TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 342, Number 2, April 1994

ON THE DISCRIMINANT OF A HYPERELLIPTIC CURVE

P. LOCKHART

ABSTRACT. The minimal discriminant of a hyperelliptic curve is defined and used to generalize much of the arithmetic theory of elliptic curves. Over number fields this leads to a higher genus version of Szpiro's Conjecture. Analytically, the discriminant is shown to be related to Siegel modular forms of higher degree.

Let K be a field and C a hyperelliptic curve of genus g defined over K (thus $g > 0$ and there exists a map $C \to \mathbb{P}^1$ of degree two). When $g = 1$, so that C is an elliptic curve, there is an extensive theory, both analytic and algebraic, of the minimal discriminant ideal $\mathfrak{D}_{C/K}$ (see [13]). In this paper we study the minimal discriminant for hyperelliptic curves of arbitrary genus $g \geq 1$. Thus we obtain a natural generalization of those parts of the theory of elliptic curves which do not involve the group structure.

To be precise, we will actually consider *pointed* hyperelliptic curves, which we define in the following way. Let C and K be as above. For a divisor D, let $L(D)$ denote the vector space of global sections of the line bundle associated to D (i.e. $L(D)$ consists of those rational functions f on C which satisfy $(f) + D \geq 0$). Let $P \in C$. P is a *Weierstrass point* if $\dim L(2P) > 1$ (i.e. if there exists a function whose only pole is a double one at P). When $g = 1$, every point is a Weierstrass point. However, when $g > 1$ there are at most $2g + 2$ Weierstrass points of C, and exactly this many when $\operatorname{char}(K) \neq 2$ (see [1]). If P is a K-rational Weierstrass point of C, we will say that the pair (C, P) *is hyperelliptic over* K (or simply hyperelliptic, if K is understood). Thus when $g = 1$, (C, P) being hyperelliptic means that C is an elliptic curve with origin P.

The structure of the paper is as follows: In §1 we define the notion of a hyperelliptic Weierstrass equation and the discriminant of such an equation. The main result (Theorem 1.7) is that there is a natural discriminant attached to a hyperelliptic Weierstrass equation which detects singularities in all characteristics. Section 2 deals with hyperelliptic curves over local and global fields, including minimal discriminants, reduction, and S-minimal equations. In §3 we consider hyperelliptic curves over $\mathbb{C}$ and show that the discriminant can be expressed in terms of Siegel modular forms. This is then used to give analytic upper bounds on $\mathfrak{D}_{C/K}$. Finally, in §4 we examine a hyperelliptic generalization of a conjecture of Szpiro concerning the arithmetic of the global minimal

Received by the editors March 24, 1992 and, in revised form, June 15, 1992.
1991 *Mathematics Subject Classification*. Primary 11G30, 14G25.
Key words and phrases. Hyperelliptic, discriminant.
This work was partially supported by a grant from the Alfred P. Sloan Foundation.

discriminant ideal. We show that for two infinite families of curves C this conjecture follows from the so-called ABC Conjecture (see [11, 16]).

1. Weierstrass equations and the discriminant

The main purpose of this section is to define the discriminant of a hyperelliptic Weierstrass equation over an arbitrary field K. Let g be a positive integer.

Definition 1.1. A *Weierstrass equation* E/K *of genus* g is an equation of the form

$$E\colon y^2 + q(x)y = p(x) \tag{1.1}$$

where p and q are polynomials with coefficients in K, $\deg(q) \le g$, and p is monic of degree $2g+1$.

Proposition 1.2. *Let* (C, P) *be hyperelliptic over* K *with genus* g. *Then there exist nonconstant functions* $x, y \in K(C)$ *with* $x \in L(2P)$, $y \in L((2g+1)P)$, *which satisfy a Weierstrass equation of genus* g *over* K. *Moreover, such an equation is unique up to a change of coordinates of the form*

$$x = u^2\hat{x} + r, \quad y = u^{2g+1}\hat{y} + t(\hat{x}) \tag{1.2}$$

where $u \in K^*$, $r \in K$ *and* t *is a polynomial over* K *of degree* $\le g$.

Proof. Since P is a K-rational Weierstrass point, there exists a nonconstant function $x \in K(C)$ with a double pole at P. By the theorem of Riemann-Roch, we have

$$\dim L(2gP) = g+1, \quad \dim L((2g+1)P) = g+2.$$

The functions $1, x, x^2, \dots, x^g$ form a basis for $L(2gP)$. Let $y \in K(C)$ be an element of $L((2g+1)P)$ which does not lie in the subspace $L(2gP)$. Consider the $3g+4$ functions

$$1, x, \dots, x^{2g+1}, y, xy, \dots, x^g y, y^2. \tag{1.3}$$

Each of these functions is an element of the vector space $L((4g+2)P)$, which has dimension $3g+3$. Hence there must be a K-linear dependence relation among them. Moreover, the functions (1.3) each have poles at P of different orders, except for x^{2g+1} and y^2 which both have a pole at P of exact order $4g+2$. Thus the coefficients of x^{2g+1} and y^2 must both be nonzero. Multiplying the relation by a suitable constant and rescaling x and y, we may assume that x^{2g+1} and y^2 both occur with coeficient 1. Thus x and y satisfy a Weierstrass equation of genus g over K.

Now suppose $\hat{x}$ and $\hat{y}$ are another such pair of functions. Since C is hyperelliptic, $\dim L(2P) = 2$. Hence we must have $x = a\hat{x} + r$ for some $a \in K^*$, $r \in K$. Similarly, $y = b\hat{y} + t(\hat{x})$ where $b \in K^*$ and $\deg(t) \le g$. Since this yields an equation with monic coefficients for $\hat{x}^{2g+1}$ and $\hat{y}^2$, we have $b^2 = a^{2g+1}$. Let $u = ba^{-g}$. Then $u \in K^*$, $a = u^2$ and $b = u^{2g+1}$. This completes the proof.

Remark. When $\mathrm{char}(K) \ne 2$, one may complete the square on the left side of (1.1), giving rise to a Weierstrass equation for (C, P) of the form $y^2 = f(x)$. Equations of this form are unique up to changes of coordinates (1.2), with $t = 0$.

Let E and $\hat{E}$ be Weierstrass equations which are related by the change of coordinates (1.2). Write

$$E\colon y^2 + q(x)y = p(x), \quad \hat{E}\colon \hat{y}^2 + \hat{q}(\hat{x})\hat{y} = \hat{p}(\hat{x}).$$

The relations between the coefficients of E and $\hat{E}$ are then given by

$$\begin{aligned} u^{2g+1}\hat{q}(\hat{x}) &= q(u^2\hat{x} + r) + 2t(\hat{x}), \\ u^{4g+2}\hat{p}(\hat{x}) &= p(u^2\hat{x} + r) - t(\hat{x})q(u^2\hat{x} + r) - t(\hat{x})^2. \end{aligned} \tag{1.4}$$

Given a Weierstrass equation E, we consider the embedding of the affine curve E in $\mathbb{P}^{g+2}$ via $(x, y) \mapsto [1, x, x^2, \dots, x^{g+1}, y]$. Let $\mathfrak{M}_E$ denote the closure of the image of E under this map. It is easily shown that $\mathfrak{M}_E$ has a unique point at infinity which is always nonsingular and whose complement is isomorphic to E. In the elliptic case, $\mathfrak{M}_E$ may be defined simply as the closure of E in $\mathbb{P}^2$. If E is nonsingular, then $\mathfrak{M}_E$ is a hyperelliptic curve of genus g with Weierstrass equation E. Conversely, if (C, P) is hyperelliptic with Weierstrass equation E, then the above map induces an isomorphism of C onto $\mathfrak{M}_E$, which is therefore a nonsingular subvariety of $\mathbb{P}^{g+2}$. Thus a Weierstrass equation E arises from some (C, P) if and only if E has no singular points, and in this case the set of such E form an equivalence class of Weierstrass equations related by the transformations (1.2).

We now consider the problem of determining when a given Weierstrass equation E is singular. Since we want to work with fields of arbitrary characteristic, it is perhaps best to consider a generic Weierstrass equation and its specializations.

Definition 1.3. Let $\mathfrak{R} = \mathbb{Z}[P_0, P_1, \dots, P_{2g}, Q_0, Q_1, \dots, Q_g]$ be the polynomial ring over $\mathbb{Z}$ in $3g+2$ variables. Let

$$P(x) = x^{2g+1} + \sum_{k=0}^{2g} P_k x^k, \quad Q(x) = \sum_{k=0}^{g} Q_k x^k.$$

Given a field K and a Weierstrass equation E, we obtain a homomorphism $\pi_E\colon \mathfrak{R} \to K$ by sending the indeterminates P_k and Q_k to the corresponding coefficients of E. For $r \in \mathfrak{R}$ we write $r_E = \pi_E(r)$. Thus $P_E(x) = p(x)$, $Q_E(x) = q(x)$.

Let F and G be any two polynomials, and let $\operatorname{Res}(F, G)$ denote their resultant. The following facts follow easily from the definitions (see [6, Chapter V, §10]):

(R1) $\operatorname{Res}(F, G)$ is a polynomial over $\mathbb{Z}$ in the coefficients of F and G.
(R2) $\operatorname{Res}(F, G) = 0$ if and only if F and G have a common root.
(R3) $\operatorname{Res}(F, GH) = \operatorname{Res}(F, G)\operatorname{Res}(F, H)$.
(R4) If $\deg(GH) \le \deg(F)$ then $\operatorname{Res}(F + GH, G) = \operatorname{Res}(F, G)$.
(R5) If c is a constant, $\operatorname{Res}(cF, G) = c^{\deg(G)}\operatorname{Res}(F, G)$.
(R6) If F is monic, then $\operatorname{Res}(F, F') = \operatorname{Disc}(F)$, the discriminant of F.
(R7) If $F, G \in \mathfrak{R}[x]$ and the leading coefficients of F_E and G_E are not both zero, then $\operatorname{Res}(F, G)_E = 0$ if and only if $\operatorname{Res}(F_E, G_E) = 0$.

Lemma 1.4. *Write*

$$\begin{aligned} F(x) &= 4P(x) + Q(x)^2, \\ G(x) &= P'(x)^2 - P(x)Q'(x)^2 + P'(x)Q'(x)Q(x). \end{aligned}$$

Then a Weierstrass equation E/K is singular if and only if $\mathrm{Res}(F, G)_E = 0$.

Proof. Since $P(x)$ is monic of degree $2g+1$ and $\deg(Q) \leq g$, the leading coefficient of $F(x)$ is 4. Similarly, the leading coefficient of $G(x)$ is $(2g+1)^2$. These cannot both be zero in K. Thus using (R2) and (R7), we need only show that E is singular if and only if F_E and G_E have a common root.

Suppose $\mathrm{char}(K) \neq 2$. The transformation $y \mapsto y - \frac{1}{2}q(x)$ is of the form (1.2) and yields the equation $y^2 = \frac{1}{4}F_E(x)$. Thus E has a singular point if and only if F_E has a multiple root, i.e. F_E and F_E' have a root in common. But $G = (F'/4)^2 - (Q'/2)^2 F$, so F_E and F_E' have a common root precisely when F_E and G_E do.

If $\mathrm{char}(K) = 2$, then the singularity of E is equivalent to the existence of $\alpha, \beta \in \bar{K}$ with

$$\beta^2 + q(\alpha)\beta = p(\alpha), \quad q(\alpha) = 0, \quad q'(\alpha)\beta = p'(\alpha)$$

which is the same as $q(\alpha) = 0$ and $q'(\alpha)^2 p(\alpha) - p'(\alpha)^2 = 0$. Thus E is singular if and only if q and $p'^2 - pq'^2$ have a common root. But $F_E = q^2$ and $G_E = p'^2 - pq'^2 + p'q'q$, so this condition is again equivalent to F_E and G_E having a root in common.

Lemma 1.5. *Let F and G be as above. Then*

$$\mathrm{Res}(F, G) = 2^{8g}\,\mathrm{Disc}(\tfrac{1}{4}F)^2.$$

Proof. Since $\deg((Q'/2)^2 F) = 4g - 1 < 4g = \deg((F'/4)^2)$, properties (R3) through (R6) give us

$$\begin{aligned}\mathrm{Res}(F, G) &= \mathrm{Res}(F, (F'/4)^2 - (Q'/2)^2 F)\\ &= \mathrm{Res}(F, (F'/4)^2) = \mathrm{Res}(F, F'/4)^2\\ &= (4^{\deg(F')}\,\mathrm{Res}(F/4, F'/4))^2 = 2^{8g}\,\mathrm{Disc}(\tfrac{1}{4}F)^2.\end{aligned}$$

Definition 1.6. The *hyperelliptic discriminant for genus g* is the polynomial

$$\Delta = 2^{4g}\,\mathrm{Disc}(P(x) + \tfrac{1}{4}Q(x)^2).$$

Theorem 1.7. *Δ is an irreducible polynomial in $3g+2$ variables with coefficients in $\mathbb{Z}$ with the property that for all K and all Weierstrass equations E/K,*

$$E \text{ is singular if and only if } \Delta_E = 0.$$

Proof. From (R1) and Lemma 1.5, we see that Δ^2 is an element of $\mathfrak{R}$. Hence by Gauss' Lemma, $\Delta \in \mathfrak{R}$. Lemmas 1.4 and 1.5 imply that E is singular precisely when $\Delta_E = 0$. Since the discriminant of a polynomial with indeterminate coefficients is irreducible over the constant field, Δ is irreducible in $\mathfrak{R} \otimes \mathbb{Q}$. Moreover, Δ cannot be divisible by a prime p, since there exist nonsingular Weierstrass equations over the field of p elements. Therefore Δ is irreducible.

Remark. A similar argument may be used to show that (up to sign) Δ is in fact the unique polynomial with these properties.

When $\mathrm{char}(K) \neq 2$, the change of coordinates $y \mapsto y - \frac{1}{2}q(x)$ transforms the Weierstrass equation (1.1) into $E : y^2 = f(x)$ where $f(x) = p(x) + \frac{1}{4}q(x)^2$. Clearly E is singular if and only if $\mathrm{Disc}(f) = 0$. Thus $\mathrm{Disc}(p(x) + \frac{1}{4}q(x)^2)$

acts as a discriminant for genus g except over fields of characteristic two. To get Δ, we must multiply $\operatorname{Disc}(p(x)+\frac{1}{4}q(x)^2)$ by the correct power of 2, so that it detects singularities over fields of characteristic 2 as well.

Definition 1.8. If E is a Weierstrass equation, Δ_E will be called the *discriminant of* E.

Thus if (C, P) is hyperelliptic over K with Weierstrass equation E, we have $\Delta_E \in K^*$. In the case $g = 1$, the above computations reduce to the standard formulas for the discriminant of an elliptic Weierstrass equation. In this case, one can actually write down the polynomial Δ explicitly [13, Chapter III].

Example 1.9. For the elliptic Weierstrass equation $E: y^2 = x^3 + Ax + B$, we have the usual $\Delta_E = -16(4A^3 + 27B^2)$.

An important property of the discriminant of an elliptic Weierstrass equation is its homogeneity under changes of coordinates. We now show that the hyperelliptic discriminant also has this property.

Proposition 1.10. *Let* $E \mapsto \hat{E}$ *be a change of coordinates of the form* (1.2). *Then*

$$\Delta_E = u^{4g(2g+1)}\Delta_{\hat{E}}.$$

Proof. Regarding (1.2) as a purely formal substitution, we apply it to the generic Weierstrass equation given by P and Q. From (1.4) we get $u^{4g+2}\hat{F}(x) = F(u^2x + r)$. If we write $F(x) = 4\prod(x - \alpha_i)$ and $\hat{F}(x) = 4\prod(x - \beta_i)$, we get $\beta_i = (\alpha_i - r)/u^2$. Thus

$$\operatorname{Disc}(\hat{F}/4) = \prod(\beta_i - \beta_j)^2 = \prod\left(\frac{\alpha_i - \alpha_j}{u^2}\right)^2 = u^{-4g(2g+1)}\operatorname{Disc}(F/4).$$

Multiplying by 2^{4g} and applying π_E gives the result.

Remark. The preceding results could, in principle, be extended to arbitrary plane curves. In this case, elimination theory (used in place of Lemma 1.4) gives rise to an *ideal* of polynomials in the coefficients of the defining equation, rather than a single polynomial Δ. The computation of such "discriminants" can be quite involved.

Let (C, P) be hyperelliptic over K with Weierstrass equation E. We now choose a basis for the space of holomorphic one-forms $H^0(C, \Omega^1_{C/K})$ which is in some sense homogeneous under changes of coordinates $E \mapsto \hat{E}$. This basis is needed for the arguments of §3.

Definition 1.11. With (C, P) and E as above, Let

$$(1.5) \qquad \omega_i = \frac{x^{i-1}dx}{2y + q(x)}, \qquad 1 \le i \le g.$$

We write $(\omega) = {}^t(\omega_1, \dots, \omega_g)$.

Proposition 1.12. *The* ω_i *form a basis for* $H^0(C, \Omega^1_{C/K})$, *and under a change of coordinates of the form* (1.2) *we have* $(\omega) = A(\hat{\omega})$, *where* $A \in \mathrm{GL}_g(K)$ *with* $\det A = u^{-g^2}$.

Proof. Differentiating $y^2 + q(x)y = p(x)$ yields

$$\omega_1 = \frac{dx}{2y + q(x)} = \frac{dy}{p'(x) - q'(x)y}.$$

Since C is nonsingular, ω_1 can have no affine poles. Away from the zeroes of $2y + q(x)$, x is a uniformizer, so ω_1 is nonzero. When $2y + q(x) = 0$, we have $p'(x) - q'(x)y \neq 0$ and y is a uniformizer. Thus ω_1 has no affine roots. Since the canonical class of C has degree $2g - 2$, we must have $\operatorname{div}(\omega_1) = (2g - 2)P$.

Now $\operatorname{div}(x) \geq -2P$, so $\operatorname{div}(\omega_i) \geq (2g - 2i)P \geq 0$. Therefore the ω_i are holomorphic. There are $g = \dim H^0(C, \Omega^1_{C/K})$ of them, hence they must form a basis, as they are clearly linearly independent.

Let $E \mapsto \hat{E}$ be a change of coordinates given by (1.2). Then

$$\omega_i = \frac{(u^2\hat{x} + r)^{i-1}u^2 d\hat{x}}{2u^{2g+1}\hat{y} + 2t(\hat{x}) + q(u^2\hat{x} + r)}.$$

Using equations (1.4), we get

$$\omega_i = \frac{u^{1-2g}(u^2\hat{x} + r)^{i-1}d\hat{x}}{2\hat{y} + \hat{q}(\hat{x})} = \sum_{j=1}^{i} \binom{i-1}{j-1} u^{2j-2g-1} r^{i-j} \hat{\omega}_j.$$

Thus $(\omega) = A(\hat{\omega})$, where A is a lower triangular matrix with diagonal elements $u^{2i-2g-1}$, $1 \leq i \leq g$. Thus $\det A = u^n$ with $n = \sum_{i=1}^{g}(2i - 2g - 1) = -g^2$.

Remark. When $\operatorname{char}(K) \neq 2$, we may choose E so that $q = 0$. In this case one has the customary $\omega_i = \frac{1}{2}x^{i-1}dx/y$.

2. The minimal discriminant

In this section we study the minimal discriminant of a hyperelliptic curve over a local or global field. The results are for the most part natural generalizations of those concerning elliptic curves (see for example [13]).

Let K be a local field with discrete valuation v, and let $\bar{K}$ be its separable closure. Let R be the valuation ring of v, $\mathfrak{p}$ the maximal ideal of R, and k the residue field $R/\mathfrak{p}$. We assume k is perfect with algebraic closure $\bar{k}$. Let $\bar{R}$ denote the integral closure of R in $\bar{K}$. We write $\tilde{x}$ for the image of x under the canonical reduction map $\bar{R} \to \bar{k}$.

Let (C, P) be hyperelliptic over K, with Weierstrass equation E. Using a suitable change of coordinates to clear denominators, we may assume that all the coefficients of E are in R. Such an equation will be called *integral.* Note that if E is an integral Weierstrass equation, $\Delta_E \in R$. Hence $v(\Delta_E)$ takes on a discrete set of nonnegative integral values as E runs through the set of integral Weierstrass equations for (C, P).

Definition 2.1. A Weierstrass equation E for (C, P) is said to be *minimal* if E is integral and $v(\Delta_E)$ is minimal among all integral Weierstrass equations for (C, P). The ideal $\mathfrak{p}^{v(\Delta_E)}$ will be called the *minimal discriminant of* (C, P).

Let E be any integral Weierstrass equation for (C, P) and suppose the change of coordinates $E \mapsto \hat{E}$ given by

$$x = u^2\hat{x} + r, \quad y = u^{2g+1}\hat{y} + t(\hat{x}) \tag{2.1}$$

yields a minimal Weierstrass equation $\hat{E}$. By Proposition 1.10 we have $v(\Delta_E) = \lambda v(u) + v(\Delta_{\hat{E}})$, where $\lambda = 4g(2g+1)$. Thus $v(u) \geq 0$, so $u \in R$ (and in particular, $u \in R^*$ if and only if E was already minimal).

Remark. It can also be shown that in the above situation we have $r \in R$ and $t(x) \in R[x]$. We leave the details to the reader.

Now, let (C, P) be hyperelliptic over K with minimal Weierstrass equation E. Let $\tilde{E}$ denote the equation obtained by reducing the coefficients of E modulo $\mathfrak{p}$. This defines a plane curve $\tilde{C}$, called the *reduction* of C. More precisely, $\tilde{C}$ is the variety defined by reduction of the coefficients of the Weierstrass model $\mathfrak{M}_E$ of §1. Since the coefficients of E are integral, $\mathfrak{M}_E$ may be viewed as a scheme over $\operatorname{Spec}(R)$. Then $\tilde{C}$ is just the special fibre of this scheme. The unique point at infinity of $\tilde{C}$ is nonsingular, and thus by the properties of the discriminant, $\tilde{C}$ is singular if and only if $v(\Delta_E) > 0$.

Now suppose E is a singular Weierstrass equation over k (e.g. the reduction of a hyperelliptic curve over K) with singular point Q. If $\operatorname{char}(k) \neq 2$, we can change coordinates to get a Weierstrass equation of the form $y^2 = f(x)$. Thus $Q = (\alpha, 0)$, with α a multiple root of f.

Definition 2.2. The *order* d_Q of the point Q is the multiplicity of the root α of f. If Q is a regular point, we set $d_Q = 1$.

A point of order 2 is called a *node*, and a point of order 3 a *cusp*. In the elliptic case, these are the only types of singularities that can occur (we always have $d_Q \leq 2g+1$) and the singular point is always unique. When $g > 1$, however, more complicated things can happen. For example, when $g = 2$ there are seven possibilities, e.g. a node and a cusp, two nodes, a single point of order 4, etc. The order of a singular point can also be defined when the characteristic is equal to two (see [7]).

We close our discussion of the local field case with the following useful result.

Lemma 2.3. *Assume* $\operatorname{char}(K) \neq 2$. *Let* (C, P) *be hyperelliptic over* K *of genus* g *with integral Weierstrass equation* $E : y^2 = f(x)$. *Write*

$$f(x) = \prod_{i=1}^{2g+1} (x - \alpha_i), \quad \alpha_i \in \bar{R}.$$

Suppose that $\tilde{E}$ *does not have a singularity of degree* $2g+1$ (*i.e. the* $\tilde{\alpha}_i$ *are not all equal in* $\bar{k}$). *Then any change of coordinates which yields a minimal Weierstrass equation must satisfy* $v(u) \leq v(2)$. *In particular, if* $\operatorname{char}(k) \neq 2$ *then* E *is already minimal.*

Proof. Let L be the splitting field of $f(x)$ over K, and w the valuation on L which extends v. Suppose the change of coordinates $x \mapsto u^2x + r$; $y \mapsto u^{2g+1}y + t(x)$ (with $u \in K^*$, $r \in K$, and $t \in K[x]$) yields a minimal Weierstrass equation. This equation has the form

$$y^2 + q(x)y = \frac{f(u^2x + r)}{u^{4g+2}} - \frac{1}{4}q(x)^2$$

where $q(x) = 2t(x)/u^{2g+1}$. Being minimal, this equation must be integral. Hence $4f(u^2x + r)/u^{4g+2}$ has coefficients in R, and therefore so does

$$\frac{4^{2g+1} f(u^2x/4 + r)}{u^{4g+2}}.$$

This polynomial is monic with integral roots $4u^{-2}(\alpha_i - r) \in L$. If $v(u) > v(2)$, then $w(\alpha_i - r) > 0$. But this means that r is integral and $\tilde{\alpha}_i = \tilde{r}$ for all i, contradicting the assumption that the $\tilde{\alpha}$ are not all equal. Therefore $v(u) \leq v(2)$.

Now suppose K is a number field with ring of integers R. Let M_K^0 denote the set of finite places of K. For each $v \in M_K^0$, let K_v denote the completion of K at v, R_v the valuation ring in K_v, and $\mathfrak{p}_v$ the maximal ideal of R_v, viewed also as a prime ideal of R. Let (C, P) be hyperelliptic of genus g over K, and set $\lambda = 4g(2g+1)$.

Definition 2.4. Let E be a Weierstrass equation for (C, P) over K. If $v \in M_K^0$ we say E is *integral* (resp. *minimal*) *at* v if E is integral (resp. minimal) when viewed as a Weierstrass equation over K_v. A Weierstrass equation over K is *integral* (resp. *minimal*) if it is integral (resp. minimal) at v for all $v \in M_K^0$.

Thus a Weierstrass equation over K is integral precisely when all of its coefficients lie in R. It is easy to see that (C, P) always has an integral Weierstrass equation, but it may not be possible to find a minimal one.

Definition 2.5. For each $v \in M_K^0$, let Δ_v be the discriminant of a minimal Weierstrass equation for (C, P) over K_v. The *minimal discriminant* of (C, P) over K is the ideal

$$\mathfrak{D}_{C/K} = \prod_{v \in M_K^0} \mathfrak{p}_v^{v(\Delta_v)}.$$

In other words, the (global) minimal discriminant is the product of all the local minimal discriminants.

Remark. In the elliptic case, the minimal discriminant $\mathfrak{D}_{C/K}$ is independent of the choice of origin P. This is due to the fact that any two such points P and P' are related by a K-rational isomorphism (e.g. a translation). When $g > 1$, this is not necessarily the case, so that for a given hyperelliptic curve C there may be several minimal discriminants $\mathfrak{D}_{C/K}$, depending on the choice of P. On the other hand, there can be at most $2g+2$ such choices, so that we may consider P fixed without loss of generality.

Now, let E be an integral Weierstrass equation for (C, P) over K, and for each v let

$$x \mapsto u_v^2 x + r_v, \quad y \mapsto u_v^{2g+1} y + t_v(x) \tag{2.2}$$

be a change of coordinates which yields a minimal equation over K_v, where $u_v \in K_v^*$, $r_v \in K_v$, and $t_v \in K_v[x]$. Thus by Proposition 1.10, $v(\Delta_E) = \lambda v(u_v) + v(\Delta_v)$. Let $\mathfrak{a}_E$ denote the integral ideal $\prod \mathfrak{p}_v^{v(u_v)}$. Then

$$(\Delta_E) = \mathfrak{a}_E^{\lambda} \mathfrak{D}_{C/K}. \tag{2.3}$$

Note that $\mathfrak{a}_E$ depends only on E and not on the choices (2.2) since for all v, $v(\mathfrak{a}_E) = (v(\Delta_E) - v(\mathfrak{D}_{C/K}))/\lambda$.

Lemma 2.6. *Let* $E \mapsto \hat{E}$ *be a change of coordinates of the form* (2.1). *Then* $\mathfrak{a}_E = (u)\mathfrak{a}_{\hat{E}}$.

Proof. For each $v \in M_K^0$ we have

$$\begin{aligned} v(\mathfrak{a}_E) &= (v(\Delta_E) - v(\mathfrak{D}_{C/K}))/\lambda \\ &= (\lambda v(u) + v(\Delta_{\hat{E}}) - v(\mathfrak{D}_{C/K})/\lambda \\ &= v(u) + v(\mathfrak{a}_{\hat{E}}). \end{aligned}$$

and the result follows easily.

Thus the $\mathfrak{a}_E$ all represent the same element of the ideal class group $\mathfrak{C}_K$ of K.

Definition 2.7. The *Weierstrass class* $\mathfrak{w}_{C/K}$ of (C, P) is the ideal class in $\mathfrak{C}_K$ of any $\mathfrak{a}_E$.

Proposition 2.8. *Let $\mathfrak{a} \in \mathfrak{w}_{C/K}$ be an integral ideal of K. Then there exists an integral Weierstrass equation E for (C, P) such that $(\Delta_E) = \mathfrak{a}^\lambda \mathfrak{D}_{C/K}$.*

Proof. Let E be any integral Weierstrass equation for (C, P). From (2.3) we have $(\Delta_E) = \mathfrak{a}_E^\lambda \mathfrak{D}_{C/K}$. Now $\mathfrak{a}$ and $\mathfrak{a}_E$ are both in the class $\mathfrak{w}_{C/K}$, so there exists an $u \in K^*$ with $\mathfrak{a}_E = (u)\mathfrak{a}$. Thus

$$(u^{-\lambda}\Delta_E) = \mathfrak{a}^\lambda \mathfrak{D}_{C/K}. \tag{2.4}$$

For each $v \in M_K^0$, let $u_v \in K_v^*$, $r_v \in K_v$, and $t_v(x) \in K_v[x]$ be chosen so that the change of coordinates (2.2) yields a minimal equation at v. Thus $v(\Delta_E) = \lambda v(u_v) + v(\Delta_v)$. Combining this with (2.4) we find that $v(u/u_v) = v(u) - v(u_v) = -v(\mathfrak{a}) \leq 0$, since $\mathfrak{a}$ is an integral ideal. Hence the further change of coordinates $x \mapsto (u/u_v)^2 x$, $y \mapsto (u/u_v)^{2g+1} y$ yields an equation E'_v which is integral at v. The coordinate change relating E and E'_v is given by

$$x \mapsto u^2 x + r_v, \quad y \mapsto u^{2g+1} y + t_v(x). \tag{2.5}$$

Let Δ'_v denote the discriminant of E'_v. Equations (2.4) and (2.5) then give $v(\Delta'_v) = -\lambda v(u) + v(\Delta_E) = v(\mathfrak{a}^\lambda \mathfrak{D}_{C/K})$.

Let S be the set of places where u is not a local unit. By the approximation theorem (see [12, Chapter 1]) we can choose $r \in K$, $t(x) \in K[x]$ so that for each $v \in S$, r is close to r_v and the coefficients of $t(x)$ are close to the corresponding coefficients of $t_v(x)$; and for each $v \notin S$, $r \in R_v$ and $t(x) \in R_v[x]$. Let E' be the Weierstrass equation obtained from E via the change of coordinates

$$x \mapsto u^2 x + r, \quad y \mapsto u^{2g+1} y + t(x). \tag{2.6}$$

For each $v \in M_K^0$, E' is integral at v and $v(\Delta_{E'}) = v(\Delta'_v) = v(\mathfrak{a}^\lambda \mathfrak{D}_{C/K})$. For $v \in S$ this follows by continuity, and for $v \notin S$ it is obvious. Thus E' is the desired equation.

Remark. When K has class number 1 (e.g. $K = \mathbb{Q}$), Proposition 2.8 shows that (C, P) always has a minimal Weierstrass equation. If E is such an equation, then $\Delta_E \in R$ is called the *global minimal discriminant* of (C, P). The global minimal discriminant is unique up to multiplication by the λth power of a unit. In particular, when $K = \mathbb{Q}$ it is unique.

In general, (C, P) may not possess a minimal Weierstrass equation, but we can consider the next best thing.

Definition 2.9. Let S be a finite set of places of K which contains the infinite places. Let (C, P) be hyperelliptic over K with Weierstrass equation E. E is called *S-minimal* if E is minimal at v for all $v \notin S$.

Corollary 2.10. *Given a number field K, there exists a fixed set of places S_0 such that for all (C, P) hyperelliptic over K, there is an S_0-minimal Weierstrass equation for (C, P).*

Proof. For each class in the ideal class group $\mathfrak{C}_K$, choose a fixed integral ideal. Let S_0 consist of all primes which divide any of these ideals. Given g and (C, P), let $\mathfrak{a}$ be the ideal which was chosen for the class $\mathfrak{w}_{C/K}$. By Proposition 2.8 there is a Weierstrass equation E with $(\Delta_E) = \mathfrak{a}^\lambda \mathfrak{D}_{C/K}$, which is clearly minimal at v for all $v \notin S_0$.

The next result says that not only can we choose our equations to be S-minimal, but by altering them only slightly (i.e. scaling) we can even control somewhat the behavior at the places in S. We will need this sharper statement in §4.

Corollary 2.11. *Let S_0 be as in Corollary 2.10, let S be a finite set of places containing S_0, and let E be an S-minimal Weierstrass equation for (C, P). Then there exists a change of coordinates*

$$x \mapsto u^2 x, \quad y \mapsto u^{2g+1} y \tag{2.7}$$

with u an S-unit (i.e. $v(u) = 0$ for all $v \notin S$) yielding a new S-minimal equation E' such that $v(\Delta_{E'}) - v(\mathfrak{D}_{C/K})$ is bounded by a constant which depends only on the field K. In other words,

$$v(\Delta_{E'}) - v(\mathfrak{D}_{C/K}) \ll 1. \tag{2.8}$$

Proof. From Corollary 2.10 we know that (C, P) has an S_0-minimal equation $\hat{E}$ with $(\Delta_{\hat{E}}) = \mathfrak{a}^\lambda \mathfrak{D}_{C/K}$, where $\mathfrak{a}$ depends only on K. Thus $v(\Delta_{\hat{E}}) - v(\mathfrak{D}_{C/K}) \ll 1$ for all $v \in M_K^0$. Now E and $\hat{E}$ are related by a change of coordinates (2.1). Since E and $\hat{E}$ are both S-minimal, u must be an S-unit and the coefficients of r and $t(x)$ must be S-integral (i.e. they have nonnegative valuation outside S). The change of coordinates $\hat{E} \mapsto E'$ given by

$$\hat{x} = x - u^{-2} r, \quad \hat{y} = y - \frac{t(x - u^{-2} r)}{u^{2g+1}} \tag{2.9}$$

does not affect the discriminant (it is a translation), and preserves the S-integrality of the coefficients. Hence the resulting equation E' is S-minimal and satisfies (2.8). The composition of (2.9) with (2.1) is precisely (2.7).

3. The discriminant as a modular form

Let C be an elliptic curve over $\mathbb{C}$. A Weierstrass equation E then gives rise to a lattice $\Lambda_E \subseteq \mathbb{C}$ and a uniformization $C \cong \mathbb{C}/\Lambda_E$. If we write $\Lambda_E = \sigma_1 \mathbb{Z} + \sigma_2 \mathbb{Z}$ with $\tau_E = \sigma_2 / \sigma_1$ in the complex upper half-plane $\mathfrak{H}$, then

$$\Delta_E = (2\pi)^{12} \sigma_1^{-12} \Delta(\tau_E) \tag{3.1}$$

where $\Delta(\tau)$ is the usual Jacobi delta function (see [13, Chapter VI]). Now let $V(\Lambda_E)$ denote the covolume of Λ_E (i.e. the volume of $\mathbb{C}/\Lambda_E$). Then $V(\Lambda_E) = |\sigma_1|^2 \operatorname{Im}(\tau_E)$, and (3.1) gives

$$|\Delta_E| \cdot V(\Lambda_E)^6 = (2\pi)^{12} \operatorname{Im}(\tau_E)^6 |\Delta(\tau_E)|. \tag{3.2}$$

Since $\Delta(\tau)$ is a modular form of weight 12, the function $\mathrm{Im}(\tau)^6|\Delta(\tau)|$ is invariant under the modular group $\mathrm{SL}_2(\mathbb{Z})$, and the quantity in (3.2) depends only on the curve (C, P). Thus the discriminant (corrected by the volume of the torus $\mathbb{C}/\Lambda_E$) is given by the value of a certain fixed continuous function (arising from a modular form) at the point on the moduli space $\mathfrak{H}/\mathrm{SL}_2(\mathbb{Z})$ corresponding to (C, P).

In [3], Goldfeld shows that for a certain class of Weierstrass equations, upper bounds for Δ_E can be obtained from lower bounds on the fundamental periods. Similarly, one can consider bounds on the discriminant in terms of the covolume of the period lattice. Since $\Delta(\tau)$ is a cusp form, the right-hand side of (2.7) is absolutely bounded on $\mathfrak{H}$, and we get $\Delta_E \ll V(\Lambda_E)^{-6}$.

In this section we generalize these results to hyperelliptic curves (C, P) of genus $g \geq 1$ defined over $\mathbb{C}$. The Siegel modular form corresponding to $\Delta(\tau)$ in (3.1) is constructed using products of special values of theta functions. This can be viewed as a generalization of the Jacobi Product Formula

$$\Delta_E = 16\pi^{12}\sigma_1^{-12}\theta_{00}(0, \tau_E)^8\theta_{10}(0, \tau_E)^8\theta_{01}(0, \tau_E)^8$$

where the θ_{ij} are the classical one-dimensional theta functions.

We first recall some basic facts about Siegel modular forms (see, for example [5]). Let $\mathfrak{H}_g = \{\tau \in M_g(\mathbb{C}) \mid {}^t\tau = \tau, \mathrm{Im}(\tau) \text{ positive definite}\}$ be the Siegel upper half-space of degree g. For $z \in \mathbb{C}^g$ (viewed as a column vector), $\tau \in \mathfrak{H}_g$, and $m = [{a \atop b}]$ with a, $b \in \frac{1}{2}\mathbb{Z}^g$, we have the *theta function with characteristic* m given by

$$\theta_m(z, \tau) = \sum_{n \in \mathbb{Z}^g} \exp\left\{i\pi\, {}^t(n+a)\tau(n+a) + 2\pi i\, {}^t(n+a)(z+b)\right\}.$$

Let Γ_N denote the congruence subgroup of level N for the symplectic modular group of degree g. Thus

$$\Gamma_N = \left\{\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z}) \mid \gamma \equiv I_{2g} \pmod{N}\right\}.$$

The group $\Gamma_1 = \mathrm{Sp}_{2g}(\mathbb{Z})$ acts on $\mathfrak{H}_g$ and on $\frac{1}{2}\mathbb{Z}^{2g}$ in the following way. Let $\sigma = \left({A \atop C}{B \atop D}\right) \in \Gamma_1$, $\tau \in \mathfrak{H}_g$, and $m \in \frac{1}{2}\mathbb{Z}^{2g}$. Then

$$\begin{aligned} \sigma\tau &= (A\tau + B)(C\tau + D)^{-1}, \\ \sigma m &= \begin{pmatrix} D & -C \\ -B & A \end{pmatrix} m + \tfrac{1}{2}\begin{pmatrix} \mathrm{diag}(C\,{}^tD) \\ \mathrm{diag}(A\,{}^tB) \end{pmatrix}. \end{aligned} \tag{3.3}$$

where $\mathrm{diag}(M)$ denotes the column vector composed of the diagonal entries of M.

Let $\varphi_m(\tau)$ denote the function $\theta_m(0, \tau)^8$. The transformation law for the theta function (see [5, Chapter V]) gives

$$\varphi_{\sigma m}(\sigma\tau) = \det(C\tau + D)^4\varphi_m(\tau), \qquad \sigma \in \mathrm{Sp}_{2g}(\mathbb{Z}). \tag{3.4}$$

We note that if $m \equiv m'$ modulo 1, then $\varphi_m = \varphi_{m'}$. Equations (3.3) and (3.4) show that φ_m is a modular form of weight four for Γ_2.

Given a Riemann surface C of genus g, let $\{A_i, B_i \mid 1 \leq i \leq g\}$ be a symplectic basis for $H_1(C, \mathbb{Z})$, i.e. a basis such that for $1 \leq i, j \leq g$,

$$A_i \cdot A_j = 0, \quad B_i \cdot B_j = 0, \quad A_i \cdot B_j = \delta_{ij}$$

where $\cdot$ is the (oriented) intersection product on C. Let $\{\omega_i \mid 1 \leq i \leq g\}$ be a basis for $H^0(C, \Omega^1)$. The period matrices σ, σ' are defined by

$$\sigma_{ij} = \int_{A_j} \omega_i, \qquad \sigma'_{ij} = \int_{B_j} \omega_i.$$

We have $\det\sigma \neq 0$ and $\tau = \sigma^{-1}\sigma' \in \mathfrak{H}_g$. We let Λ denote the lattice $\sigma\mathbb{Z}^g + \sigma'\mathbb{Z}^g$.

Now, let (C, P) be hyperelliptic over $\mathbb{C}$. Let E be a Weierstrass equation for C of the form $y^2 = f(x)$. C can thus be viewed as a branched covering of $\mathbb{P}^1$. Let B be the set of branch points. Write $f(x) = \prod_{i=1}^{2g+1}(x - a_i)$. Then $B = \{a_1, a_2, \dots, a_{2g+1}, \infty\}$. Attached to any ordering of B there is a canonical choice of symplectic basis for $H_1(C, \mathbb{Z})$ (see [10, Chapter IIIa, §5]). Using this, and the basis for $H^0(C, \Omega^1)$ given by (1.5), we get σ_E, σ'_E, τ_E, and Λ_E as above. Note that Λ_E depends only on E and not on the ordering of B.

For any subset S of $\{1, 2, \dots, 2g+1\}$, the *theta characteristic* $\eta_S \in \frac{1}{2}\mathbb{Z}^{2g}$ is defined as follows. Let

$$\eta_{2i-1} = \begin{bmatrix} {}^t(0 & \cdots & 0 & \frac{1}{2} & 0 & \cdots & 0) \\ {}^t(\frac{1}{2} & \cdots & \frac{1}{2} & 0 & 0 & \cdots & 0) \end{bmatrix}, \qquad 1 \leq i \leq g+1,$$

$$\eta_{2i} = \begin{bmatrix} {}^t(0 & \cdots & 0 & \frac{1}{2} & 0 & \cdots & 0) \\ {}^t(\frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} & 0 & \cdots & 0) \end{bmatrix}, \qquad 1 \leq i \leq g,$$

where the nonzero entry in the top row occurs in the ith position. Then we put $\eta_S = \sum_{k \in S} \eta_k$ where the sum is taken modulo 1 (see [10, Chapter IIIa]).

Definition 3.1. Let $\mathfrak{T}$ be the collection of subsets of $\{1, 2, \dots, 2g+1\}$ of cardinality $g+1$. Write $U = \{1, 3, \dots, 2g+1\}$ and let $\circ$ denote the symmetric difference operator. We then define

$$\varphi(\tau) = \prod_{T \in \mathfrak{T}} \varphi_{\eta_{T \circ U}}(\tau).$$

Thus φ is a Siegel modular form for Γ_2 which depends only on g. When $g = 1$, we have $\varphi(\tau) = 2^8\Delta(\tau)$.

Proposition 3.2. *Let (C, P) be hyperelliptic of genus g over $\mathbb{C}$ with Weierstrass equation $E : y^2 = f(x)$. Fix an ordering of the set of branch points $B = \{a_1, \dots, a_{2g+1}, \infty\}$ and let σ_E, τ_E be as above. Let $r = \binom{2g+1}{g+1}$, $n = \binom{2g}{g+1}$. Then*

$$\Delta_E^n = 2^{4gn}\pi^{4gr}(\det\sigma_E)^{-4r}\varphi(\tau_E). \tag{3.5}$$

Proof. We need the following result due to Thomae (see [10, Chapter IIIa, §8]).

Theorem. *Let $S \subseteq \{1, 2, \dots, 2g+1\}$ with $|S \circ U| = g+1$. Then*

$$\varphi_{\eta_S}(\tau_E) = (\det\sigma_E)^4\pi^{-4g} \prod_{\substack{i<j \\ i,j \in S\circ U}} (a_i - a_j)^2 \prod_{\substack{i<j \\ i,j \notin S\circ U}} (a_i - a_j)^2. \tag{3.6}$$

If $T \in \mathfrak{T}$ then $T \circ U$ is a set S of the form required in the theorem, and the correspondence $T \leftrightarrow S$ is clearly bijective. Taking the product over all $T \in \mathfrak{T}$, we get (note $r = |\mathfrak{T}|$)

$$\varphi(\tau_E) = (\det \sigma_E)^{4r}\pi^{-4gr} \prod_{T\in\mathfrak{T}} \left(\prod_{\substack{i<j \\ i,j\in T}} (a_i - a_j)^2 \prod_{\substack{i<j \\ i,j\notin T}} (a_i - a_j)^2 \right). \tag{3.7}$$

The number of times the term $(a_i - a_j)^2$ appears in the right-hand side of (3.7) is

$$\begin{aligned} |\{T \mid i, j \in T \text{ or } i, j \notin T\}| &= |\{T \mid i, j \in T\}| + |\{T \mid i, j \notin T\}| \\ &= \binom{2g-1}{g-1} + \binom{2g-1}{g+1} = \binom{2g}{g+1} = n. \end{aligned}$$

Thus (3.7) becomes

$$\varphi(\tau_E) = (\det \sigma_E)^{4r}\pi^{-4gr} \prod_{i<j} (a_i - a_j)^{2n}.$$

The discriminant of E is given by

$$\Delta_E = 2^{4g}\,\mathrm{Disc}(f) = 2^{4g} \prod_{i<j} (a_i - a_j)^2,$$

and substituting this into the previous equation yields (3.5).

Remark. Proposition 3.2 shows that a certain power of the discriminant can be obtained from a modular form. It would be interesting to know if this exponent could be removed or at least reduced. By using θ_m^2 in place of φ_m, one may take the fourth root of both sides of (3.5). This is carried out in the genus 2 case in [4]. To reduce the exponent further seems to require more subtle combinatorial arguments.

Proposition 3.3. *Let $V(\Lambda_E)$ denote the covolume of Λ_E in $\mathbb{C}^g$. The positive quantity $|\Delta_E| \cdot V(\Lambda_E)^{4+2/g}$ is an invariant of (C, P), i.e. it does not depend on E. Furthermore, the relation* (3.2) *has the hyperelliptic generalization*

$$|\Delta_E| \cdot V(\Lambda_E)^{4+2/g} = 2^{4g}\pi^{8g+4}(|\varphi(\tau_E)| \cdot \det(\mathrm{Im}(\tau_E))^{2r})^{1/n}. \tag{3.8}$$

Proof. By Proposition 1.12, a change of coordinates $E \mapsto \hat{E}$ results in a change of basis for $H^0(C, \Omega^1)$ given by $(\omega) = A(\hat{\omega})$ with $\det(A) = u^{-g^2}$. Therefore $\Lambda_E = A\Lambda_{\hat{E}}$. Hence

$$V(\Lambda_E) = |\det(A)|^2 V(\Lambda_{\hat{E}}) = |u|^{-2g^2} V(\Lambda_{\hat{E}}).$$

From Proposition 1.10 we have $\Delta_E = u^{8g^2+4g}\Delta_{\hat{E}}$, thus $|\Delta_E| \cdot V(\Lambda_E)^{4+2/g} = |\Delta_{\hat{E}}| \cdot V(\Lambda_{\hat{E}})^{4+2/g}$.

Viewing Λ_E as a lattice in $\mathbb{R}^{2g}$, we get

$$\begin{aligned} V(\Lambda_E) &= \left|\det \begin{pmatrix} \mathrm{Re}(\sigma_E) & \mathrm{Re}(\sigma_E') \\ \mathrm{Im}(\sigma_E) & \mathrm{Im}(\sigma_E') \end{pmatrix}\right| = 2^{-g} \left|\det \begin{pmatrix} \sigma_E & \sigma_E' \\ \bar{\sigma}_E & \bar{\sigma}_E' \end{pmatrix}\right| \\ &= |\det \sigma_E|^2 \det(\mathrm{Im}(\tau_E)). \end{aligned}$$

Equation (3.8) then follows directly from (3.5).

We now show that the continuous function $|\varphi(\tau)|\det(\operatorname{Im}\tau)^{2r}$ is bounded on $\mathfrak{H}_g$. We need the following facts about the Siegel-reduced domain $\mathfrak{F}_g$ (see [5, Chapter V]).

(S1) $\mathfrak{F}_g$ is a closed subset of $\mathfrak{H}_g$ and $\mathfrak{H}_g = \bigcup_{\sigma\in\Gamma_1}\sigma\mathfrak{F}_g$.

(S2) $\theta_m(0, \tau)$ is bounded on $\mathfrak{F}_g$ for all $m \in \frac{1}{2}\mathbb{Z}^{2g}$.

(S3) Suppose $m = [{a \atop b}] \in \frac{1}{2}\mathbb{Z}^{2g}$ with $a_g \notin \mathbb{Z}$. Then for any $e \geq 0$, the function $\theta_m(0, \tau)\det(\operatorname{Im}(\tau))^e$ is bounded on $\mathfrak{F}_g$.

Lemma 3.4. *Let* $\mathfrak{M} = \{\eta_{T\circ U} \mid T \in \mathfrak{T}\}$, $\sigma \in \Gamma_1$. *Then* $\sigma\mathfrak{M} = \{\sigma\eta_{T\circ U} \mid T \in \mathfrak{T}\}$ *contains at least one characteristic* $[{a \atop b}]$ *with* $a_g \notin \mathbb{Z}$.

Proof. Taking T to be of the form $U \circ \{2i-1, 2i\}$ for $1 \leq i \leq g$, we see that $\mathfrak{M}$ contains all characteristics of the form

$$p_i = \begin{bmatrix} {}^t(0 & \cdots & 0 & \cdots & 0) \\ {}^t(0 & \cdots & \frac{1}{2} & \cdots & 0) \end{bmatrix} \qquad (\tfrac{1}{2} \text{ in the } i\text{th place}).$$

Taking T to be of the form $U \circ \{2i, 2i+1, \dots, 2g+1\}$ for $1 \leq i \leq g$, we see that $\mathfrak{M}$ contains

$$q_i = \begin{bmatrix} {}^t(0 & \cdots & \frac{1}{2} & \cdots & 0) \\ {}^t(0 & \cdots & 0 & \cdots & 0) \end{bmatrix} \qquad (\tfrac{1}{2} \text{ in the } i\text{th place}).$$

Finally, letting $T = U$, we see that $0 \in \mathfrak{M}$. Write $\sigma = ({A \atop C}{B \atop D})$ and let

$$J = \frac{1}{2}\begin{pmatrix} \operatorname{diag}(C\,{}^tD) \\ \operatorname{diag}(A\,{}^tB) \end{pmatrix}.$$

From (3.3) we get

$$(\sigma p_i)_g = J_g - \tfrac{1}{2}C_{gi}, \quad (\sigma q_i)_g = J_g + \tfrac{1}{2}D_{gi}, \quad (\sigma 0)_g = J_g.$$

We claim that these cannot all be integers. Otherwise, we would have

$$C_{gi} \equiv D_{gi} \equiv 0 \pmod 2, \qquad 1 \leq i \leq g,$$

and the bottom row of σ would be even. But this contradicts the fact that $\det\sigma = \pm 1$.

Proposition 3.5. $|\varphi(\tau)|\det(\operatorname{Im}(\tau))^{2r}$ *is bounded on* $\mathfrak{H}_g$.

Proof. We have

$$\varphi(\tau) = \prod_{m\in\mathfrak{M}} \varphi_m(\tau),$$

so that for any $\sigma \in \Gamma_1$,

$$\begin{aligned} |\varphi(\sigma\tau)|\det(\operatorname{Im}(\sigma\tau))^{2r} &= \prod_{m\in\mathfrak{M}} |\varphi_m(\sigma\tau)|\det(\operatorname{Im}(\sigma\tau))^2 \\ &= \prod_{m\in\mathfrak{M}} |\varphi_{\sigma^{-1}m}(\tau)|\det(\operatorname{Im}(\tau))^2 \\ &= \prod_{m\in\sigma^{-1}\mathfrak{M}} |\varphi_m(\tau)|\det(\operatorname{Im}(\tau))^2 \end{aligned}$$

using (3.4) and the fact that $\det(\operatorname{Im}(\sigma\tau)) = \det(\operatorname{Im}(\tau))|\det(C\tau + D)|^{-2}$. From (S2), (S3), and Lemma 3.4, we see that $|\varphi(\tau)|\det(\operatorname{Im}\tau)^{2r}$ is bounded on $\sigma\mathfrak{F}_g$

for each $\sigma \in \Gamma_1$. By (S1), the $\sigma\mathfrak{F}_g$ cover $\mathfrak{H}_g$, but since φ is a modular form of level two, we need only consider the finitely many $\sigma \in \Gamma_2 \backslash \Gamma_1 \cong \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. Thus $|\varphi(\tau)| \det(\mathrm{Im}(\tau))^{2r}$ is bounded on the entire upper half-space $\mathfrak{H}_g$.

Combining Propositions 3.3 and 3.5 we obtain

Corollary 3.6. *Let (C, P) be hyperelliptic over $\mathbb{C}$ with Weierstrass equation E. Then*

$$|\Delta_E| \ll V(\Lambda_E)^{-4-2/g}$$

where the implied constant depends only on g.

4. Arithmetic conjectures

Let K be a number field, and let (C, P) be hyperelliptic of genus g over K. In this section we examine two conjectures concerning the arithmetic of the minimal discriminant ideal $\mathfrak{D}_{C/K}$. As usual, let M_K^0 and M_K^∞ denote the set of finite and infinite places of K, respectively. Recall that for each $v \in M_K^0$ we have a hyperelliptic curve C_v obtained by extension of base-field to the completion K_v. The reduction $\tilde{C}_v$ of C_v is thus a (possibly singular) curve over the residue field k_v of v.

Let S be a finite set of places containing M_K^∞. Let q_v denote the cardinality of the residue field k_v, and $N = N_{K/\mathbb{Q}}$ denote the absolute norm from K to $\mathbb{Q}$. Thus if $\mathfrak{a}$ is a fractional ideal of K, we have

$$N\mathfrak{a} = \prod_{v \in M_K^0} q_v^{v(\mathfrak{a})}.$$

For elliptic curves, L. Szpiro has made the following conjecture concerning the arithmetic of the minimal discriminant (see [15]).

Szpiro's Conjecture. *Let C be an elliptic curve over K. Then*

$$N\mathfrak{D}_{C/K} \ll \left(\prod_{v \notin S} q_v^{n_v} \right)^{1+\varepsilon} \tag{4.1}$$

where

$$n_v = \begin{cases} 0, & \tilde{C}_v \textit{ is nonsingular}, \\ 6, & \tilde{C}_v \textit{ has a node}, \\ 12, & \tilde{C}_v \textit{ has a cusp}, \end{cases}$$

and the implied constant depends only on K, S, and ε.

Remark. Szpiro's Conjecture is usually stated as $N\mathfrak{D}_{C/K} \ll N^{6+\varepsilon}$, where N denotes the absolute norm of the *conductor* of C/K. For $\mathrm{char}(k_v) > 3$ the valuation of the conductor is 0, 1, or 2, depending on whether the reduction type is good, nodal, or cuspidal. For $\mathrm{char}(k_v) \leq 3$ the valuation is at any rate bounded (the bound depending on K), hence the conjecture is equivalent to (4.1) (see [8]).

We now generalize Szpiro's Conjecture to hyperelliptic curves. Let (C, P) be hyperelliptic of genus g over K.

Conjecture 4.1. *There exist nonnegative exponents n_v, $v \notin S$ depending only on the reduction type of C_v, such that*

$$N\mathfrak{D}_{C/K} \ll \left(\prod_{v \notin S} q_v^{n_v}\right)^{1+\varepsilon} \tag{4.2}$$

where the constant depends only on K, g, S, and ε. Moreover, if $\tilde{C}_v$ is nonsingular we may take $n_v = 0$.

The last condition insures that only finitely many of the n_v are nonzero. More precisely, we have

Conjecture 4.2. *The numbers n_v are given by*

$$n_v = \sum_{Q \in \tilde{C}_v} n(d_Q) \tag{4.3}$$

where d_Q is the order of the point Q (see §2) and $n(d)$ depends only on g, d. Furthermore, $n(1) = 0$ (i.e. the sum is taken over the singularities of $\tilde{C}_v$).

Remark. When $g = 1$ the above reduces to Szpiro's Conjecture, where we take $n(d) = 6(d-1)$, $1 \le d \le 3$.

Question. What is the correct form of $n(d)$? By analogy with the elliptic case, we tentatively suggest $n(d) = (4g+2)(d-1)$.

Before we examine these conjectures, we require some additional notation. Let R denote the integers of K. For each $v \in M_K^0$ we let R_v be the valuation ring of v in K_v, $\mathfrak{p}_v$ the maximal ideal of R_v, and π_v a generator of $\mathfrak{p}_v$. We have $q_v = N\mathfrak{p}_v$. Let $M_K = M_K^0 \cup M_K^\infty$ be the set of places of K. For $v \in M_K$ we let $|\cdot|_v$ denote the absolute value at v, normalized so that $\prod_{v \in M_K} |x|_v = 1$ for all $x \in K$. In particular, we have $|x|_v = q_v^{-v(x)}$ for $x \in K_v$. If $|\cdot|$ is any absolute value, we write $|x_1, \dots, x_n| = \max_{1 \le i \le n} |x_i|$. Let S be a finite set of places containing M_K^∞. Let R_S denote the ring of S-integers of K, and R_S^* the group of S-units.

Let $x_1, \dots, x_n \in K$. For any set V of places we define

$$H_V(x_1, \dots, x_n) = \prod_{v \in V} |x_1, \dots, x_n|_v.$$

We make the following abbreviations: $H_K = H_{M_K}$, $H_0 = H_{M_K^0}$, and $H_\infty = H_{M_K^\infty}$. Thus $H_K = H_0 H_\infty$ and H_K is just the usual relative multiplicative height (see [13, Chapter VIII §5]). Let $x_i \in K$ and let $(x_1, \dots, x_n)$ denote the fractional ideal generated by the x_i. Then

$$N(x_1, \dots, x_n) = \prod_{v \in M_K^0} q_v^{\min(v(x_1), \dots, v(x_n))} = H_0(x_1, \dots, x_n)^{-1}. \tag{4.4}$$

Note also that

(4.5)

$$|Nx_1, \dots, Nx_n| = \max_{1 \le i \le n} \prod_{v \in M_K^\infty} |x_i|_v \le \prod_{v \in M_K^\infty} |x_1, \dots, x_n|_v = H_\infty(x_1, \dots, x_n).$$

Finally, for $x \in R_S$ we define

$$S_K(x) = \prod_{\substack{v \notin S \\ v|x}} q_v$$

where $v|x$ means $v(x) > 0$.

We are now in a position to state the ABC Conjecture of D. Masser and J. Oesterlé (see [16]).

ABC Conjecture. *Suppose $a, b, c \in R_S$ with $a + b + c = 0$. Then*

$$H_K(a, b, c) \ll S_K(abc)^{1+\varepsilon}$$

where the constant depends only on K, S, and ε.

It is known (see [9, 11, 14]) that the ABC Conjecture implies Szpiro's Conjecture. Moreover, Frey [2] has shown that Szpiro's Conjecture implies the ABC conjecture (with the exponent $1 + \varepsilon$ replaced by $\frac{3}{2} + \varepsilon$). Frey's argument was generalized to the hyperelliptic case in [7].

It is natural to wonder whether the ABC Conjecture implies Conjectures 4.1 and 4.2 for hyperelliptic curves of arbitrary genus. The remainder of this section is devoted to the proof of the following result in this direction.

Proposition 4.3. *Let C be given by an S-minimal Weierstrass equation of the form $y^2 = f(x)$. The ABC Conjecture implies Conjectures* 4.1 *and* 4.2 *in the following cases:*

(a) *$f(x)$ has only three nonzero coefficients. We have*

$$n(d) \le \begin{cases} 0, & d = 1, \\ 4g + 2, & 2 \le d \le 2g, \\ 2g(4g + 2), & d = 2g + 1. \end{cases} \tag{4.6}$$

(b) *$f(x)$ splits completely into linear factors over $K[x]$. We have*

$$n(d) \le \begin{cases} d(d - 1)(6g - 2d + 1), & d \le 2g, \\ 2g^2(4g + 2), & d = 2g + 1. \end{cases} \tag{4.7}$$

Remark. The two cases considered above are rather special. The first allows us to compute the disciminant easily and to apply the ABC Conjecture directly. If more than three coefficients are present, the discriminant becomes rather unwieldy. In the second case, we apply ABC to certain combinations of the roots of $f(x)$, which are thus required to lie in the ground field. It should perhaps be noted that the result in part (a) compares favorably with the conjectural $n(d) \le (4g + 2)(d - 1)$.

For the proof of Proposition 4.3(a) we will need the following lemma. This generalizes an argument due to Hindry and Silverman (see [11 and 14]) concerning the equation $z = x^3 + y^2$ over the rational integers.

Lemma 4.4. *Let $a, b \in R$. Let m and n be positive integers with $m \ge 2$ and $n \ge 3$. Suppose $x, y, z \in R$ with*

$$z = ax^n + by^m. \tag{4.8}$$

Let $F = (x^n, y^m)$ *and suppose there exists a positive integer* X *such that*

$$v(F) < mnX, \qquad v \in M_K^0. \tag{4.9}$$

Then assuming the ABC Conjecture, we have for any $\varepsilon > 0$,

$$|Nx^n, Ny^m, Nz| \ll \left(\prod_{v|F} q_v^{mnX} \prod_{\substack{v|yz\\ v\nmid F}} q_v^{n/(n-1)}\right)^{1+\varepsilon}, \tag{4.10}$$

$$|Nx^n, Ny^m, Nz| \ll \left(\prod_{v|F} q_v^{mnX} \prod_{\substack{v|z\\ v\nmid F}} q_v^{mn/(mn-m-n)}\right)^{1+\varepsilon} \tag{4.11}$$

where the constants depend only on K, a, b, *and* ε.

Proof. Let $S = M_K^\infty$. The ABC Conjecture applied to (4.8) yields

$$H_K(ax^n, by^m, z)^{1-\varepsilon} \ll S_K(abxyz).$$

Since $H_K(ax^n, by^m, z) \gg H_K(x^n, y^m, z)$ and $S_K(abxyz) \ll S_K(xyz)$, we get

$$H_K(x^n, y^m, z)^{1-\varepsilon} \ll S_K(xyz). \tag{4.12}$$

Let $M = |Nx^n, Ny^m, Nz|$. From (4.4) and (4.5) we have

$$H_0(x^n, y^m, z) = N(F)^{-1}, \quad H_\infty(x^n, y^m, z) \geq M.$$

Combining these with (4.12) yields $M^{1-\varepsilon} \ll N(F)S_K(xyz)$. Now, consider the inequalities

$$S_K(xyz) \cdot \prod_{v|F} q_v^{v(x)} \leq N(x)S_K(yz), \tag{4.13}$$

$$S_K(xyz) \cdot \prod_{v|F} q_v^{v(xy)} \leq N(xy)S_K(z), \tag{4.14}$$

which are easily verified by comparing the exponents of q_v on both sides. Using (4.13), we get

$$\begin{aligned} M^{1-\varepsilon} &\ll N(x)N(F)S_K(yz) \cdot \prod_{v|F} q_v^{-v(x)} \\ &\ll M^{1/n}S_K(yz) \cdot \prod_{v|F} q_v^{v(F)-v(x)}. \end{aligned}$$

Thus,

$$M^{1-\varepsilon} \ll \left(\prod_{v|F} q_v^{v(F)-v(x)+1} \prod_{\substack{v|yz\\ v\nmid F}} q_v\right)^{n/(n-1)}.$$

Now $v(x) \geq \frac{1}{n}v(F)$, since $F = (x^n, y^m)$. From (4.9) we have

$$v(F) - v(x) + 1 \leq \sup_{0 \leq l < mnX} \left(l + 1 - \left\lceil \frac{l}{n} \right\rceil\right) = m(n-1)X$$

which gives (4.10).

Similarly, using (4.14) we get

$$\begin{aligned} M^{1-\varepsilon} &\ll N(xy)N(F)S_K(z)\prod_{v|F} q_v^{-v(xy)} \\ &\ll M^{1/m+1/n}S_K(z)\cdot\prod_{v|F} q_v^{v(F)-v(x)-v(y)} \end{aligned}$$

Thus

$$M^{1-\varepsilon} \ll \left(\prod_{v|F} q_v^{v(F)-v(x)-v(y)+1}\prod_{\substack{v|z\\ v\nmid F}} q_v\right)^{mn/(mn-m-n)}$$

and

$$\begin{aligned} v(F)-v(x)-v(y)+1 &\leq \sup_{0\leq l<mnX}\left(l+1-\left\lceil\frac{l}{m}\right\rceil-\left\lceil\frac{l}{n}\right\rceil\right) \\ &\leq \sup_{0\leq l<mnX}\left\lfloor 1+l\left(1-\frac{1}{m}-\frac{1}{n}\right)\right\rfloor \\ &\leq \left\lfloor 1+(mnX-1)\left(1-\frac{1}{m}-\frac{1}{n}\right)\right\rfloor \\ &= (mn-m-n)X \end{aligned}$$

yielding (4.11).

Remark. Lemma 4.4 can easily be extended to S-integers. Let $a, b, x, y, z \in R_S$ satisfy (4.8). If we replace (4.9) by the conditions

$$\begin{aligned} &v(F) < mnX, && v \notin S, \\ &v(F) \ll 1, && v \in S\cap M_K^0, \end{aligned}$$

where the implied constant depends only on K, then we get (4.10) and (4.11) just as before, except that the constants may now depend on S.

Proof (*of Proposition* 4.3). Suppose we are given C with an S-minimal Weierstrass equation E: $y^2 = f(x)$, where $f(x)$ has only three nonzero coefficients. These conditions are invariant under a change of coordinates $x \mapsto u^2x$; $y \mapsto u^{2g+1}y$ with $u \in R_S^*$. Since enlarging S only helps our cause, we may assume by Corollary 2.11 that

$$v(\Delta_E/\mathfrak{D}_{C/K}) \ll 1, \qquad v\in S. \tag{4.15}$$

It will also be convenient to assume that S contains all ramified places, and all places dividing rational primes $p \leq 2g+1$.

Since C is nonsingular, $f(x)$ cannot be divisible by x^2. We thus distinguish three cases:

(1)	$E: y^2 = x^n + Ax^k + B$,	$B\neq 0$,	$n = 2g+1$,	$2\leq k\leq n-1$,
(2)	$E: y^2 = x(x^n + Ax^k + B)$,	$B\neq 0$,	$n = 2g$,	$1\leq k\leq n-1$,
(3)	$E: y^2 = x^n + Ax + B$,	$AB\neq 0$,	$n = 2g+1$,	$k = 1$.

Let $m = n-k$. Since E is S-minimal, we must have

$$\min(v(A^n), v(B^m)) < 2mn, \qquad v\notin S, \tag{4.16}$$

else the discriminant at v could be reduced by the substitution $x \mapsto \pi_v^2 x$; $y \mapsto \pi_v^{2g+1} y$. Similarly, from (4.15) we deduce that

$$\min(v(A^n), v(B^m)) \ll 1, \qquad v \in S, \tag{4.17}$$

where, as usual, the constant depends only on K.

Let $r = (n, k)$. Define $n_0 = n/r$, $k_0 = k/r$, $m_0 = m/r$, and let

$$D = {n_0}^{n_0} B^{m_0} + (-1)^{n_0 - 1} {k_0}^{k_0} {m_0}^{m_0} A^{n_0}.$$

Computing the discriminant using resultants (see §1), we get

$$\Delta_E = \begin{cases} r^n B^{k-1} D^r, & \text{case } (1), \\ r^n B^{k+1} D^r, & \text{case } (2), \\ D, & \text{case } (3). \end{cases}$$

To handle the first two cases, we set $F = (A^{n_0}, B^{m_0})$. Then (4.16) and (4.17) give

$$\begin{aligned} v(F) &< 2rm_0n_0, & v &\notin S, \\ v(F) &\ll 1, & v &\in S. \end{aligned}$$

Let $M = |NA^{n_0}, NB^{m_0}, ND|$. By the remark following Lemma 4.4, we may use the lemma with $X = 2r$ to obtain the bound

$$M^{1-\varepsilon} \ll \prod_{v|F} q_v^{2rm_0n_0} \prod_{\substack{v|BD \\ v\nmid F}} q_v^{n_0/(n_0-1)}. \tag{4.18}$$

Now,

$$N\Delta_E \ll NB^{k\pm 1} ND^r \ll M^{(k\pm 1)/m_0 + r} = M^{(n\pm 1)/m_0},$$

where the minus sign is used in case (1) and the plus sign in case (2). Using this in (4.18), we get

$$N\Delta_E^{1-\varepsilon} \ll \prod_{v|F} q_v^{2n(n\pm 1)} \prod_{v|\Delta_E v\nmid F} q_v^{n_0(n\pm 1)/m_0(n_0-1)}. \tag{4.19}$$

Here we have used the fact that BD divides Δ_E. In both cases the exponent $2n(n \pm 1)$ is equal to $2g(4g+2)$, and

$$\frac{n_0(n\pm 1)}{m_0(n_0-1)} \leq 2(n\pm 1) \leq 4g+2.$$

Since the places outside of S which divide $\mathfrak{D}_{C/K}$ are the same as those dividing Δ_E, we get

$$N\mathfrak{D}_{C/K} \ll N\Delta_E \ll \left(\prod_{\substack{v\notin S \\ v|\mathfrak{D}_{C/K}}} q_v^{n_v} \right)^{1+\varepsilon}$$

where

$$n_v = \begin{cases} 4g+2, & v \nmid F, \\ 2g(4g+2), & v|F. \end{cases} \tag{4.20}$$

Now consider the reduction of the curves in cases (1) and (2) at a place $v \notin S$. If $v \in F$, then we have $v(A) > 0$ and $v(B) > 0$, hence the reduced equation has a unique singular point of degree $2g+1$. If $v \notin F$, then the reduced equation cannot have a singular point of degree $2g+1$. It follows that the estimate for n_v in (4.20) is actually better than that given by (4.6). This completes cases (1) and (2).

In case (3), we have $F = (A^n, B^m)$ and $X = 2$. Lemma 4.4 gives

$$M^{1-\varepsilon} \ll \prod_{v|F} q_v^{2mn} \prod_{\substack{v|D \\ v\nmid F}} q_v^{mn/(mn-m-n)} \tag{4.21}$$

where $M = |NA^n, NB^m, ND|$. We have $N\Delta_E = ND \le M$ and $m = n-1$. Thus

$$N\Delta_E^{1-\varepsilon} \ll \prod_{v|F} q_v^{2n(n-1)} \prod_{\substack{v|\Delta_E \\ v\nmid F}} q_v^{(n^2-n)/(n^2-3n+1)}.$$

The first exponent is $2n(n-1) = 2g(4g+2)$, and we have

$$\frac{n^2-n}{n^2-3n+1} \le 2n = 4g+2, \qquad n \ge 3,$$

so again (4.6) is valid. The reason case (3) needs to be handled separately is that the places dividing B do not appear in the discriminant as they do in cases (1) and (2). This completes the proof of Proposition 4.3(a).

For part (b), we are given an S-minimal equation $E : y^2 = f(x)$ with

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i), \qquad \alpha_i \in R_S, \tag{4.22}$$

where $n = 2g+1$ as before. Let $a_{ij} = \alpha_i - \alpha_j$ for all $1 \le i, j \le n$. Then the discriminant of E is simply

$$\Delta_E = 2^{4g} \prod_{i<j} a_{ij}^2. \tag{4.23}$$

Let $F = (a_{ij})$, the fractional ideal generated by the a_{ij}. We will need an upper bound on the size of $v(F)$ for all $v \in M_K^0$. First, suppose $v(F) \ge 2$ for some $v \notin S$. Then $v(a_{ij}) \ge 2$ for all $1 \le i, j \le n$. Hence all the α_i are congruent mod $\mathfrak{p}_v^2$. Let α be any one of the α_i. The substitution $x \mapsto \pi_v^2 x + \alpha$, $y \mapsto \pi_v^n y$ then yields a v-integral equation with smaller $v(\Delta_E)$, contradicting the S-minimality of E. Therefore $v(F) \le 1$. We see that $v(F) = 1$ only when the reduction of E has a singularity of degree n. Otherwise, since F is an S-integral ideal, we have $v(F) = 0$.

By Corollary 2.11, we may assume (as in the proof of part (a) above) that

$$v(\Delta_E/\mathfrak{D}_{C/K}) \ll 1, \qquad v \in S. \tag{4.24}$$

This means that the α_i cannot all be very close to each other, hence the minimal $v(a_{ij})$ is bounded by a constant depending only on K. In other words,

$$v(F) \ll 1, \qquad v \in S. \tag{4.25}$$

Now, we have $a_{ij} + a_{jk} + a_{ki} = 0$, so the ABC Conjecture gives

$$H_K(a_{ij}, a_{jk}, a_{ki}) \ll S_K(a_{ij}a_{jk}a_{ki})^{1+\varepsilon}. \tag{4.26}$$

Let us write Na_{12} in the form

$$Na_{12} = \frac{N(a_{12})}{N(a_{12}, a_{23})} \times \frac{N(a_{12}, a_{23})}{N(a_{12}, a_{23}, a_{34})} \times \cdots \times \frac{N(a_{12}, \ldots, a_{n-2,n-1})}{N(a_{12}, \ldots, a_{n-1,n})} \times N(a_{12}, \ldots, a_{n-1,n}). \tag{4.27}$$

(This idea was sugested by J. Oesterlé.) To estimate the terms in this expression, we require the following:

Lemma 4.5. *Let* $x_1, \ldots, x_n, x \in K$. *Then*

$$\frac{N(x_1, \ldots, x_n)}{N(x_1, \ldots, x_n, x)} \leq H_K(x_n, x).$$

Proof. From (4.4) and (4.5) we get

$$H_K(x_n, x) = H_\infty(x_n, x) \cdot H_0(x_n, x) \geq \frac{Nx_n}{N(x_n, x)}.$$

Thus we are reduced to showing that

$$N(x_1, \ldots, x_n)N(x_n, x) \leq Nx_n \cdot N(x_1, \ldots, x_n, x). \tag{4.28}$$

We will prove the stronger statement that for any $v \in M_K^0$, the exponent of q_v on the left side of (4.28) is less than that on the right. Let $b = v(x)$, $b_i = v(x_i)$. We need to show that

$$\min(b_1, b_2, \ldots, b_n) + \min(b_n, b) \leq \min(b_1, b_2, \ldots, b_n, b) + b_n. \tag{4.29}$$

But this is always true for any integers $b_1, b_2, \ldots, b_n, b \in \mathbb{Z}$. Indeed, if $b_i \leq b$ for some i, then

$$\min(b_1, b_2, \ldots, b_n) = \min(b_1, b_2, \ldots, b_n, b), \quad \min(b_n, b) \leq b_n,$$

and if $b < b_i$ for all i, then

$$\min(b_1, b_2, \ldots, b_n) \leq b_n, \quad \min(b_n, b) = b = \min(b_1, b_2, \ldots, b_n, b).$$

In either case we have (4.29) and the lemma is proved.

Applying Lemma 4.5 to (4.27), and using the fact that $\{a_{12}, a_{23}, \ldots a_{n-1,n}\}$ generates F, we get

$$Na_{12} \leq H_K(a_{12}, a_{23}, a_{31}) \cdots H_K(a_{n-2,n-1}, a_{n-1,n}, a_{n,n-2}) \cdot N(F).$$

Here we have used the relation $H_K(a, b) = H_K(a, b, -a-b)$. Now (4.26) gives

$$Na_{12}^{1-\varepsilon} \ll N(F) \cdot \prod_{i=1}^{n-2} S_K(a_{i,i+1}a_{i+1,i+2}a_{i+2,i}). \tag{4.30}$$

Moreover, we may apply any permutation of the indices in (4.30) to obtain similar estimates for the norms of the a_{ij}. Multiplying over all such permutations yields

$$\prod_{i<j} Na_{ij}^{2(n-2)!(1-\varepsilon)} \ll N(F)^{n!} \cdot \prod_{i<j<k} S_K(a_{ij}a_{jk}a_{ki})^{6(n-2)!}$$

which gives

$$\prod_{i<j} Na_{ij}^{2(1-\varepsilon)} \ll N(F)^{n(n-1)} \cdot \prod_{i<j<k} S_K(a_{ij}a_{jk}a_{ki})^6.$$

Thus from (4.23) and (4.25) we get

$$N(\Delta_E)^{1-\varepsilon} \ll \prod_{v \notin S} q_v^{n_v}$$

with

$$n_v = n(n-1)v(F) + 6 \sum_{i<j<k} \begin{cases} 1, & v(a_{ij}a_{jk}a_{ki}) > 0 \\ 0, & \text{otherwise.} \end{cases}$$

Let T denote the number of triples (i, j, k) for which $1 \le i < j < k \le n$ and $v(a_{ij}a_{jk}a_{ki}) > 0$. Then

$$(4.31) \qquad n_v = \begin{cases} n(n-1) + 6T, & \tilde{E} \text{ has a singularity of degree } n, \\ 6T, & \text{otherwise.} \end{cases}$$

where the tilde denotes reduction mod $\mathfrak{p}_v$.

Consider the complete graph G with vertices α_i, $1 \le i \le n$. Label the edge joining α_i and α_j with the number $\tilde{a}_{ij}^2$. T then counts the number of triangles in G containing an edge labelled 0. The set of such edges of G form a collection of disjoint complete graphs, one for each multiple root of $\tilde{f}$. More precisely, a d-fold root of $\tilde{f}$ corresponds to a K_d all of whose edges are labelled 0. T thus breaks up into a sum over multiple roots of $\tilde{f}$, which are just the singularities of $\tilde{C}_v$. We have $T = \sum_{\alpha\in\tilde{C}_v} T(d_\alpha)$ where $T(d)$ is the number of triangles in G with an edge in a fixed K_d. In particular, $T(1) = 0$. A simple computation gives

$$T(d) = \binom{d}{2}(n-2) - 2\binom{d}{3} = \frac{1}{6}d(d-1)(3n-2d-2).$$

Thus

$$n_v = \sum_{\alpha\in\tilde{C}_v} n(d_\alpha)$$

with

$$n(d) = \begin{cases} d(d-1)(3n-2d-2), & d < n, \\ n(n-1)^2, & d = n. \end{cases}$$

Setting $n = 2g + 1$ gives (4.7) and the proof of Proposition 4.3 is complete.

References

1. E. Arabello, et al., *Geometry of algebraic curves*, Grundlehren Math. Wiss. 267, Springer-Verlag, New York, 1985.
2. G. Frey, *Links between stable elliptic curves and certain Diophantine equations*, Ann. Univ. Sarav. **1** (1986), 1–39.
3. D. Goldfeld, *Modular elliptic curves and Diophantine problems*, Number Theory, Proc. First Canadian Number Theory Conf., De Gruyter, New York, 1990, pp. 157–176.
4. D. Grant, *A generalization of Jacobi's derivative formula to dimension two*, J. Reine Angew. Math. **392** (1988), 125–136.
5. J. Igusa, *Theta functions*, Springer-Verlag, New York, 1972.

6. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.
7. P. Lockhart, *Diophantine equations and the arithmetic of hyperelliptic curves*, Thesis, Columbia University, 1990.
8. P. Lockhart, M. Rosen, and J. H. Silverman, *An upper bound for the conductor of an abelian variety*, J. Algebraic Geom. (to appear).
9. P. Lockhart, *The ABC Conjecture implies Szpiro's Conjecture over arbitrary number fields*, unpublished.
10. D. Mumford, *Tata lectures on theta.* I & II, Birkhäuser, Boston, Mass., 1983.
11. J. Oesterlé, *Nouvelles approches du Théorème de Fermat*, Sém. Bourbaki 694, 1988.
12. J.-P. Serre, *Local fields*, Graduate Texts in Math. 67, Springer-Verlag, New York, 1979.
13. J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. 106, Springer-Verlag, New York, 1985.
14. ——, *The abc-Conjecture implies Szpiro's Conjecture*, unpublished.
15. L. Szpiro, *Seminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque No. 3 **86** (1981), 44–78.
16. P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Math., vol. 1239, Springer-Verlag, 1980, pp. 84–88.

Brown University, Box 1917, Providence, Rhode Island 02912
E-mail address: lockhart@gauss.math.brown.edu