ACTA MATHEMATICA VIETNAMICA
Volume 37, Number 4, 2012, pp. 579–588

HANOI LECTURES ON THE ARITHMETIC OF HYPERELLIPTIC CURVES

BENEDICT H. GROSS

1. Introduction

Manjul Bhargava and I have recently proved a result on the average order of the 2-Selmer groups of the Jacobians of hyperelliptic curves of a fixed genus $n \geq 1$ over $\mathbb{Q}$, with a rational Weierstrass point [2, Thm 1]. A surprising fact which emerges is that the average order of this finite group is equal to 3, independent of the genus n. This gives us a uniform upper bound of $\frac{3}{2}$ on the average rank of the Mordell-Weil groups of their Jacobians over $\mathbb{Q}$. As a consequence, we can use Chabauty's method to obtain a uniform bound on the number of points on a majority of these curves, when the genus is at least 2.

We will state these results more precisely below, after some general material on hyperelliptic curves with a rational Weierstrass point. We end with a short discussion of hyperelliptic curves with two rational points at infinity. I want to thank Manjul Bhargava, Ngô Bảo Châu, Brian Conrad, and Jerry Wang for their comments.

2. Hyperelliptic curves with a marked Weierstrass point

For another treatment of this basic material, see [5]. Chevalley considers the more general case of a double cover of a curve of genus 0 in [3, Ch IV,§9].

Let k be a field and let C be a complete, smooth, connected curve over k of genus $n \geq 1$. Let O be a k-rational point of C, and let $U = C - \{O\}$ be the corresponding affine curve. The k-algebra $H^0(U, \mathscr{O}_U)$ of functions on C which are regular outside of O is a Dedekind domain with unit group k^*. The subset $L(mO)$ of functions with a pole of order $\leq m$ at O and regular elsewhere is a finite-dimensional k-vector space.

We henceforth assume that the vector space $L(2O)$ has dimension equal to 2. There cannot be a function having a simple pole at O and regular elsewhere, as that would give an isomorphism of C with $\mathbb{P}^1$ (and we have assumed that the genus of C is greater than 0). Hence $L(2O)$ is spanned by the constant function 1 and a function x with a double pole at O. We normalize the function x by fixing a non-zero tangent vector v to C at the point O and choosing a uniformizing

Received August 3, 2012.

2010 *Mathematics Subject Classification.* 11G30, 14H25.

Key words and phrases. Hyperelliptic curve, Weierstrass point, Selmer group, Mordell-Weil group.

parameter π in the completion of the function field at O with the property that $\frac{d}{dv}(\pi) = 1$. We then scale x so that $x = \pi^{-2} + \cdots$ in the completion. This depends only on the choice of tangent vector v, not on the choice of uniformizing parameter π adapted to v. The other functions in $L(2O)$ with this property all have the form $x + c$, where c is a constant in k. If we replace the tangent vector v by $v^* = uv$ with $u \in k^*$, then $x^* = u^2x + c$.

It follows that the space $L((2n-1)O)$ contains the vectors $\{1, x, x^2, \ldots x^{n-1}\}$. Since these functions have different orders of poles at O, they are linearly independent. But the dimension of $L((2n-1)O)$ is equal to $(2n-1)+(1-n) = n$ by the theorem of Riemann-Roch. Hence these powers of x give a basis for $L((2n-1)O)$. Since they all lie in the subspace $L((2n-2)O)$, they give a basis for that space too. Hence the dimension of $L((2n-2)O)$ is equal to the genus n. It follows from the Riemann-Roch theorem that the divisor $(2n-2)O$ is canonical.

The Riemann-Roch theorem also shows that the dimension of $L((2n)O)$ is equal to $n+1$, so a basis is given by the vectors $\{1, x, x^2, \ldots, x^n\}$. Similarly, the dimension of $L((2n+1)O)$ is equal to $n+2$. Hence there is a function y with a pole of exact order $(2n+1)$ at O, which cannot be equal to a polynomial in x. We use the uniformizing parameter π to normalize the function y by insisting that $y = \pi^{-(2n+1)} + \cdots$ in the completion. Again, this depends only on the tangent vector v. The other functions in $L((2n+1)O)$ with this property all have the form $y + q_n(x)$, where $q_n(x)$ is a polynomial of degree $\leq n$ with coefficients in k. If we replace v by $v^* = uv$ with $u \in k^*$, then $y^* = u^{2n+1}y + q_n(u^2x)$.

It is then easy to show that the algebra $H^0(U, \mathscr{O}_U)$ is generated over k by the two functions x and y, and that they satisfy a single polynomial relation $G(x,y) = 0$ of the form

$$y^2 + p_n(x)y = x^{2n+1} + p_{2n}(x) = F(x),$$

where p_n and p_{2n} are polynomials in x of degree $\leq n$ and $\leq 2n$ respectively. Indeed, the $(3n+4)$ vectors $\{y^2, x^ny, x^{n-1}y, \ldots, xy, y, x^{2n+1}, x^{2n}, \ldots, x, 1\}$ all lie in the vector space $L((4n+2)O)$, which has dimension $3n+3$. Hence they are linearly dependent. Since there are no linear relations in the spaces with poles of lesser order, this relation must involve a non-zero multiple of y^2 and a non-zero multiple of x^{2n+1}. By our normalization, we can scale the relation so that the multiple is 1. Hence the k-algebra $H^0(U, \mathscr{O}_U)$ is a quotient of the ring $k[x,y]/(G(x,y) = 0)$. Since the k-algebra $k[x] + yk[x]$ gives the correct dimensions of $L(mO)$ for all $m \geq 0$, there are no further relations, and the affine curve $U = C - \{O\}$ is defined by an equation of this form. The affine curve U is non-singular if and only if a certain universal polynomial Δ in the coefficients of $p_n(x)$ and $p_{2n}(x)$ takes a non-zero value in k [5, Thm 1.7]. Of course, changing the choice of the functions x and y in $L(2O)$ and $L((2n+1)O)$ changes the equation of the affine curve.

In the case when the genus of C is equal to 1, the pair (C, O) defines an elliptic curve over the field k. The polynomial relation above is Tate's affine equation for U (see [8, §2])

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and the condition for smoothness is the non-vanishing of the discriminant

$$\Delta(a_1, a_2, a_3, a_4, a_6).$$

The closure of this affine curve defines a smooth cubic in $\mathbb{P}^2$. For $n \geq 2$, the closure of the affine equation of degree $2n + 1$ in $\mathbb{P}^2$ is not smooth, but one has a smooth model for C defined by gluing [6, Ch II, Ex 2.14].

All of this works over a general field k, but there are some important simplifications when the characteristic of k does not divide $2(2n + 1)$. First, if the characteristic of k is not equal to 2, we can uniquely choose $y^* = y - p_n(x)/2$ to complete the square of the above equation and obtain one of the simpler form

$$y^2 = x^{2n+1} + c_1x^{2n} + c_2x^{2n-1} + \cdots + c_{2n}x + c_{2n+1} = F(x).$$

The automorphism ι of C defined by $\iota(x, y) = (x, -y)$ is the unique involution which fixes the rational point O, and y is the unique normalized element in $L((2n + 1)O)$ which is taken to its negative. The automorphism ι acts as -1 on the space of holomorphic differentials, which is spanned by

$$\{dx/2y, xdx/2y, \ldots, x^{n-1}dx/2y\}.$$

The differential $dx/2y$ has divisor $(2n - 2)O$ and the differential $-x^{n-1}dx/2y$ is dual to the tangent vector v at O. In this case, the fact that U is smooth is equivalent to the non-vanishing of the discriminant of the polynomial $F(x)$, and the polynomial Δ is given by the formula $\Delta = 4^{2n} \operatorname{disc}(F)$ (see [5, 1.6]).

Next, when the characteristic of k does not divide $2n+1$, we can replace x by $x - c_1/(2n + 1)$ to obtain an equation of the form

$$y^2 = x^{2n+1} + c_2x^{2n-1} + \cdots + c_{2n}x + c_{2n+1} = F(x).$$

This equation is uniquely determined by the triple (C, O, v), where v is a non-zero tangent vector at the point O. In particular, the moduli problem of triples (C, O, v) is rigid, and represented by the complement of the discriminant hypersurface $(\Delta = 0)$ in affine space of dimension $2n$. The automorphism ι of (C, O) defines an isomorphism from (C, O, v) to $(C, O, -v)$. If we replace $v^* = uv$ with $u \in k^*$, then $x^* = u^2x$ and $y^* = u^{2n+1}y$. The coefficients c_m in the polynomial $F(x)$ are scaled by the factor u^{2m}, and the discriminant Δ of the model is scaled by the factor $u^{2(2n+1)(2n)}$ in k^*.

3. The height of the pair (C, O)

We first assume that $k = \mathbb{Q}$ is the field of rational numbers. To each pair (C, O) we will associate a positive real number $H(C, O)$, its height. Choose a non-zero tangent vector v at the point O so that the coefficients c_m of the corresponding equation of (C, O, v) are all integers with the property that no prime p has the property that p^{2m} divides c_m for all m. We call such an equation minimal. Then v is unique up to sign, and the integers c_m which appear in this minimal equation are uniquely determined by the pair (C, O). We then define

$$H(C, O) = \text{Max}\{|c_m|^{(2n+1)(2n)/m}\}.$$

The factor $(2n+1)(2n)$ is added in the exponent so that the height $H(C,O)$ and the discriminant Δ have the same homogeneous degree. Clearly there are only finitely many pairs (C,O) with $H(C,O) < X$ for any positive real number X, so the height gives a convenient way to enumerate hyperelliptic curves over $\mathbb{Q}$ of a fixed genus n with a rational Weierstrass point. The number of pairs with $H(C,O) < X$ grows like a constant times $X^{(2n+3)/(4n+2)}$.

In the case when the genus of C is equal to 1, the minimal equation has the form

$$y^2 = x^3 + c_2x + c_3$$

with c_2 and c_3 both integers, not respectively divisible by p^4 and p^6 for any prime p. We note that this is not necessarily a global minimal model at the primes $p = 2$ and $p = 3$ (cf. [6, Ch VII]). The discriminant is given by the formula $\Delta = 2^4(-4c_2^3 - 27c_3^2)$ and the height is given by the formula $H(C,O) = \mathrm{Max}\{|c_2|^3, |c_3|^2\}$. The number of elliptic curves with height less than X grows like a constant times $X^{5/6}$.

More generally, suppose that k is a number field, and that (C,O) is a pair over k. Choose a non-zero tangent vector v so that the equation determined by the triple (C,O,v)

$$y^2 = x^{2n+1} + c_2x^{2n-1} + \cdots + c_{2n+1}$$

has coefficients in the ring A of integers of k. We define the height $H(C,O)$ by modifying the naive height of the point $(c_2, c_3, \ldots, c_{2n+1})$ in weighted projective space, using the notion of size defined in [4]. Namely, define the fractional ideal

$$I = \{\alpha \in k : \alpha^4 c_2, \alpha^6 c_3, \ldots, \alpha^{4n+2} c_{2n+1} \in A\}.$$

Then I contains A and $I = A$ if and only if the coefficients c_m are not all divisible by P^{2m}, for every non-zero prime ideal P of A. We define the height of the pair by

$$H(C,O) = (N(I))^{(2n+1)(2n)} \prod_{v|\infty} \mathrm{Max}\{|c_m|_v^{(2n+1)(2n)/m}\},$$

where the product is taken over all infinite places v of k. The product formula shows that this definition is independent of the choice of non-zero tangent vector v. When $k = \mathbb{Q}$, the choice of a minimal integral equation gives $N(I) = 1$ and we are reduced to the previous definition. In general, the number of pairs with $H(C,O) < X$ is finite, and again grows like a constant (depending on the arithmetic of k) times $X^{(2n+3)/(4n+2)}$ (cf. [4, Thm A]).

Let S be a real-valued function on pairs (C,O) over k. We say that the average value of S is equal to L if the ratios

$$\left(\sum_{H(C,O)<X} S(C,O)\right) \Bigg/ \left(\sum_{H(C,O)<X} 1\right)$$

tend to the limiting value L as $X \to \infty$. If R is a property of pairs (C,O) over $\mathbb{Q}$, we define the function S_R on pairs by $S_R(C,O) = 1$ if the pair satisfies property

R and $S_R(C,O) = 0$ otherwise. We say that the proportion of pairs satisfying property R is equal to r if the ratios

$$\left(\sum_{H(C,O)<X} S_R(C,O)\right) \Big/ \left(\sum_{H(C,O)<X} 1\right)$$

tend to the limiting value r as $X \to \infty$. If this limit exists, then clearly $0 \le r \le 1$. If the *liminf* is greater than r, we say the proportion is greater than r.

For example, let R be the property that O is the *only* k-rational point of the curve C. When the genus of C satisfies $n \ge 2$ we suspect that the proportion of pairs (C,O) with this property is equal to 1. When the genus of C is equal to 1, we suspect that this proportion is equal to $\frac{1}{2}$.

4. The 2-torsion subgroup and the 2-descent

Let (C,O) be a pair as above, defined over a field k whose characteristic is not equal to 2. Let

$$y^2 = F(x) = x^{2n+1} + c_1 x^{2n} + \cdots$$

be an affine equation for $U = C - \{O\}$. In this section we will use the separable polynomial $F(x)$ to describe the 2-torsion subgroup $J[2]$ of the Jacobian J of C as a finite group scheme over k. We will then explicitly calculate the map in Galois cohomology involved in the 2-descent. For more details, see [7].

Since $\mathrm{disc}(F) \neq 0$, the k-algebra $L = k[x]/(F(x))$ is étale. Let λ be the image of x in L, so $L = k + k\lambda + \cdots + k\lambda^{2n}$. Let k^s denote a separable closure of k and let $G = \mathrm{Gal}(k^s/k)$. The set $\mathrm{Hom}(L, k^s)$ of homomorphisms of k-algebras has cardinality $2n+1$ and has a left action of G, so defines a homomorphism $G \to S_{2n+1}$ up to conjugacy. We will see that the kernel of this homomorphism fixes the subfield of k^s generated by the 2-torsion points in the Jacobian.

Since $C(k)$ is non-empty, the points of the Jacobian $J(K)$ over any extension field K of k are isomorphic to the quotient of the abelian group of divisors of degree zero on C which are rational over K by the subgroup of principal divisors $\mathrm{div}(f)$ with f in $K(C)^*$. For each root β of the polynomial $F(x)$ in k^s, we define the point $P_\beta = (\beta, 0)$ on C and the divisor $d_\beta = (P_\beta) - (O)$ of degree zero. The class of d_β has order 2 in the Jacobian, as $2d_\beta = \mathrm{div}(x - \beta)$. It follows from the Riemann-Roch theorem that the $2n+1$ classes d_β in $J[2](k^s)$ satisfy a single linear relation over $\mathbb{Z}/2\mathbb{Z}$:

$$\sum_\beta d_\beta = \mathrm{div}(y).$$

They therefore span a finite subgroup of order 2^{2n}. Since this is the order of the full group $J[2](k^s)$, we have found a presentation of the 2-torsion over the separable closure. The Galois group acts on the $2n+1$ classes d_β through the homomorphism $G \to S_{2n+1}$, so we have an isomorphism of group schemes over k

$$J[2] \cong \mathrm{Res}_{L/k}\,\mu_2/\mu_2 \cong (\mathrm{Res}_{L/k}\,\mathbb{G}_m/\mathbb{G}_m)[2],$$

where Res denotes the restriction of scalars. Since $2n+1$ is odd, we have a splitting

$$\mathrm{Res}_{L/k}\,\mu_2 = \mu_2 \oplus (\mathrm{Res}_{L/k}\,\mu_2)_{N=1},$$

where the latter subgroup is the kernel of the norm map $N : \mathrm{Res}_{L/k}\,\mu_2 \to \mu_2$. Hence $J[2] \cong (\mathrm{Res}_{L/k}\,\mu_2)_{N=1}$. This splitting also allows us to compute the Galois cohomology groups

$$H^0(k, J[2]) = J[2](k) = \{\alpha \in L^* : \alpha^2 = N(\alpha) = 1\}$$
$$H^1(k, J[2]) = (L^*/L^{*2})_{N\equiv 1},$$

where the subscript $N \equiv 1$ means that the norm of a class in (L^*/L^{*2}) is a square in k^*.

The homomorphism $2 : J \to J$ is a separable isogeny, so is surjective on points over k^s. The kernel is the group scheme $J[2]$, so taking the long exact sequence in Galois cohomology, we obtain a short exact sequence

$$0 \to J(k)/2J(k) \xrightarrow{\delta} H^1(k, J[2]) \to H^1(k, J)[2] \to 0.$$

If $P = (a, b)$ is a k-rational point on the curve C with $b \neq 0$, and $d = (P) - (O)$ is the class of the corresponding divisor of degree zero in $J(k)$, then the image $\delta(d)$ is the class of $(a - \lambda)$ in $H^1(k, J[2]) = (L^*/L^{*2})_{N\equiv 1}$ [7, Thm 1.2]. Note that $(a - \lambda)$ is an element of L^* with $N(a - \lambda) = b^2$ in k^*.

We remark that the elementary nature of the 2-torsion is almost a defining property of hyperelliptic curves with a marked Weierstrass point. For a general curve of genus $n \geq 1$ over the field k (of characteristic $\neq 2$), the 2-torsion on the Jacobian is rational over k^s and generates a finite Galois extension $M = k(J[2](k^s))$ of k. The Galois group of M/k acts $\mathbb{Z}/2\mathbb{Z}$-linearly on $J[2](k^s) \cong (\mathbb{Z}/2\mathbb{Z})^{2n}$ and preserves the Weil pairing $\langle , \rangle : J[2] \times J[2] \to \mu_2$, which is strictly alternating and non-degenerate. Hence the group $\mathrm{Gal}(M/k)$ is isomorphic to a subgroup of the finite symplectic group $\mathrm{Sp}_{2n}(2)$. When the curve is hyperelliptic with a k-rational Weierstrass point, the Weil pairing is given on the generators of $J[2]$ by

$$\langle d_\beta, d_\beta \rangle = +1$$
$$\langle d_\beta, d_{\beta'} \rangle = -1,$$

and the Galois group of M/k is isomorphic to the subgroup of $S_{2n+1} \subset \mathrm{Sp}_{2n}(2)$ which is determined by the étale algebra L.

We will see in the final section that the situation is similar (but a bit more complicated) for a hyperelliptic curve of genus $n \geq 2$ with a pair of k-rational points $\{O, O'\}$ which are switched by the hyperelliptic involution ι. In that case, the Galois group of M/k is isomorphic to a subgroup of $S_{2n+2} \subset \mathrm{Sp}_{2n}(2)$.

5. The 2-Selmer group

We henceforth assume that $k = \mathbb{Q}$, although we expect that the results in this section will extend to the case when k is a number field [9]. Let (C, O) be a hyperelliptic curve of genus $n \geq 1$ with a $\mathbb{Q}$-rational Weierstrass point O. The group $H^1(\mathbb{Q}, J[2])$ is infinite, but contains an important finite subgroup, the 2-Selmer group $\mathrm{Sel}(J,2)$. This is the subgroup of cohomology classes whose restriction to $H^1(\mathbb{Q}_v, J[2])$ lies in the image $\delta(J(\mathbb{Q}_v)/2J(\mathbb{Q}_v))$ of the local descent map, for all places v [8, §7]. The assertion that the subgroup $\mathrm{Sel}(J,2)$ defined in this manner is *finite* is the first half of the Mordell-Weil theorem; the proof uses the finiteness of the class group and the finite generation of the unit group for number fields. Since the 2-Selmer group contains the image of $J(\mathbb{Q})/2J(\mathbb{Q})$ under the inclusion δ, an upper bound on its order gives an upper bound on the rank of the finitely generated group $J(\mathbb{Q})$.

Here is a simple example, which illustrates the partial computation of a 2-Selmer group. Suppose that C is given by an integral equation $y^2 = F(x) = x^{2n+1} + \cdots$. Assume further that the polynomial $F(x)$ is irreducible and that the discriminant of $F(x)$ is square-free. Then the algebra $L = k[x]/(F(x))$ is a number field with ring of integers $A_L = \mathbb{Z}[x]/F(x)$. In this case, one can show that the local image $\delta(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))$ is contained in the unit subgroup of elements with even valuation in $(L_p^*/L_p^{*2})_{N\equiv 1}$ for all finite primes p. It is equal to the unit subgroup when p is odd, and has index 2^n in the unit subgroup when $p = 2$. Hence the 2-Selmer group is a subgroup of the finite group $(L^{*(2)}/L^{*2})_{N\equiv 1}$ consisting of those elements in $(L^*/L^{*2})_{N\equiv 1}$ which have even valuation at all finite primes. To see that this group is finite, note that we have an exact sequence

$$1 \to (A_L^*/A_L^{*2})_{N=1} \to (L^{*(2)}/L^{*2})_{N\equiv 1} \to \mathrm{Pic}(A_L)[2] \to 1,$$

where the map to $\mathrm{Pic}(A_L)[2]$ takes the class of α with $(\alpha) = \mathfrak{a}^2$ to the class of the ideal $\mathfrak{a}$. The 2-Selmer group is the subgroup of this finite group which is defined by the local descent conditions at the places $v = 2$ and $v = \infty$. If we assume further that $F(x)$ has only one real root, so that $(A_L^*/A_L^{*2})_{N=1}$ has order 2^n by the unit theorem, then the only local conditions remaining are at the place $v = 2$.

In general, the local conditions at a finite set of bad places for C, which always include $v = 2$ and $v = \infty$, can be difficult to compute. It is therefore much easier to obtain an upper bound on the order of the Selmer group $\mathrm{Sel}(J,2)$ than it is to determine its exact order. For some explicit computations with elliptic curves, see [6, Ch X]. The main result in [2, Th 1] gives the average order of this group, when we consider *all* hyperelliptic curves with a marked Weierstrass point over $\mathbb{Q}$.

Proposition 1. *When the pairs (C,O) of a fixed genus $n \geq 1$ are ordered by height, the average order of the group* $\mathrm{Sel}(J,2)$ *is equal to* 3.

Let m be the rank of the Mordell-Weil group $J(\mathbb{Q})$. Since we have the inequalities $2m \leq 2^m \leq \#\,\mathrm{Sel}(J,2)$ we obtain the following corollary.

Corollary 2. *When the pairs (C,O) of a fixed genus $n \geq 1$ are ordered by height, the average rank of the Mordell-Weil group $J(\mathbb{Q})$ is less than or equal to $\frac{3}{2}$.*

More precisely, the *limsup* of the average rank is less than or equal to $\frac{3}{2}$, as we do not know that the limit defining the average rank exists. We suspect that the limit does exist, and is equal to $\frac{1}{2}$.

The proof of Proposition 1 has an algebraic and an analytic part. The algebraic part of the proof identifies the elements in the 2-Selmer group of J, for any pair (C, O) of genus n over $\mathbb{Q}$, with certain orbits in a fixed linear representation of the split special odd orthogonal group $\mathrm{SO}(W) = \mathrm{SO}_{2n+1}$ over $\mathbb{Q}$. Specifically, we study the stable orbits of $\mathrm{SO}(W)$ on the highest weight submodule $V = \mathrm{Sym}^2(W)_0$ in the symmetric square of the standard representation. The vectors in this representation can be identified with self-adjoint operators $T : W \to W$ of trace 0, and a vector is stable if its characteristic polynomial $F_T(x)$ has a non-zero discriminant. Associated to a stable orbit, we obtain a pencil of quadrics in projective space of dimension $2n + 1$ with smooth base locus. The pencil is spanned by the two quadrics $q(w, a) = \langle w, w\rangle$ and $q'(w, a) = \langle w, Tw\rangle + a^2$ on $W \oplus \mathbb{Q}$, where $\langle , \rangle$ is the original bilinear form on W.

The Fano variety P_T of maximal linear subspaces of the base locus is smooth of dimension n over $\mathbb{Q}$. It forms a principal homogeneous space of order 2 for the Jacobian J of the hyperelliptic curve defined by the equation $y^2 = F_T(x)$. The orbits which correspond to classes in the Selmer group are those operators T where the Fano variety P_T has points over $\mathbb{Q}_v$ for all places v; we call these orbits locally solvable. When $n = 1$, the representation $\mathrm{Sym}^2(W)_0$ of $\mathrm{SO}_3 = \mathrm{PGL}_2$ is given by the action on the space of binary quartic forms $q(x, y)$, a vector is stable if the quartic form has a non-zero discriminant, and the Fano variety is the curve of genus 1 defined by the equation $z^2 = q(x, y)$.

The involution $\tau(w, a) = (w, -a)$ of $W \oplus \mathbb{Q}$ stabilizes the pencil spanned by q and q' and acts on the Fano variety P_T. The fixed points $P_T(\tau)$ form a finite scheme of order 2^{2n}, whose points correspond to the maximal isotropic subspaces X in W over the algebraic closure with $T(W) \subset W^{\perp}$. The fixed points form a principal homogeneous space for the subgroup $J[2]$, as well as for the stabilizer G_T of T in G. Using the principal homogeneous space $P_T(\tau)$, one can show that the two finite commutative group schemes $J[2]$ and G_T are canonically isomorphic.

Having identified classes in the Selmer group with locally solvable orbits on V, the analytic part of the proof estimates the number of locally soluble integral orbits of height less than X as $X \to \infty$. The average value of the order of the Selmer group actually appears as a sum $3 = 2 + 1$, where 2 is equal to the Tamagawa number of SO_{2n+1}. This adèlic volume computation, together with some delicate arguments from the geometry of numbers, gives the average number of non-distinguished orbits (corresponding to the non-trivial classes in the Selmer group). The distinguished orbits (which all appear near a cusp of the fundamental domain) cannot be estimated by volume arguments. However, since they correspond to the trivial class in each Selmer group, the average number of these orbits is 1.

Since the average rank of $J(\mathbb{Q})$ is less than or equal to $\frac{3}{2}$, and this upper bound is less than the genus n of the curve C once $n \geq 2$, one can use the method of Chabauty (as refined by Coleman) to provide explicit bounds for the number of rational points on a majority (= a proportion greater than $\frac{1}{2}$) of the pairs (C, O). Here is a sample result, which is due to B. Poonen and M. Stoll. A slightly weaker result is obtained in [2, Cor 4].

Corollary 3. *If $n \geq 3$, a majority of the pairs (C, O) have at most 7 rational points, and a positive proportion of the pairs have only one rational point – the Weierstrass point O.*

To be more precise, we do not yet know that the limits defining these proportions exist. What they show is that the *liminf* of the ratios is $> \frac{1}{2}$ in the first case, and is > 0 in the second.

6. Even hyperelliptic curves

The curves C with a marked Weierstrass point O are often referred to as odd hyperelliptic curves, as (when the characteristic of k is not equal to 2) they have an equation of the form

$$y^2 = F(x) = x^{2n+1} + c_1x^{2n} + \cdots$$

where the separable polynomial $F(x)$ has odd degree. We now make some general remarks on the "even" case, which is not treated in our paper but for which similar results are expected to hold. For more details, we refer the reader to the PhD thesis of X. Wang [9].

Let k be a field (not of characteristic 2) and let C be a complete, smooth, connected curve over k of genus $n \geq 1$. Let (O, O') be a pair of distinct k-rational points on C with $L((O) + (O'))$ of dimension equal to 2, and let $U = C - \{O, O'\}$ be the corresponding smooth affine curve. A similar analysis to the one we did above shows that the k-algebra $H^0(U, \mathscr{O}_U)$ is generated by functions x (with poles at O and O' of order 1) and y (with poles at O and O' of order $n + 1$). These functions can be normalized to satisfy a single equation of the form

$$y^2 = F(x) = x^{2n+2} + c_1x^{2n+1} + \cdots ,$$

where $F(x)$ has $2n + 2$ distinct roots in k^s. The automorphism ι of C defined by $\iota(x, y) = (x, -y)$ is the unique involution which switches the two rational points O and O'.

The function y is the unique normalized vector in $L((n+1)(O)+(O'))$ which lies in the minus eigenspace for ι. When the characteristic of k does not divide $2n+2$, we can modify the function x in $L((O)+(O'))$ by a constant so that the the above equation has $c_1 = 0$. Then the equation depends only on the data $(C, (O, O'))$ and the choice of a non-zero tangent vector v to C at O. If we replace v by $v^* = uv$ with $u \in k^*$, the coefficients of the equation are scaled: $c^*_m = u^m c_m$. When k is a global field we can define the height of a triple $(C, (O, O'))$ by considering the coefficients $(c_2, c_3, \ldots, c_{2n+2})$ of this equation as a point in weighted projective space and taking its size as above [4]. Since there are only finitely many triples of a fixed genus $n \geq 1$ having height less than any real number X, we can define the average of a real-valued function S on triples $(C, (O, O'))$ as before.

The 2-torsion subgroup $J[2]$ of the Jacobian is a bit more complicated to describe. It is generated by the differences of the $2n + 2$ Weierstrass points on C (none of which may be rational over k). Let $L = k[x]/(F(x))$, which is an étale

k algebra of rank $2n+2$. Then we have an isomorphism of finite group schemes over k

$$J[2] \cong ((\mathrm{Res}_{L/k}\,\mu_2)_{N=1})/\mu_2.$$

The cohomology groups of $J[2]$ are also a bit more difficult to calculate. For example, the abelian group $\{\alpha \in L^* : \alpha^2 = N(\alpha) = 1\}/\{\pm 1\}$ maps into $H^0(k, J[2])$, but this map may not be surjective. This complicates matters somewhat in the 2-descent.

The class of the divisor $d = (O) - (O')$ of degree zero is well-defined in $J(k)/2J(k)$. It is usually a non-trivial element in this quotient of the Mordell-Weil group, although there are some triples where d is divisible by 2. When the class of d is non-trivial in $J(k)/2J(k)$, it gives rise to a non-trivial class in the 2-Selmer group. We should mention that Abel [1] found a beautiful criterion, in terms of the continued fraction of the square root of $F(x)$ in the completion $k((1/x))$, for the class of d to be of finite order in the Jacobian $J(k)$.

In the even case, we expect the average order of the 2-Selmer group of the Jacobian to be equal to $6 = 4+2$. The proof is similar in structure to the odd case. First the classes in the Selmer group are identified with the locally solvable orbits of the adjoint quotient $\mathrm{PSO}_{2n+2} = \mathrm{PSO}(W)$ of the split special even orthogonal group SO_{2n+2} over $\mathbb{Q}$ on the representation $V = \mathrm{Sym}^2(W)_0$ [9]. Then the average number of these orbits will be determined using arguments from the geometry of numbers. The contribution of 4 should come from the Tamagawa number of PSO_{2n+2} over $\mathbb{Q}$ and the contribution of 2 from the distinguished classes in the Selmer group whose orbits lie near the cusp. From the average order of the 2-Selmer group, one can deduce that the average rank of the Mordell-Weil group of the Jacobian is bounded above by $\frac{5}{2} = \frac{3}{2} + 1$.

References

[1] N. Abel, Ueber die Integration der Differential-Formel $\frac{\rho \cdot dx}{\sqrt{R}}$, *J. Crelle* **1** (1826), 185-221.

[2] M. Bhargava and B. Gross, The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point, http://arxiv.org/abs/1208.1007 (2012).

[3] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, No VI, AMS (1963).

[4] A-W. Deng, *Rational points on weighted projective spaces*, http://arxiv.org/abs/math/981-2082 (1998).

[5] P. Lockhart, On the discriminant of a hyperelliptic curve, *Trans. Amer. Math. Soc.* **342** (1994), 729-752.

[6] J. Silverman, *The arithmetic of elliptic curves*, Springer GTM **106** (1986).

[7] E. F. Schaefer, 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995), 219-232.

[8] J. Tate, The arithmetic of elliptic curves, *Invent. Math.* **23** (1974), 179-206.

[9] X. Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, PhD Thesis, Harvard University (2013).

Department of Mathematics, Harvard University, Cambridge, MA 02138
E-mail address: gross@math.harvard.edu