p-ADIC HEIGHT PAIRINGS AND INTEGRAL POINTS ON HYPERELLIPTIC CURVES

JENNIFER S. BALAKRISHNAN, AMNON BESSER, AND J. STEFFEN MÜLLER

ABSTRACT. We give a formula for the component at p of the p-adic height pairing of a divisor of degree 0 on a hyperelliptic curve. We use this to give a Chabauty-like method for finding p-adic approximations to p-integral points on such curves when the Mordell-Weil rank of the Jacobian equals the genus. In this case we get an explicit bound for the number of such p-integral points, and we are able to use the method in explicit computation. An important aspect of the method is that it only requires a basis of the Mordell-Weil group tensored with $\mathbb{Q}$.

1. INTRODUCTION

Chabauty's method [Cha41], later made effective by Coleman [Col85a], is a fantastic tool for bounding the number of rational points of a curve X over a number field F and for finding p-adic approximations to these points, when the genus g is larger than the Mordell-Weil rank of the Jacobian J of X. This method has been put to effective use in many instances over the last thirty years. Chabauty wrote down p-adic functions that vanish on the set of F-rational points $X(F)$ and Coleman identified these functions as p-adic Coleman integrals of holomorphic forms [Col85b].

The fascinating recent work of Kim [Kim05, Kim09, Kim10b, CK10, BDCKW12] on a *non-abelian* Chabauty method gives hope that the restriction on the rank of J may be removed by using more general iterated Coleman integrals. When Kim's method applies and a Coleman function vanishing on $X(F)$ is found, it can sometimes be computed explicitly by recent progress on the computation of such functions [BBK10, Bal12, BB12].

In a recent example for Kim's method [Kim10a], as corrected in [BKK11], an explicit Coleman function was given in the case of an elliptic curve $E/\mathbb{Q}$ with Mordell-Weil rank 1 (satisfying some auxiliary conditions) and shown to vanish on all integral points. This function was furthermore explicitly computed in [BKK11] and indeed demonstrated numerically to vanish on integral points.

In [BB13], the first two named authors gave an entirely new proof of Kim's result, removing, on the way, some of the auxiliary assumptions, by showing that the function identified by Kim was essentially the component at p of the p-adic height and relying on the quadraticity of this height as a function on J and on the description of the other components as intersection multiplicities.

The goal of the present work is to extend the methods of [BB13] to hyperelliptic curves. Suppose that X is a hyperelliptic curve over $\mathbb{Q}$ given by the equation

$$(1.1) \qquad\qquad y^2 = f(x) \, ,$$

with f a monic polynomial of degree $2g + 1$ over $\mathbb{Z}$, and let $X_p = X \times \mathbb{Q}_p$. We can prove

Theorem 1.1. *If the Mordell-Weil rank of J is exactly g, then there exists a Coleman function ρ on X_p and a finite set of values T such that $\rho(\mathcal{U}(\mathbb{Z}[1/p])) \subset T$, where $\mathcal{U}(\mathbb{Z}[1/p])$ is the set of p-integral solutions to (1.1). If X has good reduction at p, then both ρ and T are effectively computable from a basis for $J(\mathbb{Q}) \otimes \mathbb{Q}$.*

A more precise version of this result will be given in Theorem 3.1 in Section 3. We use this to give an effective bound on the number of integral points in Theorem 6.4.

We expect that the result above will lead to a practical method for recovering all integral points on hyperelliptic curves satisfying the assumptions of the theorem (see Remark 3.7), although we have not attempted to carry this out in practice.

A different algorithm for the computation of integral points on hyperelliptic curves is given in [BMS+08]. Their algorithm combines linear forms in logarithms with a modified version of the Mordell-Weil sieve and does not assume that the rank of $J(\mathbb{Q})$ is equal to the genus. However, in contrast to our method, it does require generators of the free part of $J(\mathbb{Q})$ which limits its applicability, since currently there is no practical algorithm for the saturation of a finite index subgroup of $J(\mathbb{Q})$ unless $g = 2$ [Sto02]; the case $g = 3$ is currently being worked out, see [Sto13]. For a recent approach to this problem using arithmetic intersection theory, see [Hol12].

Our proof relies on the description of the p-adic height pairing given by Coleman and Gross [CG89], the quadraticity of the pairing, and p-adic Arakelov theory [Bes05]. For any X and F, the height pairing

$$h : J(F) \times J(F) \to \mathbb{Q}_p \, ,$$

depending on some auxiliary data, is defined initially for divisors D_1 and D_2 of degree zero with disjoint support as a sum of local height pairings

$$h(D_1, D_2) = \sum_v h_v(D_1, D_2)$$

over the finite places v of F. As in [BB13], a key point is to remove the disjoint support restriction by extending the local height pairings relative to a choice of tangent vectors, as suggested in the classical case in [Gro86]. For our hyperelliptic curve we make a certain consistent choice of such tangent vectors. The resulting local height pairing gives rise to a function $\tau(x) = h_p(x - \infty, x - \infty)$ which is computed explicitly as a Coleman integral in Theorem 2.1 and is the main summand for the function ρ. The finite set of values T results from the sum of the height pairings h_q for $q \neq p$ and is discussed in detail in Proposition 3.3.

Let us explain the reason for the restriction that X is assumed to have good reduction at p. As our work ultimately relies on p-adic Arakelov theory [Bes05], which has been developed using Vologodsky's integration theory [Vol03], it is insensitive to the type of reduction at p. However, Vologodsky's integration has been, so far, difficult to compute and the computation of Coleman integrals has been, thus far, done in the good reduction case. The situation will likely change with [BZ13], which will reduce Vologodsky integration on semi-stable curves to Coleman integration.

We briefly discuss possible applications (see also Remarks 3.9 and 6.7). The function ρ is given, on the residue disk of p-adic points reducing to a given point, by a convergent power series. It is therefore possible, in reasonable time, to compute all solutions of $\rho(x) \in T$ to high p-adic precision. We hope that this technique can be combined with the bounds on the size of the integral points on X [BMS$^+$08] to provide an effective algorithm for determining all integral points on hyperelliptic curves satisfying the assumptions of the theorem.

It is furthermore easy, given some initial coefficients in the power series expansions making up ρ, to deduce a bound on the total number of possible solutions to $\rho(x) \in T$, hence on the number of p-integral solutions to (1.1). A fairly crude version of this is given in Theorem 6.4. The bound depends on some computations, including those of Coleman integrals, on the curve. One might hope for a bound which, like [Col85a, (ii) on p. 765], will depend only on some simple numerical data of the curve, such as genus and types of bad reduction, but this is unfortunately not obvious at this point in time.

We also give a number of numerical examples to illustrate our techniques.

2. The local height pairing as a Coleman function

In this section we let p be a prime number and consider a smooth and proper curve C (we will later assume C is hyperelliptic) defined over the algebraic closure $\bar{\mathbb{Q}}_p$ of the field of p-adic numbers. We fix a point x_0 on C and a tangent vector t_0 to C at x_0. We further fix a decomposition

$$(2.1) \qquad H^1_{\mathrm{dR}}(C) = W \oplus \Omega^1(C)$$

such that W is isotropic with respect to the cup product and a branch of the p-adic logarithm which we denote by log. Given this data, the function $h_{\mathcal{T}}$ on the tangent bundle $\mathcal{T}$ to C outside of the point x_0 was defined in [BB13]. If G is the Green function associated to the data above, as defined in [Bes05], then $h_{\mathcal{T}}$ is defined as

$$h_{\mathcal{T}}(x,t) = G_x(x,t) - 2G_{x_0}(x) + G_{x_0}(x_0,t_0) \,,$$

where $G_y(x)$ is by definition $G(y,x)$ and the notation $G_x(x,t)$ stands for the constant term of G_x at x with respect to a local parameter z normalized with respect to t in the sense that $\partial_t(z) = 1$. This function is related to the local height pairing as follows: If all data are defined over a finite extension K of $\mathbb{Q}_p$, then the value $h_{\mathcal{T}}(x,t)$ lies in K and the local height, evaluated on the divisor $(x) - (x_0)$ with choices of tangent vectors t and t_0, is exactly the trace from K to $\mathbb{Q}_p$ of $h_{\mathcal{T}}(x,t)$, where the trace map is part of the data used to define the height pairing.

Suppose now that C is a hyperelliptic curve defined by the equation $y^2 = f(x)$ with f monic of degree $2g+1$. We have a basis $\{\omega_i\}_{i=0}^{2g-1}$ of the de Rham cohomology $H^1_{\mathrm{dR}}(C/\bar{\mathbb{Q}}_p)$ given by the forms of the second kind $\omega_i = x^i dx/2y$. The form ω_i has order $2g - 2 - 2i$ at ∞, and it has no pole away from ∞. In particular, the forms ω_i for $i \leq g-1$ are holomorphic. As in the introduction, we fix $\omega = \omega_0$. This form vanishes to order $2g - 2$ at infinity and has no other zeros or poles. It determines, by duality, a section t of $\mathcal{T}$ with a pole of order $2g-2$ at infinity and no other zeros or poles. On the other hand, the form ω_{g-1} has no zero or pole at infinity and we fix t_0 to be its value there. We pick a parameter $z = -y/x^{g+1}$ at infinity.

Using [BB12, (10)] and noting that z is minus the parameter t there, we easily see that z is normalized with respect to the dual of t_0. We note the cup product

formula [BB12, Lemma 5.10]

$$(2.2) \qquad \omega_i \cup \omega_{2g-1-j} = \frac{1}{2g - 2j - 1} \delta_{ij} \quad \text{if } i = j \text{ or } i \leq 2g - 1 - j.$$

Let $\{\bar{\omega}_i\}_{i=0}^{g-1}$ be the basis for W which is dual to the basis $\{\omega_i\}_{i=0}^{g-1}$ for the holomorphic forms via the cup product. From (2.2) it follows that

$$(2.3) \qquad \bar{\omega}_i = (2g - 2i - 1)\omega_{2g-1-i} + \text{ a holomorphic form.}$$

Theorem 2.1. *Let τ be the pullback of $h_{\mathcal{T}}$ under t. Then we have*

$$\tau(x) = -2 \int_{t_0}^{x} \left(\sum_{i=0}^{g-1} \omega_i \int_{t_0}^{y} \bar{\omega}_i \right) ,$$

where both integrals are with respect to the tangential base point t_0 at ∞ ($\int_{t_0}^{y} \bar{\omega}_i$ means more precisely, the integral normalized to have constant term 0 with respect to the parameter z).

Proof. According to [Bes05, Proposition 2.7], we have that τ, being the pullback of a log function by a section, is a Coleman function on the complement U of infinity in C and if $\bar{\partial}$ denotes the p-adic del bar operator, then $\bar{\partial} d\tau$ is the pullback of the curvature of the restriction of $h_{\mathcal{T}}$ to U under $t(x)$. But the curvature on $h_{\mathcal{T}}$ is $-2 \sum_{i=0}^{g-1} \bar{\omega}_i \otimes \omega_i$ by [BB13, Proposition 3.10], and we obtain

$$d\tau = \sum_{i=0}^{g-1} \omega_i \int \bar{\omega}_i + \theta$$

where θ is a holomorphic form on U and the integrals are indefinite. There is the indeterminancy of the constant of integration and of the form θ. Note that the constant of integration for the $\bar{\omega}_i$ simply adds to θ holomorphic forms on C. Thus we have

$$\tau(x) + 2 \int_{t_0}^{x} \left(\sum_{i=0}^{g-1} \omega_i \int_{t_0}^{y} \bar{\omega}_i \right) = \int \theta'$$

where θ' is holomorphic on U. We would like to show that the right hand side vanishes.

First we argue that the form θ' extends to a holomorphic form on C. To see this we observe that it follows from (2.3) that $\omega_i(\int \bar{\omega}_i)$ has a simple pole at infinity and no other pole. On the other hand, since ω_0 has no poles or zeros outside infinity, $t(x)$ as a section of $\mathcal{T}$ also has no such zeros and poles outside infinity. It follows that the form $d\tau$ also has a simple pole at infinity and no other pole. Indeed, by [Bes05, Definition 4.1] and the ensuing remarks, if s is a non-vanishing section of $\mathcal{T}$, then locally for the analytic topology, τ looks like $\log_{\mathcal{T}}(s) + d \log(t/s)$ with $\log_{\mathcal{T}}(s)$ analytic. Thus, θ' has a simple pole at infinity but being meromorphic the residue theorem implies that it is in fact holomorphic on C (one can directly compute the residue at infinity and easily discover that it is 0).

Next we claim that $\theta = 0$. This is because both τ and the integral on the right hand side of the theorem are symmetric with respect to the hyperelliptic involution w. For τ this follows from functoriality of the height pairing similar to the way it is proved in [BB13]. For the integral, we first note that all forms considered are anti-symmetric with respect to w. Then the integral of a $\bar{\omega}_i$ is anti-symmetric up to a constant, and this is 0 because the constant term with respect to a parameter

which is itself anti-symmetric is 0. Thus, all terms $\omega_i \int_{t_0}^{y} \bar{\omega}_i$ are symmetric, and their integral is so as well. Consequently, θ is a holomorphic symmetric form on C, hence 0.

It follows that the equality in the statement of the theorem holds up to a constant. It suffices to show that the constant term of τ at infinity is 0. This is true for τ replaced by the pullback of $h_{\mathcal{T}}$ under the dual of ω_{g-1}. Indeed, as ω_{g-1} is dual to the non-vanishing t_0 at infinity, the result follows from [BB13, Proposition 3.10]. However, this pullback differs from τ by $\log(x^{g-1}) = (g-1)\log(x)$. One easily checks the expansion $x = z^{-2}(1 + \cdots)$ from which we have

$$\log(x) = -2\log(z) + \text{ a power series vanishing at } 0.$$

The constant term of x with respect to z is therefore 0. $\qquad\square$

3. APPLICATION TO p-INTEGRAL POINTS

The results of the previous section may be used, in a similar way to the results in [BB13], to obtain a p-adic characterisation of p-integral points on hyperelliptic curves, a kind of "quadratic Chabauty." Let $f \in \mathbb{Z}[x]$ be a separable and monic polynomial of degree $2g + 1 \geq 3$.

Let $\mathcal{U} = \mathrm{Spec}(\mathbb{Z}[x,y]/(y^2 - f(x)))$, so that $\mathcal{U}(\mathbb{Z}[1/p])$ is exactly the set of p-integral solutions to $y^2 = f(x)$. Let X be the normalization of the closure of the generic fiber of $\mathcal{U}$ and let J be its Jacobian.

Theorem 3.1. *Let f_i, for $i = 0, \ldots, g-1$, be defined by the formula*

$$f_i(z) = \int_{\infty}^{z} \omega_i,$$

and let $g_{ij} = g_{ji} = f_i \cdot f_j$ for $i \leq j$. Suppose that the Mordell-Weil rank of J is exactly g. Then either there exists a linear combination of the f_i that vanishes on $\mathcal{U}(\mathbb{Z}[1/p])$ (in other words, Chabauty's method works, at least for the p-integral points), or there exist constants $\alpha_{ij} \in \mathbb{Q}_p$ such that the function

$$(3.1) \qquad\qquad \rho(z) = \tau(z) - \sum_{i \leq j} \alpha_{ij} g_{ij}(z)$$

satisfies the following:

(1) *The function ρ vanishes on every $x \in \mathcal{U}(\mathbb{Z}[1/p])$ which does not intersect any of the singular points in any of the bad fibers of $\mathcal{U}$.*

(2) *There is a finite set of values T such that $\rho(\mathcal{U}(\mathbb{Z}[1/p])) \subset T$. Assuming Coleman integrals can be computed on X_p, the set T is effectively computable.*

Proof. We recall that the height pairing depends on the choice of a $\mathbb{Q}_p$-valued idele class character $\ell = \oplus \ell_q$, a sum over all finite primes q. Fixing a choice for the p-adic logarithm, which we simply denote by log, we can choose ℓ in such a way that $\ell_p = \log$. In this case, the trace map mentioned in the introduction is simply the identity and the local height pairing h_p is simply the pairing mentioned there, so that $h_p((x) - (\infty), (x) - (\infty))$, normalized as before, is simply $\tau(x)$.

If Chabauty's method does not work, the f_i, extended linearly, induce linearly independent $\mathbb{Q}_p$-valued functionals on the g-dimensional vector space $J(\mathbb{Q}) \otimes \mathbb{Q}$. It follows that the g_{ij} are a basis for the space of $\mathbb{Q}_p$-valued quadratic forms on $J(\mathbb{Q}) \otimes \mathbb{Q}$. The height pairing h, being another $\mathbb{Q}_p$-valued quadratic form on V,

is thus a linear combination of the above basis, $h = \sum \alpha_{ij} g_{ij}$. If $x \in X(\mathbb{Q})$, then, applying the last formula to the divisor $(x) - (\infty)$, Theorem 2.1 implies that

$$(3.2) \qquad \rho(x) = -\sum_{q \neq p} h_q((x) - (\infty), (x) - (\infty)) .$$

Note that the local heights h_q are computed using the localization of the same global tangent vectors as before. According to Proposition 3.3 below, when x is a p-integral point and either the reduction at q is good, or, more generally, the reduction is bad but x does not reduce to a singular point modulo q, we have $h_q((x) - (\infty), (x) - (\infty)) = 0$. In general, Proposition 3.3 implies that there is a proper regular model $\mathcal{X}$ of $X \times \mathbb{Q}_q$ over $\mathbb{Z}_q$ such that if x is p-integral, the above quantity depends solely (and explicitly, see Section 5) on the component of the special fiber $\mathcal{X}_q$ that the section in $\mathcal{X}(\mathbb{Z}_q)$ corresponding to x intersects. Thus, for any p-integral point x, the right hand side of (3.2) can only take a finite number of explicitly computable values, completing the proof. $\qquad \square$

Remark 3.2. From the proof it is clear that the size of the set T is bounded by $1 + \prod_q (m_q - 1)$, where m_q is the number of multiplicity one components of the special fiber $\mathcal{X}_q$, as these are the only components through which x can pass.

We construct a normal model $\mathcal{X}'$ of $X \times \mathbb{Q}_q$ over $\mathrm{Spec}(\mathbb{Z}_q)$ as follows: If $F(X, Z)$ is the degree $2g + 2$-homogenization of f, then the equation

$$Y^2 = F(X, Z)$$

gives a smooth plane projective model of C in projective space $\mathbb{P}^2_{\mathbb{Q}_q}(1, g+1, 1)$ over $\mathbb{Q}_q$ with respective weights 1, $g + 1$ and 1 assigned to the variables X, Y, Z. Let $\mathcal{X}'$ be the scheme defined by the same equation in $\mathbb{P}^2_{\mathbb{Z}_q}(1, g+1, 1)$. We call $\mathcal{X}'$ the *Zariski closure* of $X \times \mathbb{Q}_q$ over $\mathrm{Spec}(\mathbb{Z}_q)$.

By [Liu02, Corollary 8.3.51], there exists a proper regular model $\mathcal{X}$ of $X \times \mathbb{Q}_q$ over $\mathbb{Z}_q$, together with a proper birational morphism $\phi : \mathcal{X} \to \mathcal{X}'$ that is an isomorphism outside the singular locus of $\mathcal{X}'$. Such a model is called a *desingularization in the strong sense* of $\mathcal{X}'$.

If y is a $\mathbb{Q}_q$-rational point on X, then, by abuse of notation, we also denote the corresponding section $y \in \mathcal{X}(\mathbb{Z}_q)$. Let Γ_0 denote the component of the fiber of $\mathcal{X}$ above q that ∞ intersects.

Proposition 3.3. *Let $\mathcal{X}$ be as above and let x be a p-integral point. The value of $h_q((x) - (\infty), (x) - (\infty))$ depends only on the component of the fiber of $\mathcal{X}$ above q that x passes through, and is 0 if this component is Γ_0.*

Proof. Let us first recall how $h_q((x) - (\infty), (x) - (\infty))$ is computed [Gro86, Section 5]. Let $(.)$ denote the rational-valued intersection multiplicity on $\mathcal{X}$. By [Lan88, Theorem III.3.6], there is a vertical divisor $\Phi((x) - (\infty))$ on $\mathcal{X}$ with rational coefficients such that $D_x = x - \infty + \Phi((x) - (\infty))$ satisfies $(D_x . \Gamma) = 0$ for all vertical divisors $\Gamma \in \mathrm{Div}(\mathcal{X})$. The local height pairing $h_q((x) - (\infty), (x) - (\infty))$ is then given by

$$(3.3) \qquad h_q((x) - (\infty), (x) - (\infty)) = -(D_x . D_x) \log q .$$

Up to addition of a rational multiple of the entire special fiber $\mathcal{X}_q$, which is irrelevant for intersections with vertical divisors, $\Phi((x) - (\infty))$ only depends on which component the section x passes through, see also Section 5. Furthermore, if x and

∞ pass through the same component, then we can take $\Phi((x) - (\infty)) = 0$. Note that the intersection $(D_x \,.\, D_x)$ is equal to

$$(x - \infty)^2 + \Phi((x) - (\infty))^2.$$

One computes the intersection $D_x \,.\, D_x$ using the following rule for self-intersection of horizontal components: Let $x \in \mathcal{X}(\mathbb{Z}_q)$, and let t be the chosen tangent vector at x. Then:

- If t is a generator to the tangent bundle at x, then $x \,.\, x = 0$.
- More generally, if αt is a generator, with $\alpha \in \mathbb{Q}_q$, then $x \,.\, x = -v_q(\alpha)$,

where v_q is the q-adic valuation (see 3 of Definition 2.3 in [BB13]). By Lemma 3.4 (iv), we have $\infty \,.\, \infty = 0$. The intersection product is multiplied by $\ell_q(q)$ (more generally, q should be replaced with a uniformizer for the completion at q) to obtain the local height. We note that the p-integrality of x implies that $x \,.\, \infty = 0$.

In our case the tangent vector at x is determined as the dual to the value of the differential form ω at that point. The following lemma implies that the product $x \,.\, x$ depends only on which component of the special fiber x goes through and is 0 when this is the component Γ_0, completing the proof. $\qquad\square$

Lemma 3.4. *Let $\mathcal{X}$ and ω be as above and write the divisor $\mathrm{div}(\omega) \in \mathrm{Div}(\mathcal{X})$ as $\mathrm{div}(\omega) = H + V$, where H is horizontal and V is vertical. Let $x \in X(\mathbb{Q}_q)$.*

- (i) *We have $H = (2g - 2) \cdot \infty$.*
- (ii) *For the intersection product, as normalized by our chosen tangent vectors, we have $x \,.\, x = -x \,.\, \mathrm{div}(\omega)$. In particular, $x \,.\, x = -x \,.\, V$ if $x \in \mathcal{U}(\mathbb{Z}_q)$.*
- (iii) *The component Γ_0 is not contained in V.*
- (iv) *We have $\infty \,.\, \infty = -\infty \,.\, \mathrm{div}(\omega_{g-1}) = 0$, where the self-intersection is taken with respect to t_0.*

Proof. The proof of (i) is obvious. Using cotangent vectors, the formula for the self-intersection $x \,.\, x$ becomes: if $\alpha\omega(x)$ is a generator for the cotangent bundle at x, with $\alpha \in \mathbb{Q}_p$, then $x \,.\, x = v_q(\alpha)$. But this is exactly $-x \,.\, \mathrm{div}(\omega)$. Indeed, for any line bundle $\mathcal{L}$ on $\mathcal{X}$ and any meromorphic section s of $\mathcal{L}$ that has no zeros or poles at x on the generic fiber, the pullback $x^*\mathcal{L}$ is a free $\mathbb{Z}_q$-module of rank 1 and $s(x)$ is a non-zero element of $x^*\mathcal{L} \otimes \mathbb{Q}_q$. When $s(x) \in x^*\mathcal{L}$ and $\alpha \,.\, s(x)$ is a generator for $x^*\mathcal{L}$ we have

$$v_q(\alpha) = -\log_q \#(x^*\mathcal{L}/s(x)\mathbb{Z}_q)$$

and the right hand side is well-known to be equal to $-\mathrm{div}(s) \,.\, x$. The behavior of intersection with a principal divisor implies that this continues to hold without the assumption $s(x) \in x^*\mathcal{L}$. When $x \in \mathcal{U}(\mathbb{Z}[1/p])$ we know that $x \,.\, \infty = 0$, so using (i) we get $x \,.\, x = -x \,.\, V$.

For (iii), note that on the integral affine subscheme $\mathcal{U} \times \mathbb{Z}_q$ of $\mathcal{X}'$, both the relative cotangent bundle and the relative dualizing sheaf over $\mathrm{Spec}(\mathbb{Z}_q)$ are generated by $\omega|_{\mathcal{U} \times \mathbb{Z}_q}$, see [Liu02, §6.4]. Hence t generates the tangent bundle on $\mathcal{U}$. But since $\mathcal{X}'$ and $\mathcal{X}$ are isomorphic outside the singular locus of $\mathcal{X}'$ by assumption, (ii) implies

$$0 = (x \,.\, x) = -(V \,.\, x)$$

for any $\mathbb{Q}_q$-rational point x such that x does not reduce to ∞ or a singular point modulo q. So $\mathrm{div}(\omega)$ cannot contain Γ_0.

Finally, (iv) follows similarly: The form ω_{g-1} is just $-du/2v$ on the affine patch of X given by $v^2 = m(u)$, where $u = 1/x, v = y/x^{g+1}$ and $m(u) = u^{2g+2}f(1/u)$. We

know that ∞ does not reduce to a singular point modulo q by our assumptions on f. So (iv) follows, using the fact that $du/2v$ generates $\Omega^1_{\mathrm{Spec}(\mathbb{Z}_q[u,v]/v^2 - m(u))/\mathrm{Spec}(\mathbb{Z}_q)}$.
$\square$

Remark 3.5. If $g = 1$ and the given equation of C is a minimal Weierstraß equation, then we can take $\mathcal{X}$ to be the minimal regular model of C. In this case it is easy to show that $\mathrm{div}(\omega) = 0$.

Remark 3.6. The computation of the function ρ requires the following ingredients.
- Coleman integration, including iterated Coleman integrals [Bal12], for the computation of τ
- Computation of p-adic height pairings [BB12, BMS12].
- A basis for the Mordell-Weil group of J tensored with $\mathbb{Q}$. Typically one computes this by searching for points of small height in $J(\mathbb{Q})$ (or differences of rational points on X) until we have found g independent points. Note that we first need to verify that the rank of $J(\mathbb{Q})$ is indeed g, for instance using 2-descent on J, cf. [Sto01].

Clearly, computing the height pairings between all pairs of elements of the above basis, together with the computation of the integrals of the ω_i on elements of this basis, suffice for the determination of the constants α_{ij}. Integrals of holomorphic forms give the f_i's, hence the g_{ij}'s, and iterated Coleman integrals give τ. Note that one can get bounds on the number of integral points without computing iterated integrals, see Remark 6.5.

Remark 3.7. Here we describe how to use these ideas to give an algorithm to find integral points on a genus g hyperelliptic curve X with Mordell-Weil rank g:
(1) Let $D_1, \ldots, D_g \in \mathrm{Div}^0(X)$ be representatives of the elements of a basis for the Mordell-Weil group of the Jacobian tensored with $\mathbb{Q}$. We compute the global p-adic height pairings $h(D_1, D_1), h(D_1, D_2), \ldots, h(D_g, D_g)$ and the $\frac{g(g+1)}{2} \times \frac{g(g+1)}{2}$ matrix of the Coleman integrals $\int_{D_i} \omega_k \int_{D_j} \omega_l$ for $1 \leq i \leq j \leq g$ and $0 \leq k \leq l \leq g-1$. Solving a linear system (see Example 7.2) gives the vector of α_{ij} values in (3.1).
(2) Compute the finite set T of possible values that ρ can take on p-integral points.
(3) Compute the value of $\tau(P)$ for some point P on the curve. Use (4.1) and the power series expansions of the Coleman integrals $\{f_\ell(t) = \int_\infty^t \omega_\ell\}_{\ell=0}^{g-1}$ to give a power series describing $\tau(t)$ in each residue disk.
(4) The integral points are solutions to $\tau(t) - \sum \alpha_{ij} f_i(t) f_j(t) = b$ across the various residue disks, where b runs through the elements of T.
(5) Use bounds on the size of integral points to determine precision and provably terminate the algorithm.

We show how to carry out steps (1)–(4) in practice in Section 7.

Remark 3.8. Consider the more general case where our curve is given by an equation $y^2 = f(x)$, but we only assume that f is integral, not necessarily monic. Then the intersection $(\infty . \infty)$ at a prime q, computed using t_0, is still given by

$$(\infty . \infty) = -(\mathrm{div}(\omega_{g-1}) . \infty),$$

but the right hand side may be nontrivial. This means that we can generalize the results of the present section to this case, at least under the assumption that f is

not a square modulo q for any prime q (including the case that f vanishes mod q). This assumption is trivially satisfied if f is monic and guarantees that there is a unique component Γ_0 which dominates the special fiber of the Zariski closure of X over $\mathrm{Spec}(\mathbb{Z})$, since this closure is normal with irreducible special fibers. However, ∞ will not necessarily intersect Γ_0 any longer.

- Proposition 3.3 and Lemma 3.4 (i), (ii), (iii) continue to hold.
- The self-intersection $(\infty . \infty)$ can only be nontrivial if ∞ is singular modulo q, i.e. if q divides the leading coefficient of f.
- Let a denote the global intersection $a = \sum_{q \neq p} (\infty . \infty)_q \cdot \log(q)$. Then Theorem 3.1 almost continues to hold; the only difference being that on p-integral points z not reducing to any singular point, we have $\rho(z) = a$.
- The sum a is effectively computable using linear algebra, essentially using the techniques described in Section 5.

The only problem is that we assume f to be monic for several p-adic analytic statements. However, this can be rectified and we will come back to this in future work.

Remark 3.9. It would be interesting to try to use height pairings to find integral points for number fields other than $\mathbb{Q}$. The problem is that in this case the p-adic manifold obtained by tensoring with $\mathbb{Q}_p$ has dimension > 1 while the height pairing still provides only one equation. A possible solution is to use more than one idele class character. Let us describe one simple situation where this can be made to work.

Suppose L is an imaginary quadratic extension with class number 1 where the prime p remains inert. Since the group of units is torsion, one can lift any $\ell_p : L_p^\times \to \mathbb{Q}_p$ to an idele class character: A uniformizer at the (principal) prime ideal (α) will be sent to $-\ell_p(\alpha)$. Composing the p-adic log with a basis to the $\mathbb{Q}_p$-linear functionals $L_p \to \mathbb{Q}_p$ we get two different ℓ_p, hence two idele class characters, from which we get two p-adic equations, and we may expect these to carve out a finite number of solutions in L_p-points.

4. Computation of τ

To obtain numerical examples, we need to compute the function ρ from (3.1). This function involves height function computations for the determination of the constants α_{ij} appearing there, for which we have the algorithm of [BB12, BMS12], and the computation of Coleman integrals of holomorphic forms, which can be performed using the algorithms of [BBK10].

The remaining component is the computation of the function τ, which is an iterated Coleman integral [Bal12]. In this section, we discuss how to leverage information about local p-adic height pairings to compute iterated integrals from tangential points as an alternative to direct computation of these integrals.

One way to avoid directly computing iterated integrals from tangential points is to compute the iterated integral with one specific endpoint[1] P (chosen in a certain favorable way) in some indirect way. The integral for a general point can then be computed from this (see (4.1) below). For example, in the case of elliptic curves,

---

[1]In this section we will be using the coordinate functions extensively. We therefore denote, unlike in previous sections, points on the curve by P, Q, etc.

in [BKK11] the point P was taken to be a global two-torsion point or a tangential point at infinity, while in [BB13] a (non-global) 2 or 3-torsion point was used.

In the hyperelliptic curve case, we can also integrate from finite Weierstrass points, but this requires working over totally ramified extensions of $\mathbb{Q}_p$, which is, in practice, quite slow. As an alternative approach, we describe a technique for computing $\tau(P)$ for a general point P that does not use the description of τ in terms of iterated integrals in Theorem 2.1 but instead works directly with the description of τ as a local height pairing. Given $\tau(P)$, the value of τ at any other point P' may be computed using the following formula.

$$
\begin{aligned}
\tau(P') &= -2 \int_{t_0}^{P'} \left(\sum_{i=0}^{g-1} \omega_i \bar{\omega}_i \right) \\
(4.1) \qquad &= -2 \sum_{i=0}^{g-1} \left(\int_{t_0}^{P} \omega_i \bar{\omega}_i + \int_{P}^{P'} \omega_i \bar{\omega}_i + \int_{P}^{P'} \omega_i \int_{t_0}^{P} \bar{\omega}_i \right) \\
&= \tau(P) - 2 \sum_{i=0}^{g-1} \left(\int_{P}^{P'} \omega_i \bar{\omega}_i + \int_{P}^{P'} \omega_i \int_{t_0}^{P} \bar{\omega}_i \right)
\end{aligned}
$$

where we are using a decomposition of iterated integrals which may be found for example in [BKK11, p. 288].

We note that for applications, the description of τ in terms of local power series expansions is vital. Thus, while we are able to compute $\tau(P')$ for any given P', we will be using (4.1) after computing $\tau(P)$ for one, or possibly a finite number, of values of P, as this last formula does in fact give such a power series expansion.

The strategy for computing $\tau(P)$ is to interpret it as a normalized local height and to directly compute this using an extension of the techniques of [BB12].

To this end, it is first of all somewhat helpful to use cotangent vectors rather than tangent vectors for the normalization. Let ω denote a choice, for each point on the curve C, of a cotangent vector at that point. This could obviously come from a differential form but could also be just an arbitrary assignment. We can write $h_{\mathrm{loc}}(D_1, D_2)_\omega$ for the local height pairing of D_1 and D_2, computed with respect to the tangent vectors dual to the cotangent vectors specified in ω. This notation has the advantage that if f is an isomorphism of curves, one has, by an easy argument

$$
h_{\mathrm{loc}}(f^* D_1, f^* D_2)_{f^* \omega} = h_{\mathrm{loc}}(D_1, D_2)_\omega
$$

where $f^* \omega$ means the pointwise pullback of the cotangent vectors with respect to the differential of f at a point (this coincides with the usual pullback for holomorphic forms). Another important observation is that

$$
h_{\mathrm{loc}}(D_1, D_2)_{-\omega} = h_{\mathrm{loc}}(D_1, D_2)_\omega,
$$

because of the property [BB13, Definition 2.3] of the local height pairing. For the hyperelliptic case, the assignment ω corresponds to one form away from infinity, and to the value of another form there, but both are anti-symmetric with respect to the hyperelliptic involution w, so with that choice of ω we have

$$
h_{\mathrm{loc}}(w^* D_1, w^* D_2)_\omega = h_{\mathrm{loc}}(D_1, D_2)_\omega .
$$

Thus, with this choice of tangent vectors, the splitting into symmetric and anti-symmetric components of [BB12] extends without any difficulty. In particular, we

can use formula (19) there. Using the shorthand $h_{\mathrm{loc}}(D)_\omega$ for $h_{\mathrm{loc}}(D, D)_\omega$, and taking $D = (P) - (\infty)$, we have

$$
\begin{aligned}
\tau(P) &= h_{\mathrm{loc}}((P) - (\infty))_\omega \\
&= \frac{1}{4}h_{\mathrm{loc}}((P) - (\infty) + w((P) - (\infty)))_\omega + \frac{1}{4}h_{\mathrm{loc}}((P) - (\infty) - w((P) - (\infty)))_\omega \\
&= \frac{1}{4}h_{\mathrm{loc}}((P) + (w(P)) - 2(\infty))_\omega + \frac{1}{4}h_{\mathrm{loc}}(P - (w(P)))_\omega \; .
\end{aligned}
$$

Suppose now that $P = (a, b)$ is a point with non-Weierstrass reduction. We compute $h_{\mathrm{loc}}((P) + (w(P)) - 2(\infty))_\omega$. Since $(P) + (w(P)) - 2(\infty)$ is the divisor of the function $x - a$, this local term is log on the normalized value of $x - a$ on $(P) + (w(P)) - 2(\infty)$. To compute this, we note that a normalized parameter with respect to ω at P is

$$
\tag{4.2}
z = \frac{x - a}{2b},
$$

and so the normalized value $(x - a)[P]$ is just $2b$. On the other hand, a normalized parameter with respect to t_0 at infinity is given by $-y/x^{g+1}$. Therefore, the normalized value of $x - a$ at infinity is

$$
\lim_{x \to \infty} (x - a)\frac{y^2}{x^{2g+2}} = \lim_{x \to \infty} (x - a)\frac{f(x)}{x^{2g+2}} = 1 \; .
$$

Collecting all the data and using [BB13, Definition 2.3] we find

$$
h_{\mathrm{loc}}((P) + (w(P)) - 2(\infty))_\omega = \log(-4b^2) = \log(4b^2) \; .
$$

Next we compute the anti-symmetric part, $h_{\mathrm{loc}}((P) - (w(P)))_\omega$. By [BB13, Proposition 3.4], the local height pairing for two divisors (which are not necessarily disjoint) is given by

$$
h_{\mathrm{loc}}(D_1, D_2)_\omega = G_{D_1}[D_2]
$$

where, by [Bes05, Theorem 7.3], if the degree of D_1 is 0, the Green function G_{D_1} coincides with with the Coleman integral $\int \omega_{D_1}$. Here ω_{D_1} is, as in [BB12], a certain form of the third kind whose residue divisor is D_1, and the value of this integral on D_2 is normalized by taking constant terms with respect to local parameters which are normalized with respect to the chosen cotangent vectors.

In our case we have $D_1 = D_2 = D = (P) - (\infty)$. As in [BB12, Algorithm 5.8] we can decompose ω_D as $\nu - \eta$, where ν is an arbitrary form of the third kind with residue divisor D while η is holomorphic and is computed from ν and from the decomposition (2.1) as in [BB12, Subsection 5.6]. We consequently have

$$
h_{\mathrm{loc}}(P - (w(P)))_\omega = \int_{w(P)}^{P} \nu - \int_{w(P)}^{P} \eta \; .
$$

The integral of η can be computed using the techniques in [BBK10]. The integral $\int_{w(P)}^{P} \nu$ has to be normalized since ν has poles at the endpoints P and $w(P)$. To properly account for this normalization, we use an auxiliary point Q in the same residue disk as P.

More concretely, by [BB12, Proposition 5.13] we may take $\nu = \frac{b\,dx}{y(x-a)}$, which is anti-symmetric. Using this and breaking the path of integration into several pieces,

we obtain

$$\int_{w(P)}^{P} \nu = \int_{w(P)}^{Q} \nu + \int_{Q}^{P} \nu = \int_{w(Q)}^{P} \nu + \int_{Q}^{P} \nu,$$
$$= \int_{Q}^{P} \nu + \int_{w(Q)}^{Q} \nu + \int_{Q}^{P} \nu$$
$$= -2 \int_{P}^{Q} \nu + \int_{w(Q)}^{Q} \nu .$$

The first integral is a tiny integral, but again, since it has a pole at P, this has to be normalized with respect to the chosen cotangent vector, which we do below. The second integral was considered in [BB12, Algorithm 4.8]; here we make a small modification, also discussed below, to handle a subsequent part of the computation (that of a tiny integral with a pole within the disk of integration).

4.1. Computing $\int_P^Q \nu$.

Let z be a parameter at P, e.g., (4.2), which is normalized with respect to ω. Writing ν in terms of z we get $\nu = (z^{-1} + a_0 + a_1 z + \cdots)dz$, since ν has a simple pole with residue 1 at P. The normalized integral $\int_P^Q \nu$ is the normalized integral of ν evaluated at Q. The normalization means that the constant term with respetct to z of the integral is 0, i.e., that it is of the form $\log(z) + a_0 z + a_1 z^2/2 + \cdots$. If we use the parameter $t = (x - a) = 2bz$ instead we can rewrite this as $\log(t) - \log(2b) +$ some power series in t, where this power series is nothing but the term by term integral of $\nu - t^{-1}dt$. Thus, in terms of the parameter t the formula for the integral is

$$\int_P^Q \nu = \log(t(Q)) - \log(2b) + \int_0^{t(Q)} (\nu - t^{-1}dt).$$

4.2. Computing $\int_{w(Q)}^Q \nu$.

By [BB12, (14)], we know

$$(4.3) \qquad \int_{w(Q)}^{Q} \nu = \frac{1}{1-p} \left(\Psi(\alpha) \cup \Psi(\beta) + \sum_{A \in \mathcal{S}} \mathrm{Res}_A \left(\alpha \int \beta \right) - 2 \int_Q^{\phi(Q)} \nu \right),$$

where $\alpha = \phi^*\nu - p\nu$ (a form constructed via a p-power lift of Frobenius ϕ), $\mathcal{S}$ is the set of closed points, β has residue divisor $Q - w(Q)$, and Ψ is a logarithm map.

Each of the quantities in (4.3) can be computed using the techniques in [BB12], except for $\mathrm{Res}_{A \in \mathcal{S}} \left(\alpha \int \beta \right)$, since β has poles in certain residue disks which, by construction, are disks which contain points in $\mathcal{S}$ – i.e., disks where the integration will take place. Here we give an elementary lemma which allows us to extend the techniques of [BB12] to handle this case.

Lemma 4.1. *Suppose β has residue divisor $Q - wQ$, where Q is assumed to be non-Weierstrass. The integral of β computed between points P, P' distinct from Q but contained in the residue disk of Q, written as*

$$\int_P^{P'} \beta = \int_P^{P'} \frac{f(x(Q)) - f(x)}{y(x - x(Q))(y(Q) + y)} dx + \log \left(\frac{x(P') - x(Q)}{x(P) - x(Q)} \right)$$

converges.

Proof. Since P, P' are in the same residue disk, we compute a locally analytic parametrization $(x(t), y(t))$ from P to P' and use this to rewrite:

$$\int_P^{P'} \beta = \int_P^{P'} \frac{y(Q)dx}{y(x - x(Q))}$$

$$= \int_P^{P'} \frac{y(Q)dx}{x - x(Q)} \left(\frac{1}{y} - \frac{1}{y(Q)} \right) + \int_P^{P'} \frac{dx}{x - x(Q)}$$

$$= \int_0^1 \frac{f(x(Q)) - f(x(t))}{y(t)(x(t) - x(Q))(y(Q) + y(t))} dx(t) + \log \left(\frac{x(P') - x(Q)}{x(P) - x(Q)} \right).$$

It remains to check the convergence of the integrand. Since Q is non-Weierstrass, both $y(t)$ and $y(Q) + y(t)$ are p-adic units.

The claim is then that $v_p \left(\frac{f(x(Q)) - f(x(t))}{x(t) - x(Q)} \right) \geq 0$. Indeed, since $x(Q) - x(t)$ divides $f(x(Q)) - f(x(t))$, we see that $v_p \left(\frac{f(x(Q)) - f(x(t))}{x(t) - x(Q)} \right)$ is simply the p-adic valuation of the linear coefficient of $f(x)$, which is assumed to be integral.

$\square$

5. COMPUTING ALL POSSIBLE VALUES OF ρ ON $X(\mathbb{Z}[1/p])$

Let q be a prime and let $\phi : \mathcal{X} \to \mathcal{X}'$ denote desingularization in the strong sense of the Zariski closure $\mathcal{X}'$ of $C := X \times \mathbb{Q}_q$ over $\mathrm{Spec}(\mathbb{Z}_q)$.

For $D \in \mathrm{Div}(C)$ we also write, by abuse of notation, D for the Zariski closure (with multiplicities) of D in $\mathrm{Div}(\mathcal{X})$. If $D \in \mathrm{Div}^0(C)$, then there exists a vertical $\mathbb{Q}$-divisor $\Phi_q(D) \in \mathrm{Div}(\mathcal{X}) \times \mathbb{Q}$ such that $D + \Phi_q(D)$ has trivial intersection multiplicities with all vertical divisors on $\mathcal{X}$, see [Lan88, Theorem III.3.6]. Since $\Phi_q(D)$ is vertical itself, we have

$$(\Phi_q(D) . D)_q = -\Phi_q(D)^2 \geq 0.$$

From now on, we will assume that $\mathcal{X}$ is a desingularization in the strong sense of the Zariski closure $\mathcal{X}'$ of $X \times \mathbb{Q}_q$ over $\mathbb{Z}_q$. It follows from the proof of Theorem 3.1, from (3.3) and from Lemma 3.4 that a point $x \in X(\mathbb{Z}[1/p])$ satisfies

$$\rho(x) = -\sum_{q \neq p} \left(\Phi_q((x) - (\infty))^2 + (x . V_q) \right)_q,$$

where V_q is the vertical part of $\mathrm{div}(\omega)$ over q. Note that only bad primes can contribute toward the sum on the right hand side.

In the remainder of this subsection we discuss how the quantity

$$\left(\Phi_q((x) - (\infty))^2 + (x . V_q) \right)_q$$

can be computed for a given prime q and $x \in C(\mathbb{Z}_q)$. Let $M_q = (m_{ij})_{i,j}$ denote the intersection matrix of the special fiber $\mathcal{X}_q = \sum a_i \Gamma_i$. Its entries are given by $m_{ij} = (a_i \Gamma_i . a_j \Gamma_j)$. For simplicity, we drop the subscript q in the following, as we will work over a fixed prime q.

The matrix M has rank $n - 1$, where n is the number of irreducible components of $\mathcal{X}_q$, and its kernel is spanned by the vector $(1, \ldots, 1)^T$, see [Lan88, § III.3]. Let M^+ denote the Moore-Penrose pseudoinverse of M and let $u(x)$ denote the column vector whose ith entry is $(x - \infty . a_i \Gamma_i)$. Then it is easy to see that we have

$$(5.1) \qquad \Phi((x) - (\infty))^2 = u(x)^T M^+ u(x).$$

We sketch a different method to compute $\Phi((x) - (\infty))^2$. By [CR93] one can associate a metrized graph G to the special fiber $\mathcal{X}_q$ such that if $\mathcal{X}_q$ is semistable, then we can take G to be the dual graph of $\mathcal{X}_q$, suitably metrized.

Let Γ_x and Γ_0 denote the component of $\mathcal{X}_q$ that x reduces to. Then we have

$$\Phi((x) - (\infty))^2 = -r(\Gamma_x, \Gamma_0),$$

where $r(\Gamma_x, \Gamma_0)$ is the resistance between the nodes Γ_x and Γ_0 if we consider the graph G as a resistive electric circuit such that the resistance of each edge is equal to its length. Using work from [BGX03], there is a purely graph-theoretic formula for the resistance when all edges have length 1, which is the case for semistable $\mathcal{X}_q$.

Now we discuss the computation of $(x . V)$. Recall that $\operatorname{div}(\omega) = H + V$, where H is horizontal and V is vertical. We call a $\mathbb{Q}$-divisor $\mathcal{K}$ on $\mathcal{X}$ a *canonical $\mathbb{Q}$-divisor on $\mathcal{X}$* if $\mathcal{O}(\mathcal{K}) \cong \boldsymbol{\omega}_{\mathcal{X}/\operatorname{Spec}(\mathbb{Z}_q)}$, where $\boldsymbol{\omega}_{\mathcal{X}/\operatorname{Spec}(\mathbb{Z}_q)}$ is the relative dualizing sheaf of $\mathcal{X}$ over $\operatorname{Spec}(\mathbb{Z}_q)$.

Since $\operatorname{div}(\omega)|_X = (2g - 2) \cdot \infty$ is a canonical divisor on X, it follows from [CK09, Proposition 2.5] that we can extend H to a canonical $\mathbb{Q}$-divisor $\mathcal{K} = H + V'$ on $\mathcal{X}$ if V' is a vertical $\mathbb{Q}$-divisor such that $\mathcal{K}$ satisfies the adjunction formula

$$(5.2) \qquad\qquad \mathcal{K} . \Gamma = -\Gamma^2 + 2g(\Gamma) - 2$$

for all components Γ of the special fiber of $\mathcal{X}$. Such an extension always exists (see [KM12, §2] for a more general statement), but it is not unique, because the validity of (5.2) is unchanged if we add a multiple of the entire special fiber $\mathcal{X}_q$ to V'. If we also require that V' does not contain the component Γ_0, then V' is uniquely determined.

It is not true in general that $\operatorname{div}(\omega)$ is a canonical divisor on $\mathcal{X}$, since $\boldsymbol{\omega}_{\mathcal{X}/\operatorname{Spec}(\mathbb{Z}_q)}$ may differ from the relative cotangent bundle $\Omega^1_{\mathcal{X}/\operatorname{Spec}(\mathbb{Z}_q)}$. But restricting to the smooth locus $\mathcal{X}^{\mathrm{sm}}$, we have

$$\boldsymbol{\omega}_{\mathcal{X}/\operatorname{Spec}(\mathbb{Z}_q)}|_{\mathcal{X}^{\mathrm{sm}}} \cong \Omega^1_{\mathcal{X}/\operatorname{Spec}(\mathbb{Z}_q)}|_{\mathcal{X}^{\mathrm{sm}}}$$

by [Liu02, Corollary 6.4.13]. Hence $V - V'$ is supported in the vertical divisors of multiplicity at least 2, which immediately implies

$$(x . V) = (x . V').$$

Therefore it suffices to compute V'. The adjunction formula (5.2) and the constraint $\Gamma_0 \notin \operatorname{supp}(V')$ reduce the computation of V' to a system of linear equations which has a unique solution by the above discussion.

5.1. **Local contributions for ρ in genus 2.** Keeping the notation of the previous subsection, we now compute all possible values of

$$\left(\Phi((x) - (\infty))^2 + (x . V) \right)$$

if the genus of C is 2 and $\mathcal{X}_q$ has semistable reduction. The possible special fibers of minimal regular models of curves of genus 2 have been classified by Namikawa-Ueno [NU73]. In particular, it is known that if $\mathcal{X}$ is semistable, then the reduction types of $\mathcal{X}$ are either $[I_{n_1} - I_{n_2} - m]$ or $[I_{n_1 - n_2 - n_3}]$, where $m, n_1, n_2, n_3 \geq 0$ are integers.

In Table 1 we list the stable model corresponding to each reduction type and the relation to the discriminant Δ of a minimal Weierstraß model of X. Because of our assumptions on f, the reduction type $[I_{n_1 - n_2 - n_3}]$ cannot occur, since the reduction of f modulo q would have to be a square.

reduction type	stable reduction	$v_q(\Delta)$
$[I_{0-0-0}]$	smooth curve of genus 2	0
$[I_{n_1-0-0}]$	genus 1 curve with a unique node	n_1
$[I_{n_1-n_2-0}]$	genus 0 curve with exactly 2 nodes	$n_1 + n_2$
$[I_{n_1-n_2-n_3}]$	union of 2 genus 0 curves, intersecting in 3 points	$n_1 + n_2 + n_3$
$[I_0 - I_0 - m]$	union of two smooth genus 1 curves, intersecting in 1 point	$12m$
$[I_n - I_0 - m]$	union of a smooth genus 1 curve and a genus 0 curve with a unique node, intersecting in 1 point	$12m + n_1$
$[I_{n_1} - I_{n_2} - m]$	union of 2 genus 0 curves with a unique node, intersecting in 1 point	$12m + n_1 + n_2$

TABLE 1. Semistable reduction types in genus 2

We now list all possible values $\Phi((x) - (\infty))^2$, where $x \in X(\mathbb{Q}_q)$. We also list all possible values $x \, . \, \infty$ and the possible sums $\Phi((x) - (\infty))^2 + (x \, . \, \infty)$.

First we consider reduction type $[I_{n_1-n_2-0}]$, where $n_1, n_2 \geq 0$. It is easy to see that we have $V = V' = 0$. The set of all possible values for $\Phi((x) - (\infty))^2$ is

$$\left\{ -\frac{i(n_1 - i)}{n_1} \right\} \cup \left\{ -\frac{j(n_2 - j)}{n_2} \right\}, \quad 0 \leq i \leq \lfloor n_1/2 \rfloor, \ 0 \leq j \leq \lfloor n_2/2 \rfloor,$$

see [MS13, §6]. The possible values for reduction type $[I_{n_1} - I_{n_2} - m]$, where $n_1, n_2, m \geq 0$, depend on where ∞ intersects the special fiber. This information can be obtained easily from the equation of C.

If ∞ intersects a component corresponding to I_{n_1}, then it is easy to see that $(x \, . \, V) \in \{0, -1, \ldots, -m\}$. Moreover, we have

$$(5.3) \qquad \Phi((x) - (\infty))^2 \in \left\{ -i, \ -\frac{j \cdot (n_1 - j)}{n_1}, \ -m - \frac{k \cdot (n_2 - k)}{n_2} \right\},$$

and

$$(5.4) \qquad \Phi((x) - (\infty))^2 + (x \, . \, \infty) \in \left\{ -2i, \ -\frac{j \cdot (n_1 - j)}{n_1}, \ -2m - \frac{k \cdot (n_2 - k)}{n_2} \right\},$$

where $i \in \{0, \ldots, m\}$, $j \in \{0, \ldots, \lfloor n_1/2 \rfloor\}$ and $k \in \{0, \ldots, \lfloor n_2/2 \rfloor\}$. If ∞ intersects a component corresponding to I_{n_2}, then we get all possible values upon swapping both n_1 and n_2 and j and k in (5.3) and (5.4).

Remark 5.1. If we have two singular points in the reduction of X modulo q which are conjugate over $\mathbb{F}_{q^2}$, then we know that x must intersect Γ_0 and hence $\Phi((x) - (\infty))^2 + (x \, . \, \infty) = 0$.

Remark 5.2. Note that the denominators are contained in $\{1, n_1, n_1 n_2\}$.

6. BOUNDS ON THE NUMBER OF p-INTEGRAL POINTS

In this section we sketch how one may use the techniques of this paper to obtain a bound on the number of p-integral points on a hyperelliptic curve. We hope that these techniques will eventually lead to an effective bound that will only depend on the genus and the bad reduction types.

The following is a trivial extension of Lemma 2 in [Col85a].

Lemma 6.1. *Let $f(t) = \sum a_n t^n$ be a power series with coefficients in $\mathbb{C}_p$. Let β be the function whose graph is the bottom of the Newton polygon for f, and let $k \geq 0$ be an integer. Then, for any $s > 0$ we have*

$$\#\{z \in \mathbb{C}_p,\ v(z) \geq s,\ f(z) = 0\} \leq \max\{n \geq k,\ v(a_k) - s(n - k) \geq \beta(n)\},$$

where v is the p-adic valuation normalized so that $v(p) = 1$.

Proof. Suppose that there are m zeros of f with valuation $\geq s$. Since $\beta(k) \leq v(a_k)$ it suffices to show that $\beta(m) \geq \beta(k) - s(m - k)$. But this is clear, as by assumption, by the properties of the Newton polygon, the slopes of β up to the point where $x = m$ are at most $-s$. $\qquad\square$

Obviously, in the above lemma, any lower bound for β may be used instead of β to obtain an upper bound on the number of zeros. To use this in our setting, we need the following obvious lemma.

Lemma 6.2. *Suppose, under the assumptions of the above lemma, that f is an r-fold iterated integral of forms $\omega_1, \ldots, \omega_r$ which have integral coefficients, and that furthermore the constants of integration at each integration are integral as well. Then we have the lower bound $\beta(k) \geq -r \log_p(n)$.*

In [Col85a], Coleman uses the following corollary to get an upper bound on the number of rational points.

Corollary 6.3. *Suppose under the assumptions of Lemma 6.1 that f' has integral coefficients and that its reduction has order k. Then,*

$$\#\{z \in \mathbb{C}_p,\ v(z) \geq s,\ f(z) = 0\} \leq \max\{n \geq k,\ s(n - k) \leq [\log_p(n)]\}\ .$$

Coleman then uses a bound on the sum of all possible k's in the above corollary, over all power series occurring as local power series expansions of a Coleman integral, to obtain a global bound on the number of rational points, when Chabauty's method applies, which depends only on the genus and the number of points in the reduction of the curve.

As an application of our techniques, we give a fairly easily computed bound on the number of integral points. The reader will recognize that one may improve the bound and remove restrictions at the cost of making the bound depend on more complicated data.

Specializing Lemmas 6.1 and 6.2 to the case $r = 2$, $k = s = 1$, we get that for power series satisfying the conditions of Lemma 6.2, the number of $p\mathbb{Z}_p$ roots is bounded from above by

$$(6.1) \qquad \Upsilon(v(a_1))\ ,\ \text{with}\ \Upsilon(m) = \max\{n \geq 1,\ m - (n - 1) \geq -2 \log_p(n)\}\ .$$

We note, for ease of application that

(1) if $m + 3 < p$, then $\Upsilon(m) = m + 2$.
(2) if $m + 5 < p^2$, then $\Upsilon(m) = m + 4$.

Theorem 6.4. *Suppose, under the assumptions of Theorem 3.1 that the polynomial f has no roots modulo p. Let α_{ij} be the constants appearing in the theorem and let Υ be the function from (6.1).*

Let P_m be $\mathbb{Z}_p$-points of X lifting all $\mathbb{Z}/p$ points of the special fiber save ∞, and for each m, let t_m be local parameters at P_m, whose reduction modulo p is also a parameters. Define constants β_{im}, γ_{im}, $\bar{\gamma}_{im}$ by

$$\beta_{im} = \frac{\omega_i}{dt_m}(P_m)$$

and

$$\gamma_{im} = \int_{t_0}^{P_m} \omega_i \ , \ \bar{\gamma}_{im} = \int_{t_0}^{P_m} \bar{\omega}_i \ .$$

Let $L = \max\{0, -v(\alpha_{ij}), 0 \le i, j \le g-1\}$ and let

$$\delta_m = 2\sum_{i=0}^{g-1} \beta_{im}\bar{\gamma}_{im} + \sum_{i \le j} \alpha_{ij}(\beta_{im}\gamma_{jm} + \beta_{jm}\gamma_{im}).$$

Then, the number of integral solutions to $y^2 = f(x)$ is bounded from above by

$$(1 + \prod_q (m_q - 1))\sum_m \Upsilon(v_p(\delta_m) + L)$$

where, as in Remark 3.2, m_q denotes the number of multiplicity 1 components at the fiber above q.

Proof. Note that the combined assumption that we are looking at integral, rather than p-integral points, and that f has no roots modulo p, means that we only need to consider non-Weierstrass residue disks. Multiplying by p^L clears denominators from the α_{ij} and it is therefore evident that the expansion of $p^L\rho$ around P_m satisfies the condition of Lemma 6.2, except possibly that the constant coefficient of the power series is not integral. The first coefficient is exactly $p^L\delta_m$. Thus, to conclude the proof by Theorem 3.1 Lemma 6.1, Lemma 6.2 and Remark 3.2, it suffices to note that having a non-integral value for the constant coefficient of the power series flattens the Newton polygon and so improves the bound on the number of solutions. $\qquad\square$

Remark 6.5. To use the theorem above to compute a bound on the number of integral points, one needs the following

- Non-iterated Coleman integrals. These are required for the computation of γ_{ij} and $\bar{\gamma}_{ij}$, and also for the computation of the α_{ij}.
- A basis of $J(\mathbb{Q}) \otimes \mathbb{Q}$.
- Computation of p-adic height pairings [BB12, BMS12]

Iterated Coleman integrals are not required. One may use them, however, or the techniques of Section 4, to get the values of τ at the points P_m, and these may be used to give a more precise bound, typically though with a lot more work.

At the moment, we are unfortunately unable to produce a Coleman-Chabauty-like bound, because we are unable to control a quantity like the sum of all k's in Coleman's case for iterated Coleman integrals. We plan to return to this question in future work.

Remark 6.6. We may observe that we can treat primes in the denominators of our points, at the cost of extending the set T, as long as we have a bound on the denominator.

Remark 6.7. We briefly sketch how one may try to use the techniques of this paper to find S-integral points where S is a finite set of primes. Suppose, for example, that $S = \{p, q\}$, where p and q are two distinct primes where X has good reduction. The case where x is either p or q-integral is already covered by our results, so we may assume that x reduces to infinity at both p and q. Since we do not assume integrality at q, the local contribution to the height pairing there is going to be of the form $2g(x \cdot \infty)_q \log_p q$, where $(x \cdot \infty)_q$ is the intersection index of x and ∞ at q. This follows easily from the description of this contribution in the proof of Proposition 3.3 and from Lemma 3.4. Therefore, the new p-adic equation for x would read $\rho(x) + 2g(x \cdot \infty)_q \log_p q \in T$. Thus, the integer $n = (x \cdot \infty)_q$ influences linearly the constant term of the power series equation for x, which we may write $a_0(n)$. As n tends to infinity we may neglect other terms and we can see that with probability 1 if $n = O(p^k)$, then $v_p(a_0(n)) \leq k$. As k tends to infinity this implies that the p-adic valuation of a solution to the power series equation is bounded roughly by k, which means that $(x \cdot \infty)_p$ is bounded roughly by k. Reversing the roles of p and q we can repeat the process, which results in a bound for $(x \cdot \infty)_p$ and $(x \cdot \infty)_q$. Now we use the previous remark.

7. Examples

Here we give some examples illustrating the techniques described in this paper.

7.1. Genus 1. Let $X : y^2 = x^3 - 3024x + 70416$, which has minimal model with Cremona label "57a1." We have that $X(\mathbb{Q})$ has Mordell-Weil rank 1, with $P = (60, -324)$ the generator of the free part of the Mordell-Weil group. We take as our working prime $p = 7$. Since the given equation of X is not a minimal Weierstraß equation, Remark 3.5 does not apply. The only primes q where the Zariski closure of X over $\mathrm{Spec}(\mathbb{Z}_q)$ is not already regular are $q = 2, 3$. Using `Magma` [BCP97], we compute a desingularization $\mathcal{X}$ of the Zariski closure of X in the strong sense. The special fibers are of the form

$$\mathcal{X}_2 = \Gamma_{2,0} + \Gamma_{2,1} + 2\Gamma_{2,2}$$

and

$$\mathcal{X}_3 = \Gamma_{3,0} + \Gamma_{3,1} + \Gamma_{3,2} + 2\Gamma_{3,3},$$

where all components $\Gamma_{q,i}$ have genus 0 and $\Gamma_{q,0}$ is the component which ∞ intersects. The intersection matrices are given by:

$$M_2 = \begin{pmatrix} -2 & 0 & 1 \\ 0 & -2 & 1 \\ 1 & 1 & -1 \end{pmatrix} \quad M_3 = \begin{pmatrix} -2 & 0 & 0 & 1 \\ 0 & -4 & 2 & 1 \\ 0 & 2 & -2 & 0 \\ 1 & 1 & 0 & -1 \end{pmatrix}.$$

Writing $\mathrm{div}(\omega) = V_2 + V_3$, we have

(7.1) $V_2 = -\Gamma_{2,1} + a_{2,2}\Gamma_{2,2}$ and $V_3 = -\Gamma_{3,1} - \Gamma_{3,2} + a_{3,3}\Gamma_{3,3}$,

computed using the method alluded to in Section 5. Here $a_{2,2}$ and $a_{3,3}$ are irrelevant, since no $\mathbb{Q}_q$-rational point can intersect a component of multiplicity at least 2.

7.1.1. *Computing local and global p-adic heights of the Mordell-Weil generator.* Using Sage [S$^+$13], we compute the local height above 7 using Coleman integration and cotangent vectors:

$$h_7(P - wP, P - wP) = 4 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + O(7^7),$$

and we can compute the contributions away from $p = 7$ using (7.1) and (5.1) to deduce the global 7-adic height:

$$h(P - wP, P - wP) = h_7(P - wP, P - wP) - 2\log_7(2) - 2\log_7(3)$$
$$= 6 \cdot 7 + 5 \cdot 7^2 + 4 \cdot 7^3 + 4 \cdot 7^5 + 7^6 + O(7^7),$$

which one can check agrees with Harvey's implementation [Har08] of Mazur-Stein-Tate's algorithm [MST06] for $h(2P)$.

This gives

$$\tau(P) = \frac{1}{4}\log_7(4y(P)^2) + \frac{1}{4}h(P - wP, P - wP)$$
$$= 4 \cdot 7^2 + 4 \cdot 7^3 + 5 \cdot 7^4 + 3 \cdot 7^5 + 6 \cdot 7^6 + O(7^7).$$

Since $\tau(P)$ is the local component of the 7-adic height above 7 (that is, by definition, we have $\tau(P) = h_7(P - \infty, P - \infty)$), we can put this together with the contributions away from $p = 7$ to compute the global 7-adic height:

$$h(P - \infty) = h(P - \infty, P - \infty) = \tau(P) - 2\log_7(2) - \frac{5}{2}\log_7(3)$$
$$= 5 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 5 \cdot 7^4 + 2 \cdot 7^5 + O(7^7).$$

7.1.2. α_{00}. We have

$$\alpha_{00} = \frac{h(P - \infty)}{\left(\int_\infty^P \omega_0\right)^2}.$$

This gives

$$\rho(P) = \tau(P) - \alpha_{00}\left(\int_\infty^P \omega_0\right)^2$$
$$= 2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^5 + 6 \cdot 7^6 + O(7^7).$$

7.1.3. $\rho(z)$ *values.* By (3.2), we can combine (5.1) and (7.1) to compute the set T of all possible values of $\rho(z)$ for 7-integral points z on X. It turns out that we have

$$T = \{i \cdot \log_7(2) + j \cdot \log_7(3) \; : \; i = 0, 2, \; j = 0, 2, 5/2\} \, .$$

We compute the values of

$$\rho(z) = \tau(z) - \alpha_{00}\left(\int_\infty^z \omega_0\right)^2$$

for the sixteen integral points:

$$(-48, \pm 324), (-12, \pm 324), (24, \pm 108), (33, \pm 81),$$
$$(40, \pm 116), (60, \pm 324), (132, \pm 1404), (384, \pm 7452),$$

and find that they all lie in the set T.

z	$\rho(z)$ (computed)	$\rho(z)$
$(-48, 324)$	$2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^5 + 6 \cdot 7^6 + O(7^7)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$
$(-12, 324)$	$5 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 2 \cdot 7^5 + 5 \cdot 7^6 + O(7^7)$	$2\log_7(2) + 2\log_7(3)$
$(24, 108)$	$5 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 2 \cdot 7^5 + 5 \cdot 7^6 + O(7^7)$	$2\log_7(2) + 2\log_7(3)$
$(33, 81)$	$6 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 5 \cdot 7^4 + 7^5 + 4 \cdot 7^6 + O(7^7)$	$\frac{5}{2}\log_7(3)$
$(40, 116)$	$3 \cdot 7 + 4 \cdot 7^2 + 5 \cdot 7^3 + 7^4 + 6 \cdot 7^5 + 7^6 + O(7^7)$	$2\log_7(2)$
$(60, 324)$	$2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^5 + 6 \cdot 7^6 + O(7^7)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$
$(132, 1404)$	$5 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 2 \cdot 7^5 + 5 \cdot 7^6 + O(7^7)$	$2\log_7(2) + 2\log_7(3)$
$(384, 7452)$	$2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^5 + 6 \cdot 7^6 + O(7^7)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$
$(-48, -324)$	$2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^5 + 6 \cdot 7^6 + O(7^7)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$
$(-12, -324)$	$5 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 2 \cdot 7^5 + 5 \cdot 7^6 + O(7^7)$	$2\log_7(2) + 2\log_7(3)$
$(24, -108)$	$5 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 2 \cdot 7^5 + 5 \cdot 7^6 + O(7^7)$	$2\log_7(2) + 2\log_7(3)$
$(33, -81)$	$6 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 5 \cdot 7^4 + 7^5 + 4 \cdot 7^6 + O(7^7)$	$\frac{5}{2}\log_7(3)$
$(40, -116)$	$3 \cdot 7 + 4 \cdot 7^2 + 5 \cdot 7^3 + 7^4 + 6 \cdot 7^5 + 7^6 + O(7^7)$	$2\log_7(2)$
$(60, -324)$	$2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^5 + 6 \cdot 7^6 + O(7^7)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$
$(132, -1404)$	$5 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 2 \cdot 7^5 + 5 \cdot 7^6 + O(7^7)$	$2\log_7(2) + 2\log_7(3)$
$(384, -7452)$	$2 \cdot 7 + 4 \cdot 7^2 + 7^3 + 7^5 + 6 \cdot 7^6 + O(7^7)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$

Remark 7.1. Note that this is recovering the result in [BDCKW12, p. 23] describing the integral points within the set $\mathcal{X}(\mathbb{Z}_p)_2$ of weakly global points of level 2 for a semistable rank 1 elliptic curve, up to normalization. (Our $\rho(z)$ values, calculated on a minimal model, are twice the corresponding values of $\|w\|$.)

7.2. **Genus 2.** Let $X : y^2 = x^3(x-1)^2 + 1$. Using a 2-descent as implemented in Magma, one checks that $J(X)$ has Mordell-Weil rank 2 over $\mathbb{Q}$. We are grateful to Michael Stoll for checking that X has only the six obvious integral points $(2, \pm 3), (1, \pm 1), (0, \pm 1)$, using the methods of [BMS+08]. Let $P = (2, -3), Q = (1, -1), R = (0, 1)$. Then $[P - \infty]$ and $[Q - R]$ are generators of the free part of the Mordell-Weil group. We take as our working prime $p = 11$. The only prime q where the Zariski closure of X over $\mathrm{Spec}(\mathbb{Z}_q)$ is not already regular is $q = 2$. Using Magma, we find that there is a desingularization of the Zariski closure of X in the strong sense such that

$$\mathcal{X}_2 = \Gamma_0 + \Gamma_1 + \Gamma_2 + \Gamma_3,$$

where all components Γ_i have genus 0. Since the intersection matrix is

$$M = \begin{pmatrix} -4 & 2 & 1 & 1 \\ 2 & -2 & 0 & 0 \\ 1 & 0 & -2 & 1 \\ 1 & 0 & 1 & -2 \end{pmatrix}$$

this implies that $\mathrm{div}(\omega) = 2\infty$ has no vertical component. Note that Γ_0 and Γ_1 have an intersection point of multiplicity 2 and $\Gamma_0, \Gamma_2, \Gamma_3$ intersect in one point, so $\mathcal{X}$ is not semistable.

7.2.1. *Heights of Mordell-Weil generators.* Let $D_1 = P - \infty$ and $D_2 = Q - R$. Using Sage, we compute the local 11-adic height above 11 as

$$h_{11}(D_1, D_1) = \frac{1}{4}\log_{11}(4y(P)^2) + \frac{1}{4}h_{11}(P - wP, P - wP)$$
$$= 10 \cdot 11 + 2 \cdot 11^2 + 9 \cdot 11^3 + 9 \cdot 11^4 + 8 \cdot 11^5 + O(11^7).$$

Away from $p = 11$, $h(D_1, D_1)$ only has a contribution at 2 (computed using (5.1)), and we have

$$h(D_1, D_1) = -\frac{2}{3} \log_{11}(2) + h_{11}(D_1, D_1)$$
$$= 7 \cdot 11 + 11^2 + 8 \cdot 11^3 + 8 \cdot 11^4 + 7 \cdot 11^5 + 2 \cdot 11^6 + O(11^7).$$

Using $2P - S - wS \sim 2P - 2\infty$, where $S = (-2/9, -723/9^3)$, we compute

$$h_{11}(D_1, D_2) = \frac{1}{2} \left(h_{11}(P - S, Q - R) - h_{11}(P - wS, wQ - wR) \right)$$
$$= 4 \cdot 11 + 4 \cdot 11^2 + 8 \cdot 11^3 + 4 \cdot 11^4 + 9 \cdot 11^5 + O(11^7)$$

and

$$h(D_1, D_2) = \frac{1}{2} \left(h(P - S, Q - R) - h(P - wS, wQ - wR) \right)$$
$$= \frac{1}{2} \left(h_{11}(P - S, Q - R) - \left(-\frac{1}{3} \log_{11}(2) + h_{11}(P - wS, wQ - wR) \right) \right)$$
$$= 3 \cdot 11 + 10 \cdot 11^2 + 9 \cdot 11^3 + 6 \cdot 11^4 + 4 \cdot 11^5 + 4 \cdot 11^6 + O(11^7).$$

Finally, we have

$$h_{11}(D_2, D_2) = h_{11}(Q - R, wR - wQ)$$
$$= 3 \cdot 11 + 4 \cdot 11^2 + 4 \cdot 11^3 + 11^4 + 11^5 + 3 \cdot 11^6 + O(11^7)$$

and

$$h(D_2, D_2) = \frac{5}{6} \log_{11}(2) + h_{11}(D_2, D_2)$$
$$= 8 \cdot 11 + 2 \cdot 11^4 + 6 \cdot 11^5 + 6 \cdot 11^6 + O(11^7).$$

Note that for $h(D_1, D_2)$ and $h(D_2, D_2)$ our chosen representatives are disjoint, so we can use the techniques of [BB12, BMS12].

7.2.2. *The coefficients α_{ij}.* We compute the coefficients α_{ij} using the matrix of the various products of Coleman integrals evaluated at D_1, D_2 (as in [BBK10]) and the global 11-adic heights computed above:

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \int_{D_1} \omega_0 \int_{D_1} \omega_0 & \int_{D_1} \omega_0 \int_{D_1} \omega_1 & \int_{D_1} \omega_1 \int_{D_1} \omega_1 \\ \int_{D_1} \omega_0 \int_{D_2} \omega_0 & \int_{D_1} \omega_0 \int_{D_2} \omega_1 & \int_{D_1} \omega_1 \int_{D_2} \omega_1 \\ \int_{D_2} \omega_0 \int_{D_2} \omega_0 & \int_{D_2} \omega_0 \int_{D_2} \omega_1 & \int_{D_2} \omega_1 \int_{D_2} \omega_1 \end{pmatrix}^{-1} \begin{pmatrix} h(D_1, D_1) \\ h(D_1, D_2) \\ h(D_2, D_2) \end{pmatrix}.$$

This gives

$$\alpha_{00} = 8 \cdot 11^{-1} + 8 + 5 \cdot 11 + 3 \cdot 11^2 + 2 \cdot 11^3 + 9 \cdot 11^4 + O(11^5),$$
$$\alpha_{01} = 6 \cdot 11^{-1} + 3 + 10 \cdot 11 + 3 \cdot 11^2 + 10 \cdot 11^3 + 3 \cdot 11^4 + O(11^5),$$
$$\alpha_{11} = 8 \cdot 11^{-1} + 8 + 3 \cdot 11 + 10 \cdot 11^2 + 4 \cdot 11^3 + 8 \cdot 11^4 + O(11^5).$$

7.2.3. *Values of ρ on 11-integral points.* Since $\text{div}(\omega)$ is horizontal, we only need (5.1) to compute the set

$$T = \left\{ 0, \frac{1}{2} \log_{11}(2), \frac{2}{3} \log_{11}(2) \right\}$$

of all possible values of ρ on 11-integral points. Computing $\rho(z)$ using (3.1) we find that the resulting values on all integral points indeed lie in our predicted set T.

z	$\rho(z)$ (computed)	$\rho(z)$
$(2,-3)$	$4 \cdot 11 + 10 \cdot 11^2 + 7 \cdot 11^4 + 10 \cdot 11^5 + 4 \cdot 11^6 + O(11^7)$	$\frac{2}{3}\log_{11}(2)$
$(1,-1)$	$3 \cdot 11 + 2 \cdot 11^2 + 6 \cdot 11^3 + 2 \cdot 11^4 + 5 \cdot 11^5 + 6 \cdot 11^6 + O(11^7)$	$\frac{1}{2}\log_{11}(2)$
$(0,1)$	$4 \cdot 11 + 10 \cdot 11^2 + 7 \cdot 11^4 + 10 \cdot 11^5 + 4 \cdot 11^6 + O(11^7)$	$\frac{2}{3}\log_{11}(2)$
$(2,3)$	$4 \cdot 11 + 10 \cdot 11^2 + 7 \cdot 11^4 + 10 \cdot 11^5 + 4 \cdot 11^6 + O(11^7)$	$\frac{2}{3}\log_{11}(2)$
$(1,1)$	$3 \cdot 11 + 2 \cdot 11^2 + 6 \cdot 11^3 + 2 \cdot 11^4 + 5 \cdot 11^5 + 6 \cdot 11^6 + O(11^7)$	$\frac{1}{2}\log_{11}(2)$
$(0,-1)$	$4 \cdot 11 + 10 \cdot 11^2 + 7 \cdot 11^4 + 10 \cdot 11^5 + 4 \cdot 11^6 + O(11^7)$	$\frac{2}{3}\log_{11}(2)$

References

[Bal12]   J. S. Balakrishnan. Iterated Coleman integration for hyperelliptic curves. In *Algorithmic number theory (ANTS X)*. 2012.

[BB12]   J. S. Balakrishnan and A. Besser. Computing local p-adic height pairings on hyperelliptic curves. *IMRN*, 2012(11):2405–2444, 2012.

[BB13]   J. S. Balakrishnan and A. Besser. Coleman-Gross height pairings and the p-adic sigma function. To appear in Crelle, 2013.

[BBK10]   J. S. Balakrishnan, R. W. Bradshaw, and K. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010.

[BCP97]   W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BDCKW12]   J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves. *Preprint*, 2012. `http://arxiv.org/abs/1209.0640`.

[Bes05]   A. Besser. p-adic Arakelov theory. *J. Number Theory*, 111(2):318–371, 2005.

[BGX03]   R. B. Bapat, I. Gutman, and W. Xiao. A simple method for computing resistance distance. *Z. Naturforsch.*, 58a:494–498, 2003.

[BKK11]   J. S. Balakrishnan, K. S. Kedlaya, and M. Kim. Appendix and erratum to "Massey products for elliptic curves of rank 1". *J. Amer. Math. Soc.*, 24(1):281–291, 2011.

[BMS+08]   Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and S. Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885, 2008.

[BMS12]   J. S. Balakrishnan, J. S. Müller, and W. Stein. A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties. *Preprint*, 2012. `http://arxiv.org/abs/1210.2739`.

[BZ13]   A. Besser and S. Zerbes. Vologodsky integration on semi-stable curves. In preparation, 2013.

[CG89]   R. Coleman and B. Gross. p-adic heights on curves. In J. Coates, R. Greenberg, B. Mazur, and I. Satake, editors, *Algebraic number theory*, volume 17 of *Advanced Studies in Pure Mathematics*, pages 73–81. Academic Press, Boston, MA, 1989.

[Cha41]   C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[CK09]   C. Curilla and U. Kühn. On the arithmetic self-intersection number of the dualizing sheaf for Fermat curves of prime exponent. *Preprint*, 2009. `http://arxiv.org/abs/0906.3891`.

[CK10]   J. Coates and M. Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010.

[Col85a]   R. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Col85b]   R. Coleman. Torsion points on curves and p-adic abelian integrals. *Annals of Math.*, 121:111–168, 1985.

[CR93]   T. Chinburg and R. Rumely. The capacity pairing. *J. Reine Angew. Math.*, 434:1–44, 1993.

[Gro86]   B. H. Gross. Local heights on curves. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 327–339. Springer, New York, 1986.

[Har08]   D. Harvey. Efficient computation of p-adic heights. *LMS J. Comput. Math.*, 11:40–59, 2008.

[Hol12]   D. Holmes. An Arakelov-theoretic approach to naive heights on hyperelliptic Jaco-
           bians. *Preprint*, 2012. `http://arxiv.org/abs/1207.5948`.
[Kim05]   M. Kim. The motivic fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel.
           Invent. Math., 161(3):629–656, 2005.
[Kim09]   M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res.
           Inst. Math. Sci.*, 45(1):89–133, 2009.
[Kim10a]   M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*,
           23(3):725–747, 2010.
[Kim10b]   M. Kim. p-adic L-functions and Selmer varieties associated to elliptic curves with
           complex multiplication. *Ann. of Math. (2)*, 172(1):751–759, 2010.
[KM12]   U. Kühn and J. S. Müller. Lower bounds on the arithmetic self-intersection number
           of the relative dualizing sheaf on arithmetic surfaces. *Preprint*, 2012. `http://arxiv.
           org/abs/1205.3274`.
[Lan88]   S. Lang. *Introduction to Arakelov theory*. Springer-Verlag, New York, 1988.
[Liu02]   Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate
           Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the
           French by Reinie Erné, Oxford Science Publications.
[MS13]   J. S. Müller and M. Stoll. Canonical heights on genus two Jacobians. In preparation,
           2013.
[MST06]   B. Mazur, W. Stein, and J. Tate. Computation of p-adic heights and log convergence.
           Doc. Math., (Extra Vol.):577–614 (electronic), 2006.
[NU73]   Y. Namikawa and K. Ueno. The complete classification of fibres in pencils of curves
           of genus two. *Manuscripta Math.*, 9:143–186, 1973.
[S+13]   W. A. Stein et al. *Sage Mathematics Software (Version 5.6)*. The Sage Development
           Team, 2013. `http://www.sagemath.org`.
[Sto01]   M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*,
           98:245–277, 2001.
[Sto02]   M. Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104:165–
           182, 2002.
[Sto13]   M. Stoll. An explicit theory of heights for hyperelliptic Jacobians of genus three. In
           preparation, 2013.
[Vol03]   V. Vologodsky. Hodge structure on the fundamental group and its application to
           p-adic integration. *Moscow Mathematical Journal*, 3(1):205–247, 2003.

Jennifer S. Balakrishnan, Department of Mathematics, Harvard University, 1 Ox-
ford Street, Cambridge, MA 02138

Amnon Besser, Mathematical Institute, 24–29 St Giles', Oxford OX1 3LB, United
Kingdom

J. Steffen Müller, Department of Mathematics, Universität Hamburg, Bundesstrasse
55, 20146 Hamburg, Germany