Rational points on hyperelliptic curves: Recent developments

M. Stoll
(Universität Bayreuth)

Michael.Stoll@uni-bayreuth.de

Abstract

We give an overview over recent results concerning rational points on hyperelliptic curves. One result says that 'most' hyperelliptic curves of high genus have very few rational points. Another result gives a bound on the number of rational points in terms of the genus and the Mordell-Weil rank, provided the latter is sufficiently small. The first result relies on work by Bhargava and Gross on Selmer groups of hyperelliptic Jacobians, and both results use Chabauty's method.

Introduction

A *hyperelliptic curve C of genus $g \geq 2$* over $\mathbb{Q}$ is given by an equation of the form

$$C\colon y^2 = f(x) = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1} + \ldots + f_1 x + f_0\,,$$

where $f(x) \in \mathbb{Z}[x]$ is of degree at least $2g+1$ and squarefree. This equation defines a smooth irreducible algebraic curve in the affine plane. We usually consider its smooth projective model, which is obtained by adding one or two points at infinity, corresponding to the square roots of f_{2g+2} (so there is one such point when $f_{2g+2} = 0$ and two points otherwise). The *rational points* on C are the affine points $(\xi, \eta) \in \mathbb{Q} \times \mathbb{Q}$ satisfying the curve equation, together with the points at infinity if f_{2g+2} is a square in $\mathbb{Q}$. The set of rational points on C is denoted $C(\mathbb{Q})$.

In particular, for *odd degree hyperelliptic curves*, meaning that $\deg(f) = 2g+1$, we always have a unique rational point at infinity, which we denote ∞.

Faltings' [5] famous proof of the Mordell Conjecture [7] implies that $C(\mathbb{Q})$ is always finite (recall that we assume $g \geq 2$ throughout). This raises the following question:

What can we say about $\#C(\mathbb{Q})$?

Chabauty's method

For a given individual curve C, *Chabauty's method* [3, 4] can be used to produce a bound on $\#C(\mathbb{Q})$, under a technical condition. To explain this, we have to introduce the *Jacobian variety* J of C. This is an abelian variety (a projective algebraic variety that carries a group structure compatible with the geometric structure; the group is then necessarily abelian) of dimension g defined over $\mathbb{Q}$, and if $P_0 \in C(\mathbb{Q})$ is a rational point, then there is an embedding $\iota\colon C \to J$ defined over $\mathbb{Q}$ that sends P_0 to the origin of the group law on J. Weil [13] proved (generalizing a result of Mordell's on elliptic curves that appeared in the paper [7] mentioned above containing the conjecture) that the group $J(\mathbb{Q})$ of rational points on J is a finitely generated abelian group. In particular, it has a well-defined rank $r = \dim_{\mathbb{Q}} J(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$, which is called the *Mordell-Weil rank* of J or of C. The technical condition mentioned above is that $r < g$.

We fix a 'base-point' $P_0 \in C(\mathbb{Q})$ (if there is no such point, we have $\#C(\mathbb{Q}) = 0$). Chabauty's method works p-adically, so we now fix a prime p. We write $\Omega_J(\mathbb{Q}_p)$ for the space of regular (or invariant, this is here the same) 1-forms on J defined over $\mathbb{Q}_p$ and $\Omega_C(\mathbb{Q}_p)$ for the space of regular 1-forms on C defined over $\mathbb{Q}_p$. Then $\iota^*\colon \Omega_J(\mathbb{Q}_p) \to \Omega_C(\mathbb{Q}_p)$ is an isomorphism, which in fact is independent of the choice of the base-point, and both sides are vector spaces over $\mathbb{Q}_p$ of dimension g. The group $J(\mathbb{Q}_p)$ of p-adic points on J carries a natural p-adic topology and forms a p-adic Lie group. There is a unique logarithm

$$\log\colon J(\mathbb{Q}_p) \to T_O J(\mathbb{Q}_p) \cong \mathbb{Q}_p^g$$

(where $T_O J(\mathbb{Q}_p)$ denotes the tangent space of $J(\mathbb{Q}_p)$ at the origin), which is a local diffeomorphism and a group homomorphism with finite kernel $J(\mathbb{Q}_p)_{\mathrm{tors}}$. The space $\Omega_J(\mathbb{Q}_p)$ of differentials can be canonically identified with the cotangent space $(T_O J(\mathbb{Q}_p))^*$. Putting

these ingredients together, we obtain a pairing

$$J(\mathbb{Q}_p) \times \Omega_J(\mathbb{Q}_p) \to \mathbb{Q}_p\,, \quad (P,\omega) \mapsto \langle \omega, \log P\rangle\,,$$

which is additive in the first component and $\mathbb{Q}_p$-linear in the second. If $r < g$, then there will be a linear subspace V of $\Omega_J(\mathbb{Q}_p)$ of dimension at least $g - r > 0$ such that $\langle \omega, \log P\rangle = 0$ for all $\omega \in V$ and all $P \in J(\mathbb{Q})$.

Now we observe that the embedding ι maps $C(\mathbb{Q})$ into $J(\mathbb{Q})$, so we have for all $P \in C(\mathbb{Q})$ and all $\omega \in V$ that $\langle \omega, \log \iota(P)\rangle = 0$. Fixing some $0 \neq \omega \in V$, we define a function

$$\lambda_\omega : C(\mathbb{Q}_p) \to \mathbb{Q}_p\,, \quad P \mapsto \langle \omega, \log \iota(P)\rangle\,.$$

Then $C(\mathbb{Q})$ is contained in the zero set of λ_ω. Now locally $C(\mathbb{Q}_p)$ looks like a subset of $\mathbb{Q}_p$, and $C(\mathbb{Q}_p)$ is compact (recall that we work with the smooth projective model of the curve), so we can write $C(\mathbb{Q}_p)$ as a (disjoint) union of finitely many *residue disks*, subsets that are p-adically analytically isomorphic to the p-adic unit disk. Pulling back λ_ω to the parametrizing disk, we obtain a power series converging on the disk, and using the Newton polygon obtained from the valuations of the coefficients, we can deduce bounds for the number of zeros of λ_ω on the residue disk under consideration. If one takes care to pick the 'best' ω on each residue disk, this leads to the following general bound [11].

Theorem 1 If C is a hyperelliptic curve over $\mathbb{Q}$ of genus g and with Mordell-Weil rank $r < g$, then for each prime $p \geq 3$, we have

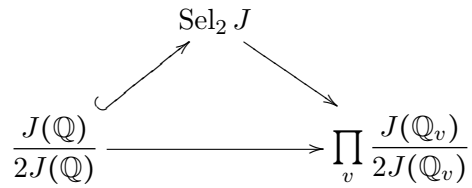
$$\#C(\mathbb{Q}) \leq d(p) + 2r + \left\lfloor \frac{2r}{p-2} \right\rfloor\,,$$

where $d(p)$ denotes the number of p-adic residue disks in $C(\mathbb{Q}_p)$. We also have the bound

$$\#C(\mathbb{Q}) \leq 2d(2) + 3r\,.$$

The 2-Selmer group

Now the question is, how to determine or at least bound the Mordell-Weil rank r. The most useful tool for this in practice as well as in theory is the *2-Selmer group* $\mathrm{Sel}_2 J$. It is defined in terms of Galois cohomology, but for us the only important properties are that it is computable (see [10] for how to compute it) and that it fits into a commutative diagram



(where v runs through all places of $\mathbb{Q}$, so that $\mathbb{Q}_v$ runs through all p-adic fields $\mathbb{Q}_p$ and $\mathbb{R}$). Since

$$\dim_{\mathbb{F}_2} \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} = \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] + r\,,$$

where $J(\mathbb{Q})[2]$ denotes the 2-torsion subgroup of $J(\mathbb{Q})$, we have

$$r \leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2 J - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]\,.$$

The dimension of $J(\mathbb{Q})[2]$ can easily be determined from the factorization of the polynomial $f(x)$ over $\mathbb{Q}$.

We will now focus on odd degree hyperelliptic curves. Because the degree of $f(x)$ is coprime to the degree of y^2 in this case, we can always scale x and y so that $f(x)$ becomes monic. For a ring R of characteristic zero, we write $\mathcal{F}_g(R)$ for the set of all monic polynomials $f \in R[x]$ of degree $2g+1$ with non-vanishing discriminant, and we just write $\mathcal{F}_g$ for $\mathcal{F}_g(\mathbb{Z})$. For $f = x^{2g+1} + f_{2g}x^{2g} + \ldots + f_1 x + f_0 \in \mathcal{F}_g$, we define the *height* of f to be

$$H(f) = \max\{|f_j|^{1/(2g+1-j)} : 0 \leq j \leq 2g\}\,.$$

(This definition has the advantage that scaling x and y while keeping the polynomial monic has the effect of scaling the height.) We can then order the polynomials f or equivalently, the curves $y^2 = f(x)$, by increasing height, which allows us to talk about the (lower) density of a set of odd degree hyperelliptic curves. First, for $X \in \mathbb{R}$ we set

$$\mathcal{F}_{g,X} = \{f \in \mathcal{F}_g : H(f) \leq X\}\,.$$

Now let $S \subset \mathcal{F}_g$. Then the *lower density* of S is

$$\underline{\delta}(S) = \liminf_{X\to\infty} \frac{\#(\mathcal{F}_{g,X} \cap S)}{\#\mathcal{F}_{g,X}}\,.$$

In a similar way, we define the *upper density* $\overline{\delta}(S)$. If both coincide, their common value is the *density* $\delta(S)$. If $\phi : \mathcal{F}_g \to \mathbb{R}$ is a function, we can define the *average* of ϕ as

$$A(\phi) = \lim_{X\to\infty} \frac{\sum_{f\in\mathcal{F}_{g,X}} \phi(f)}{\#\mathcal{F}_{g,X}}\,,$$

provided the limit exists. Now Bhargava and Gross [1], extending previous results by Bhargava and collaborators on Selmer groups of elliptic curves, have shown the following.

Theorem 2 The average size of $\mathrm{Sel}_2 J$, as J runs through the Jacobian varieties of odd degree hyperelliptic curves of genus g, is 3.

This implies that the average of 2^r is at most 3, and so r is mostly small.

Actually, Bhargava and Gross prove a bit more. Recall that there is a natural homomorphism $\mathrm{Sel}_2 J \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. The latter group is locally constant on $\mathcal{F}_g(\mathbb{Z}_p)$: over sufficiently small subsets, it can be identified with a fixed group G. Then there is the following *equidistribution property*.

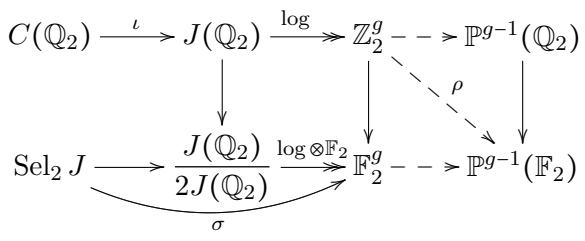
Theorem 3 Let $U \subset \mathcal{F}_g(\mathbb{Z}_p)$ be a subset such that for all $f \in U$, $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \cong G$ as above. Then the average number of nonzero preimages in $\mathrm{Sel}_2 J$ under the map $\mathrm{Sel}_2 J \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \to G$, when f ranges through $U \cap \mathcal{F}_g$, is the same for each $\gamma \in G$.

Most curves have few rational points

We continue to consider odd degree hyperelliptic curves. Each such curve has at least one rational point, namely the point at infinity. Heuristic considerations lead to the expectation that most curves actually have *only* this one rational point, in the sense that the subset of $f \in \mathcal{F}_g$ such that $C(\mathbb{Q}) = \{\infty\}$ has density 1.

Now if we want to show that even a subset of positive (lower) density of odd degree hyperelliptic curves of some fixed genus g has this property, then the general Chabauty bound of Theorem 1 is not sufficient: we would need $d(p) = 1$ (which is true for a subset of positive density) and $r = 0$, but the results of Bhargava and Gross are not strong enough to imply this for a positive proportion of the curves. The reason why the bound of Theorem 1 is too weak is that it does not look at how $J(\mathbb{Q})$ lies inside $J(\mathbb{Q}_p)$; it just takes its 'size' (as measured by r) into account. If we know something about the position of $J(\mathbb{Q})$ inside $J(\mathbb{Q}_p)$, then this can be used to obtain more precise bounds. If we know the 2-Selmer group together with the map $\mathrm{Sel}_2 J \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$, this will at least provide us with an upper bound for the image of $J(\mathbb{Q})/2J(\mathbb{Q})$ inside $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. For odd p the latter group is mostly small and does not give enough information on the image of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. For $p = 2$, however, the situation is different, and we get some sort of 'first approximation' to $J(\mathbb{Q})$ inside $J(\mathbb{Q}_2)$, which can be used in the Chabauty setup. This idea goes back to McCallum [6], who used it to prove results on the second case of Fermat's last theorem.

In our case, we obtain the following criterion. We first pick an isomorphism of $T_O J(\mathbb{Q}_p)$ with $\mathbb{Q}_p^g$ so that the image of log is $\mathbb{Z}_p^g$. Then we have the following commutative diagram.



The maps represented by dashed arrows are only partially defined (on all non-zero elements). We denote the two partially defined maps $C(\mathbb{Q}_2) \dashrightarrow \mathbb{P}^{g-1}(\mathbb{F}_2)$ and $\mathrm{Sel}_2 J \dashrightarrow \mathbb{P}^{g-1}(\mathbb{F}_2)$ by $\rho \log$ and $\mathbb{P}\sigma$, respectively. If we speak of their images, we mean the images of the maps restricted to their maximal domain of definition.

Lemma 4 For a subset of density 1 of the curves in $\mathcal{F}_g$, if $\sigma\colon \mathrm{Sel}_2 J \to \mathbb{F}_2^g$ is injective and the images of $\rho \log$ and $\mathbb{P}\sigma$ are disjoint, then $C(\mathbb{Q}) = \{\infty\}$.

The condition that σ is injective guarantees that no information is lost when mapping to $\mathbb{F}_2^g$, whereas the disjointness condition can be used to show that on each residue disk, there is a suitable function λ_ω that vanishes only at the Weierstrass point (if present). The Weierstrass points are the points with $y = 0$, together with the point at infinity (in the odd degree case). For almost all curves in the sense of density 1, ∞ is the only Weierstrass point.

The equidistribution property of Theorem 3 tells us that the average number of nonzero preimages under σ of an element $v \in \mathbb{F}_2^g$ is $2^{-(g-1)}$. Applying this to $v = 0$ shows that σ is injective for a set of curves of density $1 - 2^{-(g-1)}$. Also, the image of $\mathbb{P}\sigma$ is usually small and varies rather randomly. It remains to show that the image of $\rho \log$ is sufficiently small on average, so that it is likely to miss the image of $\mathbb{P}\sigma$. To achieve this, we bound the size of the image of $\rho \log$ on each residue disk, and we prove a bound on the average number of residue disks. We obtain the following.

Lemma 5

1. The average number of 2-adic residue disks on curves in $\mathcal{F}_g$ is less than 3.
2. The average size of the image of $\rho \log$ is at most $6g + 9$.

Combining the two lemmas leads to the following result [8].

Theorem 6 Fix $g \geq 2$. Then the lower density of odd degree hyperelliptic curves C over $\mathbb{Q}$ of genus g such that $C(\mathbb{Q}) = \{\infty\}$ is at least $1 - (12g + 20)2^{-g}$.

So the proportion of such curves tends to 1 rather quickly as g tends to infinity. In that sense, 'most' odd degree hyperelliptic curves have the point at infinity as their only rational point.

By looking at certain special subfamilies of curves, we can also show that for all $g \geq 3$, the set of curves with $C(\mathbb{Q}) = \{\infty\}$ has strictly positive lower density.

Extending the results of Bhargava and Gross and our method sketched above, Shankar and Wang [9] have shown that for curves $y^2 = f(x)$ with $f(x)$ monic and of even degree, a proportion tending to 1 as $g \to \infty$ in a similar way as in Theorem 6 above have the two points at infinity as the only rational points. For general hyperelliptic curves of genus g (such that f has even degree and does not have to be monic), Bhargava, Gross and Wang [2] have shown that, as $g \to \infty$, only a proportion of $o(2^{-g})$ of all curves have rational points at all.

Bounds for the number of points in terms of the rank and the genus

Now we consider general hyperelliptic curves again. Heuristic considerations lead to the expectation that there should be a bound in terms of g and r for the number of points $P \in C(\mathbb{C})$ such that $\iota(P)$ is contained

in any fixed finitely generated subgroup $\Gamma \subset J(\mathbb{C})$ of rank r. This is an open conjecture. It would imply that $\#C(\mathbb{Q})$ is bounded in terms of g and the Mordell-Weil rank r (taking $\Gamma = J(\mathbb{Q})$). We will now sketch how this weaker statement can be obtained in the case that $r \le g-3$. For this, we will again use Chabauty's approach. Theorem 1 gives bounds for $\#C(\mathbb{Q})$ in terms of the rank r and the number $d(p)$ of p-adic residue disks, assuming that $r < g$. The problem with that in view of obtaining uniform bounds is that the number of residue disks is unbounded. In the previous section, this was not an issue, since we can show that the *average* number of residue disks is small, which is enough for density results. But now we want a bound for *all* curves (with fixed Mordell-Weil rank r).

The main idea for circumventing this problem is to consider a more general decomposition of $C(\mathbb{Q}_p)$. Instead of just writing it as a disjoint union of disks, we allow ourselves to use disks and p-adic 'annuli' (subsets that are analytically isomorphic to an open disk minus a closed subdisk). Then one can show that it is possible to cover $C(\mathbb{Q}_p)$ by a number of disks and a number of annuli that both can be bounded in terms of g only.

The other main ingredient is to obtain a bound for the number of rational points in a given annulus. It turns out that for any given annulus A, there is a subspace V_A of $\Omega_J(\mathbb{Q}_p)$ of codimension at most 2 such that we can prove a bound for the number of zeros of λ_ω on A as long as $\omega \in V_A$. So if $r \le g-3$ and V is the subspace of differentials killing the Mordell-Weil group, then $V \cap V_A$ will be nontrivial for every annulus A. Combining the bounds for disks and the new bounds for annuli, we then obtain the following result [12].

Theorem 7 Let C be a hyperelliptic curve over $\mathbb{Q}$ of genus g and with Mordell-Weil rank $r \le g-3$. Then

$$\#C(\mathbb{Q}) \le 8(r+4)(g-1) + \max\{1, 4r\} \cdot g\,.$$

More generally, there is a bound $R(d, g, r)$ depending on the degree $[K : \mathbb{Q}]$, the genus g and the Mordell-Weil rank r such that for every hyperelliptic curve C of genus g over a number field K such that $J(K)$ has rank r, we have $\#C(K) \le R(d, g, r)$.

References

[1] Manjul Bhargava and Benedict Gross: The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. Preprint, arXiv:1208.1007v2.

[2] Manjul Bhargava, Benedict Gross and Xiaoheng Wang: Pencils of quadrics and the arithmetic of hyperelliptic curves (with an appendix by Tim and Vladimir Dokchitser). Preprint, arXiv:1310.7692v1.

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

[4] Robert F. Coleman: Effective Chabauty. *Duke Math. J.* **52**:3, 765–770 (1985).

[5] G. Faltings: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73**:3, 349–366 (1983). Erratum in: *Invent. Math.* **75**, 381 (1984).

[6] William G. McCallum: On the method of Coleman and Chabauty. *Math. Ann.* **299**:3, 565–596 (1994).

[7] L.J. Mordell: On the rational solutions of the indeterminate equations of the third and fourth degrees. *Cambr. Phil. Soc. Proc.* **21**, 179–192 (1922).

[8] Bjorn Poonen and Michael Stoll: Most odd degree hyperelliptic curves have only one rational point. Preprint, arXiv:1302.0061.

[9] Arul Shankar and Xiaoheng Wang: Average size of the 2-Selmer group of Jacobians of monic even hyperelliptic curves. Preprint, arXiv:1307.3531v2.

[10] Michael Stoll: Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.* **98**:3, 245–277 (2001).

[11] Michael Stoll: Independence of rational points on twists of a given curve. *Compos. Math.* **142**:5, 1201–1214 (2006).

[12] Michael Stoll: Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank. Preprint, arXiv:1307.1773.

[13] André Weil: L'arithmétique sur les courbes algébriques. *Acta Math.* **52**:1, 281–315 (1929).