THE CHABAUTY-COLEMAN BOUND AT A PRIME OF BAD REDUCTION

DAVID BROWN

Abstract. Let X be a curve over a number field K with genus $g \geq 2$, $\mathfrak{p}$ a prime of $\mathcal{O}_K$ over an unramified rational prime $p > 2r$, J the Jacobian of X, $r = \operatorname{rank} J(K)$, and $\mathscr{X}$ a regular proper model of X at $\mathfrak{p}$. Suppose $r < g$. We prove that $\#X(K) \leq \#\mathscr{X}(\mathbb{F}_\mathfrak{p}) + 2r$, extending the refined version of the Chabauty-Coleman bound to the case of bad reduction.

1. Introduction

Let K be a number field and X/K be a curve (i.e. a smooth geometrically integral 1-dimensional variety) of genus $g \geq 2$ and let p denote a prime which is unramified in K. Faltings' [Fal86], Vojta's [Voj91], and Bombieri's [Bom90] proofs of the Mordell Conjecture tell us that $X(K)$ is finite, but all known proofs of the Mordell Conjecture are ineffective, providing no assistance in determining $X(K)$ explicitly for a specific curve. Chabauty [Cha41], building on an idea of Skolem [Sko34], gave a proof of the Mordell Conjecture when the rank r of the Jacobian of X is strictly less than the genus g. Coleman later realized that Chabauty's proof could be modified to get an explicit upper bound for $\#X(K)$.

Theorem 1.1 ([Col85]). *Suppose $p > 2g$ and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime of good reduction which lies above p. Suppose $r < g$. Then*

$$\#X(K) \leq \#X(\mathbb{F}_\mathfrak{p}) + 2g - 2.$$

Using Proposition 2.8, one can write out weaker, but still explicit (in terms of g and p), bounds when $p \leq 2g$ or when p ramifies in K (see any of [Col85], [Sto06], or [LT02]). In [LT02], the authors ask if one can refine Coleman's bound when the rank is small (i.e. $r \leq g - 2$). Stoll proved that by choosing, for each residue class, the 'best' differential one can indeed refine the bound.

Theorem 1.2 ([Sto06, Corollary 6.7]). *With the hypothesis of Theorem 1.1,*

$$\#X(K) \leq \#X(\mathbb{F}_\mathfrak{p}) + 2r.$$

Let $\mathscr{X}$ be a minimal regular proper model of X at $\mathfrak{p}$ and denote by $\mathscr{X}_\mathfrak{p}^{\mathrm{sm}}$ the smooth locus of $\mathscr{X}_\mathfrak{p}$. In another direction, McCallum and Poonen use intersection theory on $\mathscr{X}$ to derive Coleman's bound when $\mathfrak{p}$ is a prime of bad reduction. Lorenzini and Tucker gave an earlier, alternative proof which avoids intersection theory.

Date: March 15, 2008.

This research was supported by a National Defense Science and Engineering Graduate Fellowship.

Theorem 1.3 ([LT02, Proposition 1.10], [MP07, Theorem A.5])**.** *Suppose $p > 2g$ and let $\mathfrak{p}$ be a prime above p. Let $\mathscr{X}$ be a proper regular model of X over $\mathcal{O}_{K_\mathfrak{p}}$. Suppose $r < g$. Then*

$$\#X(K) \leq \#\mathscr{X}_\mathfrak{p}^{sm}(\mathbb{F}_\mathfrak{p}) + 2g - 2.$$

1.1. **Main Result.** Michael Stoll asks [Sto06, Remark 6.5] if one can combine the methods of [Sto06] and [MP07] to generalize Theorem 1.2 to the case when $\mathfrak{p}$ is a prime of bad reduction and remarks that Theorem 1.2 is true at least for a hyperelliptic curve. The main result of this paper is such a generalization.

Theorem 1.4. *Let X be a curve over a number field K. Suppose $p > 2r + 2$ is a prime which is unramified in K and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime above p. Let $\mathscr{X}$ be a proper regular model of X over $\mathcal{O}_{K_\mathfrak{p}}$. Suppose $r < g$. Then*

$$\#X(K) \leq \#\mathscr{X}_\mathfrak{p}^{sm}(\mathbb{F}_\mathfrak{p}) + 2r.$$

Remark 1.5. The charm of these theorems is that they occasionally allow one to compute $X(K)$; see [Gra94] for the first such example and Section 5 for another which uses the the refined bound of Theorem 1.4 at a prime of bad reduction. While these examples are somewhat special (since the bound of Theorem 1.4 is not sharp in general), there are a wealth of interesting examples where a more careful analysis of Chabauty's method allows one to determine $X(K)$. Worth noting are the works [Bru99] and [PSS07], where the integral coprime solutions of the generalized Fermat equations $x^2 + y^8 = z^3$ and $x^2 + y^3 = z^7$ (both of which have large, non-trivial solutions) are completely determined by reducing to curves and using Chabauty methods.

For low genus hyperelliptic curves Chabauty's method has been made completely explicit and even implemented in [Magma], so that for a specific curve $X(K)$ can often be determined; see the survey [Poo02] for a general discussion of computational issues, [MP07, Section 7] for a discussion of effectivity of Chabauty's method, and the online documentation [Magma] for many details. See also also [BS07], where the complementary problem of proving $X(K) = \emptyset$ is discussed in detail with impressive experimental data.

Remark 1.6. The $p = 2r + 2$ case of Theorem 1.4 (i.e. $p = 2$ and $r = 0$) is [LT02, Proposition 1.10].

This paper is structured as follows. In Section 2 we review the method of Chabauty and Coleman. In Section 3 we present the main argument used to bound $\#X(K)$. In Section 4 we prove a technical proposition, necessary for the main argument, which generalizes Clifford's theorem about special divisors on curves to the case of non-reduced, reducible curves. Finally, in Section 5 we give two examples where the refined bound can be used to determine $X(K)$.

2. The Method of Chabauty and Coleman

In this section we recall the method of Chabauty and Coleman. See [MP07] for many references and a more detailed account.

Let K be a number field with valuation v normalized so that the value group is $\mathbb{Z}$. Fix a prime p and a prime $\mathfrak{p}$ of K above p. For a scheme Y over K let $Y_{\mathfrak{p}}$ be the extension of scalars $Y \times_K K_{\mathfrak{p}}$, where $K_{\mathfrak{p}}$ is the completion of K at $\mathfrak{p}$. For a scheme Y over a field denote by Y^{sm} its smooth locus. Let X be a smooth projective geometrically integral curve of genus $g \geq 2$ over K with Jacobian J; let $r = \operatorname{rank} J(K)$. Suppose that there exists a rational point $P \in X(K)$ (otherwise the conclusion of Theorem 1.4 is trivially true) and let $\iota : X \to J$ be the embedding given by $Q \mapsto [Q - P]$.

2.1. **Models and Residue Classes.** Let $\mathscr{X}$ be a proper regular model of $X_{\mathfrak{p}}$ over $\mathcal{O}_{K_{\mathfrak{p}}}$ and denote its special fiber by $\mathscr{X}_{\mathfrak{p}}$.

$$\begin{array}{ccccc} \mathscr{X}_{\mathfrak{p}} & \longrightarrow & \mathscr{X} & \overset{i}{\longleftarrow} & X_{\mathfrak{p}} \\ \downarrow{\scriptstyle \pi_{\mathfrak{p}}} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_{K_{\mathfrak{p}}}} \\ \operatorname{Spec} \mathbb{F}_{\mathfrak{p}} & \longrightarrow & \operatorname{Spec} \mathcal{O}_{K_{\mathfrak{p}}} & \longleftarrow & \operatorname{Spec} K_{\mathfrak{p}} \end{array} \tag{2.1}$$

Since $\mathscr{X}$ is proper, the valuative criterion gives a reduction map

$$r \colon X_{\mathfrak{p}}(K_{\mathfrak{p}}) = \mathscr{X}(\mathcal{O}_{K_{\mathfrak{p}}}) \to \mathscr{X}(\mathbb{F}_{\mathfrak{p}}). \tag{2.2}$$

Alternatively, r is given by smearing any $K_{\mathfrak{p}}$-point of $X_{\mathfrak{p}}$ to an $\mathcal{O}_{K_{\mathfrak{p}}}$-point of $\mathscr{X}$ and then intersecting with the special fiber $\mathscr{X}_{\mathfrak{p}}$; i.e. $r(P) = \overline{\{P\}} \cap \mathscr{X}_{\mathfrak{p}}$. Since $\mathscr{X}$ is regular, the image is contained in $\mathscr{X}_{\mathfrak{p}}^{\mathrm{sm}}(\mathbb{F}_{\mathfrak{p}})$; by Hensel's lemma we have equality.

Definition 2.3. For $\widetilde{Q} \in \mathscr{X}_{\mathfrak{p}}^{\mathrm{sm}}(\mathbb{F}_{\mathfrak{p}})$ we define the residue class $D_{\widetilde{Q}}$ to be the preimage $r^{-1}(\widetilde{Q})$ of $\widetilde{Q}$ under the reduction map (2.2).

Definition 2.4. Scale $\omega \in H^0(X_{\mathfrak{p}}, \Omega^1_{X_{\mathfrak{p}}/K_{\mathfrak{p}}})$ by $t \in K_{\mathfrak{p}}^{\times}$ so that the reduction $\widetilde{\omega}$ of $t\omega$ to the component of $\mathscr{X}_{\mathfrak{p}}$ containing $\widetilde{Q}$ is non-zero. We define

$$n(\omega, \widetilde{Q}) = \operatorname{ord}_{\widetilde{Q}} \widetilde{\omega}.$$

2.2. **p-adic Integration.** For an introduction to integration on a p-adic curve see [MP07, Sections 4 and 5]. For $\omega \in H^0(X_{\mathfrak{p}}, \Omega^1_{X_{\mathfrak{p}}/K_{\mathfrak{p}}})$ let $\eta_\omega \colon X(K_{\mathfrak{p}}) \to K_{\mathfrak{p}}$ be the function $Q \mapsto \int_P^Q \omega$. The following proposition summarizes relevant results of [LT02, Section 1].

Proposition 2.5. *Let $\widetilde{Q} \in \mathscr{X}_{\mathfrak{p}}^{sm}(\mathbb{F}_{\mathfrak{p}})$ and $Q \in D_{\widetilde{Q}}$. Let $u \in \mathcal{O}_{\mathscr{X},Q}$ such that the restriction to $\mathcal{O}_{\mathscr{X}_{\mathfrak{p}},\widetilde{Q}}$ is a uniformizer. Then the following are true.*

(1) *The function u defines a bijection*

$$D_{\widetilde{Q}} \xrightarrow{\sim} \mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}.$$

(2) *There exists $I_{\omega,Q}(t) \in K_{\mathfrak{p}}[[t]]$ which enjoys the following properties:*
   - (i) *For $Q' \in D_{\widetilde{Q}}$, $\eta_\omega(Q') = I_{\omega,Q}(u(Q')) + \eta_\omega(Q)$.*
   - (ii) $w(t) := I_{\omega,Q}(t)' \in \mathcal{O}_{K_{\mathfrak{p}}}[[t]]$.
   - (iii) *If we write $w(t) = \sum_{i=0}^{\infty} a_i t^i$, then*

$$\min\{i \colon v(a_i) = 0\} = n(\omega, \widetilde{Q}).$$

The starting point of Chabauty's method is the following proposition.

Proposition 2.6 ([Sto06], Section 6)**.** *Denote by* $V_{\mathfrak{p}}$ *the vector space of all* $\omega \in H^0\big(X_{\mathfrak{p}}, \Omega^1_{X_{\mathfrak{p}}/K_{\mathfrak{p}}}\big)$ *such that* $\eta_\omega(Q) = 0$ *for all* $Q \in X(K)$*. Then* $\dim V_{\mathfrak{p}} \geq g - r$.

2.3. **Newton Polygons.** We now will use Newton polygons to bound the number of zeroes of $I_{\omega,Q}(t)$ with $t \in \mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}$. Following [Sto06, Section 6], we let $e = v(p)$ be the absolute ramification index of $K_{\mathfrak{p}}$ and make the following definitions (where v_p is the valuation of $\mathbb{Q}_p$).

Definition 2.7. We set

$$\nu(Q) = \#\left\{t \in \mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}} \text{ such that } I_{\omega,Q}(t) = 0\right\}$$

and

$$\begin{aligned}\delta(v,n) &= \max\{d \geq 0 \mid n+d+1-v(n+d+1) \leq n+1-v(n+1)\} \\ &= \max\{d \geq 0 \mid e\,v_p(n+1)+d \leq e\,v_p(n+d+1)\}\,.\end{aligned}$$

The key proposition is [Sto06, Proposition 6.3] where a Newton polygon argument gives the following bound.

Proposition 2.8. *We have the bound*

$$\nu(Q) \leq 1 + n\big(\omega, \widetilde{Q}\big) + \delta\big(v, n\big(\omega, \widetilde{Q}\big)\big).$$

Furthermore, suppose $e < p-1$*. Then* $\delta(v,n) \leq e\lfloor n/(p-e-1)\rfloor$*. In particular, if* $p > n+e+1$*, then* $\delta(v,n) = 0$.

3. Bounding $\#X(K)$

We bound $\#X(K)$ as follows. For each $\widetilde{Q} \in \mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$, $\#\big(X(K) \cap D_{\widetilde{Q}}\big) \leq \nu(Q)$. For nonzero $\omega \in V_{\mathfrak{p}}$ (see Definition 2.6) summing the bound of Proposition 2.8 over the residue classes of each smooth point gives

$$\#X(K) \leq \#\mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) + \sum_{\widetilde{Q} \in \mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})} \Big(n\big(\omega, \widetilde{Q}\big) + \delta\big(v, n\big(\omega, \widetilde{Q}\big)\big)\Big).$$

To use this we need to bound

$$\sum_{\widetilde{Q} \in \mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})} n\big(\omega, \widetilde{Q}\big).$$

As in the good reduction case of [Col85], Riemann-Roch gives, for a fixed ω, the preliminary bound

$$\sum_{\widetilde{Q} \in \mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})} n\big(\omega, \widetilde{Q}\big) = \deg \operatorname{div} \omega = 2g-2.$$

If $p > 2g+e-1$, then in particular $p > n(\omega, \widetilde{Q}) + e + 1$ for every $\widetilde{Q}$ and Proposition 2.8 reveals that $\delta(v, n(\omega, \widetilde{Q})) = 0$, recovering the bound of Theorem 1.3

$$\#X(K) \leq \#\mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) + 2g - 2.$$

The idea of [Sto06] is to use a different differential $\omega_{\widetilde{Q}}$ for each residue class to get a better bound. Stoll does this for the good reduction case [Sto06, Theorem 6.4] and what prevents his method from working in generality is that the reduction map

$$\rho\colon \mathbb{P}\big(H^0\big(X_{\mathfrak{p}}, \Omega^1\big)\big) \to \mathbb{P}\big(H^0\big(\mathscr{X}_{\mathfrak{p}}, \Omega^1\big)\big) \tag{3.1}$$

is well behaved only when $\mathscr{X}$ is smooth. The main content of this paper is that if one replaces the sheaf of differentials with the canonical sheaf then one can recover Stoll's argument

3.1. **Main argument.** For a map $f\colon Y \to Z$ we denote by ω_f the relative dualizing sheaf. Recall the setup of (2.1). Here we describe the appropriate generalization of the above reduction map (3.1). Since π is flat [Liu06, p. 347], base change for relative dualizing sheaves [Liu06, Theorem 6.4.9] gives $i^*\omega_\pi \simeq \omega_{\pi_{K_{\mathfrak{p}}}} \simeq \Omega^1_{X_{\mathfrak{p}}/K_{\mathfrak{p}}}$. One gets an inclusion of global sections

$$H^0(\mathscr{X}, \omega_\pi) \xrightarrow{\phi} H^0(\mathscr{X}, \omega_\pi) \otimes_{\mathcal{O}_{K_{\mathfrak{p}}}} K_{\mathfrak{p}} = H^0\big(X_{\mathfrak{p}}, \Omega^1_{X_{\mathfrak{p}}/K_{\mathfrak{p}}}\big)\ .$$

A subspace $V \subset H^0\big(X_{\mathfrak{p}}, \Omega^1_{X_{\mathfrak{p}}/K_{\mathfrak{p}}}\big)$ pulls back to a submodule $V_{\mathcal{O}_{K_{\mathfrak{p}}}} := \phi^{-1}(V) \subset H^0(\mathscr{X}, \omega_\pi)$. Now let $V = V_{\mathfrak{p}}$ (see Definition 2.6), and for any $\widetilde{Q} \in \mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ let

$$n_{\widetilde{Q}} := \min\big\{n\big(\omega, \widetilde{Q}\big) \,\big|\, \omega \in V\big\}.$$

Then Proposition 2.8 becomes

$$\nu(\widetilde{Q}) \leq 1 + n_{\widetilde{Q}} + \delta\big(v, n_{\widetilde{Q}}\big)$$

and thus

$$\#X(K) \leq \#\mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) + \sum_{\widetilde{Q}\in\mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})} \big(n_{\widetilde{Q}} + \delta(v, n_{\widetilde{Q}})\big).$$

We accordingly set

$$D = \sum_{\widetilde{Q}\in\mathscr{X}^{\mathrm{sm}}_{\mathfrak{p}}(\mathbb{F})} n_{\widetilde{Q}}\widetilde{Q}, \tag{3.2}$$

and since $\sum n_{\widetilde{Q}} = \deg D$, the goal is to bound $\deg D$.

Definition 3.3. Let k be a field and let $C \xrightarrow{\pi} \operatorname{Spec} k$ be a proper geometrically connected curve whose irreducible components have dimension one. Define the function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by

$$f(r) := \max\{\deg D | D \text{ is special and} \dim_k H^0\left(C, \omega_\pi \otimes \mathcal{O}_C(-D)\right) \geq p_a - r\},$$

where ω_π is the relative dualizing sheaf of π and p_a is the arithmetic genus of C. See Definition 4.3 for the definition of special.

Lemma 3.4. *For D defined in* (3.2), $\deg D \leq f(r)$.

Proof. Set $V_s := V_{\mathcal{O}_{K_\mathfrak{p}}} \otimes_{\mathcal{O}_{K_\mathfrak{p}}} \mathbb{F}_\mathfrak{p}$. Since $V_{K_\mathfrak{p}}$ is saturated, the composition $V_s \to H^0(\mathscr{X}, \omega_\pi) \otimes_{\mathcal{O}_{K_\mathfrak{p}}} \mathbb{F}_p \to H^0(\mathscr{X}_\mathfrak{p}, \omega_\mathfrak{p})$ is an injection and

$$\dim_{\mathbb{F}_\mathfrak{p}} V_s = \dim_{K_\mathfrak{p}} V_\mathfrak{p} \geq g - r = p_a - r.$$

For $\omega \in V_{\mathcal{O}_{K_\mathfrak{p}}}$ denote by $\bar{\omega}$ its image in V_s. By construction,

$$V_s \subset H^0(\mathscr{X}_\mathfrak{p}, \omega_\mathfrak{p} \otimes \mathcal{O}_{\mathscr{X}_\mathfrak{p}}(-D)) \subset H^0(\mathscr{X}_\mathfrak{p}, \omega_\mathfrak{p}).$$

Indeed, let $\operatorname{div} \omega$ be the Cartier divisor associated to ω and let H_ω be the horizonal part of $\operatorname{div} \omega$. Then

$$\omega \in H^0(\mathscr{X}, \omega_\pi \otimes \mathcal{O}_\mathscr{X}(-H_\omega)),$$

and since

$$(\omega_\pi \otimes \mathcal{O}_\mathscr{X}(-H_\omega)) \otimes_{\mathcal{O}_{K_\mathfrak{p}}} \mathbb{F}_\mathfrak{p} \subset \omega_\mathfrak{p} \otimes \mathcal{O}_{\mathscr{X}_\mathfrak{p}}(-D),$$

we have

$$\bar{\omega} \in H^0(\mathscr{X}_\mathfrak{p}, \omega_\mathfrak{p} \otimes \mathcal{O}_{\mathscr{X}_\mathfrak{p}}(-D)).$$

By adjunction the restriction of H_ω to $\mathscr{X}_\mathfrak{p}$ is an effective canonical divisor H such that $H - D$ is effective, and since $\mathscr{X}$ is regular, $\operatorname{Supp} D \subset \operatorname{Supp} H \subset \mathscr{X}_\mathfrak{p}^{\mathrm{sm}}$. We conclude that D is special, so by definition of f, we have $\deg D \leq f(r)$. □

Lemma 3.5. *Suppose $r < p_a$. Then $f(r) \leq 2r$.*

The case of good reduction is [Sto06, Lemma 3.1]. The proof of the general case is postponed to the next section. Theorem 1.4 immediately follows.

Remark 3.6. For C smooth, $f(r) = 2r$ if and only if C is hyperelliptic, and one can often carve a better bound out of the geometry of C; see [Sto06, Section 3]. It would be interesting to understand when $f(r) < 2r$ in the case that C is not smooth; for instance a smooth genus 3 plane quartic C with $\operatorname{rank} J_C = 1$ and smooth special fiber has $f(1) = 1$, but if the special fiber of its regular proper minimal model is irreducible with an ordinary double point (so that its normalization has genus 2 and is thus hyperelliptic), then $f(1) = 2$. The situation is more delicate when C has multiple components.

4. Clifford's theorem for Singular Curves

Here we prove Lemma 3.5. The key point is to generalize Clifford's theorem [Har77, Chapter IV, Theorem 5.4] to singular curves. To this end, let k denote a field and define a curve to be a geometrically connected projective algebraic variety over k whose irreducible components are of dimension 1. Throughout we fix a curve $C \xrightarrow{\pi} k$ such that the relative dualizing sheaf ω_π is invertible (in our application this holds because C is a curve inside a regular surface).

Remark 4.1. By [Liu06, Remark 7.1.20], any invertible sheaf of $\mathcal{O}_C$-modules is a subsheaf of $\mathscr{K}_C$, the sheaf of stalks of meromorphic functions on C [Liu06, Definition 7.1.13]. Thus, the injection [Liu06, Proposition 7.1.18 (b)]

$$\operatorname{CaCl}(C) \to \operatorname{Pic}(C)$$

is an isomorphism.

Definition 4.2. Let ω be the relative dualizing sheaf of $C \xrightarrow{\pi} \operatorname{Spec} k$. We define a canonical divisor to be any Cartier divisor K such that $\mathcal{O}_C(K) \cong \omega$. By Remark 4.1 there exists a canonical divisor K.

Definition 4.3. Recall that a Cartier divisor D is effective if D can be represented by $\{(U_i, f_i)\}$ with $f_i \in \mathcal{O}_C(U_i)$. We call D special if there exists an effective canonical divisor K such that $\operatorname{Supp} K \subset C^{\mathrm{sm}}$ and $K - D$ is effective.

Lemma 4.4. *Let E be an effective Cartier divisor on C such that $\operatorname{Supp} E \subset C^{sm}$. Then the set of pairs of effective Cartier divisors (D, D') such that $D + D' = E$ is finite.*

Proof. Since $\operatorname{Supp} D \cup \operatorname{Supp} D' \subset \operatorname{Supp} E \subset C^{\mathrm{sm}}$ the result follows from the analogous result for Weil Divisors. □

Definition 4.5. For a vector space V define $\mathbb{P}(V)$ to be the projective space $\big(V - \{0\}\big)/k^*$. For a Cartier divisor D define the complete linear system $|D|$ by

$$|D| := \mathbb{P}(H^0(C, \mathcal{O}_C(D))).$$

Note that $\dim |D| = \dim_k H^0(C, \mathcal{O}_C(D)) - 1$.

Remark 4.6. When C is smooth, any non-zero $f \in |D|$ is meromorphic and defines an equivalence of Cartier divisors $D \sim E$. In general f may vanish along a component (see Remark 4.8). When f is meromorphic we will sometimes refer to its class in $|D|$ by E.

Lemma 4.7. *Let D and D' be effective Cartier divisors on a curve C defined over a field k. Suppose $\operatorname{Supp}(D)$ and $\operatorname{Supp}(D')$ are contained in C^{sm}. Then*

$$\dim |D| + \dim |D'| \leq \dim |D + D'|.$$

Proof. The bilinear map

$$H^0(C, \mathcal{O}_C(D)) \times H^0(C, \mathcal{O}_C(D')) \to H^0(C, \mathcal{O}_C(D + D'))$$

given by $(f, f') \mapsto ff'$ induces a rational map of varieties

$$\phi \colon |D| \times |D'| \dashrightarrow |D + D'|.$$

Indeed, ϕ is defined at the point (D, D') (i.e. at the pair of functions $(1, 1)$) so extends to a rational map. We claim that $\phi^{-1}(D + D')$ is finite. Suppose $\phi((f, f')) = D + D'$. By definition this means that $ff' = c$ for some non-zero constant $c \in k$. We conclude that f and f' do not vanish along any component of C; in particular they define equivalences of Cartier divisors $D \sim E$ and $D' \sim E'$ and the claim follows from Lemma 4.4. Finally,

$$\dim(|D| \times |D'|) = \dim \phi(|D| \times |D'|) \leq \dim |D + D'|$$

where the first equality is [Har77, Exercise II.3.22(b)]. □

Remark 4.8. In contrast to the proof of [Har77, Chapter IV, Theorem 5.4], the map ϕ of Lemma 4.7 may not be finite to one. For example, let X be the projective closure of $Y = \operatorname{Spec} k[x,y]/(xy)$ inside of $\mathbb{P}^2$ and denote the points at infinity of the x and y axes by ∞_x and ∞_y. The effective Cartier divisor $D = \{(X, x^2+y^2)\} + 2\infty_x + 2\infty_y$ can be written as the sum of two effective Cartier divisors in infinitely many ways. Indeed, for $\lambda \in \overline{k}^\times$, let D_λ be the Cartier divisor $\{(X, \lambda x + \lambda^{-1} y)\} + \infty_x + \infty_y$. Then $D_\lambda + D_{\lambda^{-1}} = D$, and for $\lambda \neq \pm\lambda'$, D_λ and $D_{\lambda'}$ are distinct divisors. Thus the map $\phi\colon |\infty_x + \infty_y| \times |\infty_x + \infty_y| \dashrightarrow |2\infty_x + 2\infty_y|$ is not quasi-finite.

Remark 4.9. Similarly, if $\operatorname{Supp} E$ is not contained in C^{sm} then the map ϕ of Lemma (4.7) may not be defined everywhere. Let X be as in Remark 4.8 and denote the closures of the x and y axes by X_x and X_y. Define meromorphic functions $f_x \in |\infty_x|$ as the identity on X_x and 0 on X_y and $f_y \in |\infty_y|$ as the identity on X_y and zero on X_x. Then the map $|\infty_x| \times |\infty_y| \dashrightarrow |\infty_x + \infty_y|$ is not defined at the pair (f_x, f_y) since $f_x f_y = 0$.

Theorem 4.10. *(Clifford's Theorem) Let D be a special Cartier divisor on a curve C defined over a field k. Then*

$$\dim |D| \leq \frac{1}{2} \deg D.$$

Proof. Let K be a canonical divisor. By Serre duality [Liu06, Remark 6.4.30]

$$\dim |K| = \dim H^0(C, \omega) - 1 = \dim H^1(C, \mathcal{O}_C) - 1 = p_a - 1,$$

where $p_a := 1 - \chi(\mathcal{O}_C)$ is the arithmetic genus of C. Adding the inequalities

$$\dim |D| + \dim |K - D| \leq \dim |K| = p_a - 1 \qquad \text{(by Lemma 4.7)}$$
$$\dim |D| - \dim |K - D| = \deg D + 1 - p_a \qquad \text{(by Riemann-Roch [Liu06, Theorem 7.3.26])}$$

gives the result. □

We conclude with the proof of Lemma 3.5.

Proof of Lemma 3.5. We have

$$\begin{aligned} p_a - r &\leq \dim_k H^0(C, \omega \otimes \mathcal{O}_C(-D)) && \text{(by Definition 3.3)} \\ &= \dim_k H^0(C, \mathcal{O}_C(D)) - \deg D + p_a - 1 && \text{(by Riemann-Roch)} \\ &\leq p_a - \frac{1}{2} \deg D && \text{(by Theorem 4.10)} \end{aligned}$$

and simplifying gives the result. □

5. An Example

Example 5.1. Here we give an example of a hyperelliptic curve with bad reduction where the refined bound of Theorem 1.4 is sharp. Let X be the smooth genus 3 hyperelliptic curve with affine piece

$$-2 \cdot 11 \cdot 19 \cdot 173 \cdot y^2 = (x - 50)(x - 9)(x - 3)(x + 13)(x^3 + 2x^2 + 3x + 4).$$

This curve has bad reduction at the prime 5 and its regular proper minimal model $\mathscr{X}$ over $\mathbb{Z}_5$ is given by the same equation as the above Weierstrass model. A descent calculation using Magma's `TwoSelmerGroup` function shows that its Jacobian has rank 1. A point count reveals that $7 \leq \#X(\mathbb{Q})$ and $\mathscr{X}_5^{\mathrm{sm}}(\mathbb{F}_5) = 5$. Theorem 1.4 reads

$$7 \leq \#X(\mathbb{Q}) \leq \#\mathscr{X}_5^{\mathrm{sm}}(\mathbb{F}_5) + 2 = 7,$$

which determines $X(\mathbb{Q})$.

Let J be the Jacobian of X. Then J is absolutely simple. Indeed, J has good reduction at 13 and for $i \in \{1, \ldots, 30\}$ a computation reveals that the characteristic polynomial of Frobenius for $J_{\mathbb{F}_{13^i}}$ is irreducible. By an argument analogous to [PS97, Proposition 14.4] (see also [Sto08, Lemma 3]) we conclude that $J_{\mathbb{F}_{13}}$ (and hence J) is absolutely simple.

One can check that 5 is the only prime at which the Chabauty-Coleman bound is sharp. Thus, one can use neither a map to a curve of smaller genus nor the Chabauty-Coleman bound at a prime of good reduction to determine $X(\mathbb{Q})$.

Acknowledgments

I thank Bjorn Poonen and Anton Geraschenko for many useful conversations and Michael Stoll for helpful comments on an earlier draft. Computations for the example were done using the software Magma [Magma].

References

[Bom90] Enrico Bombieri, *The Mordell conjecture revisited*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, 615–640. MR **1093712 (92a:**11072) ↑1

[Bru99] Nils Bruin, *The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$*, Compositio Math. **118** (1999), no. 3, 305–321. MR **1711307 (2001d:**11035) ↑1.5

[BS07] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment* (2007). Preprint, to appear in *Experimental Mathematics*. ↑1.5

[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). MR 0004484 (3,14d) ↑1

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR **808103 (87f:**11043) ↑1.1, 1, 3

[Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 9–27. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. MR 861971 ↑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. MR **1242084 (94k:**14019) ↑1.5

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116) ↑4, 4, 4.8

[Liu06] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2006. Translated from the French by Reinie Erné; Oxford Science Publications. ↑3.1, 4.1, 4

[LT02] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. MR **1892843 (2003d:**11088) ↑1, 1.3, 1.6, 2.2

[Magma] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). Magma is available at `http://magma.maths.usyd.edu.au/magma/` .MR1484478 ↑1.5, 5

[Poo02] Bjorn Poonen, *Computing rational points on curves*, Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 149–172. MR **1956273 (2003k:**11105) ↑1.5

[MP07] William McCallum and Bjorn Poonen, *On the Method of Chabauty and Coleman* (2007), available at `"http://math.berkeley.edu/~poonen/papers/chabauty.pdf"`. ↑1.3, 1.1, 1.5, 2, 2.2

[PSS07] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to* $x^2 + y^3 = z^7$, Duke Math. J. **137** (2007), no. 1, 103–158. MR 2309145 ↑1.5

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR **1465369 (98k:**11087) ↑5.1

[Sko34] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen,* 8. Scand. Mat. Kongr. (1934), 163-169. ↑1

[Sto08] Michael Stoll, *Rational 6-cycles under iteration of quadratic polynomials* (2008), available at `"http://www.faculty.iu-bremen.de/mstoll/papers/Xdyn06.pdf"`. ↑5.1

[Sto06] ———, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR 2264661 ↑1, 1.2, 1.1, 2.6, 2.3, 2.3, 3, 3.1, 3.6

[Voj91] Paul Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548. MR **1109352 (93d:**11065) ↑1

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `brownda@math.berkeley.edu`
URL: `http://math.berkeley.edu/~brownda/`