UNIFORM BOUNDS FOR THE NUMBER OF RATIONAL POINTS ON HYPERELLIPTIC CURVES OF SMALL MORDELL-WEIL RANK

MICHAEL STOLL

ABSTRACT. We show that there is a bound depending only on $g$ and $[K : \mathbb{Q}]$ for the number of $K$-rational points on a hyperelliptic curve $C$ of genus $g$ over a number field $K$ such that the Mordell-Weil rank of its Jacobian is at most $g - 3$.

The proof is based on Chabauty’s method; the new ingredient is an estimate for the number of zeros of a logarithm in a $p$-adic ‘annulus’ on the curve, which generalizes the standard bound on disks. The key observation is that for a $p$-adic field $k$, the set of $k$-points on $C$ can be covered by a collection of disks and annuli whose number is bounded in terms of $g$ (and $k$).

1. Introduction

Since Faltings’ proof [Fal83] of Mordell’s conjecture, we know that a curve of genus $g \geq 2$ can have only finitely many rational points. This raises the question whether there might be uniform bounds of some sort on the number of rational points. Caporaso, Harris, and Mazur have shown [CHM97] that the validity of the Bombieri-Lang conjecture on rational points on varieties of general type would imply the existence of a bound depending only on the genus $g$. On the other hand, considering an embedding of the curve into its Jacobian variety, which identifies the set of rational points on the curve with the intersection of the curve and the Mordell-Weil group, one can ask the following purely geometric question: Given a curve $C$ of genus $g \geq 2$ over an algebraically closed field $k$ of characteristic zero, embedded in its Jacobian $J$, and a finitely generated subgroup $\Gamma$ of $J(k)$ of rank $\dim_{\mathbb{Q}} \Gamma \otimes_{\mathbb{Z}} \mathbb{Q} \leq r$, is there a uniform bound in terms of $g$ and $r$ for the number of points in $C \cap \Gamma$? That this number is finite for each individual curve follows from further work by Faltings [Fal94]. Heuristic arguments suggest that such a uniform bound should exist.

However, to our knowledge, so far not even a uniform (and unconditional) bound for the number of rational torsion points on curves of some fixed genus $g \geq 2$ has been obtained! In this note, we finally obtain such a bound for hyperelliptic curves of genus at least 3 (but the method should generalize to arbitrary curves). More generally, we can show that on a hyperelliptic curve $C$ of genus $g$ over number field of degree $\leq d$, there can be at most $R(d, g)$ rational points mapping into a given subgroup of rank $\leq g - 3$ of the Mordell-Weil group, where $R(d, g)$ depends only on $d$ and $g$. This implies uniform bounds in terms of $g$ and $d$ only for the number of rational points on such curves as long as the Mordell-Weil rank is at

**Date:** July 6, 2013.

2010 Mathematics Subject Classification. Primary 14G05, 11G20 11G30; Secondary 14G20, 14G25, 14H25, 14K15, 14K20.
most $g - 3$ and also for the number of rational points in a torsion packet when $g \geq 3$, see Theorem 6.1 and Remark 6.2 below.

The proof is based on Chabauty’s method [Cha41, Col85, MP13, Sto06]. If $C$ is a curve over $\mathbb{Q}$, with Jacobian $J$ and minimal regular model $\mathcal{C}$ over $\mathbb{Z}_p$, where the prime $p$ is sufficiently large, and we assume that $r = \text{rank } J(\mathbb{Q}) < g$, then one can bound $\#C(\mathbb{Q})$ by the number of smooth $\mathbb{F}_p$-points on the special fiber of $\mathcal{C}$ plus $2r$, see [KZB13]. This bound is obtained as follows. Consider the Chabauty-Coleman pairing (defined below in Section 2)

$$\Omega^1_j(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p, \quad (\omega, P) \mapsto \int_{\mathcal{O}}^P \omega$$

This pairing is $\mathbb{Q}_p$-linear in $\omega$ and additive in $P$; its kernel on the left is trivial. If $r < g$, then there is a subspace $V \subset \Omega^1_j(\mathbb{Q}_p)$ of dimension at least $g - r \geq 1$ that annihilates the Mordell-Weil group $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$ under the pairing. Let $P_0 \in C(\mathbb{Q})$ and use $P_0$ as basepoint for an embedding $i: C \rightarrow J$. Then for all $P \in C(\mathbb{Q})$ and all $\omega \in V$, we have

$$0 = \int_{\mathcal{O}}^{i(P)} \omega = \int_{P_0}^P i^* \omega$$

where $i^* \omega \in \Omega^1_C(\mathbb{Q}_p)$ is a regular differential on $C$. The integral on the right is defined by this equality. One then shows (see for example [Sto06]) that the number of zeros of the function

$$P \mapsto \int_{P_0}^P i^* \omega$$

on a $p$-adic residue disk of $C$, which is the set of $p$-adic points reducing mod $p$ to a given smooth point on the special fiber of $\mathcal{C}$, is at most one plus the number of zeros (counted with multiplicity) of $\omega$ on that residue disk. (Here we use that $p$ is large enough, otherwise the bound has to be modified.) Choosing a ‘good’ $\omega \in V$ for each residue disk leads to the bound

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p)^{\text{smooth}} + 2r$$

mentioned earlier.

The problem with this approach is that the bound depends on the complexity of the special fiber of $\mathcal{C}$, which is unbounded — there can be arbitrarily long chains of rational curves in the special fiber, which can lead to an arbitrarily large number of smooth $\mathbb{F}_p$-points. The idea for overcoming this problem is to parametrize the subset of $C(\mathbb{Q}_p)$ corresponding to such a chain not by a union of (an unbounded number of) disks, but by an ‘annulus’. We can then obtain a bound for the number of points in that subset that is independent of the number of residue disks. Since both the number of such annuli and the number of remaining residue disks are bounded in terms of the genus (and $p$), we do obtain a uniform bound. The price we have to pay is that on (at least some of) the annuli, we need to impose additional linear conditions on the differential $\omega$, so that we need the space of differentials annihilating the relevant subgroup of $J(\mathbb{Q}_p)$ to be of dimension at least three. This translates into the rank bound $r \leq g - 3$. The key result for our application is Proposition 4.4, which gives a precise comparison of the abelian integral pulled back to an annulus and the $p$-adic integral of the pulled-back 1-form. It turns out that the difference between the two is a linear function of the valuation.
We carry out this approach in the case of hyperelliptic curves. We expect that the approach can be generalized to arbitrary curves; we will pursue this in future work.

Acknowledgments. The vague idea that one should be able to use Chabauty’s method to prove uniform upper bounds for the number of rational points had long been in the author’s mind, but was put aside as infeasible because of the apparent problems described above. The new activity leading to the results presented here was prompted by a question Manjul Bhargava asked related to [PS13]: could we give a family of odd degree hyperelliptic curves \( C \) of any genus, defined by congruences, such that our method would not work for any curve in the family? The intuition that this should not be possible for large genus led to the idea of using integration on annuli to prove that the image of \( C(\mathbb{Q}_2) \) in \( \mathbb{P}^{g-1}(\mathbb{F}_2) \) under the ‘\( \rho \log \)’ map of [PS13] is bounded by a polynomial in \( g \). This result will be presented in a separate paper or in a later version of this article. The idea then extended naturally to the original question. So I would like to thank Manjul for asking the right question. I also wish to thank Amnon Besser for help with questions about \( p \)-adic integration and Stefan Wewers for answering my questions on stable models.

2. Notation

Until further notice, we fix the following notation.

Let \( p \) be a prime number. As usual, \( \mathbb{Q}_p \) denotes the field of \( p \)-adic numbers and \( \mathbb{C}_p \) the completion of an algebraic closure of \( \mathbb{Q}_p \). We let \( v: \mathbb{C}_p \rightarrow \mathbb{Q} \cup \{ \infty \} \) denote the valuation on \( \mathbb{C}_p \) that is normalized by \( v(p) = 1 \). We also fix an absolute value \( |\cdot| \) on \( \mathbb{C}_p \). Throughout the paper, \( k \subset \mathbb{C}_p \) stands for a finite field extension of \( \mathbb{Q}_p \) with ramification index \( e \); we write \( \mathcal{O} \) for its ring of integers, \( \pi \) for a uniformizer, and \( \mathbb{F} = \mathcal{O}/\pi\mathcal{O} \) for the residue field. We set \( q := \# \mathbb{F} \); \( k_{\text{unr}} \subset \mathbb{C}_p \) is the maximal unramified extension of \( k \).

Let \( g \geq 3 \) be an integer and let \( C \) be a smooth, projective, and geometrically integral curve of genus \( g \) over \( k \). The Jacobian variety of \( C \) is denoted \( J \); the origin on \( J \) is \( O \). We denote the image of the divisor \( (P)-(Q) \) on \( C \) in \( J \) by \( [P-Q] \). We denote by \( \log_f \) the \( p \)-adic abelian logarithm \( J(k) \rightarrow T_OJ(k) \cong k^g \). On a sufficiently small subgroup neighborhood of \( O \), it is given by evaluating the formal logarithm, and then extended to all of \( J(k) \) by linearity. The space \( \Omega^1_J(k) \) of global regular 1-forms on \( J \) defined over \( k \) agrees with the space of invariant (under translations) 1-forms on \( J \) and can be identified with the cotangent space \( (T_OJ(k))^* \) of \( J \) at the origin. This induces a pairing

\[
\Omega^1_J(k) \times J(k) \rightarrow k, \quad (\omega, P) \mapsto \langle \omega, \log_f(P) \rangle =: \int_O^P \omega,
\]

which we call the Chabauty-Coleman pairing. It is \( k \)-linear in \( \omega \) and additive (and \( \mathcal{O} \)-linear on the kernel of reduction) in \( P \). Its kernel on the left is trivial, and its kernel on the right is the torsion subgroup of \( J(k) \).

Let \( P_0 \in C(k) \) and let \( i: C \rightarrow J \) be the embedding given by \( P \mapsto [P-P_0] \). Then \( i^*: \Omega^1_C \rightarrow \Omega^1_J \) is an isomorphism (which does not depend on \( P_0 \)). If \( \omega \in \Omega^1_C(k) \) is \( i^* \omega_J \) for some \( \omega_J \in \Omega^1_J(k) \),
then we set for points $P, Q \in C(k)$

$$
\oint_P^Q \omega := \oint_{i(P)}^{i(Q)} \omega_j = \oint_{O_j}^{[Q-P]} \omega_j.
$$

We use the symbol $\oint$ to distinguish this integral defined via abelian logarithms from the $p$-adic integral $\int$ given by $p$-adic integration theory.

Inclusions ‘$A \subset B$’ are meant to be non-strict.

3. Partition into disks and annuli

Until further notice we let $C$ be a semistable curve of genus $g \geq 2$ over $k$. Let $\mathcal{C}$ denote the minimal regular model of $C$ over $O$, and let $\mathcal{C}'$ denote the stable model, which is obtained from $\mathcal{C}$ by contracting chains of $(-2)$-curves. Let $R(C)$ be the dual graph of the special fiber $C'_s$ of $C'$, the edges correspond to the singular points and join the two vertices (which can be identical) given by the two branches at the singularity.

We define the weight of a vertex of $R(C)$ to be twice the geometric genus of the corresponding component plus the degree of the vertex minus 2. (The degree is the number of half-edges incident with the vertex.) Then the definition of what a stable model is implies that every vertex has positive weight.

Let $t$ be the number of independent loops of $R(C)$ (this is the dimension of the toric part of the connected component of the special fiber of the Néron model of the Jacobian of $C$); then $t$ plus the sum of the geometric genera of the components of $C'_s$ equals $g$, and the number of edges of $R(C)$ equals the number of vertices of $R(C)$ plus $t - 1$. For the sum of the weights we then get

$$2(g - t) + 2\#\{\text{edges}\} - 2\#\{\text{vertices}\} = 2(g - t) + 2(t - 1) = 2g - 2,$$

so $R(C)$ has at most $2g - 2$ vertices and at most $(2g - 2) + (t - 1) \leq 3g - 3$ edges. Write $N$ for the number of vertices and number the components of $C'_s$ as $\Gamma_1, \ldots, \Gamma_N$. Then the number of edges (or singular points on $C'_s$) is $N + t - 1$.

Each smooth $\mathbb{F}$-point $P$ on $C'_s$ gives rise to a residue disk in $C(k)$, which is the set of $k$-points reducing to $P$. The number of such residue disks is therefore

$$
\#C'_s(\mathbb{F})^{\text{smooth}} \leq \sum_{j=1}^N (q + 1 + 2p_0(\Gamma_j)\sqrt{q}) \leq (q + 1)N + 2\sqrt{q}g
$$

$$
\leq 2(q + 1)(g - 1) + 2\sqrt{q}g = 2(q + \sqrt{q} + 1)(g - 1) + 2\sqrt{q}.
$$

For each singular point $P \in C'_s(\mathbb{F})$, the preimage in the special fiber $C_s$ of $C$ is a chain of $(-2)$-curves of some length $m$ (so that $m$ is the number of components of $C_s$ in the chain). It is known that the subset of $C(k^{\text{unr}})$ of points reducing to a (smooth) point on this chain and therefore to $P$ on $C'_s$ is analytically isomorphic to the set of $k^{\text{unr}}$-points of an ‘annulus’

$$A_m = \{\xi : |\pi^{m+1}| < |\xi| < 1\}$$

such that points $\xi \in A_m$ with $|\xi| = |\pi^j|$ reduce to points on the $j$th component of the chain (fixing one orientation for the numbering). If the Galois group of $\mathbb{F}$ acts on the edge of $R(C)$
corresponding to \( P \) by reversing its orientation, then at most one of these components (the middle one if \( m \) is odd) is defined over \( \mathbb{F} \). Since \( C(k) \subset C(k^{\text{unr}}) \) and the bounds we obtain on annuli are actually valid for \( k^{\text{unr}} \)-points, we will not distinguish between this case and that of trivial Galois action.

See [BL85] or the discussion in [Bak08, Section 5.1].

Since every point in \( C(k) \) reduces to some point in \( C'(\mathbb{F}) \), the union of residue disks and annuli as constructed above covers \( C(k) \). The number of annuli is bounded (we only count singular points defined over \( \mathbb{F} \)) by the number \( N + t - 1 \leq 3g - 3 \) of edges of \( R(C) \).

Let \( C_D(k) \) be the set of points in \( C(k) \) whose image in \( C'(\mathbb{F}) \) is smooth (this is the union of the residue disks) and \( C_A(k) \) the set of points whose image in \( C'(\mathbb{F}) \) is singular (this is the union of the annuli).

4. The pull-back of an abelian logarithm to an annulus

Let \( \omega \) be a regular differential on \( C \) and denote by \( \omega_J \) the corresponding regular and invariant 1-form on \( J \). We fix a basepoint \( P_0 \in C(k) \) and write for \( P \in C(k) \)

\[
\lambda_{\omega}(P) = \int_{P_0}^{P} \omega = \int_{P_0}^{[P-P_0]} \omega_J = \langle \omega_J, \log[P - P_0] \rangle .
\]

Let \( D_0 = \{ \xi : |\xi| < 1 \} \) be the unit disk. If \( \varphi : D_0 \to C \) parametrizes a residue disk, then

\[
\varphi^* \omega = w(z) \, dz
\]

with a power series \( w(z) \) converging on \( D_0 \). Let \( \ell \) be a power series whose derivative is \( w \).

Then it is well-known that for \( \xi_0, \xi_1 \in D_0(k) \) we have

\[
\int_{\varphi(\xi_0)}^{\varphi(\xi_1)} \omega = \int_{\xi_0}^{\xi_1} w(z) \, dz = \ell(\xi_1) - \ell(\xi_0) .
\]

Using Newton polygons, one then shows (see for example [Sto06]) that the number of zeros of \( \lambda_{\omega} \) on \( \varphi(D_0(k)) \) is bounded by 1 plus the number \( n \) of zeros of \( \omega \) (counted with multiplicity) on \( \varphi(D_0) \) plus a term (denoted by \( \delta(v, n) \) in [Sto06]) that depends only on \( n, p \) and the ramification index \( e \) of \( k \), and which vanishes if \( p > n + e + 1 \). Since \( n \leq 2g - 2 \), this will be the case whenever \( p > 2g + e - 1 \). Let \( B_D(p, e, g) \) be a bound for the extra term valid for all \( n \leq 2g - 2 \). Then we have the following.

**Lemma 4.1.** Let \( \omega \neq 0 \) be a regular differential on \( C \). Then \( \lambda_{\omega} \) has at most

\[
N_D + 2g - 2 + N_D B_D(p, e, g)
\]

zeros in \( C_D(k) \). Here

\[
N_D = \# C'(\mathbb{F})^{\text{smooth}} \leq 2(q + \sqrt{q} + 1)(g - 1) + 2\sqrt{q}
\]

is the number of the residue disks whose union is \( C_D(k) \).

If \( p > 2g + e - 1 \), then we can take the bound to be \( 2(q + \sqrt{q} + 2)(g - 1) + 2\sqrt{q} \).
Now we consider the situation for an annulus \( A = \{ \xi : \rho_1 < v(\xi) < \rho_2 \} \) parametrizing the preimage under reduction of a singular point on \( C'_s \). Let \( \varphi : A \rightarrow C \) be the parametrization. Pulling back \( \omega \), we obtain, using \( z \) as coordinate on \( A \),

\[
\varphi^* \omega = w(z) \, dz = d\ell(z) + c(\omega) \frac{dz}{z}
\]

for Laurent series \( w \) and \( \ell \) converging on \( A \) and some constant \( c(\omega) \in k \). Let \( \text{Log}_0 \) denote the branch of the \( p \)-adic logarithm that takes the value 0 at \( p \). Then, given this choice, there is a unique global integral on \( A \) that in our case is given by

\[
\int_{\xi_0}^{\xi_1} \varphi^* \omega = \left( \ell(\xi_1) + c(\omega) \text{Log}_0(\xi_1) \right) - \left( \ell(\xi_0) + c(\omega) \text{Log}_0(\xi_0) \right).
\]

We want to compare this with

\[
\int_{\varphi(\xi_0)}^{\varphi(\xi_1)} \omega.
\]

Perhaps surprisingly, these two integrals can differ.

The following result is crucial. It was first suggested by numerical computations and appears to be new. When we asked Amnon Besser about this, we learned that a related result also is part of current work of his with Sarah Zerbes. To make this paper independent of (so far) unpublished work, a (different) proof is presented here.

**Proposition 4.2.** Let \( \omega, A \) and \( \varphi : A \rightarrow C \) be as above, and write

\[
\varphi^* \omega = d\ell(z) + c(\omega) \frac{dz}{z}.
\]

Then there is a constant \( a(\omega) \) depending linearly on \( \omega \) such that for \( \xi_0, \xi_1 \in A(k) \) we have

\[
\int_{\varphi(\xi_0)}^{\varphi(\xi_1)} \omega = \left( \ell(\xi_1) + c(\omega) \text{Log}_0(\xi_1) + a(\omega) v(\xi_1) \right) - \left( \ell(\xi_0) + c(\omega) \text{Log}_0(\xi_0) + a(\omega) v(\xi_0) \right)
\]

\[
= \int_{\xi_0}^{\xi_1} \varphi^* \omega + a(\omega) \left( v(\xi_1) - v(\xi_0) \right).
\]

**Proof.** We assume without loss of generality that \( 1 \in A \). Let \( i : C \rightarrow J \) be the embedding sending \( \varphi(1) \) to \( O \).

According to [BL84, Proposition 6.3], the analytic map \( i \circ \varphi : A \rightarrow J \) can be written uniquely as

\[
i(\varphi(\xi)) = \psi_1(j(\xi)) + \psi_2(\xi)
\]

where \( j : A \rightarrow \mathbb{G}_m \) is the natural inclusion, \( \psi_1 : \mathbb{G}_m \rightarrow J \) is a group homomorphism and \( \psi_2 : A \rightarrow U \) is an analytic map, where \( U \) denotes the formal fiber of the origin on \( J \) (so that \( U(k) \) is the subgroup of points reducing to the origin). We write \( \omega_J \) for the 1-form on \( J \) such that \( i^* \omega_J = \omega \); \( \omega_J \) is translation invariant. On \( U \), \( \omega_J \) is exact, so \( \omega_J = d\lambda \) for some analytic function \( \lambda \) on \( U \); we can assume \( \lambda(0) = 0 \). The pull-back \( \psi^*_1 \omega_J \) is a translation invariant differential on \( \mathbb{G}_m \), so it has the form \( c \, dz/z \) for some \( c \in k \). The pull-back \( \psi^*_2 \omega_J \) is \( \psi^*_2 d\lambda = d(\lambda \circ \psi_2) \). Since

\[
\varphi^* \omega = \varphi^* i^* \omega_J = \psi^*_1 \omega_J + \psi^*_2 \omega_J = c \frac{dz}{z} + d\lambda(\psi_2(z))
\]
we see that \( \ell(z) = \lambda(\psi_2(z)) \) (up to a constant) and \( c = c(\omega) \). Fix \( \xi \in A(k) \). We obtain on the one side that
\[
\oint_{\varphi(1)} \omega = \oint_{O} \omega = \oint_{O} \psi_1(\xi) + \psi_2(\xi) \omega = \oint_{O} \psi_1(\xi) \omega_J + \int_{O} \psi_2(\xi) d\lambda = \oint_{O} \omega + \lambda(\psi_2(\xi))
\]
and on the other side that
\[
\int_{1}^{\xi} \varphi^* \omega = \int_{1}^{\xi} (d\ell(z) + c \frac{dz}{z}) = \ell(\xi) - \ell(1) + c \log_0(\xi) = \lambda(\psi_2(\xi)) + c \log_0(\xi).
\]
So the difference is
\[
\delta(\xi) = \oint_{\varphi(1)} \omega - \int_{1}^{\xi} \varphi^* \omega = \oint_{O} \psi_1(\xi) \omega_J - c \log_0(\xi).
\]
Since \( \psi_1 \) is a group homomorphism, the first term is a homomorphism \( k^\times \to k \); the same is true for the second term. Both terms agree on the residue disk \( U_1 \) of 1, since they are given by the same formal integral on \( U_1 \). Since \( \mathcal{O}^\times / U_1 \) is torsion-free, we have \( \delta = 0 \) on \( \mathcal{O}^\times \). This implies that \( \delta(\xi) \) is a linear function of the valuation \( v(\xi) \), so there is \( a = a(\omega) \in k \) such that \( \delta(\xi) = av(\xi) \). This gives the claim for \( (\xi_0,\xi_1) = (1,\xi) \); by taking differences the more general statement follows.

That \( a(\omega) \) is linear in \( \omega \) is clear, since \( \ell \) (if we set \( \ell_0 = 0 \)), \( c(\omega) \) and the left-hand side are. \( \square \)

Remark 4.3. The numerical example mentioned above shows that it is possible to have \( a(\omega) \neq 0 \) and \( c(\omega) = 0 \), so that the appearance of \( a(\omega) \) cannot in all cases be avoided by choosing a suitable branch of the \( p \)-adic logarithm.

In this situation we have \( \psi_1^* \omega_J = 0 \) and the difference term above is given by \( \oint_{O} \psi_1(\xi) \omega_J \). Even though the pull-back of \( \omega_J \) along \( \psi_1 \) vanishes, it does not follow that the abelian integral vanishes on the image of \( \psi_1 \). Consider for example \( \xi = p \) and \( P = \psi_1(p) \in J(k) \). There is a positive integer \( n \) such that \( nP \in U \); then
\[
\oint_{O} \psi_1(p) \omega_J = \frac{1}{n} \oint_{O} nP \omega_J = \frac{1}{n} \lambda(nP).
\]
There is no reason to assume that \( \log_J(nP) \) is parallel to the derivative of \( \psi_1 \) at 1, so \( \psi_1^* \omega_J = 0 \) does not in general imply that \( \lambda(nP) \) vanishes.

We say that \( \omega \) is good for the subset of \( C(k) \) parametrized by \( A \) if both \( c(\omega) \) and \( a(\omega) \) in Proposition 4.2 vanish. This is a linear condition on \( \omega \) of codimension at most two.

Recall that we fix some \( P_0 \in C(k) \) and set
\[
\lambda_\omega : C(k) \to k, \quad \quad P \mapsto \oint_{P_0} \omega.
\]

**Proposition 4.4.** In the situation of Proposition 4.2 assume that \( \omega \) is good. Assume further that \( C \) is hyperelliptic and that \( p \) is odd. Then the number of zeros of \( \lambda_\omega \) on \( \varphi(A(k)) \) is bounded by a number \( B_\Lambda(p,e,g) \) that depends only on \( g, p \) and the ramification index \( e \) of \( k \). If \( p > 2g + e - 1 \), then we can take \( B_\Lambda(p,e,g) = 2g - 2 \).
If denote by $J$ number $\leq C$ Let $k$ only on and $q$ Theorem 5.1. In this section we state and prove our main result. We begin with a special case.

Proposition 4.4 the number of zeros of $\lambda$ pick a nontrivial $\omega$ which is $\leq 1$ $\omega$ A proof is given in Lemma 7.1 below.

Proof. For each annulus $A$ of all $C$ dimension at least 3, where $\omega$ is a nontrivial $\omega$ which is $\leq 1$ $\omega$ which by assumption has no $z^{-1}$ term. Then $w(z) = u(z)h(z)$ with a Laurent polynomial $u$ and a Laurent series $h$ such that $|h(\xi) - 1| < 1$ for all $\xi \in A$. We assume that the terms in $u$ have exponents between $n_1$ and $n_2$ such that $n_1 < -1 < n_2$ and $n_2 - n_1 \leq 2g - 2$. Given this, the proof can be done using Newton polygons in essentially the same way as for power series.

Now one can check by an explicit computation using the description of stable models of hyperelliptic curves over $p$-adic fields with odd residue characteristic that this condition is satisfied when $C$ is a hyperelliptic curve and $p$ is odd. If $\omega$ is allowed to vary in a linear space (of good differentials) of dimension $m$, then the bound for $n_2 - n_1$ can be reduced to $\max\{2(g - m), 2\}$. This can be used to obtain better bounds later; see Remark 5.4 below. A proof is given in Lemma 7.1 below.

Corollary 4.5. Let $V$ be a linear subspace of the space of regular differentials on $C$ of dimension at least 3, where $C$ is as in Proposition 4.4. Then the number of common zeros of all $\lambda_\omega$ for $\omega \in V$ in $C_A(k)$ is bounded by

$$(3g - 3)B_A(p, e, g),$$

which is $\leq 6(g - 1)^2$ if $p > 2g + e - 1$.

Proof. For each annulus $A$ parametrizing the preimage $X$ of one singular point on $C', \omega$ we pick a nontrivial $\omega \in V$ that is good for $X$. This is possible since $\dim V \geq 3$. Then by Proposition 4.4 the number of zeros of $\lambda_\omega$ on $X$ is bounded by $B_A(p, e, g)$. Multiply by the number $\leq N + t - 1 \leq 3g - 3$ of singular points in $C'_s(\mathbb{F})$ to obtain the result.

5. Bounding the number of points mapping into a subgroup of small rank

In this section we state and prove our main result. We begin with a special case.

Theorem 5.1. Let $k$ be a $p$-adic field with $p$ odd and write $e$ for the ramification index of $k$ and $q$ for the size of its residue field. Let $g \geq 3$. Then there is a bound $N(k, g)$ depending only on $k$ and $g$ such that the following holds.

Let $C: y^2 = f(x)$ be a hyperelliptic curve of genus $g$ over $k$ with semistable reduction. We denote by $J$ the Jacobian variety of $C$. Let $\Gamma \subset J(k)$ be a subgroup of rank $\leq g - 3$. Let $i: C \to J$ be an embedding given by choosing some basepoint $P_0 \in C(k)$. Then

$$\# \{P \in C(k) : i(P) \in \Gamma\} \leq N(k, g).$$

If $p > 2g + e - 1$, then we can take

$$N(k, g) = 6(g - 1)^2 + 2(q + \sqrt{q} + 2)(g - 1) + 2\sqrt{q} \leq g^2 + qg.$$ 

Proof. The rank condition implies that there is a $k$-vector space $V$ of regular differentials on $C$ such that $\dim V \geq 3$ and such that each $\omega \in V$ annihilates $\Gamma$ under the Chabauty-Coleman pairing. This means that (taking $P_0$ to be the basepoint for $\lambda_\omega$) the set of points in question is contained in the common zero set of all $\lambda_\omega$ for $\omega \in V$. 

8
Now take any $0 \neq \omega \in V$. Then by Lemma 4.1 the number of zeros of $\lambda_\omega$ in $C_D(k)$ is at most
\[ N_D + 2g - 2 + N_DB_D(p,e,g) \]
with
\[ N_D \leq 2(g + \sqrt{q} + 1)(g - 1) + 2\sqrt{q} , \]
so this contribution is bounded in terms of $p$, $e$, $q$ and $g$, which means that it depends only on the field $k$ and the genus $g$.

Similarly, by Corollary 4.5, the number of common zeros of the $\lambda_\omega$ for $\omega \in V$ in $C_A(k)$ is at most
\[ (3g - 3)B_A(p,e,g) , \]
which is bounded in terms of $p$, $e$ and $g$ only. Adding these bounds gives the result.

If $p > 2g + e - 1$, then $B_D(p,e,g) = 0$ and $B_A(p,e,g) = 2g - 2$, leading to a bound of
\[ N_D + 2g - 2 + (3g - 3)(2g - 2) \leq 6(g - 1)^2 + 2(q + \sqrt{q} + 2)(g - 1) + 2\sqrt{q} . \]

\[ \square \]

Remark 5.2. It is conceivable that a more careful analysis of the functions $\lambda_\omega$ on annuli will result in a bound for the number of zeros that applies to differentials $\omega$ that do not necessarily satisfy the conditions that $c(\omega)$ and/or $a(\omega)$ (in the notation of Proposition 4.2) vanish. If this is indeed the case, then the condition $r \leq g - 3$ can be relaxed to $r \leq g - 2$ or even $r \leq g - 1$. This will be the subject of future work.

Based on this special case we can deduce a more general result.

Theorem 5.3. Let $k$ be a $p$-adic field with $p$ odd and write $e$ for the ramification index of $k$ and $q$ for the size of its residue field. Let $g \geq 3$. Then there is a bound $\tilde{N}(k,g)$ depending only on $k$ and $g$ such that the following holds.

Let $C$: $y^2 = f(x)$ be a hyperelliptic curve of genus $g$ over $k$, denote by $J$ its Jacobian variety and let $\Gamma \subset J(k)$ be a subgroup of rank $\leq g - 3$. Let $i$: $C \to J$ be an embedding given by choosing some basepoint $P_0 \in C(k)$. Then
\[ \# \{ P \in C(k) : i(P) \in \Gamma \} \leq \tilde{N}(k,g) . \]

Proof. There is a field extension $k'$ of $k$ of bounded degree such that $C$ acquires semistable reduction over $k'$. For example, the proof of the ‘irreducibility theorem’ in [DM69] shows that one can take $k' = k[J[n]]$ for any $n \geq 3$ prime to $p$. There are only finitely many extensions of bounded degree of a $p$-adic field; let $E(k)$ be the finite set of extensions that occur. Then the statement obviously holds with
\[ \tilde{N}(k,g) = \max \{ N(k',g) : k' \in E(k) \} . \]

\[ \square \]

Remark 5.4. A more careful analysis using the explicit computations mentioned in the proof of Proposition 4.4 and a study of the non-semistable case shows that one can obtain good bounds that have an explicit dependence on the rank $r$. If $p > 2e + 1$ and $\Gamma \subset J(k)$ has rank $r \leq g - 3$, then one such bound is
\[ \# \{ P \in C(k) : i(P) \in \Gamma \} \leq 4 \left( q + r + 1 + e \left\lceil \frac{2r}{p - 2e - 1} \right\rceil \right) g - 2r . \]
In particular, taking $r = 0$, we obtain a bound of $4(q + 1)g$ for the number of $k$-points in any torsion packet on a hyperelliptic curve of genus $g \geq 3$ over a $p$-adic field $k$ such that $p > 2e + 1$.

Details will appear in a later version of (or a sequel to) this paper.

6. A UNIFORM BOUND ON THE NUMBER OF RATIONAL POINTS

We can apply the result of the previous section to obtain bounds for the number of rational points on hyperelliptic curves with small Mordell-Weil rank relative to the genus.

**Theorem 6.1.** Let $g \geq 3$ and $d \geq 1$. Then there is a bound $R(d, g)$ depending only on $d$ and $g$ such that for any hyperelliptic curve $C$ of genus $g$ over a number field $K$ of degree at most $d$ such that the Mordell-Weil rank of its Jacobian is at most $g - 3$, we have $\#C(K) \leq R(d, g)$.

**Proof.** Fix some odd prime $p$. Then there are only finitely many possible completions $k$ at places above $p$ of number fields of degree $\leq d$. We take $R(d, g)$ to be the maximum of the bounds $\tilde{N}(k, g)$ of Theorem 5.3 over all these $k$.

Let $C$ be a curve as in the statement. If $C(K) = \emptyset$, there is nothing to prove. So we can assume that there is some $P_0 \in C(K)$, which we use as basepoint for an embedding $i: C \to J$. We can then apply Theorem 5.3 to $C$ base-changed to a completion $k$ of $K$ at a place above $p$ and to $\Gamma = J(K) \subset J(k)$. □

**Remark 6.2.** For $K = \mathbb{Q}$ we can use the bound given in Remark 5.4 with $k = \mathbb{Q}_5$ (then $p = 5 > 3 = 2e + 1$). This gives

$$\#C(\mathbb{Q}) \leq 8rg + 24g - 2r$$

for a hyperelliptic curve $C$ over $\mathbb{Q}$ with Jacobian of Mordell-Weil rank $r \leq g - 3$. Applying this to $J(\mathbb{Q})_{\text{tors}}$ instead of $J(\mathbb{Q})$, we see that no torsion packet on a hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 3$ can contain more than $24g$ rational points.

7. EXPLICIT RESULTS FOR HYPERELLIPITIC CURVES

In this section, we show that the assumption we needed for the proof of Proposition 4.4 holds in the case of hyperelliptic curves over a $p$-adic field with $p$ odd.

**Lemma 7.1.** Let $k = \mathbb{Q}_p$ with $p$ odd, and let $C$ be a hyperelliptic curve over $k$ of genus $g$. Assume that $A$ is an annulus centered at zero and $\varphi: A \to C$ is an analytic embedding whose image is the formal fiber of a singular point in $C_s'$. Let $V \subset \Omega^1_C$ be a linear subspace of dimension $m \geq 1$ of the space of regular differentials on $C$ such that $c(\omega) = a(\omega) = 0$ for all $\omega \in V$ in the notation of Proposition 4.2. Then there is some $0 \neq \omega \in V$ such that $\varphi^*\omega = u(z)h(z)dz$ with a Laurent series $h$ satisfying $|h(\xi) - 1| < 1$ on $A$ and a Laurent polynomial $u$ with the property that all its terms have exponents between $n_1$ and $n_2$ where $n_1 < -1 < n_2$ and $n_2 - n_1 \leq \max\{2(g - m), 2\}$. 

10
Proof. It follows from the description of stable models of hyperelliptic curves in odd residue characteristic (see for example [BW13]) that the images in \( \mathbb{P}^1 \) of residue disks of \( C \) are either maximal disks not containing any branch point or maximal disks containing exactly one branch point. The images in \( \mathbb{P}^1 \) of annuli in \( C \) are either maximal annuli not containing any branch point and partitioning the set of branch points into two subsets of size at least 3 or maximal disks containing exactly two branch points. We consider these two latter cases separately. We assume that \( C \) is given by the affine equation \( y^2 = f(x) \) (with \( f \) squarefree of degree \( 2g + 1 \) or \( 2g + 2 \)); we write \( \Theta' \) for the set of roots of \( f \) and \( \Theta = \Theta' \cup \{ \infty \} \) if \( \deg f = 2g + 1 \). Let \( c \) be the leading coefficient of \( f \), so that

\[
f(x) = c \prod_{\theta \in \Theta'} (x - \theta).
\]

Let \( A' \subset \mathbb{P}^1 \) be a (maximal) annulus with \( A' \cap \Theta = \emptyset \). We can assume that \( A' \) has the form

\[
A' = \{ \xi : \rho_1 < v(\xi) < \rho_2 \} \subset \mathbb{A}^1 \subset \mathbb{P}^1;
\]

we set

\[
\Theta_0 = \{ \theta \in \Theta : v(\theta) \geq n_2 \}, \quad \Theta_{\infty} = \Theta \setminus \Theta_0 \text{ and } \Theta'_{\infty} = \Theta_{\infty} \cap \Theta' = \{ \theta \in \Theta' : v(\theta) \leq n_1 \}.
\]

We can then write

\[
f(x) = c \prod_{\theta \in \Theta'_{\infty}} (x - \theta) \prod_{\theta \in \Theta_0} (x - \theta)
= c \prod_{\theta \in \Theta'_{\infty}} (-\theta) \cdot x^{#\Theta_0} \prod_{\theta \in \Theta_0} \left(1 - \frac{x}{\theta}\right) \prod_{\theta \in \Theta_{\infty}} \left(1 - \frac{\theta}{x}\right).
\]

Each factor \( 1 - \theta/x \) or \( 1 - x/\theta \) can be written as the square of a Laurent series that converges on \( A' \), so that

\[
f(x) = \gamma x^{#\Theta_0} \tilde{h}(x)^2
\]

for some Laurent series \( \tilde{h} \) converging on \( A' \), where \( \gamma = c \prod_{\theta \in \Theta'_{\infty}} (-\theta) \in k^\times \) and \( |\tilde{h}(\xi) - 1| < 1 \) for all \( \xi \in A' \).

a) In the odd case with \( #\Theta_0 = 2\nu + 1 \), say (with \( 1 \leq \nu \leq g - 1 \)), we can take

\[
A = \{ \tau : \gamma \tau^2 \in A' \};
\]

then we obtain an analytic embedding

\[
\varphi : A \rightarrow C, \quad \tau \mapsto (\gamma \tau^2, \gamma^{\nu+1} \tau^{2\nu+1} \tilde{h}(\gamma \tau^2))
\]

that is equivariant with respect to \( \tau \mapsto -\tau \) on the left and the hyperelliptic involution on the right. (The annulus corresponds to an edge of \( R(C) \) that is fixed as an oriented edge by the hyperelliptic involution.)

b) In the even case we write \( #\Theta_0 = 2\nu \) (with \( 2 \leq \nu \leq g - 1 \)) and we let \( \alpha \in k \) denote a square root of \( \gamma \). Then the preimage of \( A' \) in \( C \) splits as a disjoint union of two copies of \( A' = A \), parametrized by

\[
\varphi_\pm : A \rightarrow C, \quad \tau \mapsto (\tau, \pm \alpha \tau^\nu \tilde{h}(\tau)).
\]
c) Now consider a (maximal) disk \( D \subset \mathbb{P}^1 \) such that \( D \cap \Theta = \{ \theta_1, \theta_2 \} \) has two elements. We can assume that \( D = \{ \xi : v(\xi) > \rho \} \). In a similar way as above, we can write

\[
f(x) = \gamma \tilde{h}(x)^2(x - \theta_1)(x - \theta_2)
\]

with a power series \( \tilde{h} \) converging on \( D \) such that \( |\tilde{h}(\xi) - 1| < 1 \) for \( \xi \in D \). Without loss of generality, we can assume that \( \theta_2 = -\theta_1 \), so that \( (x - \theta_1)(x - \theta_2) = x^2 - a \) for some \( a \in k^\times \). Let \( \alpha \in k \) be a square root of \( \gamma \). Setting \( y = \alpha \tilde{h}(x)\bar{y} \), the equation of \( C \) becomes \( \bar{y}^2 = x^2 - a \). This can be parametrized by setting \( t = x + \bar{y} \), so that

\[
x = \frac{1}{2} \left( t + \frac{a}{t} \right) \quad \text{and} \quad \bar{y} = \frac{1}{2} \left( t - \frac{a}{t} \right), \quad \text{so} \quad y = \frac{\alpha}{2} \left( t - \frac{a}{t} \right) \tilde{h}\left( t + \frac{a}{t} \right).
\]

Taking \( A = \{ \tau : \rho < v(\tau) < \rho + v(a) \} \), we get that \( \tilde{h}(t - a/t) \) converges on \( A \) with values close to \( 1 \); also for \( (x, y) \in C(k') \) with \( x \in D \), we have \( t \in A \), so we obtain an analytic embedding. We note that \( t \mapsto a/t \) fixes \( x \) and changes the sign of \( y \), so it corresponds to the hyperelliptic involution on the image of \( \varphi \). (The annulus corresponds to an edge of \( R(C) \) that is fixed, but whose orientation is reversed by the hyperelliptic involution).

Now we consider a regular differential \( \omega \) on \( C \). It can be written in the form

\[
\omega = \tilde{u}(x) \frac{dx}{2y}
\]

with a polynomial \( \tilde{u} \) of degree at most \( g - 1 \). This leads to \( \varphi^*\omega = u(t)\tilde{h}(t) \, dt \) with a Laurent series \( \tilde{h}(t) \) such that \( |\tilde{h}(\tau) - 1| < 1 \) on \( A \) and a Laurent polynomial \( u \) given by

\[
\text{a) } \frac{\tilde{u}(\gamma t^2)}{(\gamma t^2)^\nu}, \quad \text{b) } \frac{\tilde{u}(t)}{2\alpha t^\nu}, \quad \text{or} \quad \text{c) } \frac{\tilde{u}(t + at^{-1})}{2\alpha t}.
\]

Since we are free to impose up to \( m - 1 \) linear conditions on \( \omega \), we can arrange for the terms in \( \tilde{u} \) to have exponents in any interval of length \( g - m \) containing \( \nu \) in cases a) and b), or in the interval \([0, g - m]\) in case c). Writing \( \nu_1 \) and \( \nu_2 \) for the minimal and maximal degree of a term in \( u \), we can therefore arrange in all cases to have \( \nu_1 \geq n_1, \nu_2 \leq n_2 \) such that \( n_2 - n_1 = \max\{2(g - m), 2\} \) and \( n_1 < -1 < n_2 \). This proves the claim. \( \square \)

References

[Bak08] Matthew Baker, An introduction to Berkovich analytic spaces and non-Archimedean potential theory on curves, p-adic geometry, Univ. Lecture Ser., vol. 45, Amer. Math. Soc., Providence, RI, 2008, pp. 123–174. MR2482347 (2010g:14029) ↑3

[BL84] Siegfried Bosch and Werner Lütkebohmert, Stable reduction and uniformization of abelian varieties. II, Invent. Math. 78 (1984), no. 2, 257–297, DOI 10.1007/BF01388596. MR767194 (86j:14029) ↑4

[BL85] Siegfried Bosch and Werner Lütkebohmert, Stable reduction and uniformization of abelian varieties. I, Math. Ann. 270 (1985), no. 3, 349–379, DOI 10.1007/BF01473432. MR774362 (86j:14030a) ↑3

[BL84] Siegfried Bosch and Werner Lütkebohmert, Stable reduction and uniformization of abelian varieties. II, Invent. Math. 78 (1984), no. 2, 257–297, DOI 10.1007/BF01388596. MR767194 (86j:14029) ↑4

[BW13] Irene Bouw and Stefan Wewers, Computing L-functions and semistable reduction of superelliptic curves, June 14, 2013. Preprint, arXiv:1211.4459v3. ↑7

[CHM97] Lucia Caporaso, Joe Harris, and Barry Mazur, Uniformity of rational points, J. Amer. Math. Soc. 10 (1997), no. 1, 1–35, DOI 10.1090/S0894-0347-97-00195-1. MR1325796 (97d:14033) ↑1
[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) ↑1
[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. 52 (1985), no. 3, 765–770. MR808103 (87f:11043) ↑1
[DM69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. 36 (1969), 75–109. MR0262240 (41 #6850) ↑5
[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), no. 3, 349–366 (German). Erratum in: Invent. Math. 75 (1984), 381. MR718935 (85g:11026a) ↑1
[Fal94] Gerd Faltings, *The general case of S. Lang’s conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182. MR1307396 (95m:11061) ↑1
[KZB13] Eric Katz and David Zureick-Brown, *The Chabauty–Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*, January 25, 2013. Preprint, arXiv:1204.3335v3. ↑1
[MP13] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Panoramas et Synthèses, vol. 36, Société Math. de France, 2013. ↑1
[PS13] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, May 21, 2013. Preprint, arXiv:1302.0061v2. ↑1
[Sto06] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. 142 (2006), no. 5, 1201–1214. MR2264661 ↑1, 4

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail address: Michael.Stoll@uni-bayreuth.de

URL: http://www.mathe2.uni-bayreuth.de/stoll/