RATIONAL POINTS ON CURVES

MICHAEL STOLL

In these lectures we will discuss how to determine the set of rational points on a curve of genus at least 2 over $\mathbb{Q}$. We will use hyperelliptic curves throughout as our main examples, since they are fairly well amenable to explicit computations. Most of the statements and techniques generalise to arbitrary curves and to curves over arbitrary number fields, at least in principle. Practical computations tend to become prohibitive pretty soon, however, when leaving the realm of hyperelliptic curves of moderate genus and coefficients of moderate size over $\mathbb{Q}$.

As a good reference for the topic we recommend the survey paper [Sto11].

1. How to show that a hyperelliptic curve has no rational points

In this section, we sketch various possibilities of showing that a given hyperelliptic curve has no rational points.

1.1. Hyperelliptic Curves.

A *hyperelliptic curve* C over a field k not of characteristic 2 is the smooth projective curve associated to an affine plane curve given by an equation of the form

$$y^2 = f(x)\,,$$

where f is a squarefree polynomial of degree at least 5. If the degree of f is $2g+1$ or $2g+2$, then the curve has genus g (this is also true for $\deg(f) < 5$). In the former case, we have to add one (k-rational) point ∞ at infinity, in the latter case, there are two points $\infty_{\pm s}$ at infinity (where s is a square root of the leading coefficient of f), which are k-rational if and only if $s \in k$, i.e., the leading coefficient of f is a square in k. We write $C(k)$ for the set of k-rational points on C; then $C(k)$ consists of the zero, one, or two k-rational points at infinity, together with the affine points $(\xi, \eta) \in k \times k$ such that $\eta^2 = f(\xi)$.

We can realise C as a smooth curve in the weighted projective plane $\mathbb{P}_{1,g+1,1}$: Homogenise f to obtain $F(x,z)$ of 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 $v^2 = F(1,u)$.

Recall the following fact.

Theorem 1.1 (Faltings [Fal83])**.** *If C is a smooth, projective and absolutely irreducible curve over $\mathbb{Q}$ of genus $g \ge 2$, then $C(\mathbb{Q})$ is finite.*

So at least in principle, we can write down the finite set $C(\mathbb{Q})$. To do so in practice for a given (hyperelliptic, say) curve C remains a major open problem. However, there are reasons to hope for a solution.

Date: September 19, 2015.

Consider a hyperelliptic curve $C\colon y^2 = f(x)$ over $\mathbb{Q}$. By scaling y, we can arrange that f has integral coefficients. We define the *height* of the equation $y^2 = f(x)$ with $f \in \mathbb{Z}[x]$ (squarefree) to be the maximum of the absolute values of the coefficients of f. It is clear that the number of such equations of height $\le X$ is finite, so we can define (upper/lower) densities and averages by looking at the relevant fractions or averages for equations of height $\le X$ and then taking the (upper/lower) limit as $X \to \infty$.

In this sense, one expects heuristically that 100% of all hyperelliptic curves of fixed genus $g \ge 2$ have no rational point. (Bhargava has shown [Bha13] that the lower density is $1 - o(2^{-g})$; we will come back to this at the end of this lecture.)

So in most cases, the problem of writing down $C(\mathbb{Q})$ means proving that $C(\mathbb{Q}) = \emptyset$. In this first lecture, I will explain several possible ways of doing that.

1.2. **Local Solubility.**

$C(\mathbb{Q}) \neq \emptyset$ implies that $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p. This prompts the following definition.

Definition 1.2. Let C be a curve (or, more generally, a variety) over $\mathbb{Q}$. Then C 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.

We then have the obvious implication

$$C \text{ is not ELS} \quad \Longrightarrow \quad C(\mathbb{Q}) = \emptyset\,. \tag{1.1}$$

Examples 1.3.

(1) If $C\colon y^2 = -x^6 - x^2 - 17$, then clearly $C(\mathbb{R}) = \emptyset$, so $C(\mathbb{Q}) = \emptyset$ as well.

(2) For $C\colon y^2 = -x^6 - 3x^5 + 4x^4 + 2x^3 + 4x^2 - 3x - 1$, we have $C(\mathbb{F}_{11}) = \emptyset$ (the polynomial on the right remains squarefree when reduced mod 11, so we obtain a hyperelliptic curve over $\mathbb{F}_{11}$), which implies $C(\mathbb{Q}_{11}) = \emptyset$ (since every $\mathbb{Q}_{11}$-rational point must reduce to an $\mathbb{F}_{11}$-rational point) and then $C(\mathbb{Q}) = \emptyset$.

Why do we consider the ELS property? The general idea here is that 'local' (i.e., over the completions $\mathbb{R}$ and $\mathbb{Q}_p$ of $\mathbb{Q}$) properties are usually 'easy' to check or understand, whereas 'global' ones (over $\mathbb{Q}$) are often difficult. This is illustrated by the following result.

Proposition 1.4. *There is an algorithm that decides if a given (hyperelliptic, say) curve C is ELS or not.*

Sketch of proof.

(1) We have $C(\mathbb{R}) = \emptyset$ if and only if f has no real roots and the leading coefficient of f is negative.

(2) For any given prime p, we can use Hensel's Lemma to reduce checking if $C(\mathbb{Q}_p) = \emptyset$ to checking the solubility mod p^n for some $n \ge 1$ (which is a finite problem).

(3) If $p + 1 > 2g\sqrt{p}$ and p does not divide the discriminant of f, then C reduces to a smooth hyperelliptic curve of genus g over $\mathbb{F}_p$, which by the Weil bounds has $\mathbb{F}_p$-rational points (and all these points are smooth). By Hensel's Lemma, a smooth $\mathbb{F}_p$-point lifts to a point over $\mathbb{Q}_p$, so $C(\mathbb{Q}_p) \neq \emptyset$.

(4) The previous observation allows us to reduce to $\mathbb{R}$ and finitely many $\mathbb{Q}_p$, and for each of these, we can effectively check for local points. □

If the genus is zero, then the converse of (1.1) holds, too ('Hasse Principle'). This is no longer true for $g \geq 1$, however.

For fixed g, the subset of hyperelliptic curves that are ELS has a density $0 < \delta_g < 1$, see [PS99]. For example, $\delta_2 \approx 0.84$–0.85. The density δ_g seems to increase with g, but stays away from 1. So for a large fraction of the curves without rational points, we will not be able to prove $C(\mathbb{Q}) = \emptyset$ by showing that C is not ELS. So we need some other methods.

1.3. **Descent.**

Consider a hyperelliptic curve $C\colon y^2 = f(x)$ such that we have a factorisation $f(x) = f_1(x)f_2(x)$ with at least one of $\deg(f_1)$ and $\deg(f_2)$ even. If we have a point $P = (\xi, \eta) \in C(\mathbb{Q})$, then $f_1(\xi) \neq 0$ or $f_2(\xi) \neq 0$ (or both), so there are a unique squarefree integer d and $\eta_1, \eta_2 \in \mathbb{Q}$ such that $f_1(\xi) = d\eta_1^2$ and $f_2(\xi) = d\eta_2^2$. We can describe this situation in geometric terms by saying that P lifts to a rational point on the curve

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

under the morphism $\pi_d\colon D_d \to C$, $(x, y_1, y_2) \mapsto (x, dy_1y_2)$. (This also works for the points at infinity, as one can see by considering the other affine chart. Note that we need the condition on the parity of the degrees of f_1 and f_2 to make sure that D_d is smooth at infinity.)

Assume that f_1 and f_2 have integral coefficients and let R denote their resultant. If the prime p does not divide R, but divides d, then a p-adic point on D_d would have $v_p(f_1(x))$ and $v_p(f_2(x))$ both odd (or one of them infinite). Assuming $x \in \mathbb{Z}_p$, this leads to the contradiction that the reductions of f_1 and f_2 mod p have a common root. For $x \notin \mathbb{Z}_p$, the same argument with an affine chart around infinity gives a contradiction again. This shows that the possible squarefree d are products of -1 and primes dividing R; this gives an explicit finite set T of possible values for d such that D_d might be ELS.

We can now check, for each $d \in T$, whether D_d is ELS. If it turns out that no D_d is ELS, then $D_d(\mathbb{Q}) = \emptyset$ for all d, so a rational point on C cannot lift anywhere, hence $C(\mathbb{Q}) = \emptyset$.

Example 1.5. Consider

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

One can check the following (Exercise!).

(1) C is ELS.
(2) The resultant of the two factors is 19; this gives $T = \{\pm 1, \pm 19\}$.
(3) If $d < 0$, then $D_d(\mathbb{R}) = \emptyset$ (note that f_2 is positive on $\mathbb{R}$).
(4) If $d \equiv 1 \bmod 3$, then $D_d(\mathbb{F}_3) = \emptyset$, hence $D_d(\mathbb{Q}_3) = \emptyset$.

We conclude that $C(\mathbb{Q}) = \emptyset$.

We note that $\pi_1\colon D_1 \to C$ is an unramified covering. The approach described here in this special case generalises to arbitrary unramified coverings $\pi\colon D \to C$ such that the extension $\bar{\mathbb{Q}}(C) \subset \bar{\mathbb{Q}}(D)$ of function fields is Galois: There is a finite number of *twists* $\pi_d\colon D_d \to C$ (coverings of C that over $\bar{\mathbb{Q}}$ become isomorphic to π) such that each rational point on C lifts to a rational point on one of these twists. See [Sto07] for a detailed discussion.

1.4. **The fake 2-Selmer set.**

What can we do if the polynomial f does not factor over $\mathbb{Q}$ (most polynomials don't)?

We can try to consider all possible factorisations (which will in general not be defined over $\mathbb{Q}$, but over some number fields) simultaneously. Since the Galois group of $\mathbb{Q}$ permutes them, the whole setting is again 'defined over $\mathbb{Q}$'. For this, we consider a 'generic' linear factor of f and look at its class modulo squares. Since the degree of this linear factor is odd, we also have to disregard scaling by rational numbers (this is plausible when looking at the homogenised polynomial: scaling the projective coordinates scales the linear factor correspondingly).

Set $L := \mathbb{Q}[x]/\langle f(x)\rangle$ and $L_v := \mathbb{Q}_v[x]/\langle f(x)\rangle$ for $v = p$ a prime or $v = \infty$ with $\mathbb{Q}_\infty := \mathbb{R}$. We write T for the image of x in these étale algebras. We further set

$$H := \{\alpha L^\square \mathbb{Q}^\times : cN_{L/\mathbb{Q}}(\alpha) \in \mathbb{Q}^\square\} \subset \frac{L^\times}{L^\square \mathbb{Q}^\times},$$

where c is the leading coefficient of f (which we assume has even degree). Here $L^\square$ and $\mathbb{Q}^\square$ denote the subgroups of squares in $L^\times$ and $\mathbb{Q}^\times$, respectively. We define H_v analogously with L_v and $\mathbb{Q}_v$ in place of L and $\mathbb{Q}$. Then we have natural maps $\rho_v \colon H \to H_v$.

Next, we define the '$x - T$ map'

$$\delta\colon C(\mathbb{Q}) \longrightarrow H\,, \quad \begin{cases} (\xi,\eta) \longmapsto (\xi - T)L^\square\mathbb{Q}^\times & \text{if } \eta \neq 0 \\ (\xi, 0) \longmapsto (\xi - T + f_1(T))L^\square\mathbb{Q}^\times & \text{where } f(x) = (x-\xi)f_1(x) \\ \infty_{\pm s} \longmapsto L^\square\mathbb{Q}^\times & \end{cases}$$

(the first definition does not work when $\eta = 0$, since then $x - T$ is not invertible in L) and define $\delta_v \colon C(\mathbb{Q}_v) \to H_v$ analogously. Note that $cN_{L/\mathbb{Q}}(\xi - T) = f(\xi) = \eta^2$, so that the image of δ really is contained in H (and similarly for δ_v).

Now we consider the following commutative square:

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\delta"] \arrow[d] & H \arrow[d, "(\rho_v)_v"] \\
\prod_v C(\mathbb{Q}_v) \arrow[r, "\prod_v \delta_v"] & \prod_v H_v
\end{tikzcd}$$

Definition 1.6. Let C be a hyperelliptic curve over $\mathbb{Q}$ as above. The *fake 2-Selmer set* of C is the subset

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

of H.

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

Theorem 1.7 ([BS09])**.** *The set* $\mathrm{Sel}_2^{\text{fake}}(C)$ *is finite and computable.*

Sketch of proof. In a similar way as in the previous section, one can reduce to a finite subset H_S of H, where S is the set of places of L that are archimedean or divide $2c\,\mathrm{disc}(f)$ and

$$H_S := \{\alpha L^\square\mathbb{Q}^\times : v_\mathfrak{p}(\alpha) \in 2\mathbb{Z} \text{ for all } \mathfrak{p} \notin S\}\,.$$

(To show that H_S is indeed finite, one uses the finiteness of the ideal class group and the finite generation of the unit group of a number field; to actually compute an $\mathbb{F}_2$-basis of H_S, one needs to find generators of (the 2-torsion of) the class group and of the units modulo squares.) For sufficiently large primes p not dividing $c\,\mathrm{disc}(f)$, one shows that $\mathrm{im}(\delta_p)$ equals the part of H_p that comes from p-adic units, which contains $\rho_p(H_S)$, so no information is obtained from these primes. The remaining finitely many places v can be dealt with by a finite computation each. (But note that the bound for these primes gets quite large with increasing genus. Already for genus 2, it is 1153. The growth is exponential in g.) □

Remarks 1.8.

(1) There is a 2-*Selmer set* $\mathrm{Sel}_2(C)$ of C (without the 'fake'). It classifies ELS '2-coverings' of C, see [Sto07]. There is a surjective map $\mathrm{Sel}_2(C) \to \mathrm{Sel}_2^{\mathrm{fake}}(C)$, which is sometimes a bijection and usually a 2–1 map. We can distinguish between these two cases by looking at the factorisation of f over $\mathbb{Q}$ and over quadratic number fields, see [BS09].

(2) Manjul Bhargava [Bha13] has actually shown the following: As $g \to \infty$, the (fake) 2-Selmer set is empty for a set of hyperelliptic curves of genus g (with integral coefficients, ordered by height as above) of lower density $1 - o(2^{-g})$. So this method comes close to being always successful!

Example 1.9. In [BS08], we considered all curves of genus 2 (they are all hyperelliptic) of height at most 3. There are close to $200,000$ isomorphism classes. All but about $1,500$ either

(1) have a (fairly small) rational point,

(2) are not ELS, or

(3) have empty 2-Selmer set.

The remaining ones can be dealt with a further technique called the *Mordell-Weil Sieve*, see [BS10], which we will say more about in the last lecture of this series.

1.5. **Exercises.**

(1) Work out the proof of Proposition 1.4 and formulate a detailed algorithm for checking the ELS property.

(2) Construct other examples like Example 1.5. Generalise the method to factorisations into more than two factors and find an example where this is needed to prove that there is no rational point.

(3) Show that if the approach as in Example 1.5 is successful, then the fake 2-Selmer set is empty.

(4) Compute the fake 2-Selmer set for some hyperelliptic curve, e.g., for

$$y^2 = -23(x^3 - x^2 + 1)(x^3 - x + 1).$$

Hint. You may want to use that $\mathbb{Q}(\alpha)$ has trivial class group, ring of integers $\mathbb{Z}[\alpha]$ and fundamental unit α, where $\alpha^3 - \alpha + 1 = 0$.

2. The Jacobian

In this lecture we give an overview over the main facts concerning the Jacobian variety of a (hyperelliptic) curve.

2.1. **Divisors and divisor classes.**

Let K be a perfect field; we write G_K for the absolute Galois group of K. If C is a 'nice' (i.e., smooth, projective and geometrically irreducible) curve over K, then we define its *group of divisors* Div_C to be the free abelian group generated by the set $C(\bar{K})$ of all points of C defined over the algebraic closure $\bar{K}$ of K. Its elements are *divisors* on C, so a divisor D is a formal integral linear combination of points. D is said to be *effective* if all its coefficients are nonnegative.

The group G_K acts on $C(\bar{K})$ in a natural way; this induces an action on Div_C by group automorphisms. Divisors that are invariant under this action are said to be *K-rational*; we write $\operatorname{Div}_C(K)$ for the subgroup of K-rational divisors.

Example 2.1. Let $C\colon y^2 = f(x)$ be a hyperelliptic curve over K. Fix $\xi \in K$ and let $\eta \in \bar{K}$ be such that $\eta^2 = f(\xi)$. Then $D_\xi = (\xi, \eta) + (\xi, -\eta)$ is a K-rational divisor on C. Similarly, we can define $D_\infty = \infty_s + \infty_{-s} \in \operatorname{Div}_C(K)$.

A divisor has a *degree*, which is the sum of its coefficients:

$$\text{if } D = \sum_P n_P P, \quad \text{then} \quad \deg(D) = \sum_P n_P \in \mathbb{Z}.$$

This gives a (surjective) group homomorphism $\deg\colon \operatorname{Div}_C \to \mathbb{Z}$; its kernel is Div_C^0, the subgroup of divisors of degree zero. We also write $\operatorname{Div}_C^0(K)$ for the group of K-rational divisor of degree zero.

If $f \in \bar{K}(C)^\times$ is a rational function on C, then we can associate to it a divisor

$$\operatorname{div}(f) = \sum_P v_P(f) \cdot P \in \operatorname{Div}_C .$$

Here $v_P(f)$ denotes the order of vanishing of f at the point P (which is the negative of the pole order if f has a pole at P). Any nonzero function on C has only finitely many zeros and poles, so $\operatorname{div}(f)$ is indeed a divisor. Any such divisor is said to be *principal.* We obtain a group homomorphism

$$\operatorname{div}\colon \bar{K}(C)^\times \longrightarrow \operatorname{Div}_C,$$

whose image (which is the group of principal divisors) we denote by Princ_C. The cokernel of div is the *Picard group*

$$\operatorname{Pic}_C = \operatorname{Div}_C / \operatorname{Princ}_C .$$

It is clear that div is equivariant with respect to the natural actions of G_K, which implies that if $f \in K(C)^\times$, then $\operatorname{div}(f) \in \operatorname{Div}_C(K)$.

Lemma 2.2.

$$\operatorname{Princ}_C \subset \operatorname{Div}_C^0 .$$

Sketch of proof. Consider any non-constant morphism $\pi\colon C \to \mathbb{P}^1$. This induces homomorphisms $\pi_*\colon \operatorname{Div}_C \to \operatorname{Div}_{\mathbb{P}^1}$ and $\pi_*\colon \bar{K}(C)^\times \to \bar{K}(\mathbb{P}^1)^\times = \bar{K}(x)^\times$ (the latter is the norm map associated to the extension $\pi^*\colon \bar{K}(x) \to \bar{K}(C)$ of function fields) that are compatible with the formation of principal divisors. It follows that for any $f \in \bar{K}(C)^\times$, $\deg(\operatorname{div}(f)) = \deg(\pi_*(\operatorname{div}(f))) = \deg(\operatorname{div}(\pi_*(f)))$. So we reduce to the case $C = \mathbb{P}^1$, where it is easy to check that all principal divisors have degree zero. □

So deg descends to $\deg\colon \operatorname{Pic}_C \to \mathbb{Z}$ with kernel

$$\operatorname{Pic}^0_C = \operatorname{Div}^0_C \,/\, \operatorname{Princ}_C \,.$$

We say that two divisors D and D' are *linearly equivalent*, $D \sim D'$, if they have the same image in the Picard group, which means that their difference is a principal divisor. We denote the image of D in Pic_C by $[D]$ and call it the *divisor class* of D.

Since div is G_K-equivariant, Princ_C is a G_K-invariant subgroup of Div_C (or Div^0_C), and we obtain an induced G_K-action on Pic_C and Pic^0_C. We write again $\operatorname{Pic}_C(K)$ and $\operatorname{Pic}^0_C(K)$ for the subgroups of G_K-invariant divisor classes and say that they are *K-rational.*

Example 2.3. The divisors D_ξ from Example 2.1 are all linearly equivalent, since

$$D_\xi - D_{\xi'} = \operatorname{div}\Bigl(\frac{x-\xi}{x-\xi'}\Bigr) \qquad \text{and} \qquad D_0 - D_\infty = \operatorname{div}(x).$$

The class $[D_\xi]$ is a K-rational divisor class of degree 2.

Remark 2.4. It is not true in general that every K-rational divisor class can be represented by a K-rational divisor.

This is true, however, when $C(K) \neq \emptyset$, or when $K = \mathbb{Q}$ and C is ELS.

The most important fact in this context is that the group Pic^0_C together with the G_K-action on it can be realised as the set of $\bar{K}$-points of a suitable projective group variety (an abelian variety) defined over K.

Theorem 2.5. *Let C be a nice curve over K. Then there is an abelian variety J over K such that there is an isomorphism of G_K-modules $\operatorname{Pic}^0_C \to J(\bar{K})$. The dimension of J agrees with the genus of C.*

This abelian variety J is called the *Jacobian variety* or just the *Jacobian* of C. We usually identify $J(\bar{K})$ and Pic_C. In particular, we have $J(K) = \operatorname{Pic}^0_C(K)$.

Examples 2.6. If C is a curve of genus zero, then J is trivial (just a point).

If C is a curve of genus one, then J is a one-dimensional abelian variety, hence an elliptic curve. If C has a K-rational point (so is an elliptic curve itself), then J and C are isomorphic. Otherwise, C and J cannot be isomorphic, since J always has a K-rational point, namely the zero of the group law.

Even though J is a projective variety, it is not of much use to try to work with explicit equations defining J as a subset of some projective space, since any fairly natural realisation will require a projective space of large dimension and lots of equations. For example, the Jacobian of a curve of genus two has a natural embedding into $\mathbb{P}^{15}$, whose image is described by 72 quadratic equations (which are explicitly known, due to Cassels and Flynn). To my knowledge, no explicit equations are known for Jacobians of curves of any genus ≥ 3. For practical purposes, it is much more convenient to represent points on J by divisors on C.

However, it is still useful to know that Pic^0_C can be realised geometrically, since this allows us to use geometric constructions. For example, we have the following fact.

Proposition 2.7. *Let C be a nice curve over K of genus $g \geq 1$ and with Jacobian J, and let $[D_0]$ be a K-rational divisor class of degree 1 (for example, D_0 could be a K-rational point on C). Then*

$$i_{[D_0]} \colon C \longrightarrow J, \quad P \longmapsto [P - D_0]$$

is an embedding of K-varieties.

The basic idea to approach $C(\mathbb{Q})$ is now to use such an embedding i of C into J, then i induces a bijection between $C(\mathbb{Q})$ and the intersection of $J(\mathbb{Q})$ with $i(C)$. We can hope to make use of the additional (group) structure of J to help us determine $C(\mathbb{Q})$.

2.2. **The Mordell-Weil theorem.**

We know that J is an abelian variety, so $J(\bar{K})$ and $J(K)$ are abelian groups. The following famous theorem tells us more.

Theorem 2.8 (Mordell [Mor22], Weil [Wei29])**.** *Let K be $\mathbb{Q}$ (or, more generally, a number field, or even a field finitely generated over its prime field) and let J be the Jacobian of a nice curve over K. Then the abelian group $J(K)$ is finitely generated.*

By the structure theorem for finitely generated abelian group, we therefore have

$$J(K) \cong J(K)_{\text{tors}} \times \mathbb{Z}^r,$$

where $J(K)_{\text{tors}}$ denotes the (finite) torsion subgroup of $J(K)$ and the *rank* r is a nonnegative integer.

The proof is in two parts. The first step is to show that $J(K)/2J(K)$ (or $J(K)/mJ(K)$ for some $m \geq 2$) is finite ('Weak Mordell-Weil Theorem'). The second step uses the fact that there is a suitable 'height function' on $J(K)$ to deduce from the result of the first step that $J(K)$ is indeed finitely generated.

If we grant that we know that $J(K)$ is finitely generated, then knowledge of $J(K)_{\text{tors}}$ (or just the 2-torsion $J(K)[2]$) and a bound on the order of $J(K)/2J(K)$ will give us an upper bound on the rank r, since

$$J(K)/2J(K) \cong J(K)_{\text{tors}}/2J(K)_{\text{tors}} \times (\mathbb{Z}/2\mathbb{Z})^r \cong J(K)[2] \times (\mathbb{Z}/2\mathbb{Z})^r.$$

We obtain lower bounds on r by finding points in $J(K)$ and checking them for independence.

2.3. **The torsion subgroup.**

We now discuss how one can try to determine $J(\mathbb{Q})_{\text{tors}}$ when J is the Jacobian of a (nice) curve C over $\mathbb{Q}$. Let p be a prime of good reduction for C (this means that we can write down equations with integral coefficients defining C such that the same equations, with coefficients reduced mod p, again define a nice curve $\bar{C}$ of the same genus as that of C). There is a canonical reduction map $C(\mathbb{Q}) \to \bar{C}(\mathbb{F}_p)$, $P \mapsto \bar{P}$.

Proposition 2.9. *In this situation, p is also a prime of good reduction for J. The associated reduction map $J(\mathbb{Q}) \to \bar{J}(\mathbb{F}_p)$ is a group homomorphism. If $p \geq 3$, then this homomorphism is injective when restricted to the torsion subgroup $J(\mathbb{Q})_{\text{tors}}$.*

If $P_0 \in C(\mathbb{Q})$ defines the embedding $i_{P_0} \colon C \to J$, then the following diagram commutes:

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "i_{P_0}"] \arrow[d] & J(\mathbb{Q}) \arrow[d] \\
\bar{C}(\mathbb{F}_p) \arrow[r, "i_{\bar{P}_0}"] & \bar{J}(\mathbb{F}_p)
\end{tikzcd}$$

The proof of the first part is based on the fact that (when $p > 2$) the kernel of the reduction map on $J(\mathbb{Q}_p)$ is isomorphic as a group to $\mathbb{Z}_p^g$ and thus torsion-free. The second part will be useful later.

This result allows us to obtain upper bounds for the order of $J(\mathbb{Q})_{\text{tors}}$, since it implies that $\#J(\mathbb{Q})_{\text{tors}}$ divides $\#\bar{J}(\mathbb{F}_p)$ for all odd primes p of good reduction. We obtain lower bounds by actually finding torsion points.

Example 2.10. Consider $C\colon y^2 = x^5 + 1$. One can check that $[(-1,0) - \infty] \in J(\mathbb{Q})$ has order 2 (note that $2\big((-1,0) - \infty\big) = \operatorname{div}(x+1)$ is principal) and that $[(0,1) - \infty] \in J(\mathbb{Q})$ has order 5 (since $5\big((0,1) - \infty\big) = \operatorname{div}(y-1)$). So $\#J(\mathbb{Q})_{\text{tors}}$ is divisible by 10.

On the other hand, $p = 3$ is a prime of good reduction (for a hyperelliptic curve $y^2 = f(x)$ with $f \in \mathbb{Z}[x]$, any odd prime p such that $\bar{f}$ has no multiple roots mod p is a prime of good reduction), and one can check that $\#\bar{J}(\mathbb{F}_3) = 10$, so $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/10\mathbb{Z}$.

For odd degree hyperelliptic curves, the 2-torsion subgroup of $J(K)$ has a simple explicit description.

Lemma 2.11. *Let $C\colon y^2 = f(x)$ be hyperelliptic over K with $\deg(f) = 2g+1$. Let $f = f_1 f_2 \cdots f_n$ be a factorisation into irreducible polynomials over K. Then $J(K)[2]$ is generated by $P_1, P_2, \ldots, P_n$, where*

$$P_j = \Big[\sum_{\xi : f_j(\xi)=0} (\xi, 0) - \deg(f_j)\cdot\infty\Big]$$

and the only relations are $2P_j = 0$ and $P_1 + P_2 + \ldots + P_n = 0$.

In particular, $\dim_{\mathbb{F}_2} J(K)[2] = n - 1$.

2.4. **The 2-Selmer group.**

It remains to determine the rank r of $J(\mathbb{Q})$. This is, in general, a rather difficult problem. In particular, it is not presently known whether there is an algorithm (however inefficient) that is guaranteed to find r in all cases, not even for curves of genus 2 (or genus 1, for that matter).

What we can do is to search for points on $J(\mathbb{Q})$ (and test them for independence, for example by considering the image of the group they generate under a diagonal map $J(\mathbb{Q}) \to \prod_{p\in S} \bar{J}(\mathbb{F}_p)$, where S is some finite set of good primes); this will give us a lower bound on r. The hard part is to get an upper bound. One possibility for this is to compute the (size of) the 2-Selmer group.

Let $C\colon y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$; we assume that f has odd degree $2g+1$ and is monic to simplify things. Recall the algebra $L = \mathbb{Q}[x]/\langle f\rangle$ and the map $\delta\colon C(\mathbb{Q}) \to L^\times/L^\square$ (when $\deg(f)$ is odd there is no need to also factor out $\mathbb{Q}^\times$), which is given on points $P = (\xi, \eta)$ with $\eta \neq 0$ by $\delta(P) = (\xi - T)L^\square$, where T is the image of x in L. We extend this to K-rational divisors: if $D = \sum_P n_P \cdot P$ is a K-rational divisor whose support avoids ∞ and the points with $y = 0$, then

$$\delta(D) = \prod_P (x(P) - T)^{n_P} L^\square = (-1)^{\deg(a)} a(T) L^\square,$$

where $a = \prod_P (x - x(P))^{n_P} \in \mathbb{Q}(x)$. One can extend this to include divisors whose support meets ∞ or one of the points $(\xi, 0)$ and obtains a group homomorphism

$$\delta\colon \operatorname{Div}_C(\mathbb{Q}) \longrightarrow H = \{\alpha L^\square : N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Q}^\square\} \subset L^\times/L^\square.$$

The same construction works over any field K instead of $\mathbb{Q}$.

Lemma 2.12. *δ is trivial on $\operatorname{Princ}_C(K)$: for any $f \in K(C)^\times$, we have $\delta(\operatorname{div}(f)) = L^\square$. In particular, δ induces a homomorphism $\delta\colon J(K) = \operatorname{Pic}^0_C(K) \to H$.*

Proposition 2.13. *The kernel of δ on $J(K)$ is exactly $2J(K)$.*

This tells us that the image of δ is isomorphic to $J(K)/2J(K)$. This does not immediately help, but it allows us to obtain an upper bound on $\#\bigl(J(\mathbb{Q})/2J(\mathbb{Q})\bigr)$ by comparing with 'local' information. We write $\mathbb{Q}_\infty = \mathbb{R}$ and use v as a variable running over the places of $\mathbb{Q}$ (the primes and ∞). Then we have $\delta_v\colon J(\mathbb{Q}_v) \to H_v$ for each v. There is a commutative diagram

$$\begin{tikzcd}
J(\mathbb{Q}) \arrow[r, "\delta"] \arrow[d] & H \arrow[d, "\prod_v \operatorname{res}_v"] \\
\prod_v J(\mathbb{Q}_v) \arrow[r, "\prod_v \delta_v"] & \prod_v H_v
\end{tikzcd}$$

and we define the *2-Selmer group* of J to be

$$\operatorname{Sel}_2(J) = \{\alpha \in H : \forall v\colon\ \operatorname{res}_v(\alpha) \in \operatorname{im}(\delta_v)\}.$$

The first assertion in the following theorem actually gives the proof of the 'Weak Mordell-Weil Theorem'.

Theorem 2.14. *The 2-Selmer group is a finite-dimensional $\mathbb{F}_2$-vector space; it is explicitly computable. It gives the upper bound*

$$r \le \dim_{\mathbb{F}_2} \operatorname{Sel}_2(J) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2].$$

Sketch of proof. One can again reduce to a finite group

$$H_S = \{\alpha L^\square : v_{\mathfrak{p}}(\alpha) \in 2\mathbb{Z} \text{ for all } \mathfrak{p} \notin S_L\},$$

where S is the set of primes dividing $2\operatorname{disc}(f)$ and S_L is the set of places of L lying above a prime in S. (The proof that H_S is finite is again based on finiteness of class groups and finite generation of unit groups of algebraic number fields. A basis of H_S can be computed.) This already shows finiteness. One can then show that

$$\operatorname{Sel}_2(J) = \{\alpha \in H_S : \operatorname{res}_v(\alpha) \in \operatorname{im}(\delta_v) \text{ for all } v \in S \cup \{\infty\}\}.$$

The further fact that

$$\dim_{\mathbb{F}_2} J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) = \dim_{\mathbb{F}_2} J(\mathbb{Q}_v)[2] + \begin{cases} 0 & \text{if } v \neq \infty, 2, \\ g & \text{if } v = 2, \\ -g & \text{if } v = \infty \end{cases}$$

allows us to determine $\operatorname{im}(\delta_v)$ by picking random points in $J(\mathbb{Q}_v)$ until their images generate a subspace of the correct dimension. □

If we can find as many independent points in $J(\mathbb{Q})$ has specified by the upper bound coming from the 2-Selmer group, then we have determined the rank r, and we know a set of generators of a subgroup of $J(\mathbb{Q})$ of finite index. This is what we need as input to Chabauty's method and the Mordell-Weil sieve in the next lecture.

2.5. **Exercises.**

(1) Construct an example for the first statement in Remark 2.4.

(2) Let $C\colon y^2 = f(x)$ be hyperelliptic over K with $\deg(f) = 2g+1$ odd. Show that there is a bijection between $J(K)$ and the set

$$\{(a,b) : a, b \in K[x], a \text{ monic}, \deg(a) \le g, \deg(b) < \deg(a), a \mid f - b^2\},$$

which associates to (a,b) the class of the divisor

$$D = \sum_{j=1}^{n} (\alpha_n, b(\alpha_n)) - n \cdot \infty$$

when $a = (x-\alpha_1)\cdots(x-\alpha_n)$.

Hint. The Riemann-Roch Theorem might be helpful here. What are the functions whose only possible pole is at ∞?

Note that this gives a way of representing rational divisor classes in terms of rational data.

(3) Let $C\colon y^2 = f(x)$ be of genus 2 over K (all curves of genus 2 are hyperelliptic).

(a) Show that every point $0 \neq P \in J(K)$ can be uniquely written as $P = [D_P] - [D_\xi]$ with $D_P \in \operatorname{Div}_C(K)$ effective of degree 2 (D_ξ is as in Example 2.1).

Hint. You may want to use the Riemann-Roch Theorem. Note that $[D_\xi]$ is the class of canonical divisors.

(b) Now take $K = \mathbb{F}_p$ (with $p \ge 3$). Show that

$$\#J(\mathbb{F}_p) = \frac{\#C(\mathbb{F}_{p^2}) + \#C(\mathbb{F}_p)^2}{2} - p.$$

(c) Determine $J(\mathbb{Q})_{\text{tors}}$ for

$$C\colon y^2 = 4x^6 + 4x^5 - 7x^4 - 4x^3 + 8x^2 + 8x + 4.$$

Hint. Determine $\operatorname{div}(h_j)$ for the following functions:

$$h_1 = y - (2x^3 + x^2 - 2x), \quad h_2 = y + (2x^3 + x^2 + 2x + 2), \quad h_3 = y + (2x^3 + x^2 - 2x - 2)$$

and use them to determine the order of $[\infty_2 - \infty_{-2}]$.

(4) Try to compute the dimension of the 2-Selmer group (and, if possible, the rank) of the Jacobian of some hyperelliptic curve, for example of the form

$$y^2 = x(x-a_1)(x-a_2)(x-a_3)(x-a_4)$$

with distinct (small) integers $a_1, a_2, a_3, a_4 \neq 0$, for example $1, 2, 5, 6$.

3. Methods for determining the set of rational points on a curve

Let C be a nice curve over $\mathbb{Q}$ of genus $g \ge 2$. We now assume that we have found a rational point $P_0 \in C(\mathbb{Q})$ and that we want to determine the finite set $C(\mathbb{Q})$. We remark that one expects the rational points on C to be reasonably 'small' (in terms of a suitable height, say) relative to the coefficients of the defining equation(s), so that usually it is easy to actually find all the rational points. The hard part is then to prove that the list is indeed complete.

The methods we describe in this lecture are based on the embedding

$$i = i_{P_0} \colon C \longrightarrow J, \quad P \longmapsto [P - P_0]$$

that identifies $C(\mathbb{Q})$ with the subset of the Mordell-Weil group $J(\mathbb{Q})$ consisting of points in the image $i(C)$ of the curve in J. We will assume that we know explicit generators of a subgroup of $J(\mathbb{Q})$ of finite index.

3.1. **Differentials and integration.**

The first method I would like to explain goes back to Chabauty [Cha41], who proved Mordell's Conjecture in the case $r < g$, but the version described here is due to Coleman [Col85b]. It is based on p-adic integration of regular differentials on the curve, so we first have to introduce these concepts.

Let C be a nice curve over a field K. The space of *differentials* of C over K is a one-dimensional vector space $\Omega_C(K)$ over the function field $K(C)$. There is a nontrivial K-linear derivation $d \colon K(C) \to \Omega_C(K)$, i.e., a K-linear map satisfying $d(fg) = (df)g + f(dg)$. If $\eta, \omega \in \Omega_C(K)$ with $\omega \neq 0$, then there is a unique $f \in K(C)$ such that $\eta = f\omega$. We also write $f = \eta/\omega$.

Let $0 \neq \omega \in \Omega_C(K)$. If $P \in C(\bar{K})$ is a point and $t \in \bar{K}(C)$ is a uniformiser at P, then $dt \neq 0$ and so $\omega/dt \in \bar{K}(C)^\times$. We define the order of vanishing of ω at P to be $v_P(\omega/dt)$; this does not depend on the choice of t. In this way, we can define the divisor of ω,

$$\operatorname{div}(\omega) = \sum_P v_P(\omega) \cdot P \in \operatorname{Div}_C(K).$$

Since the quotient of two differentials is a function, it follows that these divisors are all in the same divisor class (and every K-rational divisor in the class arises from some $\omega \in \Omega_C(K)$), which is called the *canonical class*; any divisor in the canonical class is a *canonical divisor*. One can show that the degree of any canonical divisor is $2g - 2$.

A differential ω is said to be *regular at* P if $v_P(\omega) \geq 0$ (this includes the case $\omega = 0$, where $v_P(\omega) = +\infty$). ω is *regular* if it is regular at every point. It is a fact that the set of regular differentials on C forms a finite-dimensional K-vector space $\Omega_C^{\mathrm{reg}}(K)$, of dimension g, the genus of C.

Example 3.1. Let $C \colon y^2 = f(x)$ be hyperelliptic over K of genus g. Then

$$\Omega_C^{\mathrm{reg}}(K) = \left\langle \frac{dx}{2y}, \frac{x\,dx}{2y}, \ldots, \frac{x^{g-1}\,dx}{2y} \right\rangle_K,$$

so that each $\omega \in \Omega_C^{\mathrm{reg}}(K)$ can be written uniquely as $\omega = h(x)\,dx/2y$ with a polynomial $h \in K[x]$ of degree at most $g - 1$.

If $K = \mathbb{C}$, then our regular differentials are regular 1-forms on the Riemann Surface $C(\mathbb{C})$, which we can integrate along paths. Such an integral depends only on the homotopy class of the path, but can take different values on non-homotopic paths with the same endpoints. In contrast to this, it is possible to define integrals of regular differentials over p-adic fields that depend only on the endpoints.

Theorem 3.2 (Coleman [Col85a])**.** *Let C be a nice curve over $\mathbb{Q}_p$ that has good reduction. Then there is an integral that assigns to each pair of points $P, Q \in C(\bar{\mathbb{Q}}_p)$ and each regular differential $\omega \in \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p)$ a value*

$$\int_P^Q \omega \in \bar{\mathbb{Q}}_p$$

and that has the following properties.

(1) *For fixed P and Q, $\int_P^Q \omega$ is $\bar{\mathbb{Q}}_p$-linear in ω.*

(2) *('Fundamental Theorem of Calculus')*
Let t be a uniformiser at P that reduces to a uniformiser $\bar{t}$ at the reduction $\bar{P}$ of P. Then we can write

$$\omega = w(t)\,dt$$

where w is a power series whose coefficients have bounded (p-adic) absolute value. Let $\ell(t)$ be the formal integral of $w(t)$ with vanishing constant term. If Q also reduces to $\bar{P}$, then $|t(Q)| < 1$, $\ell(t(Q))$ converges and we have

$$\int_P^Q \omega = \ell(t(Q)).$$

In particular, $\int_P^P \omega = 0$.

(3) *(Additivity)*
For any three points P, P', P'', we have $\displaystyle\int_P^{P'} \omega + \int_{P'}^{P''} \omega = \int_P^{P''} \omega$.
This implies that $\displaystyle\int_P^{Q} \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega$.
It then makes sense to define $\int^D \omega$ for a divisor $D = \sum_{j=1}^n (Q_j - P_j) \in \mathrm{Div}_C^0(\bar{\mathbb{Q}}_p)$ as

$$\int^D \omega = \sum_{j=1}^n \int_{P_j}^{Q_j} \omega.$$

(4) *If D is a principal divisor, then $\int^D \omega = 0$.*

(5) *The integral is compatible with the action of the absolute Galois group of $\mathbb{Q}_p$.*

We note that the good reduction assumption is unnecessary here, but it simplifies the statement of property (2). Note that (2) allows us to compute integrals numerically when the two endpoints are 'p-adically close'.

From properties (3), (4) and (5) we deduce that

$$\Omega_C^{\mathrm{reg}}(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p, \quad (\omega, P) \longmapsto \langle \omega, P \rangle := \int^D \omega,$$

where $D \in \mathrm{Div}_C^0$ satisfies $[D] = P$, is well-defined, $\mathbb{Q}_p$-linear in ω and additive in P. We call this the *Chabauty-Coleman pairing.*

3.2. **Chabauty's Method.**

We return to $K = \mathbb{Q}$. Assume that the rank r of $J(\mathbb{Q})$ is strictly less than the genus g of C. Pick a prime p of good reduction for C. Set

$$V = \{\omega \in \Omega_C^{\mathrm{reg}}(\mathbb{Q}_p) : \forall P \in J(\mathbb{Q})\colon \langle \omega, P \rangle = 0\};$$

this is the annihilator of the Mordell-Weil group under the Chabauty-Coleman pairing. It follows from the properties of the p-adic integral that $\dim V \geq g - r > 0$, so there are nontrivial regular differentials that kill the Mordell-Weil group. For any $\omega \in V$ and any $P \in C(\mathbb{Q})$ we must then have (recall that $P_0 \in C(\mathbb{Q})$ was our chosen basepoint)

$$\int_{P_0}^{P} \omega = \int^{P-P_0} \omega = \langle \omega, [P - P_0] \rangle = 0,$$

since $[P - P_0] = i(P) \in J(\mathbb{Q})$.

We can compute a basis of V to any desired p-adic accuracy by evaluating $\int^{P_j} \omega_i$ where $(\omega_1, \ldots, \omega_g)$ is a basis of $\Omega_C^{\mathrm{reg}}(\mathbb{Q}_p)$ and $(P_1, \ldots, P_r)$ generate a subgroup of $J(\mathbb{Q})$ of finite index; then we use linear algebra. We can for example pick the P_j such that they are represented by divisors of the form $\sum_m (Q'_m - Q_m)$ where Q'_m and Q_m reduce to the same point mod p; then the integrals can be evaluated using property (2). Alternatively, one can use an algorithm worked out by Balakrishnan, Bradshaw and Kedlaya [BBK10].

Consider a point $\bar{P} \in \bar{C}(\mathbb{F}_p)$ and assume we know a point $P \in C(\mathbb{Q})$ reducing to $\bar{P}$. Let t be a uniformiser at P as in property (2) above. Then for every $Q \in C(\mathbb{Q})$ reducing to $\bar{P}$, $t(Q) \in p\mathbb{Z}_p$ must be a root of $\ell(t)$ for every ℓ arising from a differential $\omega \in V$. We can scale ω in such a way that its reduction $\bar{\omega}$ mod p makes sense and is nonzero. Then we have the following.

Proposition 3.3. *Assume that $p \geq 3$. Then the number of roots $\tau \in \bar{\mathbb{Q}}_p$ of ℓ such that $|\tau|_p \leq |p|_p$ is at most*

$$1 + n + \left\lfloor \frac{n}{p-2} \right\rfloor, \qquad \textit{where} \qquad n = v_{\bar{P}}(\bar{\omega}).$$

In particular, this bound applies to the number of $Q \in C(\mathbb{Q})$ with $\bar{Q} = \bar{P}$.

There is also a version for $p = 2$. The proof uses Newton Polygons and is left as an exercise.

As a consequence, we have Chabauty's partial result regarding Faltings's Theorem in Coleman's version.

Corollary 3.4. *Let C be a nice curve over $\mathbb{Q}$, of genus g and with Jacobian J. Assume that the rank r of $J(\mathbb{Q})$ is strictly less than g. Then $C(\mathbb{Q})$ is finite.*

More precisely, let p be an odd prime of good reduction for C. Then

$$\#C(\mathbb{Q}) \leq \#\bar{C}(\mathbb{F}_p) + 2g - 2 + \left\lfloor \frac{2g-2}{p-2} \right\rfloor.$$

Proof. Under the hypothesis $r < g$ there is $0 \neq \omega \in V$. We can scale ω so that $\bar{\omega}$ makes sense and is nonzero. Then we have

$$\begin{aligned} \#C(\mathbb{Q}) &= \sum_{\bar{P} \in \bar{C}(\mathbb{F}_p)} \#\{Q \in C(\mathbb{Q}) : \bar{Q} = \bar{P}\} \\ &\leq \sum_{\bar{P} \in \bar{C}(\mathbb{F}_p)} \left(1 + v_{\bar{P}}(\bar{\omega}) + \left\lfloor \frac{v_{\bar{P}}(\bar{\omega})}{p-2} \right\rfloor\right) \\ &\leq \#\bar{C}(\mathbb{F}_p) + 2g - 2 + \left\lfloor \frac{2g-2}{p-2} \right\rfloor. \end{aligned}$$

The first inequality uses Proposition 3.3 and the second inequality follows from

$$\sum_{\bar{P} \in \bar{C}(\mathbb{F}_p)} v_{\bar{P}}(\bar{\omega}) \leq \deg \operatorname{div}(\bar{\omega}) = 2g - 2. \qquad \square$$

This version is essentially due to Coleman (who formulated it explicitly under the additional assumption $p > 2g$, when the last term vanishes).

By picking the 'best' $\omega \in V$ independently for each point $\bar{P}$, the bound can be improved to

$$\#C(\mathbb{Q}) \le \#\bar{C}(\mathbb{F}_p) + 2r + \Big\lfloor \frac{2r}{p-2} \Big\rfloor .$$

See [Sto06]. There is also a version that does not assume that p is a prime of good reduction. Then $\#\bar{C}(\mathbb{F}_p)$ has to be replaced by the number of smooth $\mathbb{F}_p$-points on the special fibre of some regular proper model of C over $\mathbb{Z}_p$ [KZB13].

In concrete cases these bounds (though fairly reasonable) are rarely sharp. It may then be helpful to look at each 'residue class' (set of points reducing to a fixed point mod p) separately and to carry out the computations. If $g - r \ge 2$, it usually helps to look for common roots of the various power series coming from differentials forming a basis of V. The method of the next section can be used to rule out residue classes that appear not to contain rational points.

Example 3.5. Here is an example where the bound above is actually sharp [Gra94]. Consider the curve of genus 2

$$C\colon y^2 = x(x-1)(x-2)(x-5)(x-6).$$

By computing the 2-Selmer group, one finds that $r \le 1$, and since there is the non-torsion point $[(3,6) - \infty] \in J(\mathbb{Q})$, it follows that $r = 1$. One finds the ten points

$$\infty,\ (0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,\pm 6),\ (10,\pm 120)$$

in $C(\mathbb{Q})$. The prime 7 is a prime of good reduction, and $\#\bar{C}(\mathbb{F}_7) = 8$. So

$$10 \le \#C(\mathbb{Q}) \le 8 + 2 + \lfloor 2/5 \rfloor = 10,$$

which tells us that we have found all the rational points on C.

As a final remark, we mention that one can show [PS14] that a 2-adic version of the argument applies to show that 'most' hyperelliptic curves of odd degree have only the obvious rational point ∞, when the genus gets large.

3.3. The Mordell-Weil Sieve.

The last method we describe here can be used to show that $C(\mathbb{Q})$ is empty (when the approaches from the first lecture are unsuccessful), but also to show (for example) that certain residue classes mod p do not contain rational points. We assume that we know explicit generators of $J(\mathbb{Q})$; with some care, it is however possible to get by knowing only generators of a subgroup of finite index.

The basic idea is to combine our knowledge of the 'global' object $J(\mathbb{Q})$ with 'local' (mod q) information. So let q be a prime of good reduction (again, for simplicity; this assumption is not strictly necessary). We fix an embedding $i\colon C \to J$ given by some rational divisor (class) of degree 1. (If we already know a rational point on C, we will use it as our basepoint for the embedding. If we want to prove that no rational point exists, we have to use some other divisor of degree 1.) We will write $C(\mathbb{F}_q)$ etc. instead of $\bar{C}(\mathbb{F}_q)$ etc. for the set of $\mathbb{F}_q$-points on the reduction. Then we have a commutative diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\rho_q"] \\
C(\mathbb{F}_q) \arrow[r, hook, "i"] & J(\mathbb{F}_q)
\end{tikzcd}$$

which tells us that $i(C(\mathbb{Q})) \subset \rho_q^{-1}\bigl(i(C(\mathbb{F}_q))\bigr)$. Now the number of $\mathbb{F}_q$-points on C is roughly q (more precisely, it is $q+1 \pm 2g\sqrt{q}$ by the Hasse-Weil theorem) and the number of $\mathbb{F}_q$-points on J is about q^g (more precisely, between $(\sqrt{q}-1)^{2g}$ and $(\sqrt{q}+1)^{2g}$). So we can expect $\rho_q^{-1}\bigl(i(C(\mathbb{F}_q))\bigr)$ to be a union of about q cosets of the kernel of ρ_q, which usually will have index about q^g. So this mod q information restricts $i(C(\mathbb{Q}))$ to a set of density roughly q^{1-g} inside $J(\mathbb{Q})$.

We can improve on this by using several primes q together, via

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\prod \rho_q"] \\
\prod_{q\in S} C(\mathbb{F}_q) \arrow[r, hook] & \prod_{q\in S} J(\mathbb{F}_q)
\end{tikzcd}$$

where S is a finite set of (good) primes. This gives

$$i(C(\mathbb{Q})) \subset \bigcap_{q\in S} \rho_q^{-1}\bigl(i(C(\mathbb{F}_q))\bigr),$$

which should be of density roughly $(\prod_{q\in S} q)^{1-g}$. If we pick the primes in S in such a way that the group orders $\#J(\mathbb{F}_q)$ share many common factors, then there is a good chance that there is some interaction between the information coming from the various q, with the result that the intersection above can be written as a union of a fairly small number of cosets of $\bigcap_{q\in S} \ker(\rho_q)$.

If we use an embedding i that does not come from a rational point and $C(\mathbb{Q}) = \emptyset$, then it may well be the case that the intersection $\bigcap_{q\in S} \rho_q^{-1}\bigl(i(C(\mathbb{F}_q))\bigr)$ will be empty for some choice of S. This then gives a proof that $C(\mathbb{Q}) = \emptyset$. This approach was successful for the remaining curves in [BS08] (in some cases one needs to assume the BSD conjecture to deduce that there is in fact no rational divisor of degree 1, which obviously also gives a proof that there is no rational point).

In the other situation, we can for example restrict the set of rational points on C we consider to be the points in some residue class mod p. If there are no such points, then we may again be able to prove this fact by observing that the relevant intersection is empty. In this way it is possible to reduce to the set of residue classes that do actually contain rational points. If we pick the prime p in such a way that there is some $\omega \in V$ such that its reduction $\bar{\omega}$ does not vanish at any $\mathbb{F}_p$-point of C, then the results of the previous section imply that (as long as $p \geq 3$) each residue class contains at most one rational point. So if we can prove that certain residue classes do not contain rational points and if we find rational points in the remaining residue classes, then we have determined $C(\mathbb{Q})$. This leads to a quite efficient procedure that finds $C(\mathbb{Q})$ when C has genus 2 and $r = 1$, see [BS10].

It is also possible to use the Mordell-Weil Sieve (in combination with 'Linear Forms in Logarithms') to determine the set of *integral* points on a hyperelliptic curve [BMS+08] even when $r \geq g$. In this case, one does actually need to know explicit generators of the full Mordell-Weil group, however, which so far can be provably obtained only for $g = 2$ and $g = 3$.

3.4. Exercises.

(1) Work out the proof of Proposition 3.3 (You may first assume that $p > n + 2$).

(2) Find $C(\mathbb{Q})$ for

$$C\colon y^2 = x^6 + 2x^5 - 3x^4 - 6x^3 + 6x^2 + 8x - 7,$$

given that $J(\mathbb{Q})$ has rank 1.

Hint. You have to look at the power series expansion of ω around $(1, 1)$ (say) over $\mathbb{Q}_3$ to reduce the bound from 3 to 2 on its residue class mod 3.

(3) Let

$$C\colon y^2 = f(x) = -2x^6 + 2x^5 + 2x^4 + 3x^3 - 2x^2 - 2x - 3.$$

Then $J(\mathbb{Q})_{\text{tors}}$ is trivial (prove this!) and the free part of $J(\mathbb{Q})$ is generated by

$$[(\sqrt{-2}, 5) + (-\sqrt{-2}, 5) - D_0]$$

and

$$\Big[\big(\tfrac{1}{9}(5\sqrt{-2} - 2), \tfrac{1}{729}(418\sqrt{-2} - 205)\big) + \big(\tfrac{1}{9}(-5\sqrt{-2} - 2), \tfrac{1}{729}(-418\sqrt{-2} - 205)\big) - D_0\Big].$$

(a) Verify that C is ELS.

(b) (Optional) Verify that the fake 2-Selmer set of C is nonempty.

The polynomial $f(x)$ is irreducible, so you should enlist the help of a Computer Algebra System like Magma, pari/gp or Sage.

(c) Show that $f(x) - x^2$ factors into two polynomials of degree 3; use this to write down a rational divisor D_0 of degree 1 on C defining an embedding $i\colon C \to J$.

(d) Verify that the images in $J(\mathbb{F}_3)$ of $J(\mathbb{Q})$ under the reduction map and of $C(\mathbb{F}_3)$ under i do not intersect. Conclude that $C(\mathbb{Q}) = \emptyset$.

Hint. $J(\mathbb{F}_3) \cong \mathbb{Z}/28\mathbb{Z}$ and the image of $J(\mathbb{Q})$ has index 4.

A Computer Algebra System is helpful for doing the computations.

References

[BBK10] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 16–31, DOI 10.1007/978-3-642-14518-6_6. MR2721410 (2012b:14048) ↑3.2

[Bha13] Manjul Bhargava, *Most hyperelliptic curves over $\mathbb{Q}$ have no rational points*, 2013. Preprint, arXiv:1308.0395. ↑1.1, 2

[BS08] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR2433884 (2009d:11100) ↑1.9, 3.3

[BS09] ———, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8. MR2521292 (2010e:11059) ↑1.7, 1

[BS10] ———, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, DOI 10.1112/S1461157009000187. MR2685127 (2011j:11118) ↑1.9, 3.3

[BMS+08] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **2** (2008), no. 8, 859–885, DOI 10.2140/ant.2008.2.859. MR2457355 (2010b:11066) ↑3.3

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). MR0004484 (3,14d) ↑3.1

[Col85a] Robert F. Coleman, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168, DOI 10.2307/1971194. MR782557 (86j:14014) ↑3.2

[Col85b] ———, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR808103 (87f:11043) ↑3.1

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432 (German). MR718935 (85g:11026a) ↑1.1

[Gra94] David Grant, *A curve for which Coleman's effective Chabauty bound is sharp*, Proc. Amer. Math. Soc. **122** (1994), no. 1, 317–319, DOI 10.2307/2160877. MR1242084 (94k:14019) ↑3.5

[KZB13] 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** (2013), no. 11, 1818–1838, DOI 10.1112/S0010437X13007410. MR3133294 ↑3.2

[Mor22] Louis J. Mordell, *On the rational solutions of the indeterminate equation of the third and fourth degrees*, Proc. Cambridge Philos. Soc. **21** (1922), 179–192. ↑2.8

[PS99] Bjorn Poonen and Michael Stoll, *A local-global principle for densities*, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 241–244. MR1691323 (2000e:11082) ↑1.2

[PS14] ———, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7. MR3245014 ↑3.2

[Sto06] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214, DOI 10.1112/S0010437X06002168. MR2264661 (2007m:14025) ↑3.2

[Sto07] ———, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391, DOI 10.2140/ant.2007.1.349. MR2368954 (2008i:11086) ↑1.3, 1

[Sto11] ———, *Rational points on curves*, J. Théor. Nombres Bordeaux **23** (2011), no. 1, 257–277 (English, with English and French summaries). MR2780629 (2012d:14037) ↑(document)

[Wei29] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), 281–315. ↑2.8

Universität Bayreuth, 95440 Bayreuth, Germany