Invent. math. 148, 47–77 (2002)
Digital Object Identifier (DOI) 10.1007/s002220100186

Inventiones mathematicae

Thue equations and the method of Chabauty-Coleman

Dino Lorenzini, **Thomas J. Tucker**

Department of Mathematics, University of Georgia, Athens, GA 30602, USA
(e-mail: `lorenzini@math.uga.edu`, `ttucker@math.uga.edu`)

Oblatum 5-III-2001 & 15-VIII-2001
Published online: 18 January 2002 – © Springer-Verlag 2002

Let $\mathcal{O}_K$ be any domain with field of fractions K. Let $F(x, y) \in \mathcal{O}_K[x, y]$ be a homogeneous polynomial of degree n, coprime to y, and assumed to have unit content (i.e., the coefficients of F generate the unit ideal in $\mathcal{O}_K$). Assume that $\gcd(n, \mathrm{char}(K)) = 1$. Let $h \in \mathcal{O}_K$ and assume that the polynomial $hz^n - F(x, y)$ is irreducible in $\overline{K}[x, y, z]$. We denote by $X_{F,h}/K$ the nonsingular complete model of the projective plane curve $C_{F,h}/K$ defined by the equation $hz^n - F(x, y) = 0$. We shall assume in this article that $g(X_{F,h}) \geq 2$.

When K is a number field, Mordell's Conjecture (now Faltings' Theorem) implies that $|X_{F,h}(K)| < \infty$. Caporaso, Harris, and Mazur ([CHM, 1.1]) have shown that if Lang's conjecture for varieties of general type is true, then for any number field K, the size $|X(K)|$ of the set of K-rational points of any curve X/K of genus $g(X) \geq 2$ can be bounded by a constant depending only on $g(X)$. Prior to the paper [CHM], Mazur and others had asked whether $|X(K)|$ can be bounded by a constant depending only on $g(X)$ and the Mordell-Weil rank of X/K over K (that is, the rank of the group $J(K)$ of K-rational points of the jacobian J/K of X/K). These far-reaching questions are totally open. As we shall recall in Sect. 1, the method of Chabauty-Coleman sometimes yields a bound for $|X_{F,h}(K)|$ depending only on $g(X_{F,h})$ when it is known in advance that the Mordell-Weil rank of $X_{F,h}/K$ is small. Unfortunately, the Chabauty-Coleman method does not yield a bound for $|X_{F,h}(K)|$ independent of the coefficients of $hz^n - F(x, y)$ for all curves of the form $X_{F,h}$. It does, however, produce such a nice bound for the number of primitive integral solutions of $F(x, y) = h$, as we now explain.

Let $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$. A classical Thue equation is an equation $F(x, y) = h$ where $F(x, 1)$ does not have repeated roots. Thue showed in 1909 that such an equation has finitely many solutions $(x, y) \in \mathbb{Z}^2$ if $n \geq 3$.

Mathematics Subject Classification (2000): 11D41, 14G25, 11G30

Let us say that (x, y) is a primitive solution if $\gcd(x, y) = 1$. In this work, we are interested in the following open question raised for instance by Erdös, Stewart, and Tijdeman ([Ste, p. 816]). Let $N(F, h)$ denote the cardinality of the set

$$\{(x, y) \in \mathbb{Z}^2 \mid F(x, y) = h \text{ and } \gcd(x, y) = 1\}.$$

Is there a bound for $N(F, h)$ in terms of n only whenever $n \geq 3$? Two known results on $N(F, h)$ are as follows:

Theorem (Bombieri-Schmidt, [B-S]). *Assume that $F(x, 1)$ is irreducible. There exists a constant B_1, which can be taken to be 215 when n is sufficiently large, such that $N(F, h) \leq B_1 n^{w(h)+1}$, where $w(h)$ equals the number of prime factors of h.*

This bound depends on n and h. A generalization to the case where $F(x, 1)$ has distinct roots is given in [Ste, Theorem 1]. Let $r(X_{F,h})$ denote the Mordell-Weil rank over $\mathbb{Q}$ of the jacobian of $X_{F,h}/\mathbb{Q}$.

Theorem (Silverman, [Si1]). *Assume that $F(x, 1)$ has distinct roots in $\overline{\mathbb{Q}}$. There exists an ineffective constant $h(F)$ such that for all n^{th} power-free $h > h(F)$, the bound $N(F, h) \leq n^{2n^2}(8n^3)^{r(X_{F,h})}$ holds.*

For a fixed F, this bound depends only on n and $r(X_{F,h})$, but only works for h sufficiently large. For an improvement in the special case where $F(x, 1)$ has a root in $\mathbb{Q}$, see [Fuj]. Our main theorem is:

Theorem 3.9. *If $r(X_{F,h}) < g(X_{F,h})$, then $N(F, h) \leq 2n^3 - 2n - 3$.*

This bound only holds when $r(X_{F,h})$ is small, but when it holds, it depends only on n. We are able to refine our method in some special cases to obtain a bound of the form $N(F, h) \leq O(n^2)$. There is no empirical evidence that would indicate that $N(F, h)$ cannot always be bounded by $O(n)$.

Both [B-S] and [Si1] make use of diophantine approximation methods, and in particular make use of the Thue-Siegel-Roth theorem on approximations of algebraic numbers. The proof of Theorem 3.9, by contrast, does not involve diophantine approximation; it relies instead on the method of Chabauty-Coleman. In order to use this method to bound $|X_{F,h}(\mathbb{Q})|$, one needs to pick a prime p and compute enough of a regular model $\mathcal{X}/\mathbb{Z}_p$ of $X_{F,h}/\mathbb{Q}_p$ to be able to bound the number N_1 of components of multiplicity 1 in the special fiber $\overline{\mathcal{X}}/\mathbb{F}_p$. The number N_1 is not, in general, bounded by a constant depending only on $g(X_{F,h})$. Hence, this method does not always enable us to bound $|X_{F,h}(\mathbb{Q})|$ in terms of $g(X_{F,h})$ only. Surprisingly, however, it is possible to bound, in terms of n only, the number of reduction classes in the special fiber of a regular model $\mathcal{X}/\mathbb{Z}_p$ of the primitive solutions of $F(x, y) = h$. Let $F(x, 1) = c\prod_{i=1}^{s}(x - \alpha_i)^{n_i}$ in $\overline{\mathbb{Q}}[x]$, and set $d^*(F) := c^{s(s-1)}\prod_{i\neq j}(\alpha_i - \alpha_j) \in \mathbb{Z}$. To obtain a bound on the number of reduction classes in the special fiber of the primitive solutions, the most difficult case to be treated is when $p \mid d^*(F)$ and $p \mid h$. In this case, our main result is:

Theorem 3.5/3.8. *Let $X_{F,h}/\mathbb{Q}$ be such that for some prime $p > n$, $p \mid d^*(F)$ and $p \mid h$. Let $\mathcal{X}/\mathbb{Z}_p$ be the regular minimal model of $X_{F,h}/\mathbb{Q}_p$. Let N denote the set of reductions in the special fiber $\mathcal{X}_{\mathbb{F}_p}$ of the solutions of $F(x, y) = h$ in $\mathbb{Z}_p^2$ with $\gcd(x, y) = 1$. Then $|N| \leq snp$.*

In the cases where p fails to divide both h and $d^*(F)$, similar results are obtained in the proofs of 3.1, 3.2, and 3.3. Determining whether $J(\mathbb{Q})$ has rank less than $g(X_{F,h})$ is in general very difficult. There is no known algorithm that provably determines the Mordell-Weil rank of a jacobian, even for elliptic curves. Upper bounds for the rank are obtainable, at least in theory, by computing the size of a suitable Selmer group. The Mordell-Weil rank in the case of superelliptic curves of the form $y^p = f(x)$ with p prime is treated in [P-S] and [Sch]. A computational implementation in the case $p = 2$ and $\deg(f) = 6$ is discussed in [St3]. There are at this time no educated guesses regarding the proportion of isomorphism classes of non-singular plane Thue curves of degree n whose Mordell-Weil rank over $\mathbb{Q}$ is less than $(n-1)(n-2)/2$. Similarly, fixing F, there are no general results on the proportion of the n-th power free integers h such that the Mordell-Weil rank of $X_{F,h}$ is less than $g(X_{F,h})$. To our knowledge, it is not known whether the set of such integers is always infinite, or even non-empty. On a more positive note, we can produce in 3.10 infinitely many explicit examples of Thue equations where the bound given in Theorem 3.9 holds.

The method of Chabauty-Coleman, when applicable, very often also provides bounds for $|X_{F,h}(\mathbb{Q})|$ and not just for $N(F, h)$. In particular, we show:

Theorem 3.1/3.2. *Let $p > n$ be a prime with $p \nmid d^*(F)$. Assume that $r(X_{F,h}) < g(X_{F,h})$. Then $|X_{F,h}(\mathbb{Q})| \leq np + \frac{p-1}{p-2}(2g - 2)$. In particular, there always exists such a prime p with $p \leq \max(2n, 2d^*(F))$, so $|X_{F,h}(\mathbb{Q})|$ is bounded by a constant depending only on F, and not on h.*

This explicit theorem is a special case of [Si2, Theorem 1], which states that if X/K is any curve of genus $g \geq 2$ over a number field, and X_h/K is any twist of X, then $|X_h(K)|$ can be bounded in terms of a constant $c = c(X/K)$ and the Mordell-Weil rank of X_h/K.

This paper is organized as follows. In the first section, we refine the method of Chabauty-Coleman so that it can be applied to any regular model over $\mathbb{Z}_p$ of a curve $X/\mathbb{Q}$ of genus $g \geq 1$ with $p^2 > 2g + 1$. In the second section, we describe some regular models of the curves $X_{F,h}$. We then prove in the third section our main theorem on primitive solutions of Thue equations using these models.

1. The method of Chabauty-Coleman

Let K be any number field with a place v over a prime p. Let K_v denote the completion of K at v, with uniformizer π and residue field $\mathbb{F}_q$, where q is a power of p. Let X/K be a smooth proper geometrically connected curve of genus $g \geq 1$, with Jacobian J/K. When the rank of $J(K)$ is less than g, the method of Coleman-Chabauty allows one to bound $|X(K)|$ in terms of the number of zeros of a well-chosen p-adic analytic function $\lambda_w : X(K_v) \to K_v$. Coleman [Co2, 0.ii] considered the case where the curve X has good reduction at v (that is, where X/K_v has a smooth model $\mathcal{X}$ over $\mathcal{O}_{K_v}$). McCallum [McC1] applied the method of Chabauty-Coleman at primes of bad reduction in the special case of Fermat curves. In Theorem 1.1 below, we show that the method of Chabauty-Coleman produces bounds for $|X(K)|$ even when X/K is not assumed to have good reduction. At the 1999 Arizona Winter School, McCallum suggested that a slight variant of [Co2, 0.ii] should hold on any regular model $\mathcal{X}/\mathcal{O}_{K_v}$; we prove that his suggestion is indeed correct in 1.11.

Let A/K be any abelian variety of dimension g. We will write $\Gamma(A, \Omega_{A/K_v})$ for the module of global sections over A_{K_v} of the sheaf of differentials $\Omega_{A_{K_v}/K_v}$. As a p-adic Lie group, $A(K_v)$ is endowed with a logarithm map

$$\log : A(K_v) \to \mathrm{Hom}(\Gamma(A, \Omega_{A/K_v}), K_v) \cong K_v^g,$$

as we shall recall below, borrowing from [Wet]. The *Chabauty rank of A at v*, denoted by $\mathrm{Chab}(A, K, v)$, is the dimension of the K_v-subvector space of K_v^g generated by the elements of $\log(A(K))$. Note that since log is a homomorphism, $\mathrm{Chab}(A, K, v)$ is less than or equal to the Mordell-Weil rank of $A(K)$. Define the *Chabauty rank of a curve X/K at v* to be $\mathrm{Chab}(J, K, v)$, and denote it by $\mathrm{Chab}(X, K, v)$. Let $\overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$ denote the subset of non-singular $\mathbb{F}_q$-points of the special fiber $\overline{\mathcal{X}}$ of a proper flat model $\mathcal{X}/\mathcal{O}_{K_v}$ of X/K_v. Let $r : X(K_v) \to \overline{\mathcal{X}}(\mathbb{F}_q)$ denote the reduction map. The main theorem of this section is:

Theorem 1.1. *Let X/K be a curve of genus $g \geq 1$ defined over a number field K with completion K_v unramified over $\mathbb{Q}_p$. Assume that* $\mathrm{Chab}(J, K, v) < g$. *Let d be a positive integer such that $p > d$ and $p^d > 2g-1+d$. Then, for any subset $\mathcal{U} \subset \overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$ of the special fiber $\overline{\mathcal{X}}$ of a model $\mathcal{X}/\mathcal{O}_{K_v}$ of X/K_v, we have*

$$|r^{-1}(\mathcal{U}) \cap X(K)| \leq |\mathcal{U}| + \left(\frac{p-1}{p-d}\right)(2g-2).$$

Our theorem applies whenever p is such that $p^{p-1} - p > 2g-2$. The only obstacle to applying the Chabauty-Coleman method to even smaller primes is finding a suitable variant of Lemma 1.5. The key to the method of Chabauty-Coleman is the remark that if $\mathrm{Chab}(A, K, v) < g$, then there exists a linear projection $\theta : K_v^g \to K_v$ such that the composition $\theta \circ \log :$

$A(K_v) \to K_v$ is an analytic function λ that vanishes on $A(K)$. As we shall recall, it turns out that there always exists a differential $\eta \in \Gamma(A, \Omega_{A/K_v})$ such that $d(\lambda) = \eta$. Given a curve X/K and a map $j : X \to J$ defined over K, one can consider the associated analytic function $\lambda \circ j : X(K_v) \to J(K_v) \to K_v$ and the differential $j^*(\eta)$. A bound for $|X(K)|$ is obtained by bounding the number of zeros of $\lambda \circ j$ in terms of the number of zeros of $j^*(\eta)$. The proof of 1.1 is postponed to 1.8.

We begin by fixing some notation. Let V/K_v be a proper, geometrically integral variety of dimension e. A *model* $\mathcal{V}/\mathcal{O}_{K_v}$ of V/K is an integral scheme $\mathcal{V}$ and a flat proper morphism $\mathcal{V} \to \mathrm{Spec}(\mathcal{O}_{K_v})$ such that the generic fiber of this morphism is the given map $V \to \mathrm{Spec}(K)$. Let $\overline{\mathcal{V}} := \mathcal{V} \times_{\mathrm{Spec}(\mathcal{O}_{K_v})} \mathrm{Spec}\,(\mathcal{O}_{K_v}/(\pi))$ denote the special fiber of $\mathcal{V}$. Since $\mathcal{V}$ is proper, we have a reduction map $r : \mathcal{V}(\overline{K}_v) \longrightarrow \overline{\mathcal{V}}(\overline{\mathbb{F}}_q)$, which sends points in $\mathcal{V}(K_v)$ to points in $\overline{\mathcal{V}}(\mathbb{F}_q)$. More precisely, let P be a point in $\mathcal{V}(\overline{K}_v)$. The image of P under the map r is the intersection of $\overline{\mathcal{V}}$ with the closure of the image of P in V_{K_v}. This map is well-defined because the closure of the image of P in V_{K_v} corresponds to the prime spectrum of the ring of integers $\mathcal{O}_L$ in some finite extension L/K_v, and such a ring $\mathcal{O}_L$ is local when K_v is complete. If $Q \in \overline{\mathcal{V}}(\mathbb{F}_q)$, denote by $D_Q(L)$ the set $r^{-1}(Q) \cap V(L)$. When $P \in V(K_v)$, the set $D_{r(P)}(\overline{K}_v)$ is called the residue class of P. For simplicity, we may denote the set $D_Q(K_v)$ simply by D_Q.

Let now $\mathscr{A}$ be the Néron model over $\mathcal{O}_{K_v}$ of an abelian variety A/K. The scheme $\mathscr{A}$ is not in general proper over $\mathcal{O}_{K_v}$, but the natural map $\mathscr{A}(\mathcal{O}_{K_v}) \to A(K_v)$ is always an isomorphism. We use this map to define a reduction map $r : \mathscr{A}(K_v) \to \overline{\mathscr{A}}(\mathbb{F}_q)$.

Denote by $\overline{\mathcal{V}}_{ns}(\mathbb{F}_q)$ the set of points of $\overline{\mathcal{V}}(\mathbb{F}_q)$ which are smooth points of the map $\mathcal{V} \to \mathrm{Spec}\,(\mathcal{O}_{K_v})$. Since the field $\mathbb{F}_q$ is also the ground field for $\overline{\mathcal{V}}$, we find that the set $\overline{\mathcal{V}}_{ns}(\mathbb{F}_q)$ is in fact the set of regular points of $\overline{\mathcal{V}}$ with residue field $\mathbb{F}_q$. Let $Q \in \overline{\mathcal{V}}_{ns}(\mathbb{F}_q)$. Each point $P \in V(K_v)$ for which $r(P) = Q$ gives rise to a prime $\mathscr{P}$ in $\mathcal{O}_{\mathcal{V},Q}$ of height e. Since $\mathcal{O}_{\mathcal{V},Q}$ is a regular local ring, $\mathscr{P}$ can be generated by e elements $z_1, \ldots, z_e$. We will call these z_i *local coordinates* for P. Each z_i can be evaluated at any other point $P' \in D_Q(\overline{K}_v)$ by setting $z_i(P')$ equal to the image of z_i in $\mathcal{O}_{\mathcal{V},Q}/\mathscr{P}'$, where $\mathscr{P}'$ is the prime in $\mathcal{O}_{\mathcal{V},Q}$ corresponding to P'. A set of local coordinates defines a bijection between $D_Q(K_v)$ and $\pi\mathcal{O}_{K_v} \times \cdots \times \pi\mathcal{O}_{K_v}$ (where the product contains e terms). Indeed, let $\hat{\mathcal{O}}_{\mathcal{V},Q}$ denote the completion of the ring $\mathcal{O}_{\mathcal{V},Q}$ with respect to the prime ideal $\mathscr{P}$. One shows that the canonical map from $\mathrm{Hom}_{\mathcal{O}_{K_v}}(\hat{\mathcal{O}}_{\mathcal{V},Q}, \mathcal{O}_{K_v})$ to $\mathrm{Hom}_{\mathcal{O}_{K_v}}(\mathcal{O}_{\mathcal{V},Q}, \mathcal{O}_{K_v})$ is a bijection. We say that the formal power series

$$\sum_{i_1,\ldots,i_e \geq 0} a_{i_1,\ldots,i_e} z_1^{i_1} \cdots z_e^{i_e} \in K_v[[z_1, \ldots, z_e]]$$

converges in $D_Q(\overline{K}_v)$ if, for any $P' \in D_Q(\overline{K}_v)$ with residue field L_w, the sum

$$\sum_{i_1,\dots,i_e\geq 0} a_{i_1,\dots,i_e} z_1(P')^{i_1}\cdots z_e(P')^{i_e}$$

converges in L_w. This power series defines an analytic map from $D_Q(K_v)$ to K_v. We shall use repeatedly the following important fact: Given any analytic map λ on $V(K_v)$ which, when restricted to $D_Q(K_v)$, is equal to an analytic map given as above by a power series expansion converging on $D_Q(K_v)$, then the determination of the zeros of λ on $D_Q(K_v)$ is equivalent to the determination of the zeros of the power series on the set $(\pi\mathcal{O}_{K_v})^e$.

Proposition 1.2. *Let A be an abelian variety of dimension g and let $\eta \in \Gamma(A, \Omega_{A/K_v})$. Then there exists a unique map $\lambda_\eta : A(K_v) \longrightarrow K_v$ such that: a) λ_η is analytic, b) $d(\lambda_\eta) = \eta$, and c) λ_η is a group homomorphism. Let $\mathcal{A}$ be the Néron model of A over $\mathcal{O}_{K_v}$. Let $P \in A(K_v)$, and choose a set $z_1, \dots, z_g$ of local coordinates for P. Then there is a nonzero $t \in \mathcal{O}_{K_v}$ (independent of P) such that $t\lambda_\eta$ restricted to $D_{r(P)}(K_v)$ has a local power series expansion*

$$t\lambda_\eta = b_0 + \sum_{i_1,\dots,i_g\geq 0} b_{i_1,\dots,i_g} z_1^{i_1}\cdots z_g^{i_g}$$

with $b_0 \in K_v$ and $i_\ell b_{i_1,\dots,i_g} \in \mathcal{O}_{K_v}$ for $\ell = 1,\dots,g$. This power series expansion converges on $D_{r(P)}(\overline{K}_v)$.

Proof. Let 0 denote the identity in $\mathcal{A}(K_v)$. The multiplication law $\mathcal{A}\times_{\mathrm{Spec}(\mathcal{O}_{K_v})}\mathcal{A}\to\mathcal{A}$ gives a map $\mathcal{O}_{\mathcal{A},r(0)} \longrightarrow \mathcal{O}_{\mathcal{A},r(0)}\otimes_{\mathcal{O}_{K_v}}\mathcal{O}_{\mathcal{A},r(0)}$. Since $\mathcal{O}_{\mathcal{A},r(0)}$ is a smooth local ring, we can choose a set of local coordinates at 0, and obtain by completion the formal group law $\mathcal{F}$:

$$\mathcal{O}_{K_v}[[z_1,\dots,z_g]] \longrightarrow \mathcal{O}_{K_v}[[z_1,\dots,z_g]]\otimes_{\mathcal{O}_{K_v}}\mathcal{O}_{K_v}[[z_1,\dots,z_g]].$$

Let $\eta \in \Gamma(A, \Omega_{A/K_v})$. Thus η is an invariant differential on A (see, e.g., [Sha], page 168). There is a nonzero $t \in \mathcal{O}_{K_v}$ such that $t\eta \in \Gamma(\mathcal{A}, \Omega_{\mathcal{A}/\mathcal{O}_{K_v}})$. The invariant differential $t\eta$ induces an invariant differential for the formal group law, in the sense of [Hon], page 216, and can be written as

$$t\eta = \sum_{\ell=1}^{g}\sum_{i_1,\dots,i_g\geq 0} a_{i_1,\dots,i_g,\ell} z_1^{i_1}\cdots z_g^{i_g} dz_\ell$$

with $a_{i_1,\dots,i_g,\ell}\in\mathcal{O}_{K_v}$. It is shown in [Hon], 1.3, that a formal integral $G_{t\eta}\in K_v[[z_1,\dots,z_g]]$ of $t\eta$ exists. We choose $G_{t\eta}$ such that $G_{t\eta}(0) = 0$. Such a formal integral converges on the kernel of the reduction $D_{r(0)}$, because $\lim_{n\to\infty} x^n/|n|_v = 0$ for any $0 \leq x < 1$. Taking a basis $\eta_1,\dots,\eta_g$ of the invariant differentials, Honda describes in [Hon], Theorem 1, a strict isomorphism f of formal groups over K_v between $\mathcal{F}$ and the additive formal group of dimension g. Evaluating on points, we obtain a group homomorphism

$$f : D_{r(0)}(K_v) = \mathcal{F}(\pi\mathcal{O}_{K_v}) \longrightarrow K_v^g,$$

given by $P \mapsto (G_{\eta_1}(P), \ldots, G_{\eta_g}(P))$. Since $t\eta$ can be written in terms of $\eta_1, \ldots, \eta_g$, it follows that there exists a projection $\rho : K_v^g \to K_v$ such that the composition $\rho \circ f : D_{r(0)}(K_v) \to K_v$ is a group homomorphism given by the power series $G_{t\eta}$.

Let H be any open subgroup of $A(K_v)$, such as $D_{r(0)}(K_v)$. Since $A(K_v)$ is compact, $[A(K_v) : H]$ is finite, so for any $P \in A(K_v)$, there is some positive integer c_P such that $c_P P \in H$. Thus, any homomorphism φ from H to a K_v-vector space W extends uniquely to a homomorphism $\tilde{\varphi} : A(K_v) \to W$ by setting $\tilde{\varphi}(P) := \varphi(P)/c_P$. In particular, the homomorphism $G_{t\eta}$ extends uniquely to a homomorphism $\lambda_{t\eta} : A(K_v) \to K_v$. We let $\lambda_\eta := \frac{1}{t}\lambda_{t\eta}$.

Let $P \in A(K_v)$, and let t_P denote the map $P' \mapsto P' + P$ on $A(K_v)$. Writing $t_P^*\lambda_\eta$ for the composition $\lambda_\eta \circ t_P$, we see that $d(t_P^*\lambda_\eta) = d(\lambda_\eta + \lambda_\eta(P)) = d\lambda_\eta$ so the differential $d\lambda_\eta$ must be translation invariant. Hence, it must be equal to η on all of $A(K_v)$ since η is also translation invariant.

To show that λ_η has the desired convergent power series expansion at any point in $A(K_v)$ (which implies in particular that λ_η is analytic), we note that if $P \in A(K_v)$, then for all P' with $r(P) = r(P')$, we can write $\lambda_\eta(P') = \lambda_\eta(P' - P) + \lambda_\eta(P)$, with $(P - P') \in D_{r(0)}(K_v)$. Let us denote as ϕ_P the map from $\mathcal{O}_{\mathcal{A},r(0)}$ to $\mathcal{O}_{\mathcal{A},r(P)}$ induced by t_P and use $z_i' := \phi_P(z_i)$, $i = 1, \ldots, g$, as local coordinates on $D_{r(P)}(K_v)$. Then, λ_η expanded on $D_{r(P)}(K_v)$ using the coordinates $z_1', \ldots z_g'$ has the 'same' power series expansion as its power series expansion on $D_{r(0)}(K_v)$ using $z_1, \ldots, z_g$, except with a different constant term (namely, $\lambda_\eta(P)$ instead of 0).

The function λ_η is unique because any analytic homomorphism $\lambda : A(K_v) \longrightarrow K_v$ with $d(\lambda) = \eta$ must have the same power series expansion as λ_η in some neighborhood of 0 and must therefore equal λ_η on this neighborhood; since any neighborhood contains an open subgroup of finite index in $A(K_v)$ this means that $\lambda = \lambda_\eta$ everywhere. This concludes the proof of 1.2. Further information about p-adic integration can be found in [Co1] and [Cz].

We define

$$\log : A(K_v) \longrightarrow \mathrm{Hom}(\Gamma(A, \Omega_{A/K_v}), K_v)$$

by the formula $\log(P)(\eta) := \lambda_\eta(P)$. This map is well-defined since λ_η is unique. It is clearly a group homomorphism since the maps λ_η are. Let

$$\theta_\eta : \mathrm{Hom}(\Gamma(A, \Omega_{A/K_v}), K_v) \longrightarrow K_v$$

denote the evaluation at η. Then $\lambda_\eta = \theta_\eta \circ \log$. It follows from the definition of Chabauty rank that whenever $\mathrm{Chab}(A, K, v) < g$, there is a nonzero differential $\eta \in \Gamma(A, \Omega_{A/K_v})$ such that $\lambda_\eta(A(K)) = 0$.

Proposition 1.3. *Let X/K_v be a smooth proper geometrically connected curve of genus $g \geq 1$. Given a differential $\omega \in \Gamma(X, \Omega_{X/K_v})$, there is an analytic map*

$$\lambda_\omega : X(K_v) \longrightarrow K_v \tag{1}$$

such that $d(\lambda_\omega) = \omega$. Moreover, let $\mathcal{X}$ be any model for X over $\mathcal{O}_{K_v}$ and assume that $\overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$ is not empty. Let $P \in X(K_v)$ be any point with $r(P) \in \overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$. Let u be a local coordinate for P. Then there is a nonzero $t \in \mathcal{O}_{K_v}$ (independent of P) such that $t\lambda_\omega$ has a local power series expansion converging on $D_{r(P)}(K_v)$ of the form

$$t\lambda_\omega = a_0 + \sum_{m=1}^{\infty} \frac{a_m}{m} u^m \tag{2}$$

with $a_0 \in K_v$ and $a_m \in \mathcal{O}_{K_v}$ for $m > 0$.

Proof. Let J/K_v denote the jacobian of X/K_v. We use $P \in X(K_v)$ to obtain an embedding $j : X \to J$ defined over K_v. This embedding induces an isomorphism j^* from $\Gamma(J, \Omega_{J/K_v})$ to $\Gamma(X, \Omega_{X/K_v})$, so every $\omega \in \Gamma(X, \Omega_{X/K_v})$ is $j^*(\eta)$ for some $\eta \in \Gamma(J, \Omega_{J/K_v})$. The function $\lambda_\omega := \lambda_\eta \circ j$ is an analytic map from $X(K_v)$ to K_v and $d(\lambda_\omega) = d(\lambda_\eta \circ j) = j^* d\lambda_\eta = j^*\eta\omega$. We may choose a non-zero $t \in \mathcal{O}_{K_v}$ for which $t\lambda_\eta$ has a power series expansion as in Proposition 1.2; we will use this expansion to derive power series expansions of the form (2) for $t\lambda_\omega$.

Let $\mathcal{X}^{sm}$ denote the subset of $\mathcal{X}$ that is smooth over $\mathcal{O}_{K_v}$. Denote the Néron model of J by $\mathcal{J}$. The universal property of Néron models implies that the map j extends to an $\mathcal{O}_{K_v}$-map $\phi : \mathcal{X}^{sm} \longrightarrow \mathcal{J}$. (In particular, $\phi \times_{\mathcal{O}_{K_v}} K_v = j$.) It follows that $j(D_{r(P)}(K_v))$ is contained in $D_{r(j(P))}(K_v)$. We also obtain a map of local rings $\mathcal{O}_{\mathcal{J},\phi(r(P))} \to \mathcal{O}_{\mathcal{X},r(P)}$ since ϕ is a $\mathcal{O}_{K_v}$-morphism. Completing $\mathcal{O}_{\mathcal{J},\phi(r(P))}$ at the prime corresponding to $j(P)$ and $\mathcal{O}_{\mathcal{X},r(P)}$ at the prime corresponding to P gives a map $\psi : \mathcal{O}_{K_v}[[z_1, \ldots, z_g]] \longrightarrow \mathcal{O}_{K_v}[[u]]$, which yields a power series for $t\lambda_\omega$ as

$$t\lambda_\omega = b_0 + \sum_{i_1,\ldots,i_g \geq 0} b_{i_1,\ldots,i_g} \psi\big(z_1^{i_1}\big) \cdots \psi\big(z_g^{i_g}\big).$$

Furthermore, since $d(t\lambda_\omega) = j^*(t\eta)$, this power series must have a derivative of the form

$$\phi^*\Big(\sum_{\ell=1}^{g} \sum_{i_1,\ldots,i_g \geq 0} a_{i_1,\ldots,i_g,\ell} z_1^{i_1} \cdots z_g^{i_g} dz_\ell\Big)$$

with $a_{i_1,\ldots,i_g,\ell} \in \mathcal{O}_{K_v}$. Computing the above out (by the chain rule) gives

$$d(\lambda_{t\omega}) = \sum_{\ell=1}^{g} \sum_{i_1,\ldots,i_g \geq 0} a_{i_1,\ldots i_g,\ell} \psi(z_1)^{i_1} \cdots \psi(z_g)^{i_g} \frac{\partial z_\ell}{\partial u} du$$

which is in $\mathcal{O}_{K_v}[[u]]du$ since $\frac{\partial z_\ell}{\partial u} \in \mathcal{O}_{K_v}[[u]]$ (since it is simply the formal derivative of $\psi(z_\ell) \in \mathcal{O}_{K_v}[[u]]$). Thus, $t\lambda_\omega$ has a power series at P that is the formal integral of a power series with $\mathcal{O}_{K_v}$ coefficients, as in (2).

1.4. Let us now prove a simple lemma that will allow us to bound the number of zeros of λ_ω in terms of information about local power series expansions. Similar arguments can be found in [Co1], [Co2], [McC1], [McC2], and [Wet]. For simplicity, let us assume that $K_v/\mathbb{Q}_p$ is unramified. Let $\lambda : X(K_v) \longrightarrow K_v$ be a p-adic analytic function. Let $P \in X(K_v)$ with reduction $r(P) = Q$ in $\mathcal{X}$ and let u be a local coordinate at P. This local coordinate induces a bijection $D_Q(K_v) \to p\mathcal{O}_{K_v}$. For simplicity, we shall denote $D_Q(K_v)$ by D_Q. Suppose that λ has a power series expansion of the form $\lambda = a_0 + \sum_{m=1}^\infty \frac{a_m}{m} u^m$, where $a_0 \in K_v$, $a_m \in \mathcal{O}_{K_v}$, and $v(a_m) = 0$ for some m, convergent on D_Q. We can thus consider λ as a power series $\lambda(u)$ in the variable u, converging on the disk $|u| \leq |p|$. The p-adic Weierstrass preparation theorem ([Kob, Thm. 14]) allows us to bound the number of zeros of λ in D_Q. As this result is most easily stated on the disc $\mathcal{O}_{K_v}$, we will make the substitution $z := u/p$. This gives us a power series expansion for λ in z as

$$\lambda(z) = a_0 + \sum_{m=1}^{\infty} \frac{a_m}{m} p^m z^m,$$

converging for all $z \in \mathcal{O}_{K_v}$. Let us make the definitions

$$I(\lambda, D_Q) := \min\{m \mid v(a_m) \leq 0\},$$
$$J(\lambda, D_Q) := \min\{m \mid v(a_\ell p^\ell/\ell) > v(a_m p^m/m) \quad \text{for all } \ell > m\},$$

(in the above formula when $m = 0$, read $a_m p^m/m$ to be a_0). The Weierstrass preparation theorem then implies that the number of $z \in \mathcal{O}_{K_v}$ for which $\lambda(z) = 0$ is at most $J(\lambda, D_Q)$. It also follows from this theorem that when $I(\lambda, D_Q) > 0$, the number of $z \in \mathcal{O}_{K_v}$ for which $\lambda'(z) = 0$ is at most $I(\lambda, D_Q) - 1$ (where $\lambda'(z)$ denotes the formal derivative of $\lambda(z)$).

Lemma 1.5. *Let $p > 2$. Assume that $K_v/\mathbb{Q}_p$ is unramified. Write $I(\lambda, D_Q)$ simply as I. Let d be any integer such that $p \geq d$ and $p^d > I + d$.*

a) *Suppose that $p \mid I+1, I+2, \ldots,$ or $I+d-1$. Then $J(\lambda, D_Q) \leq I+d-1$.*
b) *Suppose that $p \nmid I+1, I+2, \ldots,$ and $I+d-1$. Then $J(\lambda, D_Q) \leq I$.*

Proof. Consider the function $\rho(x) := x - \log_p x$. It is clear that $\rho(m)$ is a lower bound for $v(a_m p^m/m)$ when $a_m \in \mathcal{O}_{K_v}$, since $v(x) \leq \log_p x$. The derivative of $\rho(x)$ is $\rho'(x) = 1 - 1/x \ln p$, so when $p > 2$, the function ρ is increasing for $x \geq 1$. Note that $\rho(I+d) = I + d - \log_p(I+d) > I$, since $I+d < p^d$. Similarly, for all $1 \leq i \leq d-1$, we have $\rho(I+i+d) > I+i-1$. Let us now prove a). Suppose that $p \mid I+i$ for some $0 < i \leq d-1$. We find that

$$v\left(\frac{a_{I+i}}{I+i} p^{I+i}\right) \leq I + i - 1.$$

Since $p \mid I+i$, and $d-1<p$, we find that $p \nmid I+j$, for all $j = i+1,\dots,i+d-1$. Hence, $v(\frac{a_{I+j}p^{I+j}}{I+j}) \geq I+j > I+i-1$ for all $j=i+1,\dots,i+d-1$. As we mentioned above,

$$v\left(\frac{a_{I+i+d}\,p^{I+i+d}}{I+i+d}\right) \geq \rho(I+i+d) > I+i-1.$$

Since $\rho(x)$ is increasing for $x>1$, it follows that for all $j \geq I+i+1$, we have $v(a_j p^j/j) > I+i-1$. Hence, $J(\lambda, D_Q) \leq I(\lambda, D_Q)+d-1$.

Part b) is clear when $I=0$. To prove b) when $I>0$, it is easy to see that we need only show that $v(\frac{a_j}{j}p^j) > I$ for all $j>I$, since $v(\frac{a_I p^I}{I}) \leq I$ for $I>0$. Now, since $p \nmid I+i$ for $i=1,\dots,d-1$, we find that

$$v\left(\frac{a_{I+i}}{I+i}p^{I+i}\right) \geq I+i > I.$$

Recall that $\rho(I+d) > I$. Using the fact that $\rho(x)$ is increasing for $x \geq 1$, we see that $\rho(j) > I$ for all $j>I$, and Lemma 1.5 is proved.

Let us fix some notation to be used in our next proposition. Let $\mathcal{X}/\mathcal{O}_{K_v}$ be any model of X/K_v. Let $Q \in \overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$. Denote by $\mathcal{O}_Q$ the local ring $\mathcal{O}_{\mathcal{X},Q}$. Let $P_0 \in X(K_v)$ be a point reducing to Q. Choose a local coordinate u for P_0. Let $\hat{\mathcal{O}}_Q$ denote the completion of the ring $\mathcal{O}_Q$ at the prime (u). One easily shows that the natural map from the ring $\mathcal{O}_{K_v}[[u]]$ of formal power series to the ring $\hat{\mathcal{O}}_Q$ (which sends u to u) is an isomorphism. It is also easy to check that the $\hat{\mathcal{O}}_Q$-module of relative differentials $\Omega_{\hat{\mathcal{O}}_Q/\mathcal{O}_{K_v}}$ is generated by du. Any differential $\omega \in \Omega_{\mathcal{O}_Q/\mathcal{O}_{K_v}}$ can thus be written as a power series $\omega = \sum_{m=0}^{\infty} a_{m+1}u^m du$ with $a_m \in \mathcal{O}_{K_v}$ for all $m \in \mathbb{Z}_{\geq 0}$.

Since Q is a nonsingular point of $\overline{\mathcal{X}}$, the local ring $\mathcal{O}_{\overline{\mathcal{X}},Q}$ is a discrete valuation ring, and we denote by v_Q its valuation. For any $P \in X_{K_v}$, we denote by v_P the valuation of the local ring $\mathcal{O}_{X_{K_v},P}$. A differential $\omega \in \Gamma(\mathcal{X}, \Omega_{\mathcal{X}/\mathcal{O}_{K_v}})$ pulls back to a differential $i^*\omega$ via the natural map $i : \mathcal{X}_{K_v} \longrightarrow \mathcal{X}$ from the generic fiber $\mathcal{X}_{K_v}$ of $\mathcal{X}$ to $\mathcal{X}$. We denote by $(i^*\omega)_0$ the divisor of zeros of $i^*\omega$, and we shall write $(i^*\omega)_0 = \sum_P v_P(i^*\omega)P$.

Proposition 1.6. *Let X/K_v be a smooth proper geometrically connected curve of genus $g \geq 1$. Let $\mathcal{X}/\mathcal{O}_{K_v}$ be a model of X/K_v. Keep the notation introduced above. Let $\omega \in \Gamma(\mathcal{X}, \Omega_{\mathcal{X}/\mathcal{O}_{K_v}})$ and let $Q \in \overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$. Then there exists an element $t \in K_v$ (dependent on Q) such that $t\omega \in \Gamma(\mathcal{X}, \Omega_{\mathcal{X}/\mathcal{O}_{K_v}})$ and has a local power series expansion (when viewed as an element of $\Omega_{\hat{\mathcal{O}}_Q/\mathcal{O}_{K_v}}$)*

$$t\omega = \sum_{m=0}^{\infty} a_{m+1}u^m du, \tag{3}$$

with $a_{m+1} \in \mathcal{O}_{K_v}$ for all $m \in \mathbb{Z}_{\geq 0}$, such that

$$\min\{m \mid v(a_{m+1}) = 0\} = \sum_{r(P)=Q} [K_v(P) : K_v] v_P(i^*\omega), \tag{4}$$

where the sum is taken over all points P of the scheme X_{K_v} such that the intersection of the closure of P in $\mathcal{X}$ with $\overline{\mathcal{X}}$ is Q.

Proof. Since $\Omega_{\mathcal{X}/\mathcal{O}_{K_v}}$ is locally free of rank 1 at Q because Q is a smooth point by hypothesis, the element du is a generator of the stalk $\Omega_{\mathcal{O}_Q/\mathcal{O}_{K_v}}$ of $\Omega_{\mathcal{X}/\mathcal{O}_{K_v}}$ at Q. We can write the stalk of ω at Q as $s\,du$, where $s \in \mathcal{O}_Q$. Factor s as $s = \gamma_1^{\ell_1} \cdots \gamma_n^{\ell_n} \pi^{\ell'}$, where the γ_j are generators for primes corresponding to points P_j on the generic fiber of $\mathcal{X}$. It is not hard to see that $v_{P_j}(i^*\omega) = \ell_j$. Indeed, one obtains the local ring $\mathcal{O}_{X_{K_v}, P_j}$ localizing $\mathcal{O}_Q$ at the prime ideal generated by γ_j, so we see that the ideal generated by s in $\mathcal{O}_{X_{K_v}, P_j}$ is just $\mathcal{M}_{P_j}^{\ell_j}$, where $\mathcal{M}_{P_j}$ is the maximal ideal in $\mathcal{O}_{X_{K_v}, P_j}$; since f pulls back to a generator for the stalk of $\Omega_{\mathcal{X}_{K_v}/K_v}$ at P_j, $s f$ must pull back to a differential with order of vanishing equal to $v_{P_j}(s) = \ell_j$ for all j.

After dividing s by $\pi^{\ell'}$ we obtain an element s_1 that is not in $\pi\mathcal{O}_Q$ (thus $t = \pi^{-\ell'}$ will satisfy the statement of the proposition). Now complete $\mathcal{O}_Q$ at (u). We obtain a power series expansion $s_1 du = \sum_{m=0}^{\infty} a_{m+1} u^m du$. It is easy to check that $\hat{\mathcal{O}}_Q/(\pi)$ is the completion of $\mathcal{O}_Q/(\pi)$ at the maximal ideal (u). Thus the valuation v_Q of $\mathcal{O}_Q/(\pi)$ extends to a valuation on $\hat{\mathcal{O}}_Q/(\pi)$, again denoted by v_Q, and identified with ord_u. Denoting by ϕ_π the map taking $\hat{\mathcal{O}}_Q$ to $\hat{\mathcal{O}}_Q/(\pi)$, it is clear that

$$\min\{m \mid v(a_m) = 0\} = v_Q(\phi_\pi(s_1)).$$

Since $v_Q(\phi_\pi(s_1)) = \sum_{j=1}^{n} \ell_j v_Q(\phi_\pi(\gamma_j))$, it suffices to show that $v_Q(\phi_\pi(\gamma_j)) = [K_v(P_j) : K_v]$. This follows from the fact that:

$$\begin{aligned} v_Q(\phi_\pi(\gamma_j)) &= \dim_{\mathbb{F}_q}\left((\mathcal{O}_Q/\pi\mathcal{O}_Q)/(\phi_\pi(\gamma_j))\right) = \mathrm{rank}_{\mathcal{O}_{K_v}}(\mathcal{O}_Q/\gamma_j\mathcal{O}_Q) \\ &= [K_v(P_j) : K_v], \end{aligned}$$

since $\mathcal{O}_Q/\gamma_j\mathcal{O}_Q$ is a free $\mathcal{O}_{K_v}$-module. This concludes the proof of 1.6.

Let us now apply Lemma 1.5 and Proposition 1.6 to the sort of p-adic analytic function that arises in the Chabauty-Coleman method.

Proposition 1.7. *Let X/K be a curve of genus $g \geq 1$ defined over a number field K with completion K_v unramified over $\mathbb{Q}_p$. Let $\mathcal{X}/\mathcal{O}_{K_v}$ be any model for X/K_v, and let $\mathcal{U} \subset \overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$. Let d be any positive integer such that $p > d$ and $p^d > 2g - 1 + d$. If λ_ω is as in* (1), *then*

$$\left|r^{-1}(\mathcal{U}) \cap \lambda_\omega^{-1}(0)\right| \leq |\mathcal{U}| + \left(\frac{p-1}{p-d}\right)(2g-2). \tag{5}$$

Proof. Choose $Q \in \mathcal{U}$. For any nonzero element $t \in K_v$, multiplying λ_ω by t will not change the zeros of λ_ω. Furthermore, $\lambda_{t\omega} = t\lambda_\omega$ (since $d\lambda_{t\omega} = d(t\lambda_\omega)$ and $\lambda_{t\omega}(0) = 0 = t\lambda_\omega(0)$), so $|r^{-1}(Q)\cap\lambda_\omega^{-1}(0)| = |r^{-1}(Q)\cap\lambda_{t\omega}^{-1}(0)|$. Thus, we may choose $t_Q \in K_v$ and apply Proposition 1.6 to obtain a power series expansion of the form (3) for which equation (4) holds (since $\omega \in \Gamma(X, \Omega_{X/K_v})$ in (1), we first choose t' so that $t'\omega \in \Gamma(\mathcal{X}, \Omega_{\mathcal{X}/\mathcal{O}_{K_v}})$ and apply 1.6 to $t'\omega$). We denote by $Z(\omega, Q)$ the sum $\sum_{r(P)=Q}[K_v(P) : K_v]v_P(i^*\omega)$ appearing in the statement of Proposition 1.6. When $I(\lambda_{t_Q\omega}, D_Q) > 0$, we must have $Z(\omega, Q) = I(\lambda_{t_Q\omega}, D_Q) - 1$, since $d(\lambda_{t\omega}) = t\omega$. Since

$$\sum_{Q\in\mathcal{U}} Z(\omega, Q) \le \sum_{P\in X_{K_v}} [K_v(P) : K_v]v_P(i^*\omega) = 2g - 2 < p^d - d - 1,$$

we find that $I(\lambda_{t_Q\omega}, D_Q) < p^d - d$, and we can apply Lemma 1.5 (note that the hypothesis on the coefficients of λ in 1.4 is satisfied since $Z(w, Q) \ge 0$). When $I(\lambda_{t_Q\omega}, D_Q) = 0$, then λ_ω is invertible and $|D_Q \cap \lambda_\omega^{-1}(0)| = 0$. We obtain

$$\begin{aligned}\left|r^{-1}(\mathcal{U}) \cap \lambda_\omega^{-1}(0)\right| &\le \sum_{\substack{Q\in\mathcal{U}\\ |D_Q\cap\lambda_\omega^{-1}(0)|>0}} \left|D_Q \cap \lambda_\omega^{-1}(0)\right| \\ &\le \sum_{Q\in\mathcal{U}} J(\lambda_{t_Q\omega}, D_Q) \\ &\le \sum_{\substack{p|(Z(\omega,Q)+2),\dots,\\ \text{or } p|(Z(\omega,Q)+d)}} (Z(\omega, Q) + d) \\ &\quad + \sum_{\substack{p\nmid(Z(\omega,Q)+i),\\ i=2,\dots,d}} (Z(\omega, Q) + 1).\end{aligned} \tag{6}$$

If $p \mid (Z(\omega, Q) + i)$ for some $i = 2, \dots, d$, then $Z(\omega, Q) \ge p - d$. Since $\sum_{Q\in\mathcal{U}} Z(\omega, Q) \le 2g - 2$, there are at most $(2g - 2)/(p - d)$ points $Q \in \overline{\mathcal{X}}_{ns}(\overline{\mathbb{F}}_q)$ for which $p \mid (Z(\omega, Q) + i)$ for some $i = 2, \dots, d$. Plugging this information into (6) shows that $|r^{-1}(\mathcal{U})\cap\lambda_\omega^{-1}(0)|$ is bounded as desired by

$$\sum_{Q\in\mathcal{U}} Z(\omega, Q) + |\mathcal{U}| + (d - 1)\frac{2g - 2}{p - d} \le |\mathcal{U}| + \left(1 + \frac{d - 1}{p - d}\right)(2g - 2).$$

We are now ready prove Theorem 1.1.

1.8. Proof of 1.1. Each differential $\eta \in \Gamma(J, \Omega_{J/K_v})$ gives rise to a homomorphism $\lambda_\eta : J(K_v) \longrightarrow K_v$. Since $\mathrm{Chab}(J, K, v) < g$, there is a nonzero η for which $\lambda_\eta(J(K)) = 0$. We may assume that $X(K)$ contains a point Q, as otherwise our assertion is trivial. Hence, we may embed $X(K_v)$ into J

via the mapping $j : X \to J$, which sends $P \in X(K_v)$ to the class of $P - Q$. Now, η pulls back to a differential ω on X, and λ_η restricts to a function λ_ω that vanishes on $X(K)$ (because j sends points in $X(K)$ to points in $J(K)$). Applying Proposition 1.7 then gives the desired result.

1.9. Note that if an abelian variety A/K is K-isogenous to a product $\prod A_i$, then $\mathrm{Chab}(A, K, v) = \sum \mathrm{Chab}(A_i, K, v)$. Thus, the method of Chabauty-Coleman can be applied to A if and only if $\mathrm{Chab}(A_i, K, v) < \dim(A_i)$ for some i. We will use this fact later.

Note that the Chabauty rank $\mathrm{Chab}(A, K, v)$ is zero if and only if the Mordell-Weil rank of A/K is zero. When this is the case, we can strengthen Theorem 1.1 as follows.

Proposition 1.10. *Let X/K be a curve of genus $g \geq 1$ defined over a number field K with completion $K_v/\mathbb{Q}_p$ such that $v(p) < p - 1$. Let $\mathcal{X}/\mathcal{O}_{K_v}$ be any regular model for X/K_v. If the Mordell-Weil rank of X/K is zero, then $|X(K)| \leq |\overline{\mathcal{X}}_{ns}(\mathbb{F}_q)|$.*

Proof. We claim that for each $Q \in \overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$, the set $r^{-1}(Q)$ contains at most one K-rational point of X. Indeed, suppose that P and P' belong to $r^{-1}(Q) \cap X(K)$. Then $P' - P$ belongs to the kernel of reduction of $J(K)$, which does not contain any torsion point other than 0 (see for instance [Ser, LG 4.25–4.26]). Thus, $P' = P$.

The following statement, suggested by McCallum at the 1999 Arizona Winter School, is obtained from Theorem 1.1 by considering $d = 1$ and $\mathcal{U} = \overline{\mathcal{X}}_{ns}(\mathbb{F}_q)$.

Corollary 1.11. *Let X/K be a curve of genus $g \geq 1$ defined over a number field K with completion K_v unramified over $\mathbb{Q}_p$. Let $\mathcal{X}/\mathcal{O}_{K_v}$ be any regular model for X/K_v. If $p > 2g$ and* $\mathrm{Chab}(J, K, v) < g$*, then $|X(K)| \leq |\overline{\mathcal{X}}_{ns}(\mathbb{F}_q)| + 2g - 2$.*

In view of 1.10 and 1.11, it is natural to wonder, under the hypotheses of 1.11, whether the bound for $|X(K)|$ can be made to depend on the precise value of $\mathrm{Chab}(J, K, v)$, such as a bound of the form $|X(K)| \leq |\overline{\mathcal{X}}_{ns}(\mathbb{F}_q)| + 2\mathrm{Chab}(J, K, v)$.

2. Constructing regular models of curves

Let K be a field with a discrete valuation v_K. Let $\mathcal{O}_K$ denote the ring of integers of K, with maximal ideal (π_K) and residue field k. Let $p := \mathrm{char}(k)$. Let X/K be the nonsingular proper model of the plane curve C/K given by a homogeneous equation $f(x, y, z) \in \mathcal{O}_K[x, y, z]$ with unit content. Explicitly resolving the singularities of $\mathrm{Proj}(\mathcal{O}_K[x, y, z]/(f))$ to produce a regular model $\mathcal{X}/\mathcal{O}_K$ of X/K is very difficult in general; in this article, we use instead a quotient construction to obtain information on a regular model of X/K. This construction can be summarized as follows. It may happen that over a Galois extension L/K, a normal model $\mathcal{Y}/\mathcal{O}_L$ of X_L/L can be described. If the Galois group $\mathrm{Gal}(L/K)$ acts on $\mathcal{Y}$, lifting its action on $\mathrm{Spec}(\mathcal{O}_L)$, then we may consider the quotient $\mathcal{Y}/\mathrm{Gal}(L/K)$ as a scheme over $\mathrm{Spec}(\mathcal{O}_K)$. The scheme $\mathcal{Y}/\mathrm{Gal}(L/K)$ is a normal model of X/K and, thus, a desingularization $\rho : \mathcal{X} \to \mathcal{Y}/\mathrm{Gal}(L/K)$ leads to a regular model $\mathcal{X}/\mathcal{O}_K$ of X/K. A key feature of this method is the fact that when $\mathcal{Y}$ is regular, the singularities of $\mathcal{Y}/\mathrm{Gal}(L/K)$ are quotient singularities and that when L/K is tame, such singularities are well-understood and, thus, a model for X/K can be described.

To apply the Chabauty-Coleman method to the case of the curves $X_{F,h}/\mathbb{Q}$, we need a description of a regular model for $X_{F,h}$ over $\mathbb{Z}_p^{unr}$. These models are obtained in two steps, first by describing a model of $X_{F,h}$ over a well-chosen extension $L/\mathbb{Q}_p^{unr}$, and then by using the quotient construction to obtain a model over $\mathbb{Z}_p^{unr}$. The second step is done in the next section, in Propositions 3.1, 3.2, 3.3, and 3.5. In this section, we first construct regular models of the curves $X_{F,h}$ over the appropriate extensions L, and then we review for the convenience of the reader the details of the quotient construction. To deal with the cases where $F(x,1)$ does not have simple roots, we introduce the following notation. Let $F(x,1) = c\prod_{i=1}^{s}(x-\alpha_i)^{n_i}$ in $\overline{K}[x]$. Let

$$d^*(F) := c^{s(s-1)} \prod_{i \neq j} (\alpha_i - \alpha_j) \in \mathcal{O}_K.$$

When a curve has potentially good reduction after a tame extension L/K, such as the superelliptic curves $X := X_{F,h}$ with $\pi_K \nmid d^*(F)$ and $p > n$ (see 2.1 below), the quotient construction is applied to the smooth minimal model $\mathcal{Y}/\mathcal{O}_L$ of X_L/L, where L/K is chosen large enough to ensure that X_L/L has good reduction. In this case, the resulting model for X/K is not hard to describe and this description is reviewed in 2.15.

The core of this section is the study of the difficult case where $\pi_K \mid d^*(F)$ and $\pi_K \mid h$. In this case, we are not able to describe a proper regular model for $X_{F,h}$ over $\mathbb{Z}_p^{unr}$, but we will construct in 3.5 just enough of a regular model to be able to bound the number of residue classes of primitive integral solutions to the Thue equation $F(x,y) = h$. Let L/K be the splitting field over K of the polynomial $F(x,1)$, and let $\mathcal{Y}/\mathcal{O}_L$ be the normalization of the model

$$\mathcal{C} := \mathrm{Proj}\ \mathcal{O}_L[x,y,z]/(hz^n - F(x,y)).$$

The quotient construction is applied to $\mathcal{Y}/\mathcal{O}_L$ in 3.5. In this section, we describe some smooth open affine subsets of the model $\mathcal{Y}$ and prove in 2.6 the crucial result that the reductions of the primitive integral solutions are contained in at most n such open subsets. Let us start with a couple of preliminary lemmas.

Lemma 2.1. *Assume that* $\mathrm{char}(k) \nmid n$. *Let* $X := X_{F,h}/K$.

a) *If* $\pi_K \nmid d^*(F)$ *and* $\pi_K \nmid h$, *then* X/K *has good reduction.*
b) *If* $\pi_K \nmid d^*(F)$ *and* $\pi_K \mid h$, *then* X/K *achieves good reduction over* $L := K(\sqrt[n]{h})$.

Proof. Consider the model $\mathcal{C}/\mathcal{O}_K$ given by $\mathrm{Proj}(\mathcal{O}_K[x,y,z]/(hz^n - F(x,y))$ and its normalization $\mathcal{C}^{nor}/\mathcal{O}_K$. The generic fiber of $\mathcal{C}^{nor}$, that is, the curve $X_{F,h}$, has genus equal to $2g(X) - 2 = n(s-2) - \sum_{i=1}^{s} \gcd(n, n_i)$. If $g(X) = 0$, then X/K has obviously good reduction over $\mathcal{O}_K$. Assume then that $g(X) > 0$. Recall that $\deg(F)F = x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y}$. Thus, at a singular point (x_0, y_0) of the reduction $\overline{F} - \overline{h} = 0$, we find that $\overline{\deg(F)F}(x_0, y_0) = 0$. Since $\overline{h} \neq 0$, $p \mid \deg(F)$ when the reduction has a singular point. When $\pi_K \nmid h$ and $\pi_K \nmid d^*(F)$, we find that the geometric genus of $\mathcal{C}_k^{nor}$ is equal to $g(X)$. Thus, $\mathcal{C}_k^{nor}$ is non-singular since its arithmetical genus is equal to the genus of X. It follows that $\mathcal{C}^{nor}/\mathcal{O}_K$ is the (minimal) regular model of X/K.

If $\pi_K \mid h$, consider the change of variables $z' = \sqrt[n]{h}z$, $x' = x$ and $y' = y$. Then $\mathrm{Proj}(\mathcal{O}_L[x', y', z']/(z'^n - F(x', y')))$ is a model for X_L/L. Hence, we may apply a) to find that X_L/L has good reduction. This concludes the proof of 2.1.

For most of the applications that we have in mind, the residue field $\mathcal{O}_K/(\pi_K)$ will be $\mathbb{F}_p$, and we will assume that $p > n$. The following lemma shows that we may assume, under these hypotheses, that $F(x, 1)$ is monic.

Lemma 2.2. *Assume that* $|\mathcal{O}_K/(\pi_K)| > s$. *Then, up to a change of variable, we may assume that* $F(x, 1)$ *is monic in* $\mathcal{O}_K[x]$.

Proof. Let L/K be an extension such that $F(x, y) = \prod_{i=1}^{s}(\beta_i x - \rho_i y)^{n_i}$, with β_i, ρ_i in $\mathcal{O}_L$. The substitution $y' = y + ux$ yields $F(x, y') = \prod_{i=1}^{s}((\beta_i + \rho_i u)x - \rho_i y)^{n_i}$. Since the coefficients of F have no common factor, we must have $\min(v_L(\beta_i), v_L(\rho_i)) = 0$ for each i. Thus, for each i, we will have $\rho_i u + \beta_i \in \mathcal{O}_L^*$ for all but one choice of residue class for u. We have s expressions $\rho_i u + \beta_i$ and more than s residue classes in $\mathcal{O}_K/(\pi_K)$, so we can choose $u \in \mathcal{O}_K$ with $\rho_i u + \beta_i \in \mathcal{O}_L^*$ for all i. Then, the coefficient of x^n in $F(x, y') = \prod_{i=1}^{s}((\beta_i + \rho_i u)x - \rho_i y)^{n_i}$ will be in $\mathcal{O}_L^* \cap \mathcal{O}_K = \mathcal{O}_K^*$.

2.3. Some regular affine subsets of the normalization of $\mathcal{C}$

In what follows, we assume that $F(x, 1)$ is monic, that $\pi_K \mid h$ and that $\pi_K \mid d^*(F)$. Assume also that K is complete, so that for any finite extension L/K, the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L is a local ring.

Let L/K be the splitting field over K of the polynomial $F(x, 1)$. We denote by v the valuation of $\mathcal{O}_L$, and let π be a uniformizer of $\mathcal{O}_L$. We write our original equation $F(x, y) = h$ as

$$\prod_{i=1}^{s}(x - \alpha_i y)^{n_i} = \mu \pi^w,$$

where μ is unit in $\mathcal{O}_L$ and $w = v(h)$. Let us say that $P = (a, b)$ is a *primitive integral solution* to $F(x, y) = h$ if $a, b \in \mathcal{O}_K$ and $\gcd(a, b) = 1$. We will sometimes also refer to such an (a, b) as a *primitive integral point*. We describe below an affine regular scheme $\mathcal{U}/\mathcal{O}_L$ such that $\mathcal{U} \times_{\mathrm{Spec}(\mathcal{O}_L)} \mathrm{Spec}(L)$ is open in $X_{F,h,L}$ and $P \in \mathcal{U}(L)$ has a non-trivial reduction modulo (π). In other words, the closure of P in $\mathcal{U}$ includes a point on the special fiber of $\mathcal{U}$.

Consider any root α_i of $F(x, 1)$ such that $v(a-\alpha_i b) = \max_j(v(a-\alpha_j b))$. Let $t := v(a - \alpha_i b)$. Change variables from x to $z_0 := x - \alpha_i y$, so that $F(z_0, y) = z_0 \prod_{j=1}^{s-1}(z_0 - \gamma_j y)^{n_i}$, where $\gamma_j := \alpha_j - \alpha_i$ for $j < i$ and $\gamma_j := \alpha_{j+1} - \alpha_i$ for $j \geq i$. Define $s_0 := 0$, and then recursively define

$$s_k := \min\{v(\gamma_j) \mid t \geq v(\gamma_j) > s_{k-1}\},$$

for $k \geq 1$. We obtain in this way a finite increasing sequence of integers. If t is not the largest integer of this sequence, add t to the sequence. Denote the elements of the new sequence by $s_0 < s_1 < \cdots < s_m = t$. Define, for $k < m$,

$$\mathcal{S}_k := \{\gamma_j \mid v(\gamma_j) = s_k\}.$$

The set $\mathcal{S}_m$ is defined to be $\{\gamma_j \mid v(\gamma_j) \geq s_m\}$. If γ is a root of $F(z_0, 1)$, let $n(\gamma)$ denote its multiplicity. Then, for $k \leq m$, define z_k to be z_0/π^{s_k}, and let F_k be the polynomial

$$F_k(z_k, y) := \prod_{j=0}^{k} \prod_{\gamma \in \mathcal{S}_j} \left(\pi^{s_k - s_j} z_k - \gamma \pi^{-s_j} y\right)^{n(\gamma)} \prod_{\gamma \notin \cup_{j=0}^{k} \mathcal{S}_j} \left(z_k - \gamma \pi^{-s_k} y\right)^{n(\gamma)}.$$

Set

$$u_k := \sum_{j=0}^{k} \Big(\sum_{\gamma \in \mathcal{S}_j} n(\gamma)\Big) s_j + \sum_{j=k+1}^{m} \Big(\sum_{\gamma \in \mathcal{S}_j} n(\gamma)\Big) s_k.$$

Then $F_k(z_k, y) = F_0(z_0, y)\pi^{-u_k}$. Finally, let

$$A_k := \mathcal{O}_L[z_k, y]/\big(F_k(z_k, y) - \mu\pi^{w-u_k}\big),$$

for $k \leq m$ (recall that $h = \mu\pi^w$). Note now that when (a, b) is primitive and $\pi \mid h$, then $v(b) = 0$. Indeed, if $v(b) > 0$ and (a, b) is primitive, then $v(a) = 0$. Thus, $v(a - \alpha_j b) = 0$ for all j, contradicting the fact that $v(F(a, b)) = v(h) > 0$. Hence, $v(b) = 0$. If follows that for $j \neq i$, the inequality

$$v(a - b\alpha_j) \geq \min(v(a - b\alpha_i), v(b\alpha_i - b\alpha_j))$$

implies that either $v(a - b\alpha_j) = t$ and $v(\alpha_i - \alpha_j) \geq t$, or $v(a - b\alpha_j) < t$ and $v(a - b\alpha_j) = v(\alpha_i - \alpha_j)$. In particular, we find that when (a, b) is primitive, $w = u_m$.

Lemma 2.4. *Assume that $p \nmid n$. The ring A_m is regular and* $\operatorname{Spec}(A_m)/\operatorname{Spec}(\mathcal{O}_L)$ *is smooth.*

Proof. The generic fiber of A_m is easily checked to be smooth. Hence, we need only check points on the special fiber of A_m. We note that modulo π, the equation $F_m(z_m, y) = \mu$ is equivalent to the equation

$$\left(\prod_{\gamma \in \mathcal{S}_m} \left(z_m - (\overline{\gamma/\pi^t})y\right)^{n(\gamma)}\right)\left(\prod_{j=0}^{m-1}\prod_{\gamma\in\mathcal{S}_j}\left(-(\overline{\gamma/\pi^{s_j}})y\right)^{n(\gamma)}\right) - \overline{\mu} = 0,$$

because $\pi^{w-u_m} = 1$ as noted earlier. Since $\overline{\mu} \neq 0$ and $p \nmid n$, this equation defines a nonsingular affine curve in $\mathbb{A}^2$. Thus, the special fiber of A_m is nonsingular; therefore all the points on the special fiber of A_m are regular and A_m is a regular ring.

Lemma 2.5. *Assume that $p \nmid n$. The affine scheme* $\operatorname{Spec} A_m$ *is an open subset of $\mathcal{Y}$, the normalization of $\mathcal{C} :=$* $\operatorname{Proj} \mathcal{O}_L[x, y, z]/(hz^n - F(x, y))$.

Proof. Since A_m contains A_0 and is regular, A_m contains the integral closure of A_0. Thus we have a natural map $\psi : \operatorname{Spec}(A_m) \to \mathcal{Y}$, with $\mathcal{Y}$ normal and ψ generically an isomorphism. We are going to show below that ψ is quasi-finite. It follows then from Zariski's Main Theorem that j is an open immersion. There is a natural ring homomorphism $A_{k-1} \to A_k$ that sends z_{k-1} to $\pi^{s_k - s_{k-1}} z_k$. Define

$$G_k(z_k, y) := \prod_{j=0}^{k}\prod_{\gamma\in\mathcal{S}_j}\left(\pi^{s_k - s_j} z_k - \gamma\pi^{-s_j}y\right)^{n(\gamma)}.$$

Let S_k denote the multiplicative subset of A_k generated by $G_k(z_k, y)$. We claim that A_k is integral over $S_{k-1}^{-1}(A_{k-1})$. Indeed, it suffices to show that z_k is integral over $S_{k-1}^{-1}(A_{k-1})$. Recall that in A_k,

$$\begin{aligned} F_k(z_k, y) - \mu\pi^{w-u_k} &= G_{k-1}(z_{k-1}, y)\prod_{j=k}^{m}\prod_{\gamma\in\mathcal{S}_j}\left(z_k - \gamma\pi^{-s_k}y\right)^{n(\gamma)} - \mu\pi^{w-u_k} \\ &= 0. \end{aligned}$$

Thus, the image of z_k in A_k is the root of a monic polynomial over $S_{k-1}^{-1}(A_{k-1})$ (since G_{k-1} is of course a unit in this ring). Hence, it follows that the map $\operatorname{Spec}(A_k) \to \operatorname{Spec}(A_{k-1})$ is quasi-finite for any $k \geq 1$, which concludes the proof of 2.5.

Let $\mathcal{U}(\alpha_i) := \operatorname{Spec}(A_m)$. The primitive integral point $P = (a, b)$ in $X_{F,h}(L)$ corresponds to the point $(\pi^{-t}(a - \alpha_i b), b)$ in $\mathcal{U}(\alpha_i)(L)$. Since this point is integral, it has a non-trivial reduction in the special fiber of $\mathcal{U}(\alpha_i)$. Denote by $\mathcal{P}$ the set of integral primitive solutions, so that

$$\mathcal{P} := \{(x, y) \in (\mathcal{O}_K)^2 \mid F(x, y) = h \text{ and } \gcd(x, y) = 1\}.$$

Proposition 2.6. *Assume that $p \nmid n$. The closure of $\mathcal{P}$ in the normalization $\mathcal{Y}/\mathcal{O}_L$ of $\mathcal{C}/\mathcal{O}_L$ is contained in at most s regular affine open sets; namely, this closure is contained in the union of the images of the sets $\mathcal{U}(\alpha_i)$, where α_i runs through all the roots of $F(x,1)$ such that there exists a primitive integral point (a,b) with $v(a-\alpha_i b) = \max_j(v(a-\alpha_j b))$.*

Proof. The proposition follows from our next lemma.

Lemma 2.7. *Let $\pi \mid h$. Let (a,b) and (a',b') be elements of $\mathcal{P}$. Suppose that $v(a-\alpha_i b) = \max_j(v(a-\alpha_j b))$ and $v(a'-\alpha_i b') = \max_j(v(a'-\alpha_j b'))$. Then $v(a-\alpha_i b) = v(a'-\alpha_i b')$.*

Proof. Recall that $v(b)=0$ when $\pi \mid h$ and (a,b) is primitive. Suppose that $v(a-\alpha_i b)$ and $v(a'-\alpha_i b')$ are not equal. We may assume without loss of generality that $v(a/b-\alpha_i) > v(a'/b'-\alpha_i)$. We claim that this inequality implies that $v(a/b-\alpha_j) \geq v(a'/b'-\alpha_j)$ for all j. Indeed, $v(a/b-\alpha_j) \geq v(a'/b'-\alpha_j)$ is clear if $v(a'/b'-\alpha_i) \leq v(a/b-\alpha_j)$. Thus we may assume that $v(a'/b'-\alpha_i) > v(a/b-\alpha_j)$. From $v(a/b-\alpha_i) > v(a'/b'-\alpha_i)$ we find that $v(a/b-a'/b') = v(a'/b'-\alpha_i)$. It follows from $v(a/b-a'/b') > v(a/b-\alpha_j)$ that $v(a'/b'-\alpha_j) = v(a/b-\alpha_j)$, and our claim is proved. This claim contradicts the fact that $v(F(a,b)) = v(F(a',b')) = v(h)$, and the lemma follows.

Slightly more can be said about the closure of $\mathcal{P}$ in $\mathcal{Y}/\mathcal{O}_L$. Consider the following two schemes, $\mathcal{U}(\alpha_i)$ attached to a primitive integral point (a,b) with associated valuation t, and $\mathcal{U}(\alpha_j)$ attached to a primitive integral point (a',b') with associated valuation t'. We claim that if $v(\alpha_i-\alpha_j) \geq \min(t,t')$, then the images of $\mathcal{U}(\alpha_i)$ and $\mathcal{U}(\alpha_j)$ in $\mathcal{Y}$ are equal. Assume $t' \leq t$. It follows that $v(a'-\alpha_i b') \geq t'$. Thus, $v(a'-\alpha_i b') = t'$, and Lemma 2.7 shows that $t=t'$. We may then define an isomorphism from $\mathcal{U}(\alpha_i)$ to $\mathcal{U}(\alpha_j)$ on the level of rings

$$\mathcal{O}_L[u',y]/(F'_{m'}(u',y)-\mu) \longrightarrow \mathcal{O}_L[u,y]/(F_m(u,y)-\mu)$$

by setting $u' \mapsto u + \pi^{-t}(\alpha_i-\alpha_j)y$ and $y \mapsto y$.

We have thus shown that there exist at most s disjoint disks in $\mathcal{O}_L$, each centered at a root of $F(x,1)$, such that if α_i and α_j belong to the same disk (and have primitive solutions attached to them), then the images of $\mathcal{U}(\alpha_i)$ and $\mathcal{U}(\alpha_j)$ in $\mathcal{Y}$ are equal.

2.8. The quotient construction. Let X/K be a smooth proper geometrically connected curve of genus g. Let L/K be a cyclic Galois extension with Galois group $\mathrm{Gal}(L/K) =< \sigma >$. Let $\mathcal{Y}/\mathcal{O}_L$ be a normal model of X_L/L such that $\mathrm{Gal}(L/K)$ acts on $\mathcal{Y}$, lifting its natural action on $\mathrm{Spec}(\mathcal{O}_L)$. An example of such a model $\mathcal{Y}$ is the normalization in $L(X)$ of a normal model over $\mathcal{O}_K$ of X/K. Another example is the minimal regular model $\mathcal{Y}/\mathcal{O}_L$ of X_L/L. Indeed, the following is well-known.

2.9. Let $\mathcal{Y}/\mathcal{O}_L$ be the minimal regular model of X_L/L. The map σ induces a canonical morphism $X_L \to X_L$ over the map $\sigma : \mathrm{Spec}\,(L) \to \mathrm{Spec}\,(L)$. Since X_L is the generic fiber of $\mathcal{Y}$, the map σ induces a birational proper map $\mathcal{Y} \to \mathcal{Y} \times_{\mathrm{Spec}(\mathcal{O}_L)} \mathrm{Spec}\,(\mathcal{O}_L)$ over $\mathrm{Spec}\,(\mathcal{O}_L)$. By the universal property of a minimal model ([C-S, page 310]), this map extends to a morphism from $\mathcal{Y}$ to $\mathcal{Y} \times_{\mathrm{Spec}(\mathcal{O}_L)} \mathrm{Spec}\,(\mathcal{O}_L)$ over $\mathrm{Spec}\,(\mathcal{O}_L)$. Since $\mathcal{Y}$ is reduced and separated, this extension is unique. Hence, there exists then a unique automorphism $\tau : \mathcal{Y} \to \mathcal{Y}$ over the automorphism $\sigma : \mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_L)$.

2.10. Let $G = <\tau>$, with $\tau : \mathcal{Y} \to \mathcal{Y}$ lifting $\sigma : \mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_L)$. The following fact is standard: Since $\mathcal{Y}/\mathcal{O}_L$ is projective, the quotient $\mathcal{Z} = \mathcal{Y}/G$ can be constructed in the usual way by gluing together the rings of invariants of G-invariant affine open sets of $\mathcal{Y}$. The scheme $\mathcal{Z}/\mathcal{O}_K$ is normal and, hence, its singular points are closed points of its special fiber. We let $f : \mathcal{Y} \longrightarrow \mathcal{Z}$ denote the quotient map.

The normal scheme $\mathcal{Z}$ has quotient singularities. A desingularization $\nu : \mathcal{X} \to \mathcal{Z}$ leads to a regular model $\mathcal{X}/\mathcal{O}_K$ of X/K. Let K^{nr} denote the maximal unramified extension of K, and assume now that $K = K^{nr}$. When L/K is a tamely ramified field extension, the quotient singularities of $\mathcal{Z}$ are well-understood. We recall their properties below, closely following Viehweg's article [Vie]. We refer the reader to his work for more details. Though he states at the beginning of his paper that he considers only the equicharacteristic case, his proofs of the facts listed below are also correct in the mixed characteristic case.

2.11. ([Vie, page 303]) Let $\overline{\tau} : \overline{\mathcal{Y}} \to \overline{\mathcal{Y}}$ and $\overline{\tau}^{red} : \overline{\mathcal{Y}}^{red} \to \overline{\mathcal{Y}}^{red}$ be the natural morphisms induced by τ. Then the natural map

$$\overline{\mathcal{Y}}^{red}/<\overline{\tau}^{red}>\longrightarrow \overline{\mathcal{Z}}^{red} = \overline{\mathcal{Y}/<\tau>}^{red}$$

is an isomorphism of schemes over the residue field.

For any irreducible component $Y_i \subset \overline{\mathcal{Y}}$, let

$$D(Y_i) := \{\mu \in G \mid \mu(Y_i) = Y_i\} \text{ and } I(Y_i) := \{\mu \in G \mid \mu_{|Y_i} = \mathrm{id}\}.$$

2.12. ([Vie, page 303]) Let m_i be the multiplicity of Y_i in $\overline{\mathcal{Y}}$ and let $Z_j := f(Y_i)$. The multiplicity of Z_j in $\overline{\mathcal{Z}}$ is equal to $m_i \cdot [L : K]/|I(Y_i)|$.

Recall the following terminology. Let $(C \cdot D)$ denote the intersection number on a regular model $\mathcal{X}$ of two divisors C and D. Let us call *chain of rational curves on* $\mathcal{X}$ a divisor D such that

(1) $D = \bigcup_{i=1}^{q} E_i$, E_i smooth and rational curve for $i = 1, \dots, q$.
(2) $(E_i \cdot E_{i+1}) = 1$ for all $i = 1, \dots, q-1$ and $(E_i \cdot E_j) = 0$ for all $j \neq i+1$. Moreover, $(E_i \cdot E_i) \leq -2$ for all i. Let us call E_1 and E_q the end-components of the chain.

Consider again a normal model $\mathcal{Y}/\mathcal{O}_L$ with an action of $\mathrm{Gal}(L/K)$ lifting the action on $\mathrm{Spec}(\mathcal{O}_L)$. Assume that $\mathcal{U}/\mathcal{O}_L$ is a smooth open subset of $\mathcal{Y}/\mathcal{O}_L$ such that $\mathcal{U}$ is invariant under the action of G. Let $\mathcal{Z} := \mathcal{U}/G$.

2.13. ([Vie, Sect. 6]) There exists a regular scheme $\mathcal{X}/\mathcal{O}_K$ and a proper birational morphism $\nu : \mathcal{X} \to \mathcal{Z}$ such that ν induces an isomorphism between $\mathcal{X} - \{\nu^{-1}(\mathcal{Z}_{sing})\}$ and $\mathcal{Z} - \{\mathcal{Z}_{sing}\}$ and such that, for any $z \in \mathcal{Z}_{sing}$, $\nu^{-1}(z)$ is a connected chain of rational curves. The point z belongs to an end-component of the chain. Since $\mathcal{U}$ is smooth, we find that if z is a singular point of $\mathcal{Z}$, then $\nu^{-1}(z)$ intersects the rest of the special fiber $\overline{\mathcal{X}}$ with normal crossings in exactly one point, say on E_1. (Viehweg states in 8.1.d) on page 306 of [Vie] that the model $\mathcal{X}$, obtained by taking the quotient of $\mathcal{U}$ and then resolving the singularities, has normal crossings.) Let us call the component E_q the *terminal component* of the chain $\nu^{-1}(z)$. The other end-component of the chain $\nu^{-1}(z)$ is attached to an irreducible component of $\overline{\mathcal{X}} \setminus \nu^{-1}(z)$.

2.14. ([Vie, Sect. 6]) Let $f : \mathcal{U} \to \mathcal{Z}$ denote the quotient map. Let $z_1, \dots, z_d$ be the closed points of $\overline{\mathcal{Z}}$ that are ramification points of the morphism $\overline{f} : \overline{\mathcal{U}} \to \overline{\mathcal{Z}}^{red}$. Then $\{z_1, \dots, z_d\}$ is the set of singular points of $\mathcal{Z}$. Moreover, if $\nu : \mathcal{X} \to \mathcal{Z}$ is the desingularization of $\mathcal{Z}$ described in 2.13, then the multiplicity of the terminal component on the chain $\nu^{-1}(z_i)$ is equal to the number of closed points in the fiber $\overline{f}^{-1}(z_i)$.

2.15. We now apply the quotient construction to the case where the model $\mathcal{Y}/\mathcal{O}_L$ is smooth. The scheme $\mathcal{Z} = \mathcal{Y}/ <\tau>$ has an irreducible special fiber. The reduced special fiber $\overline{\mathcal{Z}}^{red}$ is obtained as the quotient of $\overline{\mathcal{Y}}$ by the action of $<\overline{\tau}>$ and is then a smooth and proper curve. The multiplicity of $\overline{\mathcal{Z}}$ in $\mathcal{Z}$ equals $[L : K]/I(\overline{\mathcal{Y}})$. The singular points of $\mathcal{Z}$ are the ramification points $z_1, \dots, z_d$ of the morphism $\overline{f} : \overline{\mathcal{Y}} \to \overline{\mathcal{Z}}^{red}$, and the singularity at each of these points is resolved by a chain of rational curves. The terminal curve on the chain resolving z_i has multiplicity equal to the number of closed points in the fiber $\overline{f}^{-1}(z_i)$. The regular model $\mathcal{X}/\mathcal{O}_K$ obtained as the minimal desingularization of $\mathcal{Z}$ is thus very simple.

3. Applications of the method of Chabauty-Coleman

We may now apply the method of Chabauty-Coleman to the case of Thue equations. Let $g := g(X_{F,h})$. We distinguish four cases, according to the divisibility of $d^*(F)$ and h by p. Our main result is stated in 3.9 below.

Proposition 3.1. *Let $X_{F,h}/\mathbb{Q}$ be such that for some prime p, $p \nmid d^*(F)$, $p \nmid n$, $p^2 > 2g+1$, and either $p \nmid h$ or $n \mid \mathrm{ord}_p(h)$. Let K be any number field* *having an unramified prime $\mathfrak{P}$ of norm p. Assume that* $\mathrm{Chab}(X_{F,h}, K, \mathfrak{P}) < g$. *Then*

$$|X_{F,h}(K)| \leq (2g-2)\frac{p-1}{p-2} + |\mathcal{X}_{\mathbb{F}_p}(\mathbb{F}_p)|,$$

where $\mathcal{X}/\mathbb{Z}_p$ is the minimal regular model of $X_{F,h}$.

Proof. When $n \mid \mathrm{ord}_p(h)$, an obvious change of variable over $\mathbb{Q}$ shows that $X_{F,h}$ is isomorphic to $X_{F,p^{-\mathrm{ord}_p(h)}h}$. We are thus reduced to the case where $p \nmid h$. In this case, as noted in 2.1, $X_{F,h}/\mathbb{Q}_p$ has good reduction over $\mathbb{Z}_p$. Thus, we can apply 1.1.

Proposition 3.2. *Let $X_{F,h}/\mathbb{Q}$ be such that for some prime p, $p \nmid d^*(F)$, $p \nmid n$, $p^2 > 2g+1$, $p \mid h$ and $n \nmid$* $\mathrm{ord}_p(h)$. *Let K be any number field having an unramified prime $\mathfrak{P}$ of norm p. Assume that* $\mathrm{Chab}(X_{F,h}, K, \mathfrak{P}) < g$. *Then*

$$|X_{F,h}(K)| \leq (2g-2)\frac{p-1}{p-2} + np.$$

Let s denote the number of distinct roots of $F(x,1)$ in $\overline{\mathbb{Q}}$. If $\gcd(n, \mathrm{ord}_p(h)) = 1$, *then* $|X_{F,h}(K)| \leq (2g-2)\frac{p-1}{p-2} + sp$.

Proof. Let $X := X_{F,h}$. As noted in 2.1, X has good reduction over the extension $\mathbb{Q}_p(\sqrt[n]{h})$, which is tame. Thus, we may apply the quotient construction to describe a regular model of $X/\mathbb{Q}_p^{nr}$ over $\mathbb{Z}_p^{nr}$. Let $L := \mathbb{Q}_p^{nr}(\sqrt[n]{h})$. The extension $L/\mathbb{Q}_p^{nr}$ is Galois of order $m := n/\gcd(n, \mathrm{ord}_p(h))$, with cyclic Galois group. Let ξ_m be a primitive m-th root of unity, and denote by $\sigma : L \to L$, with $\sigma(\sqrt[n]{h}) = \xi_m \sqrt[n]{h}$, a generator of $\mathrm{Gal}(L/\mathbb{Q}_p^{nr})$. The morphism σ lifts to a morphism $\sigma : X_L \to X_L$ by setting

$$\sigma : L[u,v,w]/(F(u,v) - hw^n) \longrightarrow L[u,v,w](F(u,v) - hw^n)$$

with $\sigma(u) = u$, $\sigma(v) = v$ and $\sigma(w) = w$. Let $\mathcal{Y}$ denote the normalization of $\mathrm{Proj}(\mathcal{O}_L[x,y,z]/(F(x,y) - z^n))$. Then $\mathcal{Y}/\mathcal{O}_L$ is the smooth minimal model of X_L/L (see 2.1). The morphism $\sigma : X_L \to X_L$ extends to a morphism $\sigma : \mathcal{Y} \to \mathcal{Y}$ by setting

$$\sigma : \mathcal{O}_L[x,y,z]/(F(x,y) - z^n) \longrightarrow \mathcal{O}_L[x,y,z]/(F(x,y) - z^n)$$

with $\sigma(x) = x$, $\sigma(y) = y$, and $\sigma(z) = \xi_m z$. When restricted to the special fiber $\overline{\mathcal{Y}}$ of $\mathcal{Y}$, the morphism σ becomes an automorphism $\overline{\sigma}$ over $\overline{\mathbb{F}}_p$ of $\overline{\mathcal{Y}}$, of exact order m, which lifts the standard automorphism of order m of $\mathrm{Proj}(k[x,y,z]/(\overline{F} - z^n))$. This automorphism has s fixed points. Pulling back these fixed points on $\overline{\mathcal{Y}}$ produces at most $\sum_{i=1}^{s} \gcd(n, n_i)$ fixed points for the automorphism σ of $\overline{\mathcal{Y}}$. Bounding $\sum_{i=1}^{s} \gcd(n, n_i)$ by n, we find that the quotient map $\overline{\mathcal{Y}} \to \overline{\mathcal{Y}}/\langle\overline{\sigma}\rangle$ is totally ramified over at most n points. It follows from 2.14 that the desingularization $\mathcal{X}$ of $\mathcal{Y}/\langle\sigma\rangle$ has a special fiber containing at most n (smooth rational) components of multiplicity one. Note that when $m = n$, the fixed points of the automorphism σ correspond to the totally ramified points of the map from $\overline{\mathcal{Y}}$ to $\mathbb{P}^1$ obtained by composing the map from $\overline{\mathcal{Y}}$ to $\mathrm{Proj}(k[x, y, z]/(\overline{F} - z^n))$ with the projection map from $\mathrm{Proj}(k[x, y, z]/(\overline{F} - z^n))$ onto its $[x : y]$ coordinates. This composition map has at most s totally ramified points. Thus, in this case the desingularization $\mathcal{X}$ of $\mathcal{Y}/\langle\sigma\rangle$ has a special fiber containing at most s components of multiplicity one.

Consider now the minimal regular model $\mathcal{X}_0/\mathbb{Z}_p$ of $X/\mathbb{Q}_p$. A point in $X(\mathbb{Q}_p)$ specializes in the special fiber $\overline{\mathcal{X}}_0/\mathbb{F}_p$ to a smooth point, belonging to a geometrically integral irreducible component $C/\mathbb{F}_p$ of multiplicity one. Let $\tilde{\mathcal{X}}_0 := \mathcal{X}_0 \times_{\mathbb{Z}_p} \mathbb{Z}_p^{nr}$. Since the self-intersection of C in $\mathcal{X}_0$ equals the self-intersection of $C \times_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ in $\tilde{\mathcal{X}}_0$ (see, e.g., [B-L, 1.4]), we find that $C \times_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ cannot be contracted in $\tilde{\mathcal{X}}_0$ and, thus, corresponds to a component in the minimal regular model $\tilde{\mathcal{X}}_{00}$ of $X/\mathbb{Q}_p^{nr}$. Since there is a natural morphism $\mathcal{X} \to \tilde{\mathcal{X}}_{00}$, our description above of the special fiber of $\mathcal{X}$ implies that there are at most n components of $\overline{\mathcal{X}}_0$ that can contain the reduction of a $\mathbb{Q}_p$-point, and that each such component is a smooth rational curve. Moreover, each such component C meets the divisor $\overline{\mathcal{X}}_0 - C$ in exactly one $\mathbb{F}_p$-point. Hence, the number of points in $\overline{\mathcal{X}}_0$ that can be reductions of $\mathbb{Q}_p$-rational points is at most np. This concludes the proof of 3.2.

Let K be any number field, and let $\mathfrak{P}$ be a maximal ideal of $\mathcal{O}_K$. Let $N(F,h,K,\mathfrak{P})$ denote the number of solutions $(x, y) \in (\mathcal{O}_K)^2_{\mathfrak{P}}$ of $F(x, y) = h$ with $\gcd(x, y) = 1$.

Proposition 3.3. *Let $X_{F,h}/\mathbb{Q}$ be such that for some prime p, $p \nmid h$ and $p \mid d^*(F)$, with $p \nmid n$ and $p^2 > 2g + 1$. Let K be any number field having an unramified prime $\mathfrak{P}$ of norm p. Assume that* $\mathrm{Chab}(X_{F,h}, K, \mathfrak{P}) < g$. *Let $a(p)$ denote the number of $\mathbb{F}_p$-rational points of the affine curve $F(x, y) - h = 0 \bmod p$. Then*

$$N(F, h, K, \mathfrak{P}) \leq (2g - 2)\frac{p-1}{p-2} + a(p).$$

Proof. Consider the model $\mathcal{C}/\mathbb{Z}_p$ given by $\mathcal{C} = \mathrm{Proj}(\mathbb{Z}_p[x, y, z]/(F - hz^n))$. The special fiber $\overline{\mathcal{C}}/\mathbb{F}_p$ is a plane projective curve with possible singularities only at points $(x : y : z)$ with $z = 0$. None of the singular points of $\overline{\mathcal{C}}$ can be the reduction of a primitive integral point (a, b). Resolve the singularities of $\mathcal{C}$ to obtain a regular model $\mathcal{X}/\mathbb{Z}_p$ of $X_{F,h}/\mathbb{Q}_p$. The only points in $\overline{\mathcal{X}}/\mathbb{F}_p$ that can be reductions of primitive points in $X_{F,h}(\mathbb{Q}_p)$ are the points in $\overline{\mathcal{X}}(\mathbb{F}_p)$ that correspond to $\mathbb{F}_p$-rational points of $\overline{\mathcal{C}}$ with $z \neq 0$. Applying 1.1 finishes the proof.

Remark 3.4. When p is not too large compared to n, a bound for $a(p)$ better than the Weil bound can be obtained as follows. Project an irreducible component of degree d of the curve $\overline{\mathcal{C}}/\mathbb{F}_p$ that is not a line onto an $\mathbb{F}_p$-rational projective line. Then the projection map has degree at most d. It follows that $a(p) \leq np$.

Proposition 3.5. *Let $X_{F,h}/\mathbb{Q}$ be such that for some prime p, $p \mid h$ and $p \mid d^*(F)$, with $p \nmid n$ and $p^2 > 2g+1$. Let K be any number field having an unramified prime $\mathfrak{P}$ of norm p. Assume that* $\mathrm{Chab}(X_{F,h}, K, \mathfrak{P}) < g$. *Assume also that the splitting field $L/\mathbb{Q}_p^{nr}$ of $F(x,1)$ is a tame extension (this happens for instance if $p > s$). When $p \leq s$, assume that $F(x,1)$ is monic. Then $N(F,h,K,\mathfrak{P}) \leq (2g-2)\frac{p-1}{p-2} + snp$.*

Proof. Let $X := X_{F,h}$. When $p > s$, we use 2.2 and change variables so that $F(x,1)$ is monic. We may now use Proposition 2.6, which describes smooth open sets in a regular model of X over $\mathcal{O}_L$. Since the extension $L/\mathbb{Q}_p^{nr}$ is tame, it is cyclic, and we can thus use the quotient construction to obtain information on a regular model of X over $\mathbb{Z}_p$. Let $\mathcal{Y}/\mathcal{O}_L$ be the normalization of $\mathcal{C}/\mathcal{O}_L := \mathrm{Proj}(\mathcal{O}_L[x,y,z]/(F - hz^n))$. Let $\langle\sigma\rangle = \mathrm{Gal}(L/\mathbb{Q}_p^{nr})$. The morphism σ induces obvious automorphisms $\sigma : \mathcal{Y} \to \mathcal{Y}$ and $\sigma : \mathcal{C} \to \mathcal{C}$ over $\sigma : \mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_L)$, compatible with the natural map $\mathcal{Y} \to \mathcal{C}$. We shall denote by $G := \langle\sigma\rangle$ the group of automorphisms of $\mathcal{Y}$, resp. $\mathcal{C}$, generated by σ. Fix a root α_i of $F(x,1)$ such that there exists a primitive solution $P = (a,b) \in (\mathbb{Z}_p^{nr})^2$ with $t := v_L(a - b\alpha_i) = \max_j(v_L(a - b\alpha_j))$. Recall the notation introduced just before 2.6: Let $\mathcal{U}(\alpha_i) = \mathrm{Spec}(\mathcal{O}_L[u,y]/(F_m(u,y) - \mu))$. Let

$$\psi^* : \mathcal{O}_L[x,y]/(F(x,y) - h) \longrightarrow \mathcal{O}_L[u,y]/(F_m(u,y) - \mu)$$

be given by $x \mapsto \pi_L^t u + \alpha_i y$, and $y \mapsto y$. The induced morphism $\psi : \mathcal{U}(\alpha_i) \to \mathcal{C}$ was shown to induce an open immersion $\psi : \mathcal{U}(\alpha_i) \to \mathcal{Y}$ in 2.5. The following lemma, whose proof is omitted, describes the possible components of the special fiber $\overline{\mathcal{U}(\alpha_i)}$.

Lemma 3.6. *Let k be any algebraically closed field. Let $n \in \mathbb{N}$ with* $\mathrm{char}(k) \nmid n$. *Let ξ_n denote a primitive n-th root of unity in k. Let $f(x,y)$ be homogeneous of degree n in $k[x,y]$, and let $\mu \in k^*$. Then $f(x,y) - \mu z^n$ factors in $k[x,y,z]$ if and only if there exist $d \mid n$ and $g \in k[x,y]$ with $f = g^{n/d}$. Then $f - \mu z^n = \prod_{i=1}^{n/d}(g - \xi_n^{id}\sqrt[n/d]{\mu} z^d)$.*

We will also need the following lemma describing the action of G on the components of $\overline{\mathcal{U}(\alpha_i)}$. Recall the definitions of $D(Y_i)$ and $I(Y_i)$ in 2.11.

Lemma 3.7. *Let $Y_1, \ldots, Y_{n/d}$ denote the irreducible components of $\overline{\mathcal{Y}}$ whose generic points belong to $\mathcal{U}(\alpha_i)$. Then $D(Y_\ell) = D(Y_j) = G$ and $I(Y_\ell) = I(Y_j)$ for all $\ell, j \in \{1, \ldots, n/d\}$.*

Proof. Since $p \nmid n$, the group of n-th roots of unity is contained in $\mathbb{Q}_p^{nr}$, and acts on $\mathcal{C}/\mathcal{O}_L$ as follows. A generator ξ_n induces an automorphism $\varphi : \mathcal{C} \to \mathcal{C}$ given by:

$$\mathcal{O}_L[x, y, z]/(F(x, y) - hz^n) \xrightarrow{\varphi^*} \mathcal{O}_L[x, y, z]/(F(x, y) - hz^n),$$

where $x \mapsto x$, $y \mapsto y$, and $z \mapsto \xi_n z$. The automorphism φ induces an automorphism $\varphi : \mathcal{Y} \to \mathcal{Y}$. The generator ξ_n also induces an automorphism $\varphi : \mathcal{U}(\alpha_i) \to \mathcal{U}(\alpha_i)$ given by

$$\mathcal{O}_L[u, y]/(F_m(u, y) - \mu) \xrightarrow{\varphi^*} \mathcal{O}_L[u, y]/(F_m(u, y) - \mu),$$

where $u \mapsto \xi_n^{-1} u$ and $y \mapsto \xi_n^{-1} y$. The reader will easily verify that $\psi \circ \varphi = \varphi \circ \psi$. Lemma 3.6 shows that φ acts transitively on $\{Y_1, \ldots, Y_{n/d}\}$. Since the morphisms $\sigma : \mathcal{Y} \to \mathcal{Y}$ and φ commute, and since φ acts transitively on $\{Y_1, \ldots, Y_{n/d}\}$, we find that $D(Y_\ell) = D(Y_j)$ and $I(Y_\ell) = I(Y_j)$ for all $\ell, j \in \{1, \ldots, n/d\}$. We let $D := D(Y_j)$ and $I := I(Y_j)$. Note now that $D = G$. Indeed, if $P = (a, b)$ reduces to Y_j for some j, then $\sigma(P)$ reduces to $\sigma(Y_j)$. Since $(a, b) \in (\mathbb{Z}_p^{nr})^2$, we find that P reduces to a point in $Y_j \cap \sigma(Y_j)$. Since P reduces to a non-singular point of $\overline{\mathcal{U}(\alpha_i)}$, we find that $Y_j = \sigma(Y_j)$. This concludes the proof of Lemma 3.7.

The following subset of $\mathcal{Y}$, $\mathcal{V}(\alpha_i) := \bigcap_{\tau \in G} \tau(\psi(\mathcal{U}(\alpha_i)))$, is G-invariant. Let $\tilde{P}$ denote the closure of P in $\mathcal{Y}$. Then $\tilde{P} \in \psi(\mathcal{U}(\alpha_i))$ by construction. Since P is fixed by τ, $\tau(\psi(\mathcal{U}(\alpha_i)))$ contains $\tilde{P}$ and, thus, $\tilde{P} \in \mathcal{V}(\alpha_i)$.

Let $\mathcal{D} := \mathrm{Proj}(\mathbb{Z}_p^{nr}[x, y, z]/(F - hz^n))$ and $\mathcal{D}' := \mathrm{Proj}(\mathbb{Z}_p[x, y, z]/(F - hz^n))$. Let $\mathcal{Z}'/\mathbb{Z}_p$ and $\mathcal{Z}/\mathbb{Z}_p^{nr}$ denote the normalization of $\mathcal{D}'$ and $\mathcal{D}$, respectively. Clearly $\mathcal{Z} = \mathcal{Y}/G$. We have the following commutative diagram:

$$\begin{tikzcd}
Y_j \arrow[r, phantom, "\subset"] \arrow[d] & \mathcal{Y} \arrow[r, "\rho"] \arrow[d] & \mathcal{C} \arrow[r] \arrow[d] & \mathrm{Spec}(\mathcal{O}_L) \arrow[d] \\
Z_\ell \arrow[r, phantom, "\subset"] \arrow[d] & \mathcal{Z} \arrow[r, "\varepsilon"] \arrow[d] & \mathcal{D} \arrow[r] \arrow[d] & \mathrm{Spec}(\mathbb{Z}_p^{nr}) \arrow[d] \\
Z'_\ell \arrow[r, phantom, "\subset"] & \mathcal{Z}' \arrow[r, "\varepsilon'"] & \mathcal{D}' \arrow[r] & \mathrm{Spec}(\mathbb{Z}_p),
\end{tikzcd}$$

where Y_j is one of the n/d irreducible components of the special fiber of $\mathcal{V}(\alpha_i)$, corresponding to a factor $\overline{G_j(u, y)}$ of degree d of $\overline{F_m(u, y) - \mu}$. The map ρ induces a morphism $\rho_j : Y_j \to \rho(Y_j)$, given in coordinates by the bottom horizontal map below:

$$\begin{tikzcd}
\mathcal{O}_L[x, y]/(F(x, y) - h) \arrow[r, "\psi^*"] \arrow[d] & \mathcal{O}_L[u, y]/(F_m(u, y) - \mu) \arrow[d] \\
\mathcal{O}_L[x, y]/(\pi_L, x - \alpha_i y) \arrow[r] & \mathcal{O}_L[u, y]/(\pi_L, G_j(u, y)).
\end{tikzcd}$$

This morphism is clearly of degree at most d.

Consider now the case where $I = G$. (This case happens for instance if $\alpha_i \in \mathbb{Q}_p^{nr}$.) Then $\overline{\mathcal{V}(\alpha_i)} \to \overline{\mathcal{V}(\alpha_i)/G}$ is an isomorphism. The morphism $\varepsilon'_\ell : Z'_\ell \to \varepsilon'_\ell(Z'_\ell)$ induced by ρ_j is also of degree at most d. The curve $\varepsilon'_\ell(Z'_\ell)/\mathbb{F}_p$ is a smooth projective line. The primitive integral point (a, b) cannot reduce to the intersection point Q of all the components of the special fiber of $\mathcal{D}'$. The morphism ε'_ℓ is defined over $\mathbb{F}_p$, and there are at most dp $\mathbb{F}_p$-rational points in the preimage in Z_ℓ of $\varepsilon'_\ell(Z'_\ell) \setminus \{Q\}$. Since there are at most n/d such components, we conclude that at most np points in the image of $\mathcal{V}(\alpha_i)$ in $\mathcal{Z}'$ can be residue classes of primitive integral points.

Let us now consider the case where $I \subsetneq D$. Then the image Z_ℓ of Y_j in $\mathcal{Z} = \mathcal{Y}/G$ has multiplicity $|D|/|I| > 1$, and 2.14 indicates that to count the components of multiplicity one (in a desingularization of $\mathcal{Z}'$) which contain the reduction of primitive integral points, one first needs to count the number of totally ramified points in the branch locus of $Y_j \to Z_\ell$. Consider the diagram

$$\begin{tikzcd}
\mathcal{Y} \arrow[r, "\sigma"] & \mathcal{Y} \\
\psi^{-1}(\mathcal{V}(\alpha_i)) \arrow[u, "\psi"'] \arrow[r, "\sigma"] & \psi^{-1}(\mathcal{V}(\alpha_i)), \arrow[u, "\psi"']
\end{tikzcd}$$

where $\sigma : \psi^{-1}(\mathcal{V}(\alpha_i)) \to \psi^{-1}(\mathcal{V}(\alpha_i))$ is defined so that the diagram commutes. Consider an open set $\mathcal{U}$ of $\psi^{-1}(\mathcal{V}(\alpha_i))$ that is dense in each fiber and is a special open set of $\mathcal{U}(\alpha_i)$. We find that on the level of rings, $\sigma : \mathcal{U} \to \mathcal{U}(\alpha_i)$ induces the top horizontal map below

$$\begin{tikzcd}
\mathcal{O}_L[u, y]/(F_m(u, y) - \mu) \arrow[r, "\sigma"] & S^{-1}(\mathcal{O}_L[u, y]/(F_m(u, y) - \mu)) \\
\mathcal{O}_L[x, y]/(F(x, y) - h) \arrow[u, "\psi^*"] \arrow[r, "\sigma"] & \mathcal{O}_L[x, y]/(F(x, y) - h). \arrow[u, "\psi^*"]
\end{tikzcd}$$

The bottom map σ satisfies $\sigma(x) = x$ and $\sigma(y) = y$. Since the diagram commutes, the top map satisfies $\sigma(\pi_L^t u + \alpha_i y) = \pi_L^t u + \alpha_i y$. Since $\sigma(\pi_L^t u + \alpha_i y) = \sigma(\pi_L^t)\sigma(u) + \sigma(\alpha_i)y$, we find that

$$\sigma(u) = \frac{\pi_L^t}{\sigma(\pi_L^t)} u + \frac{\alpha_i - \sigma(\alpha_i)}{\sigma(\pi_L^t)} y.$$

(Note that both $\pi_L^t/\sigma(\pi_L^t)$ and $(\alpha_i - \sigma(\alpha_i))/\sigma(\pi_L^t)$ belong to $\mathcal{O}_L$.) By hypothesis, $\overline{\sigma} := \sigma_{|Y_\ell}$ does not act trivially on Y_ℓ. The points where the morphism $Y_\ell \to Y_\ell / < \overline{\sigma} >$ is totally ramified is the set of fixed points of the map $\overline{\sigma}$. Note also that the reduction of any primitive integral point must be a fixed point of $\overline{\sigma}$. On the plane curve $\overline{G_j(u, y)} = 0$, the automorphism $\overline{\sigma}$ is given by $u \mapsto cu + c'y$ and $y \mapsto y$, for some $c, c' \in k$. Thus the fixed points of $\overline{\sigma}$ lie on the line $(c - 1)u + c'y = 0$, and we find that there are at most d such points. Let now $\nu : \mathcal{X} \to \mathcal{Z}$ denote the minimal desingularization of $\mathcal{Z}$. As we recalled in 2.14, the subset $\nu^{-1}(Z_\ell)$ of the special fiber of $\mathcal{X}$ contains then at most d components of multiplicity one, each smooth and rational, and each meeting the rest of the special fiber in a single point.

Consider now the minimal regular model $\mathcal{X}_0/\mathbb{Z}_p$ of $X/\mathbb{Q}_p$. A point in $X(\mathbb{Q}_p)$ specializes in the special fiber $\overline{\mathcal{X}_0}/\mathbb{F}_p$ to a smooth point, belonging to a geometrically integral irreducible component $C/\mathbb{F}_p$ of multiplicity one. Let $\tilde{\mathcal{X}_0} := \mathcal{X}_0 \times_{\mathbb{Z}_p} \mathbb{Z}_p^{nr}$. Since the self-intersection of such a component C in $\mathcal{X}_0$ equals the self-intersection of $C \times_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ in $\tilde{\mathcal{X}_0}$ (see, e.g., [B-L, 1.4]), we find that $C \times_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ cannot be contracted in $\tilde{\mathcal{X}_0}$ and, thus, corresponds to a component in the minimal regular model $\tilde{\mathcal{X}_{00}}$ of $X/\mathbb{Q}_p^{nr}$. Since there is a natural morphism $\mathcal{X} \to \tilde{\mathcal{X}_{00}}$, our description above of the special fiber of $\mathcal{X}$ implies that there are at most n components of $\overline{\mathcal{X}_0}$ that can contain the reduction of a $\mathbb{Q}_p$-point, and that each such component is a smooth rational curve (recall that there are n/d irreducible components Y_j). Moreover, each such component C meets the divisor $\overline{\mathcal{X}_0} - C$ in exactly one $\mathbb{F}_p$-point. Hence, the number of points in $\overline{\mathcal{X}_0}$ that can be reductions of $\mathbb{Q}_p$-rational points is at most np.

Since the contribution of an open set of the form $\mathcal{V}(\alpha_i)$ to the number of reductions of primitive integral points in the special fiber of the model $\mathcal{X}_0$ is bounded by np, and since the primitive integral points are contained in at most s such open sets (2.6), we find that the reduction of the primitive integral points in the special fiber of the model $\mathcal{X}_0$ consists in at most snp points. Thus 3.5 follows from 1.1.

3.8. The statement of Theorem 3.5/3.8 in the introduction follows immediately from the proof of 3.5. Let us now state our main theorem. Let $N(F,h)$ denote the number of solutions $(x,y) \in \mathbb{Z}^2$ of $F(x,y) = h$ with $\gcd(x,y) = 1$.

Theorem 3.9. *Let p be a prime*[1] *with $n < p < 2n$. Assume that the Chabauty rank with respect to (p) of $X_{F,h}/\mathbb{Q}$ is less than $g := g(X_{F,h})$. Then*

$$N(F,h) \leq 2n^3 - 2n - 3.$$

More precisely,

a) If $p \nmid h$ or $n \mid \mathrm{ord}_p(h)$, and if $p \nmid d^*(F)$, then $|X_{F,h}(\mathbb{Q})| \leq 2g + s - 4 + 2n(n-1)$.
b) If $p \mid h$, $n \nmid \mathrm{ord}_p(h)$, and $p \nmid d^*(F)$, then $|X_{F,h}(\mathbb{Q})| \leq 2g + s - 5 + n(2n-1)$.
c) If $p \nmid h$ and $p \mid d^*(F)$, then $N(F,h,\mathbb{Q},p) \leq 2g + s - 5 + n(2n-1)$.
d) If $p \mid h$ and $p \mid d^*(F)$, then $N(F,h,\mathbb{Q},p) \leq 2g + s - 5 + sn(2n-1)$.

[1] As C. Pomerance pointed out to us, when $n > 2,010,760$, the existence of a prime p with $n < p < (1 + 1/16597)n$ is proven in [Scho]. We leave it to the reader to sharpen the bounds presented in Theorem 3.9 using refinements of Bertrand's Postulate.

In particular, if the Mordell-Weil rank of $X_{F,h}/\mathbb{Q}$ is less than g, then $N(F, h) \leq 2n^3 - 2n - 3$.

Proof. We apply our previous results using the estimates $p \leq 2n - 1$ and $s \leq n$. The term $(2g-2)(p-1)/(p-2)$ is bounded by $2g+s-5$. To prove a), apply 3.1, and bound $|\mathcal{X}_{\mathbb{F}_p}(\mathbb{F}_p)|$ as follows. Let $\overline{X}_{F,h}$ denote the reduction of the plane curve $X_{F,h}$. We can bound $|\overline{X}_{F,h}(\mathbb{F}_p)|$ using a projection from a point P of $\overline{X}_{F,h}(\mathbb{F}_p)$ to a $\mathbb{F}_p$-line. If P is not on the line $z = 0$, we find that

$$|\overline{X}_{F,h}(\mathbb{F}_p)| \leq (n-1)(p-s+1) + \sum_{i=1}^{s}(n-n_i) + 1.$$

We then consider the normalization map $\mathcal{X}_{\mathbb{F}_p} \to \overline{X}_{F,h}$ and find that

$$|\mathcal{X}_{\mathbb{F}_p}(\mathbb{F}_p)| \leq |\overline{X}_{F,h}(\mathbb{F}_p)| + \sum_{i=1}^{s}(\gcd(n, n_i) - 1).$$

Bounding $\sum_{i=1}^{s} \gcd(n, n_i)$ by n, we find that $|\mathcal{X}_{\mathbb{F}_p}(\mathbb{F}_p)| \leq (n-1)(p+1)+1$. We leave it to the reader to check that the above bound also holds when P is on the line $z = 0$. To prove c), apply 3.3, and bound $a(p)$ using 3.4 to find that $a(p) \leq np$. To prove b) and d), use 3.2 and 3.5.

Note now that by Bertrand's postulate, there exists a prime p with $n < p < 2n$. If the Mordell-Weil rank of $X_{F,h}/\mathbb{Q}$ is less than g, then the Chabauty rank with respect to (p) of $X_{F,h}/\mathbb{Q}$ is also less than g, and we find that $N(F, h) \leq 2n^3 - 2n - 3$.

Example 3.10. Let us use known results on the Mordell-Weil rank of certain curves to obtain examples of Thue equations to which Theorem 3.9 applies. First, recall that for any integers a, b, c, d, and e such that $ad - bc \neq 0$, the curve $X_{F,h}$ is isomorphic over $\mathbb{Q}$ to X_{G,he^n}, where $G(x, y) = F(ax + by, cx + dy)$. It follows that the Chabauty rank of $X_{G,he^n}/\mathbb{Q}$ is equal to the Chabauty rank of $X_{F,h}/\mathbb{Q}$ (at any prime). Thus, when the method of Chabauty-Coleman can be applied to bound $N(F, h, \mathbb{Q}, p)$, it can also be used to bound the number of primitive solutions to any equation of the form $G(x, y) = he^n$. Note that while such a change of variables does not change the $\mathbb{Q}$-isomorphism class of the underlying curve, it *does* change the notion of a primitive integral solution.

A Thue curve $X_{F,h}$ always covers the superelliptic curve $hy^q = F(x, 1)$ for any prime divisor q of n, so it is always possible to attempt to bound the Chabauty rank of such a Thue curve $X_{F,h}$ by applying the ideas of [P-S] to compute the rank of some quotient of $X_{F,h}$. One finds in the literature a few explicit computations of Mordell-Weil ranks for superelliptic curves $D/\mathbb{Q}$ of the form $y^q = F(x, 1)$, with $n = \deg(F)$ and $q \mid n$, q prime. For instance,

$$y^3 = (x^2 - x + 6)^2(x^8 + 3x + 3) \tag{7}$$

is considered in [P-S, 14.2], with Mordell-Weil rank 2 over $\mathbb{Q}$ (see Sect. 5 of [Sch] for further examples). Let D_{d^q} denote the superelliptic curve associated with $d^q y^q = F(x, 1)$. Clearly, D_{d^q} is isomorphic to D over $\mathbb{Q}$, so the jacobians of these curves have the same rank. We may thus apply the Chabauty-Coleman method to X_{F,d^q} as soon as it is known that the rank of $D/\mathbb{Q}$ is less than the genus of D, as is the case with (7).

Let ℓ be a prime. Bounds for the Mordell-Weil rank over $\mathbb{Q}$ of the normalization C_h of the curve $Y^2 = X^\ell + h$ are given in [St1], with an 'added in proof' proven in [St2]. Using these results, one finds for instance that when $\ell = 5$ and h is as follows, the rank of the genus 2 curves C_h, C_{h^5}, and C_{h^9}, is equal to 1:

$$h = 11, h = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23, h = -3 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29.$$

Consider now $q, e \in \mathbb{Z}^+$, and the equation $q^2x^{2\ell} - y^{2\ell} = he^{2\ell}$. This Thue curve maps onto C_h, with $Y \mapsto q(x/ez)^\ell$ and $X \mapsto (y/ze)^2$. In addition to the above Thue curve, we also find that the curves given by $hx^{2\ell} - y^{2\ell} = h^{\ell+1}e^{2\ell}$ and $hx^{\ell+1} + xy^\ell = h^2e^{2\ell}$ have C_h as quotients. When the rank of C_h can be computed using [St1] and [St2], Theorem 3.9 applies to the above three examples of Thue curves having C_h as quotient.

It is quite possible that the bounds obtained in Theorem 3.9 are too large. Indeed, there are no known examples in the literature of a family of Thue equations $(F_j(x, y) = h_j)_{j=1}^\infty$ with $\lim_{j\to\infty} \deg F_j = \infty$ and $\lim_{j\to\infty} N(F_j, h_j)/\deg F_j = \infty$. The following simple examples of Thue equations with $N(G, h) \geq n$ are well-known. Take $G(x, y) = \prod_{i=1}^n (x - a_i y) + hy^n$, with $\prod_{i\neq j}(a_i - a_j) \neq 0$, $a_i \in \mathbb{Z}$. Then $\{(a_i, 1), i = 1, \ldots, n\}$ are primitive solutions.

It is known that $N(F, h) \leq O(n)$ when $\mathrm{disc}(F)$ is large compared to h (see [Ste2, page 378]). We use below the fact that any subfield of $\mathbb{Q}(\xi_{p-1})$ has an unramified prime of norm p to obtain, in some cases where the Mordell-Weil rank of $X_{F,h}$ is at most $g(X_{F,h})/n$, bounds for $N(F, h, \mathbb{Q}, p)$ of the form $O(n)$ and $O(n^2)$.

Theorem 3.11. *Let $p \geq 5$ be prime and let $n := p - 1$. Let $X := X_{F,h}$. Assume that* $\mathrm{Chab}(X, \mathbb{Q}(\xi_{p-1}), (p)) < g(X)$. *This is the case, for instance, if the Mordell-Weil rank of $X/\mathbb{Q}$ is less than $(s - 2)/2$. Then*

a) If $p \nmid d^*(F)$, then $|X(\mathbb{Q})| \leq 5n - 3$.
b) If $p \mid d^*(F)$, then $N(F, h, \mathbb{Q}, p) \leq 2n^2 + 4n - 5$.

Proof. Our hypothesis allows us to apply the results of the previous section. We bound $(2g-2)(p-1)/(p-2)$ by n^2-2n-3, and s by n. Let u denote the number of points in $X(\mathbb{Q})$ with $z = 0$. Clearly, $u \leq n$. Let $v := |X(\mathbb{Q})| - u$. Then, since n is even (and -1 is in $\mathbb{Q}$), we have $|X(\mathbb{Q}(\xi_n))| \geq u + nv/2$. For part a) when $p \nmid h$, we use the bound 3.1:

$$|X(\mathbb{Q}(\xi_n))| \leq n^2 - 2n - 3 + (n - 1)(p + 1).$$

(To bound $|\overline{X}(\mathbb{F}_p)|$, use a projection from a point in $\overline{X}(\mathbb{F}_p)$.). It follows that $u + nv/2 \leq 2n^2 - n - 5$. Hence, $v \leq 4n - 2 - 10/n - 2u/n$. Thus, $v \leq 4n - 3$. We find that $|X(\mathbb{Q})| = u + v \leq n + 4n - 3$. To prove part a) when $p \mid h$, we use 3.2,

$$|X(\mathbb{Q}(\xi_n))| \leq n^2 - 2n - 3 + np.$$

Thus, $u + nv/2 \leq 2n^2 - n - 3$. Hence, $v \leq 4n - 3$, and $|X(\mathbb{Q})| \leq 5n - 3$.

In part b), we do not consider points with $z = 0$ (since such points are not primitive integral solutions). To prove part b), we use 3.3:

$$nN(F, h, \mathbb{Q}, p)/2 \leq N(F, h, \mathbb{Q}(\xi_n), p) \leq n^2 - 2n - 3 + (n-1)(p+1).$$

as well as 3.5:

$$nN(F, h, \mathbb{Q}, p)/2 \leq N(F, h, \mathbb{Q}(\xi_n), p) \leq n^2 - 2n - 3 + n^2 p.$$

To conclude the proof of the theorem, we only need to prove that, if the Mordell-Weil rank of $X/\mathbb{Q}$ is less than $(s-2)/2$, then the Chabauty rank of $\mathrm{Jac}(X/\mathbb{Q}(\xi_{p-1}))$ is less than $g(X)$. This assertion is a consequence of the following general fact.

Proposition 3.12. *Let $X/\mathbb{Q}$ denote the smooth proper model of the affine curve given by an equation $hy^n = f(x)$, with $n \mid \deg(f)$. Write $f(x) = \prod_{i=1}^{s}(x - a_i)^{n_i}$ with $\prod_{i \neq j}(a_i - a_j) \neq 0$, and assume that $\gcd(n, n_i) < n$ for all i. Fix ξ_n, a primitive n-th root of unity. Denote by σ the automorphism of $X/\mathbb{Q}(\xi_n)$ induced by $(x, y) \mapsto (x, \xi_n y)$. Assume that the Chabauty rank (with respect to any prime) of $X/\mathbb{Q}(\xi_n)$ is equal to $g(X)$. Then the factor $A_n/\mathbb{Q}$ of the jacobian of X introduced below has Mordell-Weil rank over $\mathbb{Q}$ at least equal to $(s-2)/2$.*

Proof. Let $\Phi(t) = (t^n - 1)/(t - 1)$. Let $\Phi_d(t)$ denote the d-th cyclotomic polynomial, so that $\Phi(t) = \prod_{\substack{d \mid n \\ d \neq 1}} \Phi_d(t)$. Let $\Psi_d(t) := \Phi(t)/\Phi_d(t)$. Let $d \mid n$, and consider the abelian variety

$$A_d := \mathrm{Im}(\Psi_d(\sigma)) \subset \mathrm{Jac}(X)/\mathbb{Q}(\xi_n).$$

(Note that when $d < \gcd(n, n_i)$ for some i, it may happen that A_d is trivial.) It is clear that $A_d \subset \mathrm{Ker}(\Phi_d(\sigma))$. If $d \neq d'$, then $\Phi_d(t)$ and $\Phi_{d'}(t)$ are coprime in $\mathbb{Q}$ and, thus, generate in $\mathbb{Z}[t]$ a principal ideal $q\mathbb{Z}[t]$ for some $q \in \mathbb{Z}$. We conclude that $A_d \cap A_{d'}$ is a finite set of points, killed by q. Since the polynomials $\{\Psi_d(t)\}_{d \mid n}$ are coprime in $\mathbb{Q}$, we can find $\{a_d(t) \in \mathbb{Z}[t], d \mid n, d \neq 1\}$ such that $\sum a_d(t)\Psi_d(t) = z \in \mathbb{Z}$. Hence, given $P \in \mathrm{Jac}(X)$,

$$zP = \sum \Psi_d(\sigma)(a_d(\sigma)P) \in \langle\{A_d \mid d \mid n, d \neq 1\}\rangle \subseteq \mathrm{Jac}(X)$$

and, thus, $\mathrm{Jac}(X)$ is isogenous to $\bigoplus_{\substack{d \mid n \\ d \neq 1}} A_d$.

We claim now that A_d is an abelian variety defined over $\mathbb{Q}$. Indeed, let $P = (a, b)$, where $a, b \in \overline{\mathbb{Q}}$, be a solution of $y^n = f(x)$. Let $\mu \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\mu(\xi_n) = \xi_n^c$ for some $c \in \mathbb{Z}$ with $(c, n) = 1$. It follows that on $X(\overline{\mathbb{Q}})$, we have $\sigma^c \circ \mu = \mu \circ \sigma$ for some $c \in \mathbb{Z}$. If an element Z of $\mathrm{Jac}(X)(\overline{\mathbb{Q}})$ is of the form $Z = \Psi_d(\sigma)(\sum_{i=1}^s a_i P_i)$ with $P_i \in X(\overline{\mathbb{Q}})$, then $\mu(\Psi_d(\sigma)(\sum_{i=1}^s a_i P)) = \Psi_d(\sigma^c)(\sum_{i=1}^s a_i \mu(P_i))$. Now, since $(c, n) = 1$, there is a positive integer c' such that $cc' \equiv 1 \pmod{n}$. The polynomial $\Psi_d(t)$ is a product of cyclotomic polynomials $\Phi_e(t)$ with $e \mid n$, and for any root ξ_e of $\Phi_e(t)$, it is clear that $\xi_e^{c'}$ is a root of $\Phi_e(t^c)$. Since multiplication by c' permutes $(\mathbb{Z}/e\mathbb{Z})^*$, it follows that $\Phi_e(t)$ divides $\Phi_e(t^c)$ for any $e \mid n$, and that $\Psi_d(t)$ divides $\Psi_d(t^c)$. Hence, $\mu(Z) \in A_d(\overline{\mathbb{Q}})$, for all $\mu \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It follows that A_d is defined over $\mathbb{Q}$. We determine the dimension of A_d below.

Lemma 3.13. *Suppose that $d \mid n$ and that $d > \gcd(n, n_i)$ for all $i = 1, \ldots, s$. Let $\varphi(d)$ denote the Euler φ-function. Then* $\dim(A_d) = \varphi(d) \cdot (s - 2)/2$.

Proof. By construction, $\sigma_{|A_d}$ is such that $\Phi_d(\sigma_{|A_d}) = 0$. The characteristic polynomial $\mathrm{char}(\sigma)(t)$ of σ acting on $H_1(X(\mathbb{C}), \mathbb{C})$ is computed in [Lor, 4.1]:

$$\mathrm{char}(\sigma)(t) = \Phi(t)^{s-2} \prod_{i=1}^{s} \left(\frac{x^{\gcd(n,n_i)} - 1}{x - 1} \right)^{-1}.$$

Hence, $\mathrm{rank}_{\mathbb{Z}}(\mathrm{Ker}(\varphi_d(\sigma)_{|H_1(X(\mathbb{C}),\mathbb{C})}) = (s - 2)\varphi(d)$. Using the duality between $H_1(X(\mathbb{C}), \mathbb{C})$ and $H^1(X(\mathbb{C}), \mathbb{C})$ as well as the fact that

$$0 \to H^0(X(\mathbb{C}), \Omega_X) \to H^1(X(\mathbb{C}), \mathbb{C}) \to H^1(X, \mathcal{O}_X) \to 0$$

is exact, with $H^0(X(\mathbb{C}), \Omega_X)$ and $H^1(X, \mathcal{O}_X)$ related by Serre duality, we find that $\dim A_d = \varphi(d)(s-2)/2$. This concludes the proof of Lemma 3.13.

When n is prime, $\mathrm{rank}_{\mathbb{Z}}(\mathrm{Jac}(X/\mathbb{Q}(\xi_n))) = \mathrm{rank}_{\mathbb{Z}}(\mathrm{Jac}(X/\mathbb{Q}))(n - 1)$, as shown in Lemma 13.4 of [P-S]. The reader will easily check that the proof of 13.4 can be used, *mutatis mutandis*, to show that, for any $d \mid n$,

$$\mathrm{rank}_{\mathbb{Z}}(A_d(\mathbb{Q}))\varphi(d) = \mathrm{rank}_{\mathbb{Z}}(A_d(\mathbb{Q}(\xi_d))).$$

In particular, if the Chabauty rank of $\mathrm{Jac}(X)/\mathbb{Q}(\xi_n)$ equals $g(X)$, then

$$\mathrm{rank}_{\mathbb{Z}}(A_n(\mathbb{Q}(\xi_n))) \geq \dim(A_n),$$

so that $\mathrm{rank}_{\mathbb{Z}}(A_n(\mathbb{Q})) \geq (s - 2)/2$. This concludes the proof of 3.12.

Acknowledgements The authors wish to thank John M. Grigsby for his support of research in number theory. They would also like to thank W. McCallum, B. Poonen, E. Schaefer, M. Stoll, J. Wetherell, and the referee, for helpful comments. Lorenzini thanks the Swiss NSF for financial support, and the University of Geneva and the University of North Carolina at Chapel Hill for their hospitality.

References

[B-S] E. Bombieri, W.M. Schmidt, On Thue's equation, Invent. math. **88** (1987), 69–81

[B-L] S. Bosch, Q. Liu, Rational points in the group of components of a Néron model, Manus. Math. **98** (1999), 275–293

[CHM] L. Caporaso, J. Harris, B. Mazur, Uniformity of rational points, J. AMS **10** (1997), 1–35

[Co1] R. Coleman, Torsion points on curves and p-adic Abelian integrals, Ann. of Math. **121** (1985), 111–168

[Co2] R. Coleman, Effective Chabauty, Duke Math. J. **52** (1985), 765–770

[Cz] P. Colmez, Intégration sur les variétés p-adiques, Astérisque No. 248 (1998), SMF

[C-S] Arithmetic Geometry, G. Cornell, J. Silverman, Eds, Springer-Verlag, New York, 1986

[Fuj] M. Fujimori, On the solutions of Thue equations, Tôhoku Math. J. **46** (1994), 523–539

[Hon] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan **22** (1970), 213–246

[Kob] N. Koblitz, p-adic numbers, p-adic analysis, and Zeta-Functions, Graduate Texts in Mathematics 58, Springer-Verlag, New York, 1984

[Lor] D. Lorenzini, The characteristic polynomial of a monodromy transformation attached to a family of curves, Comment. Math. Helv. **68** (1993), 111–137

[McC1] W. McCallum, The arithmetic of Fermat curves, Math. Ann. **294** (1992), 503–511

[McC2] W. McCallum, On the method of Coleman and Chabauty, Math. Ann. **299** (1994), 565–596

[P-S] B. Poonen, E. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, J. reine angew. Math. **488** (1997), 141–188

[Sch] E. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve, Math. Ann. **310** (1998), 447–471

[Scho] L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II, Math. Comp. **30** (1976), 337–360

[Ser] J.-P. Serre, Lie algebras and Lie groups, W.A. Benjamin, Inc., New York-Amsterdam, 1965

[Sha] I. Shafarevich, Basic algebraic geometry I, Springer-Verlag, New York, 1994

[Si1] J. Silverman, Representations of integers by binary forms and the rank of the Mordell-Weil group, Invent. math. **74** (1983), 281–292

[Si2] J. Silverman, A uniform bound for rational points on twists of a given curve, J. London Math. Soc. **47** (1993), 385–394

[Ste] C. Stewart, On the number of solutions of polynomial congruences and Thue equations, J. AMS **4** (1991), 793–835

[Ste2] C. Stewart, Thue equations and elliptic curves, Number Theory (Halifax, NS, 1994), 375–386, CMS Conference Proceedings **15**, AMS, Providence, RI, 1995

[St1] M. Stoll, On the arithmetic of the curves $y^2 = x^\ell + A$ and their Jacobians, J. reine angew. Math. **501** (1998), 171–189

[St2] M. Stoll, On the arithmetic of the curves $y^2 = x^\ell + A$ II, to appear in J. Number Theory

[St3] M. Stoll, Implementing 2-descent for Jacobians of hyperelliptic curves, Acta. Arith. **98** (2001), 245–277

[Vie] E. Viehweg, Invarianten der degenerierten Fasern in lokalen Familien von Kurven, J. reine angew. Math. **293** (1977), 284–308

[Wet] J. Wetherell, Bounding the number of rational points on certain curves of high rank, Ph.D. Thesis, University of California, 1997