\geq 0}$ *(Northcott property).*
(2) h *is quadratic up to a bounded function; i.e. there is a constant* $C > 0$ *such that* $h(2P) - 4h(P) < C$ *for all* $P \in E(\mathbb{Q})$.
(3) (Tate) For all $P \in E(\mathbb{Q})$, *the* canonical height *(or* Néron-Tate height*)*

$$\hat{h}(P) := \lim_{n\to\infty} 4^{-n} h(2^n P) \in \mathbb{R}_{\geq 0}$$

exists.
(4) $h - \hat{h}$ *is bounded.*
(5) $\hat{h}(P) = 0$ *if and only if* P *has finite order.*
(6) $\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$ *is finite for all* $B \in \mathbb{R}_{\geq 0}$.
(7) $\hat{h}$ *extends to a positive definite quadratic form on the real vector space* $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$.

The proof of Mordell's theorem follows from Theorem 2.7, combined with finiteness of $E(\mathbb{Q})/nE(\mathbb{Q})$ for any $n > 1$ of your choice and the *descent lemma*:

Lemma 2.8. *Suppose that* G *is an abelian group such that*

(1) G/nG *is finite for some* $n \geq 2$.
(2) There is a quadratic form

$$q : G \to \mathbb{R}_{\geq 0}$$

such that $\{g \in G : q(g) \leq B\}$ *is finite for all* $B \in \mathbb{R}_{\geq 0}$.

Then G *is finitely generated.*

Exercise 2.1.

(a) Prove the descent lemma.
(b) Show that there is an algorithm to compute generators of $E(\mathbb{Q})$ if we have representatives of $E(\mathbb{Q})/nE(\mathbb{Q})$ for some $n \geq 2$ and if we can
  (i) compute $\hat{h}(P)$ for given $P \in E(\mathbb{Q})$ and
  (ii) enumerate $\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$ for given $B \in \mathbb{R}_{\geq 0}$.

For convenience, we recall that if G is an abelian group, a function $q\colon G \to \mathbb{R}$ is a *quadratic form* if it satisfies the following conditions:

- $q(g) = q(-g)$ for all $g \in G$.
- The pairing $G \times G \to \mathbb{R}$ which maps (g, h) to $q(g + h) - q(g) - q(h)$ is bilinear.

Your proof of (a) will probably lead you to a solution of (b) which is due to Zagier. In practice this is often good enough to solve Problem 2.4, for instance when $Q_1, \ldots, Q_r$ were obtained from an n-descent. In fact all known methods to solve Problem 2.4 require algorithms for (i) and (ii); the most efficient approach is due to Siksek [46] and is based on viewing the subgroup $\Lambda' \leq \Lambda$ generated by $Q_1, \ldots, Q_r$ as a finite index sublattice of the lattice Λ in the Euclidean vector space $(E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}, \hat{h})$ and saturating Λ' by finding the primes dividing the index $[\Lambda' : \Lambda]$ based on reduction modulo primes of

good reduction (and enlarging Λ', if necessary). An alternative algorithm based on the covering radius of Λ' is due to Stoll [53].

It turns out that computing $\hat{h}$ from its definition is not a good idea – the convergence is only linear, but the size of the coefficients increases quadratically by Theorem 2.7. Note that we can solve (ii) if we can

- enumerate $\{P \in E(\mathbb{Q}) : h(P) \leq B\}$ for given $B \in \mathbb{R}_{\geq 0}$ and
- bound $h - \hat{h}$ from above.

The first of these can be solved using Stoll's program `j-points` (see [51]); it is based on a sieving technique.

The main idea to compute $\hat{h}$ and to bound $h - \hat{h}$ is to decompose the difference $h - \hat{h}$ into local summands.

Theorem 2.9. *(Néron [43]) There is a local decomposition*

$$h - \hat{h} = \sum_{p \text{ prime}} \Psi_p + \Psi_\infty$$

such that

(i) $\Psi_v \colon E(\mathbb{Q}_v) \to \mathbb{R}$ *is v-adically continuous and bounded for every place v of $\mathbb{Q}$;*
(ii) $\Psi_p(Q)/\log(p) \in \mathbb{Q}_{\geq 0}$ *for p finite and $Q \in E(\mathbb{Q}_p)$;*
(iii) Ψ_∞ *is essentially $-\log|\sigma|$, where σ is the Weierstrass sigma-function.*
(iv) *If E is given by a Weierstrass equation which is minimal at p, then Ψ_p factors through $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ for p finite.*

In fact, Néron *defined* $\hat{h}$ using a local decomposition, whereas the limit definition in Theorem 2.7 is due to Tate. Using Theorem 2.9, the computation of $\hat{h}$ reduces to the computation of all Ψ_v (since h is trivial to compute), and bounding $h - \hat{h}$ can be done by bounding all Ψ_v. Because of (iv), only finitely many places have to be considered.

The following exercise walks you through an explicit construction of Ψ_v. Parts (a) and (b) are a bit tedious, so you might want to start with the other parts.

Exercise 2.2. It is easy to see that if the given Weierstrass equation is of the form $y^2 = x^3 + ax + b$ and if $P = (x_P, y_P) \in E(\mathbb{Q})$ is not 2-torsion, then $2P$ is an affine point with x-coordinate $g(P)/f(P)$, where

$$g(P) = x_P^4 - 2ax_P^2 - 8bx_P + a^2,$$
$$f(P) = 4x_P^3 + 4ax_P + 4b.$$

For a place v of $\mathbb{Q}$ and $P \in E(\mathbb{Q}_v) \setminus \{O\}$, define

$$\rho_v(P) := \frac{\max\{|f(P)|_v, |g(P)|_v\}}{\max\{|x_P|_v^4, 1\}} \in \mathbb{Q},$$

where the absolute values $|\cdot|_v$ are normalized to satisfy the product formula. We also set $\rho_v(O) := 1$.

(a) Show that ρ_v is continuous (with respect to the v-adic topology) and bounded.
(b) Show that $\Phi_v := \log \rho_v$ is also continuous and bounded.
(c) Show that the function defined by

$$\Psi_v(Q) := -\sum_{n=0}^{\infty} 4^{-n-1} \Phi_v(2^n Q)$$

is the unique bounded and continuous function $\Psi_v \colon E(\mathbb{Q}_v) \to \mathbb{R}$ such that $\Phi_v(P) = \Psi_v(2P) - 4\Psi_v(P)$.

Now let $P \in E(\mathbb{Q})$. Show that we have

(d) $\Phi_v(P) \neq 0$ only for finitely many v;
(e) $h(2P) - 4h(P) = \sum_v \Phi_v(P)$;
(f) $h(P) - \hat{h}(P) = \sum_v \Psi_v(P)$.

Here the *v-adic topology* on $E(\mathbb{Q}_v)$ is defined by the basis of open sets

$$\{(x,y) \in E(\mathbb{Q}_v) \,:\, |x - x_0|_v < \varepsilon \text{ and } |y - y_0|_v < \varepsilon\}$$

for all $(x_0, y_0) \in E(\mathbb{Q}_v)$ and for all $\varepsilon > 0$, and

$$\{(x,y) \in E(\mathbb{Q}_v) \,:\, |x|_v > \varepsilon\} \cup \{O\},$$

for all $\varepsilon > 0$.

Remark 2.10. If we define the canonical height by $h - \sum_v \Psi_v$, then most of its properties are simple consequences of the properties of h and Ψ_v.

Remark 2.11. Néron constructed Ψ_p for primes p in terms of intersection theory on a regular model of E over $\mathbb{Z}_p$, see [43].

Example 2.12. Suppose that E has multiplicative reduction at p and $v_p(\Delta_E) = n \geq 1$. Then the special fiber of the minimal regular model is an n-gon. Suppose that E is given by a minimal Weierstrass model, and let Γ_0 be the component containing the image of O (i.e. $\Gamma_0(\mathbb{F}_p)$ is the reduction of the subgroup $E_0(\mathbb{Q}_p)$ of nonsingular points). Order its components $\Gamma_0, \ldots, \Gamma_{n-1}$ consecutively. Then we have

$$\Psi_p(\Gamma_i) = \frac{i(n-i)}{n} \log p.$$

Note that if we can bound Φ_v, then we can bound Ψ_v using the geometric series. But it turns out that we can often do much better: For finite $v = p$, Cremona, Prickett and Siksek show how to read off optimal bounds for Ψ from the given equation of E [23]. They also discuss how to bound Ψ_∞; alternative approaches can be found in Bruin's article [11] and in [40].

Now let $P \in E(\mathbb{Q})$. The most efficient way to compute Ψ_∞ is due to Bost and Mestre [6]; it is based on an ingenious use of the arithmetic-geometric mean, which is quadratically convergent. Alternative approaches can be found in [15, §7.5.2]. Theorem 2.9 (iv) leads to a very simple and efficient algorithm to compute Ψ_p for finite primes p found by Silverman [47]. However, it first requires integer factorisation to determine those primes p for which $\Psi_p(P) \neq 0$ is possible. Alternatively, if we can bound Φ_p, then we can approximate Ψ_p to any desired precision via Exercise 2.2; using Theorem 2.9 (ii) we can even compute it exactly using a sufficiently good approximation and continued fractions. It is possible to turn this idea into an algorithm to compute $\sum_p \Psi_p(p)$ which does not require any integer factorization, see [41].

The naive height of a point $P \in E(\mathbb{Q})$ can be computed using `NaiveHeight(P)` in `Magma`, whereas `Height(P)` is an abbreviation for `CanonicalHeight(P)`. The command `Points(E : Bound := B)` lists all points of naive height up to $\exp(B)$; it also works for other curves.

If you want to compute generators of $E(\mathbb{Q})$ in one go, use `Generators(E)`. Note that this is only the tip of the iceberg; `Magma` has extensive functionality for elliptic curves – so does `Sage`. One final command to often make life much easier: For various applications, you want to replace E by `MinimalModel(E)`. In general, this will not be a short Weierstrass equation.

2.4. **Abelian varieties.**

The definition of h can be generalized to abelian varieties $A/\mathbb{Q}$ by setting $h(P) := h(\kappa(P))$, where the image of the map $\kappa\colon A \to \mathbb{P}^{2^g-1}$ is a model of the Kummer variety $A/\{\pm 1\}$. Theorem 2.7 and Theorem 2.9 remain true in this more general setting (and even over number fields), and we can solve Problem 2.4 for A if we can solve (a) and (b).

There are practical algorithms to compute $\hat{h}$ for Jacobians of hyperelliptic curves of genus 2 [28, 53, 42] and genus 3 [56], as well as an algorithm for general Jacobians based on arithmetic intersection theory [61]. Bounding $h - \hat{h}$ is more difficult and, at present, only possible in practice for hyperelliptic curves of genus at most 3 ([53, 42, 56]. In `Magma`, you can at present compute the canonical height for Jacobians of hyperelliptic curves; the computation of generators of $J(\mathbb{Q})$ is possible for curves of genus 2, but you have to combine several algorithms yourself. This will be expanded in the near future.

Using the canonical height, we can define a quantity appearing in the conjecture of Birch and Swinnerton-Dyer, see Céline Maistret's lectures. Set

$$\langle P, Q\rangle := \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2}$$

for $P, Q \in A(\mathbb{Q})$.

Definition 2.13. Let $P_1, \dots, P_r \in A(\mathbb{Q})$ such that their classes in $A(\mathbb{Q})/A(\mathbb{Q})_{\mathrm{tors}}$ are generators. Then

$$\mathrm{Reg}(A/\mathbb{Q}) := \det(\langle P_i, P_j\rangle)_{1\le i,j\le r}$$

is called the *regulator* of $A/\mathbb{Q}$.

3. Third Lecture

Let $X/\mathbb{Q}$ denote a nice curve of genus $g \geq 2$. Recall from the first lecture that when $X(\mathbb{Q}) = \varnothing$, then this can sometimes be proved by showing that $X(\mathbb{Q}_p) = \varnothing$ for some prime number p. In today's lecture, we will see that we can sometimes compute $X(\mathbb{Q})$ as a subset of $X(\mathbb{Q}_p)$, even if $X(\mathbb{Q})$ is non-empty. Most of this lecture is heavily inspired by the excellent survey paper [38] written by McCallum and Poonen.

3.1. **Chabauty.**

We fix a prime number p which, for technical reasons, we assume to be a prime of good reduction for X. We also assume that $X(\mathbb{Q}) \neq \varnothing$ and we fix a point $b \in X(\mathbb{Q})$, giving rise to an Abel-Jacobi map

$$\iota \colon X \to J\,, \quad P \mapsto [P - b]$$

which maps $X(\mathbb{Q})$ into $J(\mathbb{Q})$.

Remark 3.1. If we assume Vojta's conjecture (equivalent to a generalized version of the abc-conjecture), then we expect that the rational points on X have reasonably small height compared to the coefficients of the given equation of X. See [30] for details. Hence the main issue in the computation of $X(\mathbb{Q})$ is not to *find* the rational points – typically it is easy to find a subset $X(\mathbb{Q})_{\text{known}} \subset X(\mathbb{Q})$ such that we suspect equality. In `Magma` you can do this using `RationalPoints(X : Bound := B)`; But proving that equality indeed holds is a quite different matter.

The p-adic points on J have the structure of a p-adic Lie group whose Lie algebra is $\mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1)^*$, which is isomorphic to $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$ via ι; we will identify these two spaces. Therefore there is a continuous homomorphism

$$\log \colon J(\mathbb{Q}_p) \to \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1)^* \to \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$$

with kernel $J(\mathbb{Q}_p)_{\text{tors}}$.

It turns out that for $c \in J(\mathbb{Q}_p)$ sufficiently close to 0 and $\omega \in \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$, we can compute $\log(c)(\omega)$ by formally integrating a formal power series expansion of ω in terms of local coordinates at 0. See [38, §4.1] and [7, §III.7.6] for details.

First recall that by the Mordell-Weil theorem, we have

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

where $r \geq 0$ and T is finite. It is not hard to see that the closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ has dimension $\leq r$. Since $\dim_{\mathbb{Q}_p} \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) = g$, we find:

Lemma 3.2. *(Chabauty [13]) If $r < g$, then there is some $\omega_0 \in \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) \setminus \{0\}$ such that $\log(J(\mathbb{Q}))(\omega_0) = 0$.*

We call ω_0 an *annihilating differential*. Lemma 3.2 will be used to compute $X(\mathbb{Q})$ when $r < g$. Consider the commutative diagram

$$\begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & & \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} & \searrow & \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \end{array}$$

The idea is to pull log back to $X(\mathbb{Q}_p)$.

Definition 3.3. For $P, Q \in X(\mathbb{Q}_p)$ and $\omega \in \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)$, set

$$\int_P^Q \omega := \log([Q-P])(\omega)$$

Suppose that the reductions $\bar{P}, \bar{Q} \in \bar{X}(\mathbb{F}_p)$ of P and Q are equal. Fix a local parameter at P, that is, a uniformizer $t \in \mathbb{Q}_p(X)$ at P which reduces to a uniformizer at $\bar{P}$. Suppose that ω reduces to a nonzero differential on $\bar{X}$. Then it turns out that around P we can expand $\omega = w(t)dt$, where $w \in \mathbb{Z}_p[\![t]\!]$ converges on the *residue disk*

$$D_{\bar{P}} := \{R \in X(\mathbb{Q}_p) \,:\, \bar{R} = \bar{P}\}.$$

The uniformizer t defines an analytic isomorphism $D_{\bar{P}} \cong p\mathbb{Z}_p$. We then have

$$\int_P^Q \omega = \int_0^{t(Q)} w(t)dt \tag{3.1}$$

Such integrals are called *tiny integrals*.

3.2. **Coleman's bound.**

If $r < g$ and if P and Q are both rational points, then $\int_P^Q \omega_0 = 0$ for ω_0 as in Lemma 3.2. So if we fix P, then we are interested in the zeroes of this integral as a function in Q. We first prove a general result about zeroes of p-adic power series.

Lemma 3.4. *Let $\ell \in \mathbb{Q}_p[\![t]\!]$ such that $\ell' = w \in \mathbb{Z}_p[\![t]\!]$. Let ν denote the order of vanishing of the reduction $\bar{w} \in \mathbb{F}_p[\![t]\!]$ at $\bar{t} = 0$. Then, if $\nu \le p-2$, we have*

$$\#\{t \in p\mathbb{Z}_p \,:\, \ell(t) = 0\} \le \nu + 1.$$

So now suppose that $r < g$. Fix ω_0 as in Lemma 3.2 and assume it is scaled so that its reduction $\bar{\omega_0}$ is defined and nonzero. For $\bar{P} \in \bar{X}(\mathbb{F}_p)$ we set $\nu_{\bar{P}} := \mathrm{ord}_{\bar{P}}\, \bar{\omega_0}$.

Corollary 3.5. *If $\nu_{\bar{P}} < p-2$, then*

$$\#(D_{\bar{P}} \cap X(\mathbb{Q})) \le \nu_{\bar{P}} + 1.$$

Proof. We may assume that there is some $P \in D_{\bar{P}} \cap X(\mathbb{Q})$. Expand ω_0 into $w(t)dt$ around P, where t is a local parameter at P and $w(t) \in \mathbb{Z}_p[\![t]\!]$. Then, for every $Q \in D_{\bar{P}}$, we have

$$\int_P^Q \omega_0 = \int_0^{t(Q)} w(t)dt = \ell(t(Q)),$$

where $\ell(t) \in \mathbb{Q}_p[\![t]\!]$ satisfies the conditions of Lemma 3.4. Hence the result follows from Lemma 3.2. □

The following result gives a quantitative version of an earlier theorem of Chabauty, stating that when $r < g$, the set of rational points on X is finite.

Theorem 3.6. *(Coleman [16]) Let $p > 2g$ be a prime of good reduction for a nice curve $X/\mathbb{Q}$ of genus $g > 1$ whose Jacobian has Mordell-Weil rank $r < g$. Then*

$$\#X(\mathbb{Q}) \le \#\bar{X}(\mathbb{F}_p) + 2g - 2.$$

Proof. For $\bar{P} \in \bar{X}(\mathbb{F}_p)$, Riemann-Roch implies

$$\nu_{\bar{P}} \le \sum_{\bar{Q} \in \bar{X}(\mathbb{F}_p)} \nu_{\bar{Q}} = \deg(\mathrm{div}(\bar{\omega_0})) = 2g - 2 < p - 2.$$

Now apply Corollary 3.5 and sum over all $\bar{P} \in \bar{X}(\mathbb{F}_p)$. □

To compute $\bar{X}(\mathbb{F}_p)$ in `Magma`, use `#Points(ChangeRing(X, GF(p)))`. It turns out that in practice, the bound in Theorem 3.6 is almost never sharp. Exercise 3.1 contains one of these rare examples – it also illustrates how the problem of computing rational points on curves can arise in rather unexpected contexts.

Remark 3.7. There are various improvements of Coleman's bound.

(1) If $r < g-1$, then $\#X(\mathbb{Q}) \leq \#\bar{X}(\mathbb{F}_p) + 2r$ (Stoll [54, Corollary 6.7])
(2) One can use primes of bad reduction (Lorenzini-Tucker [37, Corollary 1.11]), Katz, Zureick-Brown [32]).
(3) If $r < g-2$, it is possible to obtain a uniform upper bound on $\#X(\mathbb{Q})$, i.e. there is no dependence on p. This is due to Stoll [57] and Katz, Rabinoff and Zureick-Brown [31].

3.3. **Beyond Coleman's bound.**

Unfortunately, even the best bounds in Remark 3.7 are hardly ever sharp. To remedy this, note that if we can compute an explicit annihilating differential ω_0, and if we find that

$$\#D_{\bar{P}} \cap X(\mathbb{Q})_{\text{known}} = \nu_{\bar{P}} + 1 \quad \text{for all} \quad \bar{P} \in \bar{X}(\mathbb{F}_p), \tag{3.2}$$

then we have also shown that $X(\mathbb{Q}) = X(\mathbb{Q})_{\text{known}}$. This approach is implemented in `Magma` for curves of genus 2; use `Chabauty(P,p)`, where $P \in J(\mathbb{Q})$ has infinite order.

Example 3.8. Consider the hyperelliptic curve $X\colon y^2 = f(x) := x^6 - 4x^4 + 8x^2 - 4$ of genus 2. We easily find $X(\mathbb{Q})_{\text{known}} := \{(\pm 1, \pm 1), \infty_\pm\} \subset X(\mathbb{Q})$. Using the `Magma` command `RankBounds(J)` or a rather painful pen-and-paper 2-descent, we can show that $r = 1$ and hence the results of this lecture are applicable. Since $\operatorname{disc}(f) = 2^{16} \cdot 11^2$, the curve X has good reduction at primes $p \neq 2, 11$. For instance, X has good reduction at $p = 3$, and we have

$$\bar{X}(\mathbb{F}_3) = \{(\pm 1, \pm 1), \infty_\pm\}. \tag{3.3}$$

So let's try to find $\nu_{\bar{P}}$ for all $\bar{P} \in \bar{X}(\mathbb{F}_3)$. First we need an annihilating differential. Recall that a basis of $\mathrm{H}^0(X_{\mathbb{Q}_3}, \Omega^1)$ is $\dfrac{dx}{2y}$ and $\dfrac{xdx}{2y}$. One way to proceed this is to show that

$$\int_{(-1,-1)}^{(1,1)} \frac{dx}{2y} = 0 \tag{3.4}$$

and

$$\int_{(-1,-1)}^{(1,1)} \frac{xdx}{2y} \neq 0. \tag{3.5}$$

Then (3.5) tells us that $[(1,1) - (-1,-1)]$ is not torsion in $J(\mathbb{Q})$ (one can also show this more directly, of course), and hence we can take $\omega_0 = \dfrac{dx}{2y}$ by (3.4). This is already scaled so that $\bar{\omega_0} \in \mathrm{H}^0(\bar{X}, \Omega^1)$ is nonzero.

We first determine $\nu_{\bar{P}}$ for $\bar{P} = (1,1)$. In this case we can take $t = x - 1$ and we find

$$\omega_0 = (t^6 + 6t^5 + 11t^4 + 4t^3 - t^2 + 6t + 1)^{-1/2} dt = (1 - 3t + 14t^2 + \ldots)dt,$$

and hence $\nu_{\bar{P}} = 0$. Therefore,

$$D_{\bar{P}} \cap X(\mathbb{Q}) = \{(1,1)\} = D_{\bar{P}} \cap X(\mathbb{Q})_{\text{known}}.$$

Via an analogous computation we can show that the same holds for all affine points in $\bar{X}(\mathbb{F}_3)$. However, we have $\nu_{\infty_+} = 1 = \nu_{\infty_-}$, so we cannot conclude that $X(\mathbb{Q}) = X(\mathbb{Q})_{\text{known}}$ yet.

In the example, we computed integrals $\int_P^Q \omega$ between points which are not in the same residue disks. There are essentially two ways to do this. First, there is always some positive integer $n \mid \#\bar{J}(\mathbb{F}_p)$ such that $n(Q-P)$ is linearly equivalent to a divisor of the form $\sum_i (Q_i - P_i)$ with P_i and Q_i in the same residue disk for every i. We find

$$\int_P^Q \omega = \frac{1}{n} \sum_i \int_{P_i}^{Q_i} \omega.$$

Note that the points P_i, Q_i might not be $\mathbb{Q}_p$-rational, but the notion of residue disks and the construction of $\int_{P_i}^{Q_i} \omega$ via extension into power series extends to $X(\bar{\mathbb{Q}}_p)$ in a Galois equivariant way.

Another possibility is to use Coleman's integration theory [17]. Coleman shows that the integrals introduced above satisfy several desirable properties, including additivity in endpoints, linearity in the integrand, a fundamental theorem of calculus and a change of variables formula with respect to a lift of Frobenius. Balakrishnan, Bradshaw and Kedlaya [3] have shown that for hyperelliptic curves the computation of the integral $\int_P^Q \omega$ can be reduced to computing the action of such a lift on a suitable p-adic cohomology group, which can be done via an algorithm due to Kedlaya, see [33], and linear algebra. This is implemented in `Sage` (use `X.coleman_integral(omega, P, Q)`). For generalizations see Tuitman's point counting papers [59, 60] and the recent work of Balakrishnan-Tuitman [2]. A `Magma`-implementation of the latter is at https://github.com/jtuitman/Coleman.

But there is yet another serious computational issue: We assume that $r < g$ – so we first have to (hope this is true and) show this! But as for elliptic curves, there is no general algorithm for the computation of the rank (due to our insufficient knowledge of Ш$(J/\mathbb{Q})$). In principle, one can still apply descent, but in practice, this is only feasible for small genus hyperelliptic curves (see [52]) and, more generally, superelliptic curves [45, 25] (using `RankBound(J)` or, for $g = 2$, `RankBounds(J)`, which also computes a lower bound), and for smooth plane quartics [8] with reasonably small coefficients. The algorithms use algebraic number theory and completely avoid actually writing down coverings of J.

But even if we can compute a suitable upper bound, for instance

$$r < \dim_{\mathbb{F}_2} \mathrm{Sel}^2(J/\mathbb{Q}) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] < g,$$

then

- this bound might not be sharp
- even if it is sharp, it be difficult to find r points in $J(\mathbb{Q})$ which are independent modulo torsion – and this is needed to find an annihilating differential ω_0 and in Lemma 3.2.

Both of these issues are addressed by Stoll in [55], where it is shown that one can apply a variant of Chabauty's method working directly with $\mathrm{Sel}^2(J/\mathbb{Q})$.

On a side note, if $r = 0$, the computation of $X(\mathbb{Q})$ is trivial. For curves of genus 2, `Magma` can do this automatically, use `Chabauty0(J)` (despite the misleading name, no Chabauty computation is involved).

Let's return to the situation where we cannot find a suitable prime p such that (3.2) holds. If we can solve the computational problems discussed above, then we can proceed as follows: The function $\rho\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ which maps P to $\int_b^P \omega_0$ vanishes in $X(\mathbb{Q})$. By properties of the integral, it can be written as a convergent p-adic power series on every residue disk, and such series only have finitely many zeroes. So if we can compute the set Z of zeroes of ρ on every disk, then we find $X(\mathbb{Q})$ among them. The only remaining task is to show that none of the points in $Z \setminus X(\mathbb{Q})_{\text{known}}$ are actually rational points. This can be done using the Mordell-Weil sieve, which we will discuss in the fourth lecture. In fact, combining Chabauty's method with the Mordell-Weil sieve leads to a very powerful algorithm for computing $X(\mathbb{Q})$ when $r < g$. See [10]; a heuristic due to Poonen [44] predicts that this should always work (in principle). The combined algorithm is currently only implemented in `Magma` for curves of genus 2 having $r = 1$; you can call it via `Chabauty(P)`, where $P \in J(\mathbb{Q})$ has infinite order.

Finally, this point of view also leads to a possible generalization when $r \geq g$. Namely, the function ρ is constructed using *linear* relations in the image of $\log|_{J(\mathbb{Q})}$. When $r = g$ and J satisfies some additional properties, then one can use quadratic relations to construct a function ρ with finitely many zeroes which vanishes in $X(\mathbb{Q})$. See [4, 1] for details. This is really only the simplest instance of a vast non-abelian extension of Chabauty due to Kim [35, 34]. It is a major open problem to make Kim's approach explicit in more complicated situations.

3.4. **Exercises.**

Exercise 3.1. (Rational right triangles and rational isosceles triangles) We call a triangle *rational* if its side lengths are rational. The goal of this problem is to give a proof of the following result:

Theorem 3.9. *(Hirakawa-Matsumura) Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area. For the representatives of the unique pair of such triangles, we can take the right triangle with sides of lengths* $(377, 135, 352)$ *and the isosceles triangle with sides of lengths* $(366, 366, 132)$.

(a) Let T_1 be a rational right triangle, and T_2 a rational isosceles triangle. Show that we can assume the side lengths of T_1 and T_2 are of the form
(1) $(k(1+t^2), k(1-t^2), 2kt)$ and $(l(1+u^2), l(1+u^2), 4lu)$ or
(2) $(k(1+t^2), k(1-t^2), 2kt)$ and $(l(1+u^2), l(1+u^2), 2l(1-u^2))$.
for some rational numbers $k, l > 0$, $0 < t, u < 1$. Suppose, from now on, that T_1 and T_2 have the same area and perimeter. By scaling both triangles, in both cases we can assume that $l = 1$, which we will do until the end of this problem.

(b) Suppose we are in case (1). Show that there is a rational number $1 < x < 2$ such that
$$2xk^2 + (-3x^3 - 2x^2 + 6x - 4)k + x^5 = 0.$$

(c) Deduce that in case (1), (T_1, T_2) induces an affine rational point on the genus 2 curve
$$X_1\colon y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

(d) Use Magma's command `RankBounds` to show that the Mordell-Weil rank of the Jacobian of X_1 is 1.

(e) Show that X_1 has precisely 10 rational points. (Hint: Eight out of ten points have (small) integral coordinates. However, the remaining pair of points could be difficult to find. If you want, you can use Magma's command `RationalPoints`.)

(f) Repeat the argument for case (2). (Hint: There's a very easy way to solve (d) and (e).)
(g) Deduce the theorem of Hirakawa and Matsumura.

Exercise 3.2. (Due to Stevan Gajovic) Find all rational points on the hyperelliptic curve defined by

$$X\colon y^2 = (x^5 + 11x^4 + 64)(x^6 + 11x^5 + 64x + 729).$$

You may want to use Magma to compute ranks, torsion subgroup(s) and numbers of $\mathbb{F}_p$-rational points.

References

[1] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019. 3.3

[2] Jennifer Balakrishnan and Jan Tuitman. Explicit coleman integration for curves. *Preprint*, 2017. 3.3

[3] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010. 3.3

[4] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller. 3.3

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 1.1

[6] Jean-Benoît Bost and Jean-François Mestre. Calcul de la hauteur archimédienne des points d'une courbe elliptique par un algorithme quadratiquement convergent et application au calcul de la capacité de l'union de deux intervalles. unpublished manuscript, 1993. 2.3

[7] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation. 3.1

[8] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. *Forum Math. Sigma*, 4:e6, 80, 2016. 3.3

[9] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009. 1.3

[10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010. 3.3

[11] Peter Bruin. Bornes optimales pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur les courbes elliptiques sur $\overline{\mathbb{Q}}$. *Acta Arith.*, 160(4):385–397, 2013. 2.3

[12] J. W. S. Cassels. Second descents for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998. Dedicated to Martin Kneser on the occasion of his 70th birthday. 1.3

[13] C. Chabauty. Sur les points rationels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci.*, 212:882–884, 1941. 3.2

[14] C. Chevalley and A. Weil. Un théorème darithmétique sur les courbes algébriques. *C. R. Acad. Sci. Paris*, 196:570–572, 1932. 1.3

[15] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. 2.3

[16] Robert F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765–770, 1985. 3.6

[17] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985. 3.3

[18] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. 2.2

[19] J. E. Cremona. On the computation of Mordell-Weil and 2-Selmer groups of elliptic curves. *Rocky Mountain J. Math.*, 32(3):953–967, 2002. 2.2

[20] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. I. Algebra. *J. Reine Angew. Math.*, 615:121–155, 2008. 1.3

[21] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. II. Geometry. *J. Reine Angew. Math.*, 632:63–84, 2009. 1.3

[22] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves III. Algorithms. *Math. Comp.*, 84(292):895–922, 2015. 1.3
[23] J. E. Cremona, M. Prickett, and Samir Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006. 2.3
[24] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441, 2003. 2.1
[25] Brendan Creutz. Explicit descent in the Picard group of a cyclic cover of the projective line. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 295–315. Math. Sci. Publ., Berkeley, CA, 2013. 3.3
[26] Brendan Creutz. Second p-descents on elliptic curves. *Math. Comp.*, 83(285):365–409, 2014. 1.3
[27] Tom Fisher. Finding rational points on elliptic curves using 6-descent and 12-descent. *J. Algebra*, 320(2):853–884, 2008. 1.3
[28] E. V. Flynn and N. P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, 79(4):333–352, 1997. 2.4
[29] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986. 2.3
[30] Su-Ion Ih. Height uniformity for algebraic points on curves. *Compositio Math.*, 134(1):35–57, 2002. 3.1
[31] Eric Katz, Joseph Rabinoff, and David Zureick-Brown. Uniform bounds for the number of rational points on curves of small Mordell-Weil rank. *Duke Math. J.*, 165(16):3189–3240, 2016. 3
[32] Eric Katz and David Zureick-Brown. The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions. *Compos. Math.*, 149(11):1818–1838, 2013. 2
[33] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001. 3.3
[34] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. 3.3
[35] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel. *Inventiones mathematicae*, 161(3):629–656, 2005. 3.3
[36] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988. 2.3
[37] Dino Lorenzini and Thomas J. Tucker. Thue equations and the method of Chabauty-Coleman. *Invent. Math.*, 148(1):47–77, 2002. 2
[38] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012. 3, 3.1
[39] J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996. 1.3
[40] J. S. Müller and C. Stumpe. Archimedean local height differences on elliptic curves. *Acta Arith.*, to appear. 2.3
[41] J. Steffen Müller and Michael Stoll. Computing canonical heights on elliptic curves in quasi-linear time. *LMS J. Comput. Math.*, 19(suppl. A):391–405, 2016. 2.3
[42] Jan Steffen Müller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016. 2.4
[43] A. Néron. Quasi-fonctions et hauteurs sur les variétés abéliennes. *Ann. of Math. (2)*, 82:249–331, 1965. 2.9, 2.11
[44] Bjorn Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15(4):415–420, 2006. 3.3
[45] Bjorn Poonen and Edward F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997. 3.3
[46] Samir Siksek. Infinite descent on elliptic curves. *Rocky Mountain J. Math.*, 25(4):1501–1538, 1995. 2.3
[47] Joseph H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988. 2.3
[48] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Math. Comp.*, 74(251):1531–1543, 2005. 2.1
[49] Sebastian Stamminger. *Explicit 8-descent on elliptic curves*. PhD thesis, International University Bremen, 2005. 1.3
[50] W. A. Stein et al. *Sage Mathematics Software (Version 6.3)*. The Sage Development Team, 2014. `http://www.sagemath.org`. 1.1

[51] Michael Stoll. Ratpoints and j-points. http://www.mathe2.uni-bayreuth.de/stoll/programs/index.html. 2.3
[52] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001. 3.3
[53] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002. 2.3, 2.4
[54] Michael Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006. 1
[55] Michael Stoll. Chabauty without the Mordell-Weil group. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 623–663. Springer, Cham, 2017. 3.3
[56] Michael Stoll. An explicit theory of heights for hyperelliptic Jacobians of genus three. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 665–715. Springer, Cham, 2017. 2.4
[57] Michael Stoll. Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank. *J. Eur. Math. Soc. (JEMS)*, 21(3):923–956, 2019. 3
[58] The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2014. available from `http://pari.math.u-bordeaux.fr/`. 1.1
[59] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Math. Comp.*, 85(298):961–981, 2016. 3.3
[60] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017. 3.3
[61] R. van Bommel, D. Holmes, and J. S. Müller. Explicit arithmetic intersection theory and computation of néron-tate heights. *Math. Comp.*, to appear. 2.4
[62] Tom Womack. *Explicit descent on elliptic curves*. PhD thesis, University of Nottingham, 2003. 1.3

Bernoulli Institute, Rijksuniversiteit Groningen, The Netherlands

Email address: `steffen.muller@rug.nl`