THE METHOD OF CHABAUTY AND COLEMAN

WILLIAM MCCALLUM AND BJORN POONEN

Abstract. This is an introduction to the method of Chabauty and Coleman, a p-adic method that attempts to determine the set of rational points on a given curve of genus $g \geq 2$. We present the method, give a few examples of its implementation in practice, and discuss its effectiveness. An appendix treats the case in which the curve has bad reduction.

1. Rational points on curves of genus ≥ 2

We will work over the field $\mathbb{Q}$ of rational numbers, although everything we say admits an appropriate generalization to a number field. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. For each finite prime p, let $\mathbb{Q}_p$ be the field of p-adic numbers (see [Kob84] for the definition). Curves will be assumed to be smooth, projective, and geometrically integral.

Let X be a curve over $\mathbb{Q}$ of genus $g \geq 2$. We suppose that X is presented as the zero set in some $\mathbb{P}^n$ of an explicit finite set of homogeneous polynomials. We may give instead an equation for a singular (but still geometrically integral) curve in $\mathbb{A}^2$; in this case, it is understood that X is the smooth projective curve birational to this singular curve. Rational points on X can be specified by giving their coordinates. (A little more data may be required if a singular model for X is used.) Let $X(\mathbb{Q})$ be the set of rational points on X.

In 1922 L. Mordell [Mor22] conjectured that $X(\mathbb{Q})$ is finite, and in 1983 this was proved by G. Faltings [Fal83]. Thus we have the following well-defined problem:

Given X of genus ≥ 2 presented as above, compute $X(\mathbb{Q})$.

An argument of A. N. Parshin (see [Szp85]) shows that Faltings' proof can be adapted to give an upper bound on the *cardinality* of $X(\mathbb{Q})$. But Faltings' proof is still ineffective in the sense that it does not provide an algorithm for finding the points in $X(\mathbb{Q})$, even in principle. In fact, it is not known whether *any* algorithm is guaranteed to solve this problem. Even the case $g = 2$ seems hard.

Nevertheless there are a few techniques that can be applied: see [Poo02] for a survey. On individual curves these seem to solve the problem often, perhaps even always when used

Date: June 14, 2010.

2000 *Mathematics Subject Classification.* Primary 11G30; Secondary 14G05, 14K20.

Key words and phrases. Chabauty, p-adic integration, Jacobian.

This article is based partially on lectures given by W. M. at the Arizona Winter School in 1999, and partially on notes from a course given by B. P. as part of the "Explicit methods in number theory" trimester at the Institut Henri Poincaré in Fall 2004; B. P. thanks all the trimester organizers, and especially Karim Belabas, for their support during the trimester. W. M. was supported by NSF grant DMS-9624219, and B. P. was supported by NSF grants DMS-0301280 and DMS-0841321 and the Miller Institute for Basic Research in Science. We thank Matthew Baker, David Brown, Brian Osserman, Michael Stoll, Anthony Várilly-Alvarado, David Zywina, and the referees for comments. This article has been published as pp. 99–117 in: Explicit methods in number theory; rational points and diophantine equations, *Panoramas et Synthèses* **36**, Société Math. de France, 2012.

together, though it seems very difficult to prove that they always work. One of the methods used is the method of Chabauty and Coleman.

Remark 1.1. By [Ih02, Theorem 1.0.1], Vojta's conjecture implies that given a family of curves of genus ≥ 2 depending algebraically on parameters $t_1, \ldots, t_n$, the numerators and denominators of the coordinates of all the rational points on a curve in the family are bounded by a polynomial function of the numerators and denominators of the parameter values specifying that curve, where the polynomial depends only on the family. Experimental evidence seems to agree with this prediction [Sto09]. In fact, experience suggests a naïve search will quickly yield a list of rational points that is almost certainly complete, at least in the case of curves of low genus ≥ 2 with small integer coefficients (and slightly less naïve algorithms should do the same when the coefficients are a little larger). The difficulty is in *proving* that the list is complete.

Remark 1.2. In contrast, one expects that for some genus-1 curves, even the simplest rational points can have exponentially large numerators and denominators: see [Elk94] for an example of an elliptic curve whose "smallest" non-torsion point has a huge numerator and denominator.

2. The Jacobian

Let J be the Jacobian of X. Thus J is an abelian variety of dimension g over $\mathbb{Q}$. Although J could in principle be presented as a projective variety, for many purposes it seems easier *not* to work with explicit defining equations for J. Instead one can use that there is an $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant isomorphism between the abelian group $J(\overline{\mathbb{Q}})$ and the group of linear equivalence classes of degree-0 divisors on $X_{\overline{\mathbb{Q}}}$ (the curve defined by the same equation as X, but considered over $\overline{\mathbb{Q}}$). Elements of $J(\mathbb{Q})$ or $J(\overline{\mathbb{Q}})$ can be represented by explicit formal integer combinations of points in $X(\overline{\mathbb{Q}})$.

From now on, we suppose that we know a point $O \in X(\mathbb{Q})$. Then we have an embedding

$$\begin{aligned} \iota\colon X &\hookrightarrow J \\ P &\mapsto [P - O], \end{aligned} \tag{1}$$

where $[D]$ denotes the class of a divisor D. Hence we identify X with a subvariety of J.

Remark 2.1. As in Remark 1.1, it is usually easy to find a rational point O if it exists. If a rational point cannot be found, we can at least find a divisor D of some degree $d > 0$. Then the morphism

$$\begin{aligned} X &\to J \\ P &\mapsto [dP - D], \end{aligned}$$

is a good substitute for (1), though if $d > 1$ it need not be an embedding.

Now one possible strategy for determining $X(\mathbb{Q})$ is:

1. First compute $J(\mathbb{Q})$.
2. Then determine which points in $J(\mathbb{Q})$ lie on X.

Although $J(\mathbb{Q})$ is not necessarily finite, the Mordell-Weil theorem states that $J(\mathbb{Q})$ is a finitely generated abelian group, so in principle it can be described by giving explicit generators (represented by divisors) and relations. "Computing $J(\mathbb{Q})$" means computing these

generators and relations. There exists an algorithm that attempts to compute $J(\mathbb{Q})$, based on descent (a vast generalization of Fermat's method of infinite descent), though it is not known whether it always succeeds. This is not the concern of this article, however: from now on, we assume that $J(\mathbb{Q})$ has been computed.

Remark 2.2. The method of Chabauty and Coleman can often succeed with less than full knowledge of $J(\mathbb{Q})$. See Remark 6.1, and Examples 1 and 2 in Section 8.

If $J(\mathbb{Q})$ is finite, then in principle it is not hard to determine $X(\mathbb{Q})$: namely, for each element of $J(\mathbb{Q})$, choose a degree-0 divisor D representing it; then the points P with $\iota(P) = [D]$ (actually there will be at most one such P), when viewed as effective degree-1 divisors, are exactly the divisors of the form $D + O + (f)$ for some nonzero rational function f in the space $L(D + O)$ defined as in the statement of the Riemann-Roch theorem. There exist efficient methods for computing the basis of $L(E)$ for any divisor E [Hes02].

More generally, if J has a nonzero abelian variety quotient A such that $A(\mathbb{Q})$ is finite, then the composition $\pi\colon X \hookrightarrow J \twoheadrightarrow A$ maps $X(\mathbb{Q})$ to $A(\mathbb{Q})$, so in principle one can determine $X(\mathbb{Q})$ by checking which of the finitely many points in $\pi^{-1}(A(\mathbb{Q}))$ are rational.

But if no such A exists, or equivalently $J(\mathbb{Q})$ is Zariski dense in J, then it is more difficult to determine which of its points lie on X.

3. A real-analytic method that does not work

We can embed $J(\mathbb{Q})$ in the Lie group $J(\mathbb{R})$, which as a compact commutative Lie group is analytically isomorphic to $(\mathbb{R}^g/\mathbb{Z}^g) \times F$ for some finite abelian group F. Let $\overline{J(\mathbb{Q})}$ be the closure of $J(\mathbb{Q})$ in $J(\mathbb{R})$ with its real topology, so $\overline{J(\mathbb{Q})}$ is a Lie subgroup of $J(\mathbb{R})$. We want to find the points in $J(\mathbb{Q})$ that lie on the submanifold $X(\mathbb{R})$ of $J(\mathbb{R})$. In particular, it would be nice if the intersection $X(\mathbb{R}) \cap \overline{J(\mathbb{Q})}$ in $J(\mathbb{R})$ were finite, because then its subset $X(\mathbb{Q})$ would be finite.

But when $J(\mathbb{Q})$ is Zariski dense in J, one conjectures that $\overline{J(\mathbb{Q})}$ is open in $J(\mathbb{R})$, just as the integer multiples of a point $(a_1, \dots, a_g) \in \mathbb{R}^g/\mathbb{Z}^g$ are dense in $\mathbb{R}^g/\mathbb{Z}^g$ whenever $1, a_1, \dots, a_g$ are $\mathbb{Q}$-linearly independent. In this case, $X(\mathbb{R}) \cap \overline{J(\mathbb{Q})}$ will contain a neighborhood of O in $X(\mathbb{R})$, so it will be infinite.

Remark 3.1. The conjecture just mentioned was made by Mazur (under the additional hypothesis that J is simple) [Maz92, Conjecture 5]. It is known to be true when J is simple and $\operatorname{rank} J(\mathbb{Q}) \geq g^2 - g + 1$ [Wal93, Theorem 2].

4. Chabauty's idea

C. Chabauty [Cha41], inspired by an analogous idea of T. Skolem [Sko34] in the context of integer points on subvarieties of tori, had the idea of using $\mathbb{Q}_p$ for a fixed finite prime p instead of $\mathbb{R}$ in the previous section.

4.1. **The structure of $J(\mathbb{Q}_p)$.** Before giving Chabauty's theorem, we need some preliminaries on the structure of the p-adic Lie group $J(\mathbb{Q}_p)$. The facts in this section are discussed (in greater generality) in [Bou98, III.§7.6].

Let $J_{\mathbb{Q}_p}$ be the variety defined by the same equations as J, but considered over $\mathbb{Q}_p$ instead of $\mathbb{Q}$. Let $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ be the (g-dimensional) $\mathbb{Q}_p$-vector space of regular 1-forms on $J_{\mathbb{Q}_p}$.

Suppose $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Using the translation-invariance of ω_J, one can show that it has an "antiderivative"

$$\begin{aligned} \eta_J \colon J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ Q &\mapsto \int_0^Q \omega_J \end{aligned}$$

characterized uniquely by the following two properties:

- It is a homomorphism.
- There is an open subgroup U of $J(\mathbb{Q}_p)$ such that if $Q \in U$, then $\int_0^Q \omega_J$ can be computed by expanding ω_J in power series in local coordinates, finding a formal antiderivative, and evaluating the power series at the local coordinates of Q. Since the coefficients in the power series expansion of ω_J grow at most geometrically, the formal antiderivative converges on a sufficiently small U.

Remark 4.1. One can take U to be the kernel $J^1(\mathbb{Q}_p)$ of the reduction map $J(\mathbb{Q}_p) \twoheadrightarrow J(\mathbb{F}_p)$. (In the case of good reduction, we may interpret $J(\mathbb{F}_p)$ as the group of $\mathbb{F}_p$-points on the good reduction. In general, $J(\mathbb{F}_p)$ should be interpreted as the group of $\mathbb{F}_p$-points on the special fiber of the Néron model of J. The Néron model is a smooth group scheme over $\mathbb{Z}_p$ [BLR90], and completing it along the zero section yields a smooth formal group over $\mathbb{Z}_p$, whose associated group of points is $J^1(\mathbb{Q}_p)$; then Proposition 14(ii) of [Bou98, III.§7.6] implies that the antiderivative above converges as claimed.)

We get a bilinear pairing

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) &\to \mathbb{Q}_p \\ Q \quad , \quad \omega_J \quad &\mapsto \int_0^Q \omega_J. \end{aligned} \tag{2}$$

Let T be the vector space dual of $H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Then we may rewrite (2) as a homomorphism

$$\log \colon J(\mathbb{Q}_p) \to T.$$

The tangent spaces at 0 of the p-adic Lie groups $J(\mathbb{Q}_p)$ and T may both be identified with T; then the derivative of log at 0 is the identity $T \to T$. Thus log is also a local diffeomorphism.

4.2. **The p-adic closure of $J(\mathbb{Q})$.** The closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ with its p-adic topology is an analytic subgroup of $J(\mathbb{Q}_p)$. So it has a dimension as a p-adic manifold. Whereas the real closure of $J(\mathbb{Q})$ in $J(\mathbb{R})$ is typically g-dimensional (see Section 3), the p-adic closure of $J(\mathbb{Q})$ is often smaller (and it is this that makes Chabauty's method work over $\mathbb{Q}_p$):

Lemma 4.2. *Define* $r' := \dim \overline{J(\mathbb{Q})}$ *and* $r := \operatorname{rank} J(\mathbb{Q})$. *Then* $r' \le r$.

Proof. We have

$$r' = \dim \overline{J(\mathbb{Q})} = \dim \log \left(\overline{J(\mathbb{Q})} \right),$$

since log is a local diffeomorphism. Since log is continuous and $\overline{J(\mathbb{Q})}$ is compact,

$$\log \left(\overline{J(\mathbb{Q})} \right) = \overline{\log J(\mathbb{Q})}.$$

But the closure of any subgroup in $\mathbb{Q}_p^{\oplus g}$ is simply its $\mathbb{Z}_p$-span. Thus

$$r' = \operatorname{rank}_{\mathbb{Z}_p} (\mathbb{Z}_p \log J(\mathbb{Q})) \leq \operatorname{rank}_{\mathbb{Z}} \log J(\mathbb{Q}) \leq \operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) = r. \tag{3}$$

□

Remark 4.3. The second $\leq$ in (3) is an equality since log has finite kernel. But the first $\leq$ need not be, since $\mathbb{Z}$-independent points in $\log J(\mathbb{Q})$ need not be $\mathbb{Z}_p$-independent. For instance, $r' \leq \dim J = g$ always, but it can happen that $r > g$. Thus $r' < r$ is possible.

4.3. **Chabauty's theorem.** Now $X(\mathbb{Q}_p)$ is a 1-dimensional submanifold of $J(\mathbb{Q}_p)$. Suppose $r' < g$. The dimensions suggest (but do not immediately prove) that the intersection $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ should be (at most) 0-dimensional, and then it will be a discrete subset of a compact space $J(\mathbb{Q}_p)$, so the intersection will be finite, and its subset $X(\mathbb{Q})$ also will be finite. It is this that Chabauty proved.

Theorem 4.4 ([Cha41])**.** *Let X be a curve of genus $g \geq 2$ over $\mathbb{Q}$. Let J be the Jacobian of X. Let p be a prime, and let r and r' be as in Lemma 4.2. Suppose $r' < g$ (by Lemma 4.2 this is automatic if $r < g$). Then $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite (and hence so is $X(\mathbb{Q})$).*

Remark 4.5. Theorem 4.4 was the only significant result towards the Mordell conjecture in its original context (over $\mathbb{Q}$) in the decades before Faltings proved the conjecture in full.

Remark 4.6. Theorem 4.4 is weaker than Faltings' theorem in that the finiteness of $X(\mathbb{Q})$ is proved only in the case $r' < g$. But Theorem 4.4 has the advantage that it leads to an explicit upper bound on $\#X(\mathbb{Q})$ that is frequently sharp.

Remark 4.7.

We omit the proof of Theorem 4.4, but we will soon prove a refined version, Theorem 5.3. That theorem has additional hypotheses, used to get a particular bound on $\#X(\mathbb{Q})$, but without them one can still prove the finiteness of $X(\mathbb{Q})$.

In order to turn Theorem 4.4 into a practical method for bounding the number of rational points, one needs a way of bounding $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$. Roughly speaking, R. Coleman's method [Col85b] is to find functions (p-adic integrals of 1-forms) on $J(\mathbb{Q}_p)$ that vanish on $\overline{J(\mathbb{Q})}$ and restrict them to a parameterization of $X(\mathbb{Q}_p)$; E. V. Flynn's [Fly97] is to find algebraic functions on $J(\mathbb{Q}_p)$ that vanish on $X(\mathbb{Q}_p)$ and restrict them to a parameterization of $\overline{J(\mathbb{Q})}$.

5. Coleman's method

We will assume that X has good reduction, i.e., that X is the generic fiber of a smooth proper curve over $\mathbb{Z}_p$. In this case, J has good reduction too, and our embedding $X \hookrightarrow J$ mapping O to 0 induces an embedding of the reduction (i.e., special fiber) of X into the reduction of J. The set $X(\mathbb{F}_p)$ is to be interpreted as the set of $\mathbb{F}_p$-points of the reduction of X.

For the general case, in which X does not necessarily have good reduction, see Appendix A.

5.1. **p-adic integrals on the curve X.** One can show that the restriction map $H^0(J_{\mathbb{Q}_p}, \Omega^1) \to H^0(X_{\mathbb{Q}_p}, \Omega^1)$ induced by $X \hookrightarrow J$ is an isomorphism of $\mathbb{Q}_p$-vector spaces [Mil86, Proposition 2.2]. Suppose that ω_J restricts to ω. For $Q, Q' \in X(\mathbb{Q}_p)$, define

$$\int_Q^{Q'} \omega := \int_0^{[Q'-Q]} \omega_J.$$

The properties below follow from the corresponding properties of integration on J:

(i) If $Q_i, Q_i' \in X(\mathbb{Q}_p)$ are such that $\sum(Q_i' - Q_i)$ is the divisor of a rational function, or more generally $[\sum(Q_i' - Q_i)]$ is a torsion element of $J(\mathbb{Q}_p)$, then $\sum \int_{Q_i}^{Q_i'} \omega = 0$.

(ii) If $Q, Q' \in X(\mathbb{Q}_p)$ have the same reduction in $X(\mathbb{F}_p)$, then $\int_Q^{Q'} \omega$ can be calculated by expanding in power series in a local parameter t on the curve X.

By the definition of η_J in Section 4.1, the restriction $\eta := \eta_J|_{X(\mathbb{Q}_p)}$ is the function

$$\begin{aligned} \eta\colon X(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ Q &\mapsto \int_O^Q \omega. \end{aligned}$$

5.2. **Residue classes on X.** Recall that X has good reduction at p. We have a surjective reduction map $X(\mathbb{Q}_p) \twoheadrightarrow X(\mathbb{F}_p)$, and the preimage of a point of $X(\mathbb{F}_p)$ will be called a *residue class*. Fix a residue class, say above $\tilde{Q} \in X(\mathbb{F}_p)$. Let t be a rational function on X that reduces to a uniformizer on $X_{\mathbb{F}_p}$ at $\tilde{Q}$ (more precisely, t is a regular function on an open neighborhood of $\tilde{Q}$ in the smooth $\mathbb{Z}_p$-model of X, such that the restriction of t to the special fiber is a uniformizer at $\tilde{Q}$). Then one can show that

(1) The function t maps the residue class bijectively to $p\mathbb{Z}_p$. (This is related to Hensel's lemma.)

(2) If we assume ω is normalized by an element of $\mathbb{Q}_p^\times$ so that it reduces to a nonzero $\tilde{\omega} \in H^0(X_{\mathbb{F}_p}, \Omega^1)$, then ω on the residue class can be expressed as $w(t)\,dt$ for some power series $w(t) \in \mathbb{Z}_p[[t]]$ such that $w(t) \bmod p$ is nonzero.

(3) The function η on the residue class is represented by a series $I(t) \in \mathbb{Q}_p[[t]]$ (usually no longer in $\mathbb{Z}_p[[t]]$) whose derivative is $w(t)$.

See Section 8.3 for an example of a parameterization and a computation of $I(t)$.

5.3. **Counting zeros of integrals.** The following lemma, which is purely about p-adic power series, will be applied to an $I(t)$ as above.

Lemma 5.1. *Suppose that $f(t) \in \mathbb{Q}_p[[t]]$ is such that $f'(t) \in \mathbb{Z}_p[[t]]$. Let $m = \mathrm{ord}_{t=0}(f'(t) \bmod p)$. If $m < p-2$, then f has at most $m+1$ zeros in $p\mathbb{Z}_p$.*

Proof. Let $v\colon \mathbb{Q}_p \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ be the p-adic valuation. Write $f(t) = \sum a_i t^i$. The conditions on $f'(t)$ and m imply that $v(a_{m+1}) = 0$ and $v(a_i) \geq -v_p(i) > m+1-i$ for $i > m+1$. So the Newton polygon of f has no slopes less than or equal to -1 to the right of $(m+1, 0)$. By the theory of Newton polygons [Kob84, IV.4], f has at most $m+1$ zeros in $p\mathbb{Z}_p$. □

Remark 5.2. Using the full theory of Newton polygons, one can obtain other statements. Coleman gives an estimate without conditions on p and with $\mathbb{Q}_p$ replaced by an arbitrary p-adic field. Alternatively, one can impose further conditions on f: for example, if the coefficient of t^{p-1} in $f'(t)$ is in $p\mathbb{Z}_p$, then one need assume only $m < 2p-2$ to obtain the same conclusion. The point is to get the Newton polygon under control.

5.4. **A function on $J(\mathbb{Q}_p)$ vanishing on $\overline{J(\mathbb{Q})}$.** The proof of Lemma 4.2 shows that $\log \overline{J(\mathbb{Q})}$ is a $\mathbb{Z}_p$-module of rank r' contained in $T \simeq \mathbb{Q}_p^{\oplus g}$. Suppose that $r' < g$. Then there is a nonzero $\mathbb{Q}_p$-linear functional $\lambda\colon T \twoheadrightarrow \mathbb{Q}_p$ that vanishes on $\log \overline{J(\mathbb{Q})}$. By the duality between T and $H^0(J_{\mathbb{Q}_p}, \Omega^1)$, the functional λ corresponds to a particular nonzero

$\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$, which in turn gives rise to η_J, ω, η as above. By definition of log, the map η_J equals the composition

$$J(\mathbb{Q}_p) \xrightarrow{\log} T \xrightarrow{\lambda} \mathbb{Q}_p.$$

Hence η_J vanishes on $\overline{J(\mathbb{Q})}$. It follows that our particular ω satisfies

(iii) If $Q_i, Q_i' \in X(\mathbb{Q}_p)$ are such that $[\sum(Q_i' - Q_i)] \in \overline{J(\mathbb{Q})}$, then $\sum \int_{Q_i}^{Q_i'} \omega = 0$.

in addition to properties (i) and (ii) of Section 5.1, and that our η vanishes on $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$. It remains to bound the zeros of η.

5.5. **Coleman's theorem.** Coleman proved the following quantitative version of Theorem 4.4:

Theorem 5.3 ([Col85b])**.** *Let X, J, p, r' be as in Theorem 4.4. Suppose also that p is a prime of good reduction for X.*

(a) *Let ω be a nonzero 1-form in $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ satisfying conditions (i)–(iii) of Sections 5.1 and 5.4. Scale ω by an element of $\mathbb{Q}_p^\times$ so that it reduces to a nonzero 1-form $\tilde{\omega} \in H^0(X_{\mathbb{F}_p}, \Omega^1)$. Suppose $\tilde{Q} \in X(\mathbb{F}_p)$. Let $m = \operatorname{ord}_{\tilde{Q}} \tilde{\omega}$. If $m < p - 2$, then the number of points in $X(\mathbb{Q})$ reducing to $\tilde{Q}$ is at most $m + 1$.*

(b) *If $p > 2g$, then*

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

Proof.

(a) If there are no points in $X(\mathbb{Q})$ reducing to $\tilde{Q}$, we are done. Otherwise, fix $Q \in X(\mathbb{Q})$ reducing to $\tilde{Q}$. Then by (iii), $\int_Q^{Q'} \omega = 0$ for any $Q' \in X(\mathbb{Q})$ reducing to $\tilde{Q}$. By Section 5.2, $\int_Q^{Q'} \omega$ as a function of Q' can be expressed as a power series $I(t)$. Lemma 5.1 applied to $I(t)$ shows that $I(t)$ has at most $m + 1$ zeros, so there are at most $m + 1$ rational points Q' in the residue class.

(b) For $\tilde{Q} \in X(\mathbb{F}_p)$, let $m_{\tilde{Q}} = \operatorname{ord}_{\tilde{Q}} \tilde{\omega}$. By the Riemann-Roch theorem, the total number of zeros of $\tilde{\omega}$ in $X(\overline{\mathbb{F}}_p)$ is $2g-2$. Thus $\sum_{\tilde{Q} \in X(\mathbb{F}_p)} m_{\tilde{Q}} \leq 2g-2$. In particular, $m_{\tilde{Q}} \leq 2g-2 < p-2$ for each $\tilde{Q}$. Applying (a) to each $\tilde{Q}$ and summing yields

$$\#X(\mathbb{Q}) \leq \sum_{\tilde{Q} \in X(\mathbb{F}_p)} (m_{\tilde{Q}} + 1) = \#X(\mathbb{F}_p) + \sum_{\tilde{Q} \in X(\mathbb{F}_p)} m_{\tilde{Q}} \leq \#X(\mathbb{F}_p) + (2g - 2). \qquad \square$$

Remark 5.4. One can give an explicit bound even if $p \leq 2g$, but it is slightly worse in this case. One can also give a version for number fields other than $\mathbb{Q}$. See [Col85b, Theorem 4].

Remark 5.5. Theorem 5.3 requires $r' < g$, but if $r' < g - 1$, then one can improve the bound. For instance, if $p > 2g$, one can prove

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r'.$$

This is a special case of [Sto06, Corollary 6.7].

Remark 5.6. See Appendix A for a version of Theorem 5.3 in which X is not required to have good reduction at p.

6. Flynn's method for genus 2

Any curve X of genus 2 over $\mathbb{Q}$ is birational to an affine curve $y^2 = f(x)$ where $f(x) \in \mathbb{Q}[x]$ is squarefree and $\deg f \in \{5, 6\}$. There is a birational morphism $\mathrm{Sym}^2 X \twoheadrightarrow J$, and an embedding $J \hookrightarrow \mathbb{P}^{15}$ (given by the linear system $|4\Theta|$, where Θ is a theta divisor on J). Cassels and Flynn describe the embedding $J \hookrightarrow \mathbb{P}^{15}$ implicitly by giving explicit equations for the composition

$$X^2 \twoheadrightarrow \mathrm{Sym}^2 X \twoheadrightarrow J \hookrightarrow \mathbb{P}^{15}$$

in terms of the functions x_1, y_1, x_2, y_2 on X^2: see [CF96] for an exposition. Using this embedding, Flynn calculates explicit formal parameters for J and an explicit formal group law [Fly90]. Furthermore, there is an explicit rational function θ on J that vanishes on X. Thus, given points $a \in J(\mathbb{Q}_p)$ and $b \in J^1(\mathbb{Q}_p)$ (the kernel of reduction), Flynn can find the power series expansion in t for $\theta(a + tb)$, $t \in \mathbb{Z}_p$. Now, assuming that $\overline{J(\mathbb{Q})}$ has dimension 1, $\overline{J(\mathbb{Q})} \cap J^1(\mathbb{Q}_p) \simeq \mathbb{Z}_p$. Letting b be a generator for $\overline{J(\mathbb{Q})} \cap J^1(\mathbb{Q}_p)$ and letting a range over a set of coset representatives for $J(\mathbb{Q})/(J^1(\mathbb{Q}_p) \cap J(\mathbb{Q}))$, he can estimate the number of zeros of θ on $\overline{J(\mathbb{Q})}$. Thus, granted that one can obtain this set of coset representatives explicitly, everything here is explicit. For details, see [Fly97].

Remark 6.1. For this method we do not need full knowledge of $J(\mathbb{Q})$. It would suffice to have explicit generators of a finite-index subgroup $G \subseteq J(\mathbb{Q})$ having the same closure in $J(\mathbb{Q}_p)$. Any G of index prime to $p \cdot \#J(\mathbb{F}_p)$ has this property.

If we have a subgroup $G \subseteq J(\mathbb{Q})$ known to be of finite index, we can usually verify that its index is not divisible by a given prime ℓ (if true) by finding a homomorphism $J(\mathbb{Q}) \to B$ to a finite abelian group B killed by ℓ such that the induced map $G/pG \to B$ is injective. In practice, taking B as a product of $J(\mathbb{F}_q)/\ell J(\mathbb{F}_q)$ over a few primes q of good reduction will usually work.

Remark 6.2. Even in the genus-2 case, experience suggests that usually Coleman's method is easier to carry out than Flynn's. But see (3) in the next section.

7. Effectiveness

The method of Chabauty and Coleman may fail to determine the rational points. There are several problems:

(1) It may be difficult to bound r' because it may be computationally difficult to bound r via a Selmer group calculation.
(2) If $r' = g$ (which is likely if $r \geq g$), then $\overline{J(\mathbb{Q})}$ is open in $J(\mathbb{Q}_p)$, so the existence of one point in $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ yields infinitely many, so we get no finite bound on $\#X(\mathbb{Q})$. Let us suppose $r' < g$ from now on.
(3) In Coleman's method, the zero set of the integral of ω may be strictly larger than $\overline{J(\mathbb{Q})}$. Even if one uses integrals of several independent ω, equal in number to the codimension $g - r'$ of $\overline{J(\mathbb{Q})}$ in $J(\mathbb{Q}_p)$, so that the common zero set of the integrals is an analytic subgroup G of the correct dimension r', it could happen that $\overline{J(\mathbb{Q})}$ has index > 1 in G. This problem is not an issue in Flynn's method.

(4) It is not clear that $\#\left(X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}\right)$ can be computed exactly, even in principle. For instance, if the p-adic submanifolds $X(\mathbb{Q}_p)$ and $\overline{J(\mathbb{Q})}$ in $J(\mathbb{Q}_p)$ are tangent, it may be impossible with finite-precision calculations to prove that they intersect.

(5) Even if $\#\left(X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}\right)$ is computed exactly, the true value of $\#X(\mathbb{Q})$ could be smaller; in other words, some of the intersection points could be irrational points in $X(\mathbb{Q}_p)$. One can give a heuristic predicting that there exist such points in most situations when $r = g - 1$ and p is large.

In this case, the upper bound on $\#X(\mathbb{Q})$ obtained is not sharp, so $X(\mathbb{Q})$ cannot be determined without further work. On the other hand, the method can restrict the possible integer combinations of generators of $J(\mathbb{Q})$ that could lie on X, and hence provide enormous lower bounds on the height of any unknown points in $X(\mathbb{Q})$, giving strong evidence that no further points exist.

Remark 7.1. If r is $\leq g-2$ instead of just $< g$, then dimension counting suggests that $X(\mathbb{Q}_p)$ and $\overline{J(\mathbb{Q})}$ should not intersect at all. Maybe in this case the problems disappear for most choices of p, and the method becomes effective, though it seems hard to prove anything along these lines.

Remark 7.2. It is sometimes possible to show $r' < g$ directly, and to construct a logarithm vanishing on the rational points, without bounding r. See [McC94].

Remark 7.3. If $r' < g$ is violated, one can try combining the method of Chabauty and Coleman with one of the following two methods:

(1) Descent, which reduces the problem for the original curve to the problem of finding rational points on finite étale covers of higher genus. Special cases of this method go back to Fermat, and in this generality it appears first in [CW30].

(2) The "Mordell-Weil sieve" introduced in [Sch04] and studied further in [Fly04, Poo06]. The information given by this practical method is equivalent to the Brauer-Manin obstruction, at least if the Shafarevich-Tate group Ш(J) is finite.

See [Sto07] for recent speculations, as well as theorems relating descent information to the method of Chabauty and Coleman, the Mordell-Weil sieve, the Brauer-Manin obstruction, and Grothendieck's section conjecture.

8. Examples

8.1. **Example 1.** Let X be (the smooth projective model of) the genus-2 curve

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

This curve has good reduction at $p = 7$, and

$$X(\mathbb{F}_7) = \{(0,0), (1,0), (2,0), (5,0), (6,0), (3,6), (3,-6), \infty\}.$$

A descent calculation (first carried out in [GG93]) shows that $J(\mathbb{Q})$ has rank 1. Theorem 5.3(b) says $\#X(\mathbb{Q}) \leq 10$. In fact, equality holds:

$$X(\mathbb{Q}) = \{(0,0), (1,0), (2,0), (5,0), (6,0), (3,\pm 6), (10,\pm 120), \infty\}.$$

8.2. **Example 2.** We will use Coleman's method to recompute the rational points on a genus-2 curve first treated by Flynn's method in [FPS97]. Once we know the Mordell-Weil group of the Jacobian, the computations will be easy enough to do by hand.

Let X be (the smooth projective model of) the genus-2 curve $y^2 = f(x)$ where

$$f(x) := x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

(This curve is a moduli space parameterizing "quadratic polynomials equipped with a 5-cycle": see [FPS97].) Since $\deg f$ is even, and the leading coefficient is a square, there are two rational points ∞^+, ∞^- at infinity (i.e., not in the given affine patch). At these two points, the rational function y/x^3 takes the values $+1$ and -1, respectively. By [FPS97, Theorem 3], we have $\operatorname{rank} J(\mathbb{Q}) = 1$.

Remark 8.1. Though we do not need this, height estimates show that $[\infty^+ - \infty^-]$ generates $J(\mathbb{Q})$. For the relevant techniques, see [Sto02] and the references listed there.

Proposition 8.2. *There are exactly six rational points on X:*

$$X(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 1), (-3, \pm 1)\}.$$

Proof. Applying Theorem 5.3(b) directly would require $p > 2g = 4$. The smallest such p is 5, which gives a bound of 9 for $\#X(\mathbb{Q})$, not good enough.

Consider $p = 3$, however. The curve has good reduction at 3, and

$$X(\mathbb{F}_3) = \{\infty^+, \infty^-, (0, \pm 1)\},$$

where we use ∞^+ and so on to denote also the corresponding points on the reduction.

Let ω be as in Theorem 5.3(a), scaled to have nonzero reduction $\tilde{\omega}$. Because X is a genus-2 curve given by an equation $y^2 = f(x)$, $\tilde{\omega}$ is an $\mathbb{F}_3$-linear combination of $\frac{dx}{y}$ and $\frac{x\,dx}{y}$. Since X has at least two rational points in the residue class of $(0, 1)$, Theorem 5.3(a) implies that $\tilde{\omega}$ vanishes at $(0, 1) \in X(\mathbb{F}_3)$. Therefore (up to an irrelevant scalar multiple) $\tilde{\omega} = \frac{x\,dx}{y}$.

Theorem 5.3(a) now gives the correct bound (namely, 1) on the number of rational points in each residue class except for $(0, \pm 1) \in X(\mathbb{F}_3)$, where the hypothesis $m < p - 2$ is violated (since $m = 1$). At $\tilde{Q} := (0, 1)$, the parameter $t := x$ satisfies the requirements of Section 5.2. Expressing y as a power series in $\mathbb{Z}_p[[x]]$ gives

$$\begin{aligned} y &= \sqrt{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1} \\ &\equiv 1 + x^2 + \cdots \pmod 3, \end{aligned}$$

so

$$\tilde{\omega} = \frac{x\,dx}{y} = (x - x^3 + \cdots)dx.$$

Since the coefficient of x^2 in $\tilde{\omega}$ is 0, we are in the situation of Remark 5.2, where only $m < 2p - 2$ is required! Thus the conclusions of Lemma 5.1 and Theorem 5.3(a) hold even though their hypotheses are violated. The same argument works for $\tilde{Q} = (0, -1)$, so when we sum over residue classes we get the same bound as in Theorem 5.3(b), namely

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_3) + (2g - 2) = 4 + (2 \cdot 2 - 2) = 6.$$

□

This example may appear very special, and it is. For instance, every point of $X(\mathbb{F}_3)$ was the reduction of a point in $X(\mathbb{Q})$. Also we were fortunate to be able to apply Remark 5.2. Finally, we needed to know ω only mod 3 instead of to higher 3-adic precision.

8.3. **Example 3.** We continue with the curve in Section 8.2, to illustrate how to determine ω to higher precision and calculate some integrals. This was not necessary in this example to determine $X(\mathbb{Q})$, but similar calculations may be necessary in other examples.

Since $(0,1)$ and $(-3,1)$ are in the same residue class on X, we may compute integrals between them by expanding in power series in the uniformizing parameter x there:

$$\begin{aligned}
\int_{(0,1)}^{(-3,1)} \frac{dx}{y} &= \int_0^{-3} (1 + 6x + 5x^2 + 22x^3 + 22x^4 + 8x^5 + x^6)^{-1/2}\, dx \\
&= \int_0^{-3} (1 - 3x + 11x^2 - 56x^3 + \cdots)\, dx \qquad \text{(note: all coefficients are in } \mathbb{Z}_3) \\
&= \left(x - 3\frac{x^2}{2} + 11\frac{x^3}{3} - 56\frac{x^4}{4} + \cdots \right)\Big|_0^{-3} \\
&= (-3) - \frac{3}{2}(-3)^2 + \frac{11}{3}(-3)^3 - \frac{56}{4}(-3)^4 + \cdots \\
&\equiv 2 \cdot 3 + 3^4 \pmod{3^5}
\end{aligned}$$

and similarly

$$\begin{aligned}
\int_{(0,1)}^{(-3,1)} \frac{x\, dx}{y} &= \left(\frac{x^2}{2} - 3\frac{x^3}{3} + 11\frac{x^4}{4} - 56\frac{x^5}{5} + \cdots \right)\Big|_0^{-3} \\
&\equiv 2 \cdot 3^2 + 2 \cdot 3^3 \pmod{3^5}.
\end{aligned}$$

By (iii), $\int_{(0,1)}^{(-3,1)} \omega = 0$. Thus, up to a scalar multiple,

$$\omega = \epsilon \frac{dx}{y} + \frac{x\, dx}{y},$$

where $\epsilon \in \mathbb{Q}_3$ satisfies

$$(2 \cdot 3 + 3^4 + \cdots)\epsilon + (2 \cdot 3^2 + 2 \cdot 3^3 + \cdots) = 0,$$

where each $\cdots$ represents terms divisible by 3^5. Solving for ϵ yields

$$\epsilon \equiv 2 \cdot 3 + 3^2 + 2 \cdot 3^3 \pmod{3^4}, \tag{4}$$

The points of $X(\mathbb{Q}_3)$ reducing to $(0,1) \in X(\mathbb{F}_3)$ are

$$Q_t := (t, (1 + 6t + 5t^2 + 22t^3 + 22t^4 + 8t^5 + t^6)^{1/2})$$

for $t \in 3\mathbb{Z}_3$, where we take the square root whose power series begins with $+1$. By (iii), $\int_O^{(0,1)} \omega = 0$ no matter which $O \in X(\mathbb{Q})$ we use as basepoint, so the integral $I(t)$ defined in

Section 5.2 is

$$\begin{aligned} I(t) &:= \int_{(0,1)}^{Q_t} \omega \\ &= \int_{(0,1)}^{Q_t} \left(\epsilon \frac{dx}{y} + \frac{x\,dx}{y} \right) \\ &= \int_0^t (\epsilon + x)(1 + 6x + 5x^2 + 22x^3 + 22x^4 + 8x^5 + x^6)^{-1/2}\,dx \\ &= \epsilon t + (-3\epsilon + 1)\frac{t^2}{2} + (11\epsilon - 3)\frac{t^3}{3} + \cdots . \end{aligned}$$

Using (4), we can compute the Newton polygon of $I(t)$ and approximate the zeros in $3\mathbb{Z}_3$. In fact, from Section 8.2 we know already that there are two such zeros, and that they are 0 and -3 (corresponding to the rational points $(0,1)$ and $(-3,1)$).

Remark 8.3. The existence of two rational points in the residue class made it unnecessary to compute integrals between points in different residue classes. If we had not had sufficiently many rational points, we could have proceeded in one of the following ways:

(1) Recall that the integral on X is really the restriction of an integral on J. Inside each residue class of J corresponding to a point in $J(\mathbb{F}_p)$ of order prime to p there is a $\mathbb{Q}_p$-rational torsion point T, which can be used to set the constant of integration since $\int_0^T \omega_J = 0$. In residue classes of order divisible by p, a $\mathbb{Q}_p$-rational T might not exist, but if we work in $J(\overline{\mathbb{Q}}_p)$ instead, we will find a torsion point that can be used.
(2) Coleman's theory of p-adic integration [Col85a] gives a method for setting the constant of integration directly in terms of calculations on X, through the notion of a Teichmüller point.
(3) Ultimately we care only about the residue classes in $J(\mathbb{Q}_p)$ containing a point of $J(\mathbb{Q})$. For each of these residue classes, we compute an explicit divisor representing a point in $J(\mathbb{Q})$ in the residue class, and use it to set the constant of integration. This idea is due to J. Wetherell.

8.4. **Example 4.** Let X be the genus-2 curve $y^2 = x^6 + x^2 + 1$, motivated by problem 17 from book 6 of the *Arithmetica* of Diophantus. Since X admits a dominant morphism to the elliptic curve $y^2 = x^3 + x + 1$, the Jacobian J of X is isogenous over $\mathbb{Q}$ to the product of this elliptic curve and another elliptic curve (namely, $y^2 = x^3 + x^2 + 1$, as one can see by dividing both sides of the equation of X by x^6). It turns out that each of these two elliptic curves is of rank 1, so $r' = r = 2$. Thus the method of Chabauty and Coleman does not apply directly.

Nevertheless, Wetherell [Wet97] used descent to replace the problem with the problem for finite étale covers of higher genus to which the method could be applied. He succeeded in proving that

$$X(\mathbb{Q}) = \{(\pm 1/2, \pm 9/8), (0, \pm 1), \infty^+, \infty^-\}.$$

9. Elliptic Chabauty

The embedding $X \hookrightarrow J$ can be replaced by a morphism $X \to A$ to some other abelian variety A. By the Albanese property of the Jacobian, if such a morphism is normalized to

map O to 0, it will factor as $X \hookrightarrow J \to A$ for some homomorphism $J \to A$. We may assume that $J \to A$ is surjective (otherwise replace A by its image); then Chabauty's argument will apply if $\operatorname{rank} A(\mathbb{Q}) < \dim A$.

An important special case, noted in [FW99, Bru03], arises when there exists a dominant morphism $X_k \twoheadrightarrow E$ for an elliptic curve E over some finite extension k of $\mathbb{Q}$; then we get a map from X to the restriction of scalars $A := \operatorname{Res}_{k/\mathbb{Q}} E$, which is an abelian variety of dimension $[k : \mathbb{Q}]$ such that $A(\mathbb{Q}) \simeq E(k)$. Typically the induced map $J \to A$ will be surjective; in this case one needs $\operatorname{rank} E(k) < [k : \mathbb{Q}]$ to apply Chabauty's argument.

This special case is useful in practice, since computations with elliptic curves tend to be simpler than computations with Jacobians, even if the elliptic curve is over a larger field.

Appendix A. The case of bad reduction

In this appendix we prove Theorem A.5, a generalization of Theorem 5.3 in which it is not required that X have good reduction.

All schemes will be assumed to be locally noetherian. For any quasi-projective l.c.i. (local complete intersection) morphism $X \to Y$, [Liu02, Definition 6.4.7] gives a definition of the *canonical sheaf* $\omega_{X/Y}$, an invertible sheaf on X satisfying the following:

Proposition A.1. (a) *If $X \to Y$ is smooth of relative dimension r, there is a canonical isomorphism $\omega_{X/Y} \simeq \bigwedge^r \Omega^1_{X/Y}$, where $\Omega^1_{X/Y}$ is the sheaf of Kähler differentials.*

(b) *(Base change) Let $Y' \to Y$ be a morphism, let $X' := X \times_Y Y'$, and let $p\colon X' \to X$ be the first projection. If either $Y' \to Y$ or $X \to Y$ is flat, then $X' \to Y'$ is an l.c.i. and there is a canonical isomorphism $\omega_{X'/Y'} \simeq p^*\omega_{X/Y}$.*

Proof. Part (i) is immediate from the definitions: see [Liu02, Definitions 6.3.7 and 6.4.7]. For (ii), see [Liu02, Theorem 6.4.9]. □

Remark A.2. If in addition $X \to Y$ is flat of relative dimension r, the sheaf $\omega_{X/Y}$ agrees with the relative r-dualizing sheaf [Liu02, Theorem 6.4.32]. We will not need this.

Let K be a field of characteristic 0 with a discrete valuation v. Let R be the valuation ring, and let $\mathbb{F}$ be the residue field. Let π be a generator of the maximal ideal of R. Let X be a smooth, projective, geometrically integral curve of genus $g \geq 2$ over K with a K-point O. Construct the minimal proper regular model $\mathcal{X}$ over R of X. (We occasionally write R for $\operatorname{Spec} R$ if there is no chance of confusion.) Let $\mathcal{X}_s$ be the special fiber $\mathcal{X} \times_R \mathbb{F}$. By a *component* of $\mathcal{X}_s$ we mean an irreducible component D with the reduced subscheme structure; we let m_D be its multiplicity in $\mathcal{X}_s$. Let $\mathcal{X}^{\mathrm{smooth}}$ be the smooth locus of $\mathcal{X} \to R$, and let $\mathcal{X}_s^{\mathrm{smooth}}$ be the smooth locus of $\mathcal{X}_s \to \mathbb{F}$. The set $\mathcal{X}_s^{\mathrm{smooth}}(\mathbb{F})$ will play the role that $X(\mathbb{F}_p)$ played earlier: we define the *residue classes on X* to be the fibers of the reduction map

$$X(K) = \mathcal{X}(R) = \mathcal{X}^{\mathrm{smooth}}(R) \to \mathcal{X}_s^{\mathrm{smooth}}(\mathbb{F}).$$

Suppose $0 \neq w \in H^0(X, \Omega^1_{X/K})$. By parts (a) and (b) of Proposition A.1, we have

$$\Omega^1_{X/K} \simeq \omega_{X/K} \simeq \omega_{\mathcal{X}/R} \otimes_R K,$$

so we may view w as a meromorphic section of $\omega_{\mathcal{X}/R}$. The associated Cartier divisor $\mathcal{K}$ on $\mathcal{X}$ is called a *canonical divisor*: see [Liu02, Definition 9.1.34].

Let C be a multiplicity-1 component of $\mathcal{X}_s$. Let $C^{\text{smooth}} := C \cap \mathcal{X}^{\text{smooth}}$. Let $\mathcal{X}^C$ be the open subscheme of $\mathcal{X}^{\text{smooth}}$ obtained by deleting all components of its special fiber except for C^{smooth}. The divisor of π on $\mathcal{X}$ contains C with multiplicity $m_C = 1$, so multiplying w by an appropriate power of π yields a 1-form w^C such that C does not occur in the associated canonical divisor $\mathcal{K}^C$. Then $\mathcal{K}^C|_{\mathcal{X}^C}$ is effective, so we may view w^C as a global section of the sheaf $\omega_{\mathcal{X}^C/R}$, which by Proposition A.1(a) is isomorphic to $\Omega^1_{\mathcal{X}^C/R}$. Since C^{smooth} does not appear in this effective divisor, the restriction $w^C|_{C^{\text{smooth}}}$ may be viewed as a nonzero 1-form $\tilde{w}^C$ on C^{smooth}. Let n_C be the number of zeros (counted with multiplicity) of $\tilde{w}^C$ in $C^{\text{smooth}}(\mathbb{F})$.

We now use intersection theory on $\mathcal{X}$. A divisor on $\mathcal{X}$ is said to be *horizontal* if it is the closure in $\mathcal{X}$ of a divisor on X, and *vertical* if it is supported on $\mathcal{X}_s$: see [Liu02, Proposition 8.3.4 and Definition 8.3.5]. Every divisor can be expressed uniquely as the sum of a horizontal and a vertical divisor. Thus we can write $\mathcal{K} = H + V$ and $\mathcal{K}^C = H + V^C$, where H is a horizontal divisor and V and V^C are vertical divisors. (The horizontal part H is independent of C, since the forms w^C differ only by multiples of $\mathcal{X}_s$, the divisor of π.)

Lemma A.3. *For every multiplicity-1 component C of $\mathcal{X}_s$, we have $n_C \leq H.C$.*

Proof. Since C does not occur in V^C, we have

$$(H.C)_P = (\mathcal{K}^C.C)_P = \operatorname{ord}_P(\tilde{w}_C)$$

for all $P \in C^{\text{smooth}}(\mathbb{F})$. Therefore

$$n_C = \sum_{P \in C^{\text{smooth}}(\mathbb{F})} \operatorname{ord}_P(\tilde{w}_C) = \sum_{P \in C^{\text{smooth}}(\mathbb{F})} (H.C)_P.$$

Furthermore, since w^C restricts to a holomorphic differential on X, the divisor H is effective, so $(H.C)_P \geq 0$ for all closed points $P \in C$. Thus

$$\sum_{P \in C^{\text{smooth}}(\mathbb{F})} (H.C)_P \leq \sum_{P \in C} (H.C)_P \, [\mathbb{F}(P) : \mathbb{F}] = H.C,$$

where $\mathbb{F}(P)$ is the residue field of P, by the relation between local and global intersection numbers [Liu02, Theorem 9.1.2(a)]. □

Lemma A.4. *Let w, w^C, $\tilde{w}^C$, n_C be as above, for each multiplicity-1 component C of $\mathcal{X}_s$. Then*

$$\sum_{C \text{ of multiplicity } 1} n_C \leq 2g - 2.$$

Proof. Since H is an effective horizontal divisor, $H.D \geq 0$ for every component D of $\mathcal{X}_s$. Now

$$\begin{aligned}
\sum_{C \text{ of multiplicity } 1} n_C &\leq \sum_{C \text{ of multiplicity } 1} H.C && \text{(by Lemma A.3)} \\
&\leq \sum_{\text{all components } D} m_D(H.D) && \text{(since } H.D \geq 0 \text{ for all } D\text{)} \\
&= H.\mathcal{X}_s && \text{(since } \mathcal{X}_s = \textstyle\sum m_D D\text{)} \\
&= \mathcal{K}.\mathcal{X}_s && \text{(since } V.\mathcal{X}_s = 0 \text{ by [Liu02, Proposition 9.1.21(a)])} \\
&= 2g - 2 && \text{(by [Liu02, Proposition 9.1.35]).}
\end{aligned}$$

□

We now take $K = \mathbb{Q}_p$ to prove the analogue of Theorem 5.3:

Theorem A.5. *Let X, p, r' be as in Theorem 4.4, let $\mathcal{X}$ over $\mathbb{Z}_p$ be a minimal regular model for $X_{\mathbb{Q}_p}$, and let $\mathcal{X}_s$ over $\mathbb{F}_p$ be its special fiber.*

(1) Let ω be a nonzero 1-form in $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ satisfying conditions (i)–(iii) of Sections 5.1 and 5.4. Let C be a component of multiplicity 1 in $\mathcal{X}_s$, and define $C^{\mathrm{smooth}} := C \cap \mathcal{X}^{\mathrm{smooth}}$. Scale ω by a power of p so that it reduces to a nonzero 1-form $\tilde{\omega} \in H^0(C^{\mathrm{smooth}}, \Omega^1)$. Let $\tilde{Q} \in C^{\mathrm{smooth}}(\mathbb{F}_p)$. Let $m = \mathrm{ord}_{\tilde{Q}} \tilde{\omega}$. If $m < p-2$, then the number of points in $X(\mathbb{Q})$ reducing to $\tilde{Q}$ is at most $m+1$.

(2) If $p > 2g$, then

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}_s^{\mathrm{smooth}}(\mathbb{F}_p) + (2g-2).$$

Proof.

(1) Since $\tilde{Q}$ is a smooth point of $\mathcal{X}_s$, the discussion in Section 5.2 about expanding functions on residue classes applies equally to the residue class of $\tilde{Q}$, and then the proof of Theorem 5.3 goes through as before.

(2) Every point in $X(\mathbb{Q})$ reduces to some smooth point $\tilde{Q}$ in $\mathcal{X}_s(\mathbb{F}_p)$, and in particular to a point on some component of multiplicity 1. For such a component C, let n_C be as in Lemma A.4. Summing over all C of multiplicity 1, we get

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}_s^{\mathrm{smooth}}(\mathbb{F}_p) + \sum_C n_C \leq \#\mathcal{X}_s^{\mathrm{smooth}}(\mathbb{F}_p) + (2g-2),$$

by Lemma A.4.

□

Remark A.6. For another approach to Theorem A.5, see [LT02].

Question A.7. As mentioned in Remark 5.5, the $2g-2$ can be improved to $2r'$ in the good reduction case. M. Stoll asks: Can one combine the methods of [Sto06] with the methods in this appendix to prove the same statement in the bad reduction case? According to [Sto06, Remark 6.5], such a statement is true at least in the case where X is hyperelliptic.

References

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034) ↑4.1

[Bou98] Nicolas Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998. Translated from the French; Reprint of the 1989 English translation. MR1728312 (2001g:17006) ↑4.1, 4.1

[Bru03] Nils Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27–49. MR2011330 (2004j:11051) ↑9

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090 (97i:11071) ↑6

[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) ↑4, 4.4

[CW30] C. Chevalley and A. Weil, *Un théorème d'arithmétique sur les courbes algébriques*, Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195** (1930), 570–572. ↑1

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

[Col85b] ———, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR808103 (87f:11043) ↑4.3, 5.3, 5.4

[Elk94] Noam D. Elkies, *Heegner point computations*, Algorithmic number theory (Ithaca, NY, 1994), Lecture Notes in Comput. Sci., vol. 877, Springer, Berlin, 1994, pp. 122–133. MR1322717 (96f:11080) ↑1.2

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German). English translation: Finiteness theorems for abelian varieties over number fields, 9–27 in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, New York, 1986. Erratum in: Invent. Math. **75** (1984), 381. MR718935 (85g:11026a) ↑1

[Fly90] Eugene Victor Flynn, *The Jacobian and formal group of a curve of genus* 2 *over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. **107** (1990), no. 3, 425–441. MR1041476 (91b:14025) ↑6

[Fly97] E. V. Flynn, *A flexible method for applying Chabauty's theorem*, Compositio Math. **105** (1997), no. 1, 79–94. MR1436746 (97m:11083) ↑4.3, 6

[Fly04] ———, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466. MR2103661 ↑2

[FPS97] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-*2 *curve*, Duke Math. J. **90** (1997), no. 3, 435–463. MR1480542 (98j:11048) ↑8.2

[FW99] E. Victor Flynn and Joseph L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533. MR1734798 (2001g:11098) ↑9

[GG93] Daniel M. Gordon and David Grant, *Computing the Mordell-Weil rank of Jacobians of curves of genus two*, Trans. Amer. Math. Soc. **337** (1993), no. 2, 807–824. MR1094558 (93h:11057) ↑8.1

[Hes02] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR1890579 (2003j:14032) ↑2

[Ih02] Su-Ion Ih, *Height uniformity for algebraic points on curves*, Compositio Math. **134** (2002), no. 1, 35–57, DOI 10.1023/A:1020246809487. MR1931961 (2004g:11052) ↑1.1

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003 (86c:11086) ↑1, 5.3

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné; Oxford Science Publications. MR1917232 (2003g:14001) ↑A, A, A.2, A, A, A

[LT02] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. MR1892843 (2003d:11088) ↑A.6

[Maz92] Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45. MR1181085 (93j:14020) ↑3.1

[McC94] William G. McCallum, *On the method of Coleman and Chabauty*, Math. Ann. **299** (1994), no. 3, 565–596. MR1282232 (95c:11079) ↑7.2

[Mil86] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 167–212. MR861976 ↑5.1

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. **21** (1922), 179–192. ↑1

[Poo02] Bjorn Poonen, *Computing rational points on curves*, Number theory for the millennium, III (Urbana, IL, 2000), 2002, pp. 149–172. MR1956273 (2003k:11105) ↑1

[Poo06] ———, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. MR2293593 (2008d:11062) ↑2

[Sch04] Victor Scharaschkin, *The Brauer-Manin obstruction for curves* (December 2004). Preprint. ↑2

[Sko34] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8. Skand. Mat.-Kongr., Stockholm, 1934, pp. 163–188 (German). ↑4

[Sto02] Michael Stoll, *On the height constant for curves of genus two. II*, Acta Arith. **104** (2002), no. 2, 165–182. MR1914251 (2003f:11093) ↑8.1

[Sto06] ———, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661 ↑5.5, A.7

[Sto07] ———, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391. MR2368954 (2008i:11086) ↑7.3

[Sto09] ———, *On the average number of rational points on curves of genus* 2, February 24, 2009. Preprint, `arXiv:0902.4165`. ↑1.1

[Szp85] Lucien Szpiro, *Un peu d'effectivité*, Astérisque **127** (1985), 275–287 (French). Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). MR801928 ↑1

[Wal93] Michel Waldschmidt, *Transcendental numbers and functions of several variables*, Advances in number theory (Kingston, ON, 1991), 1993, pp. 67–80. MR1368411 (96i:11076) ↑3.1

[Wet97] Joseph Loebach Wetherell, *Bounding the number of rational points on certain curves of high rank*, 1997. Ph.D. thesis, University of California at Berkeley. ↑8.4

Department of Mathematics, University of Arizona, Tucson, AZ 85718
E-mail address: `wmc@math.arizona.edu`

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
E-mail address: `poonen@math.mit.edu`
URL: `http://math.mit.edu/~poonen/`