Points of low height on elliptic curves and surfaces I: Elliptic surfaces over P1 with small d

Points of low height on elliptic curves and surfaces I: Elliptic surfaces over $\mathbf{P}^1$ with small d

Noam D. Elkies

Department of Mathematics, Harvard University, Cambridge, MA 02138 USA

Abstract. For each of $n = 1, 2, 3$ we find the minimal height $\hat{h}(P)$ of a nontorsion point P of an elliptic curve E over $\mathbf{C}(T)$ of discriminant degree $d = 12n$ (equivalently, of arithmetic genus n), and exhibit all (E, P) attaining this minimum. The minimal $\hat{h}(P)$ was known to equal $1/30$ for $n = 1$ (Oguiso-Shioda) and $11/420$ for $n = 2$ (Nishiyama), but the formulas for the general (E, P) were not known, nor was the fact that these are also the minima for an elliptic curve of discriminant degree $12n$ over a function field of any genus. For $n = 3$ both the minimal height $(23/840)$ and the explicit curves are new. These (E, P) also have the property that that mP is an integral point (a point of naïve height zero) for each $m = 1, 2, \ldots, M$, where $M = 6, 8, 9$ for $n = 1, 2, 3$; this, too, is maximal in each of the three cases.

1. Introduction.

1.1 Statement of results. Let K be a function field of a curve C of genus g over a field k of characteristic zero,[1] and E a nonconstant elliptic curve over K. Let d be the degree of the discriminant of E (considered as a divisor on C), a natural measure of the complexity of E; and let $\hat{h} : E(K) \to \mathbf{Q}$ be the canonical height. Necessarily $12|d$; in fact it is known that $d = 12n$ where n is the arithmetic genus of the elliptic surface $\mathcal{E}$ associated with E. It is not hard to show that, given d, the set of numbers H that can occur as the canonical height of a rational point on E is discrete. In particular, for each $d = 12n$ there is a minimal positive height $\hat{h}_{\min}(d)$, and also a minimal positive height $\hat{h}_{\min}(g, d)$ for elliptic curves over function fields of genus g (except for $g = d = 0$, when E is a constant curve over $\mathbf{P}^1$ and thus has no points of positive height). It is thus a natural problem to compute or estimate these numbers $\hat{h}_{\min}(d)$ and $\hat{h}_{\min}(g, d)$. This paper is the first of a series concerned with different aspects of this problem.

In this paper we determine $\hat{h}_{\min}(12n)$ for $n = 1, 2$ and $\hat{h}_{\min}(0, 12n)$ for $n = 1, 2, 3$. Since we are working in characteristic zero, we may assume $k = \mathbf{C}$, when every genus-zero curve is isomorphic to $\mathbf{P}^1$ and its function field is isomorphic to $\mathbf{C}(T)$.

[1] One can also usefully define the canonical height etc. in positive characteristic, but we need to use the ABC conjecture for K and thus must assume that K has characteristic zero.

Theorem 1. *i) (Oguiso-Shioda [7])* $\hat{h}_{\min}(0,12) = 1/30$.
ii) $\hat{h}_{\min}(12) = 1/30$. *Moreover, let* E *be an elliptic curve with* $d = 12$ *over a complex function field* K, *and* $P \in E(K)$. *Then the following are equivalent: (a)* $\hat{h}(P) = 1/30$; *(b) Each of* $P, 2P, 3P, 4P, 5P, 6P$ *is an integral point on* E; *(c)* $K \cong \mathbf{C}(T)$, *and* (E,P) *is equivalent to the curve*

$$E_1(q) : Y^2 + (s' - (q+1)s)XY + qss'(s-s')Y = X^3 - qss'X^2 \tag{1}$$

over the $(s : s')$ *line with the rational point* $P : (X,Y) = (0,0)$, *for some* $q \in \mathbf{C}$ *other than* 0 *or* 1.

Theorem 2. *i) (Nishiyama [6])* $\hat{h}_{\min}(0,24) = 11/420$.
ii) $\hat{h}_{\min}(24) = 11/420$. *Moreover, let* E *be an elliptic curve with* $d = 24$ *over a complex function field* K, *and* $P \in E(K)$. *Then the following are equivalent: (a)* $\hat{h}(P) = 11/420$; *(b)* mP *is an integral point on* E *for each* $m = 1, 2, \ldots, 8$; *(c)* $K \cong \mathbf{C}(T)$, *and* (E,P) *is equivalent to the curve*

$$\begin{aligned} E_2(u) : Y^2 &+ (r^2 - r'^2 + (u-2)rr')XY \\ &- r^2r'(r+r')(r+ur')(r+(u-1)r')Y \\ &= X^3 - rr'(r+r')(r+ur')X^2 \end{aligned} \tag{2}$$

over the $(r : r')$ *line with the rational point* $P : (X,Y) = (0,0)$, *for some* $u \in \mathbf{C}$ *other than* $0, 1$.

Theorem 3. *i)* $\hat{h}_{\min}(0,36) = 23/840$.
ii) Let $E/\mathbf{C}(T)$ *be an elliptic curve with* $d = 36$, *and* P *a rational point on* E. *Then the following are equivalent: (a)* $\hat{h}(P) = 23/840$; *(b)* mP *is an integral point on* E *for each* $m = 1, 2, \ldots, 9$; *(c)* (E,P) *is equivalent to the curve*

$$\begin{aligned} E_3(A) : Y^2 &+ (At^3 + (1-2A)t^2t' - (A+1)tt'^2 - t'^3)XY \\ &- t^3t'(t+t')(At+t')(At+(1-A)t')(At^2+tt'+t'^2)Y \\ &= X^3 - tt'(t+t')(At+t')(At^2+tt'+t'^2)Y \end{aligned} \tag{3}$$

over the $(t : t')$ *line with the rational point* $P : (X,Y) = (0,0)$, *for some* $A \in \mathbf{C}$ *other than* $0, 1$.

The values of $\hat{h}_{\min}(12)$ and $\hat{h}_{\min}(24)$ are new. Note that we do not claim to determine $\hat{h}_{\min}(36)$. As indicated, the values of $\hat{h}_{\min}(0,12)$ and $\hat{h}_{\min}(0,24)$ (the first parts of Theorems 1 and 2) were already known, but were obtained using techniques that are specific to the geometry of rational and K3 elliptic surfaces and do not readily generalize past $n = 2$. Our approach lets us treat all three cases uniformly, and in principle lets us determine $\hat{h}_{\min}(0,12n)$ for any n, though the computations rapidly become infeasible as n grows beyond 3. The minimizing (E,P) had not been previously exhibited, except for a single case of a rational elliptic surface with a section of height 1/30 obtained by Shioda in a later paper [11], which we will identify with $E_1(4/5)$.

The connections with integral multiples of P (see statement (b) of part (ii) of each Theorem) are also new. We do not expect them to persist past $n = 3$, and in fact find that for $n = 4$ the largest number of consecutive integral multiples occurs for (E, P) with $\hat{h}(P) = 19/630$ or $13/360$, whereas $\hat{h}_{\min}(0, 48) \leq 41/1540 < 19/630 < 13/360$. We shall say more about integrality later; for now we content ourselves with the following remarks. A point on an elliptic curve over a function field $k(C)$ is said to be integral if it is a nonzero point whose naïve height vanishes. Geometrically, if we regard E as an elliptic surface $\mathcal{E}$ over C, and a rational point $P \in E(K)$ as a section s_P of $\mathcal{E}$, this means that s_P is disjoint from the zero-section s_0 of $\mathcal{E}$. Since $g = 0$ in our case, we can give an explicit algebraic characterization of integrality. Write E in extended Weierstrass form as

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{4}$$

where each a_i is a homogeneous polynomial of degree $i \cdot n$ in two variables. Then a rational point (X, Y) is integral if X, Y are homogeneous polynomials of degrees $2n, 3n$ respectively. The equation (4) depends on the choice of coordinates X, Y on E; replacing X, Y by

$$\delta^2(X + \alpha_2), \qquad \delta^3(Y + \alpha_1X + \alpha_3) \tag{5}$$

(some α_i and nonzero δ) yields an isomorphic curve. If moreover $\delta \in \mathbf{C}^*$ and each α_i is a homogeneous polynomial of degree $i \cdot n$ then the new equation for E has the same discriminant degree and the same integral points.

1.2 Outline of this paper. For each $n = 1, 2, 3$ we prove Theorem n, except for the implications (a),(b)⇒(c) of part (ii), which require different methods that we defer to a later paper. Our proofs use the following ingredients:

- $\hat{h}(mP) = m^2\hat{h}(P)$ for all $m \in \mathbf{Z}$.
- If $mP \neq 0$ then
$$\hat{h}(mP) = h(mP) + \sum_v \lambda_v(mP), \tag{6}$$
  where $h(\cdot)$ is the naïve height and the sum extends over all places $v \in C(\mathbf{C})$ lying under singular fibers E_v of E. (All places of K are of degree 1 thanks to our use of the algebraically closed field $\mathbf{C}$ for k.) The local corrections $\lambda_v(mP)$ are described further below.
- The naïve height takes values in $\{0, 2, 4, 6, \ldots\}$, and satisfies $h(m'P) \leq h(mP)$ for any integers m, m' such that $m'|m$ and $mP \neq 0$.
- Each local correction $\lambda_v(mP)$ depends only on the Kodaira type of the fiber E_v and on the component of E_v meeting P. We shall call this component c_v. The values of $\lambda_v(\cdot)$ are known explicitly for all Kodaira types and each possible component, see for instance [13, Thm. 5.2].

– Finally, the condition that E have discriminant degree $d = 12n$ imposes two conditions on the Kodaira types of the singular fibers. The first condition is

$$d = \sum_v d_v, \tag{7}$$

where d_v is the local discriminant degree of E_v. This allows only finitely many collections of fiber types. The second condition follows from an inequality due to Shioda [9, Cor. 2.7 (p.30)], and eliminates some of these collections that have too few fibers. According to this condition, if a nonconstant elliptic curve of discriminant degree d over a function field $K = \mathbf{C}(C)$ has a nontorsion point then the conductor degree of the curve strictly exceeds $(d/6) + \chi(C)$. Here $\chi(C) = 2 - 2g$ is the Euler characteristic of C. The conductor degree may be defined as the number of multiplicative fibers plus twice the number of additive fibers; thus it is also a sum of invariants of the singular fibers. When $(g, d) = (0, 12n)$ we have $\chi(C) = 2$ and $d/6 = 2n$, so the conductor degree is at least $2n + 3$.

We shall refer to these constraints as the "combinatorial conditions" on $\hat{h}(P)$, $h(mP)$, and the collection of (E_v, c_v) that arise for (E, P). (For other uses of such conditions to obtain lower bounds on heights, see for instance [3,14] and work referenced in these sources.) In general the combinatorial conditions yield only a lower bound on $\hat{h}_{\min}(0, 12n)$, because they allow some possibilities that do not actually occur for any (E, P). But for each of $n = 1$, 2, and 3 this lower bound turns out to be attained by some (E, P) over $\mathbf{C}(T)$, namely those exhibited in statement (c) of part (ii) of Theorem n. (Note that we do not yet need to derive the formulas for these (E, P), nor to prove that they are the only ones possible.) Moreover, using (6) we can check that $\hat{h}(P) = \hat{h}_{\min}(0, 12n)$ if and only if the naïve height $h(mP)$ vanishes for all m up to 6, 8, or 9 respectively.

Still, already at $n = 1$ we see some redundancy. The combinatorial conditions allow $\hat{h}(P) = 1/30$ to be attained in any of five ways, four of which are realized by the curves $E_1(q)$ of Theorem 1 for suitable choices of q. Shioda's $E_1(4/5)$ has singular fibers of types I_5, I_3, I_2, and II. (We specify the components c_v later in the paper.) The fibers of $E_1(-1)$ have types I_5, IV, I_2, and I_1, while those of $E_1(4)$ have types I_5, I_3, III, and I_1. In all other cases, the fibers of $E_1(q)$ have types I_5, I_3, I_2, I_1, I_1: the first three at $s = 0$, $s' = 0$, $s' = s$, and the last two at the roots of the quadratic $(q+1)^3 s^2 = (11q^2 - 14q + 2)ss' + (q-1)s'^2$. When $q = 4/5$, these roots coincide and the two I_1 fibers merge to form a II; likewise at $q = -1$ or $q = 4$, one of the I_1 fibers merges with the I_3 or I_2 fiber to form a IV or III respectively. (The one merger that does not occur is $\mathrm{I}_1 + \mathrm{I}_1 \to \mathrm{I}_2$.) But none of these degenerations changes $\hat{h}(P)$, nor any $h(mP)$, nor the conductor degree N. In fact a fiber of type II, III, or IV contributes as much to our formulas for $\hat{h}(P), h(mP), N$ as a pair of fibers of types I_1 and I_ν ($\nu = 1$, 2, or 3). Thus it is enough to minimize $\hat{h}(P)$ under the further assumption that no fibers of type II, III, or IV occur. We find similar replacements for all components of fibers of the remaining additive types I_ν^*, II^*, III^*, IV^*. See Proposition 2. This simplifies the computation of the combinatorial lower bound on $\hat{h}_{\min}(0,12n)$: instead of an exhaustive search over all combinations of (E_v, c_v), we need only try those for which each E_v is multiplicative (of type I_ν for $\nu = d_v$).

We programmed the search over all partitions $\{d_v\}$ of $12n$ in GP [8] and ran it on a Sun Ultra 60. This took only a fraction of a second for $n=1$, five seconds for $n=2$, and five minutes for $n=3$. It took about an hour to carry out the same computation for $n=4$, and about 20 hours for $n=5$; but the resulting bounds are probably not attained: as we shall see in a later paper, the required (E_v, c_v) data impose more conditions than the number of parameters needed to specify (E,P). We do produce explicit (E,P) that show $\hat{h}_{\min}(0,48) \le 41/1540$ and $\hat{h}_{\min}(0,60) \le 261/10010$, and conjecture that these are the correct values of $\hat{h}_{\min}(0,12n)$ for $n=4,5$. We have not attempted to extend the computation past $n=5$.

1.3 Coming attractions. Happily, the computation of the surfaces (1,2,3) not only completes the proofs of Theorems 1 through 3 but also points the way to further results and connections. We outline these here, and defer detailed treatment to a later paper in this series. In each step of the computation we in effect obtain a new birational model for the moduli space, call it $\mathcal{X}$, of pairs (E,P) consisting of an elliptic curve and a point on it. Our new parametrizations of this rational surface $\mathcal{X}$ have several other applications. One is a geometric interpretation of Tate's method for exhibiting the generic elliptic curve with an N-torsion point: we readily locate the modular curves $\mathrm{X}_1(N)$ $(N \le 16)$ on $\mathcal{X}$, together with nonconstant rational functions of minimal degree that realize each $\mathrm{X}_1(N)$ as an algebraic curve of genus ≤ 2. Arithmetically, we can use our parametrizations of $\mathcal{X}$ to find (E,P) over $\mathbf{Q}$ (or over some other global field) such that P is a nontorsion point with small $\hat{h}(P)$, and/or with many integral multiples in the minimal model of E. For instance, we prove that there are infinitely many $(E,P)/\mathbf{Q}$ such that mP is integral for each $m = 1,2,\ldots,11,12$. Our numerical results for a isolated curves (E,P) over $\mathbf{Q}$ may be found on the Web at http://www.math.harvard.edu/~elkies/low_height.html . They include new records for consecutive integral multiples and for the Lang ratio $\hat{h}(P)/\log|\Delta_E|$. We have mP integral for each $m = 1,2,\ldots,13,14$ for

$$E : Y^2 + XY = X^3 - 139761580X + 1587303040400, \tag{8}$$

an elliptic curve of conductor $1029210 = 2\cdot 3\cdot 5\cdot 7\cdot 13^2\cdot 29$, and P the nontorsion point $(X,Y) = (11480, 1217300)$; and we find the curve

$$Y^2 + XY = X^3 - 161020013035359930X + 24869250624742069048641252 \tag{9}$$

of conductor $3476880330 = 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 23\cdot 31\cdot 2111$ with the nontorsion point $(-296994156, 6818852697078)$ of canonical height[2] $\hat{h}(P) = .0190117\ldots <$

[2] There are two standard normalizations, differing by a factor of 2, for the canonical height of a point on an elliptic curve over $\mathbf{Q}$. We use the larger one, which is the one consistent with our formulas for function fields.

$1.691732 \cdot 10^{-4} \log |\Delta_E|$. The curves (8,9) are the specializations of our formula (3) with $(A, t/t') = (35/32, -8/15)$, $(33/23, 115/77)$.

Our simplified formula for $\hat{h}(mP)$ (Proposition 2) also bears on the asymptotic behavior of $\hat{h}_{\min}(g, 12n)$ for fixed g as $n \to \infty$. Hindry and Silverman [3] used the combinatorial conditions (except for the condition: $h(m'P) \le h(mP)$ if $m'|m$) to show that there exists $C > 0$ such that

$$\hat{h}(g, 12n) \ge Cn - O_g(1), \tag{10}$$

This proved the function-field case of a conjecture of Lang [4, p.92]. The error terms $O_g(1)$ are effectively computed, and can be omitted entirely if $g \le 1$. Hindry and Silverman also produce an explicit constant C, but it is quite small: about $7 \cdot 10^{-10}$. Their approach requires a point meeting every additive fiber in its identity component, which they achieved by working with $12P$ instead of P, at the cost of a factor of $1/12^2$ in C. Our results here let one apply the same methods directly to P, thus saving a factor of 12^2 and raising C to about 10^{-7}. In a later paper we show how to gain another factor of approximately 5000, raising the lower bound on $\liminf_n \hat{h}(g, 12n)/n$ to $1/2111$. This is within an order of magnitude of the correct value: for all $n \equiv 0 \bmod 5$ we obtain $\hat{h}_{\min}(0, 12n) \le 261n/50050$ via base change from our $n = 5$ example.

2. The naïve and canonical heights.

We collect here the facts we shall use about elliptic curves E over function fields K in characteristic zero, the associated elliptic surface $\mathcal{E}$, and the naïve and canonical height functions on $E(K)$.

2.1 The naïve height. The *naïve height* $h(P)$ of a nonzero $P \in E(K)$ can be defined using intersection theory on the elliptic surface $\mathcal{E}$ associated to some model of E. Let s_0 be the zero-section of the elliptic fibration $\mathcal{E} \to C$, and s_P the section corresponding to P. Then $h(P) := 2 s_P \cdot s_0$. Since we assumed that $P \ne 0$, the sections s_0, s_P are distinct curves on $\mathcal{E}$. Hence their intersection number $s_P \cdot s_0$ is a nonnegative integer, and $h(P)$ is a nonnegative even integer. Moreover $h(P) = 0$ if and only if s_P is disjoint from s_0, in which case we say that P is an *integral point* on E.

When $C = \mathbf{P}^1$, we can give an equivalent algebraic definition of $h(P)$ in terms of a Weierstrass equation of E. This definition emphasizes the analogy with the canonical height in the more familiar case of an elliptic curve over $\mathbf{Q}$. Recall that each coefficient a_i in the Weierstrass equation (4) is a homogeneous polynomial of degree $i \cdot n$ in the projective coordinates on $\mathbf{P}^1$. Then the coordinates x, y of a nonzero $P \in E(K)$ are homogeneous rational functions of degrees $2n, 3n$. If x, y are written as fractions "in lowest terms", as quotients of coprime homogeneous polynomials, then the denominators are (up to scalar multiple) the square and cube of some polynomial ζ. The roots of ζ, with multiplicity, are the images on $\mathbf{P}^1$ of the intersection points of s_0 and s_P. Hence $s_P \cdot s_0 = \deg \zeta$. Therefore $h(P)$ is the degree of the denominator ζ^2 of x, which is also the number of poles of x counted with multiplicity. An integral point is one for which ζ is a nonzero scalar and thus x, y are homogeneous polynomials of degrees $2n, 3n$.

For an arbitrary base curve C, the coefficients a_i are global sections of $\mathcal{L}^{\otimes i}$ for some line bundle $\mathcal{L}$ on C, and x, y are meromorphic sections of $\mathcal{L}^{\otimes 2}, \mathcal{L}^{\otimes 3}$. The pole divisors of x, y are $2Z, 3Z$ for some effective divisor Z on C, whose degree is $s_P \cdot s_0$; thus again $h(P)$ is the degree of the pole divisor $2Z$ of x, and P is integral iff $Z = 0$ iff x, y are global sections of $\mathcal{L}^{\otimes 2}, \mathcal{L}^{\otimes 3}$. A linear change of coordinates according to (5) yields the same notion of integrality if and only if $\delta \in \mathbf{C}^*$ and $\alpha_i \in \Gamma(\mathcal{L}^{\otimes i})$ for each i.

We shall need one more property of the naïve height beyond its relation with the canonical height and the fact that $h(mP) \in \{0, 2, 4, 6, \ldots\}$ $(mP \neq 0)$:

Lemma 1. *Let P be a point on an elliptic curve over $k(C)$, and let m, m' be any integers such that $m'|m$ and $mP \neq 0$. Then $h(m'P) \leq h(mP)$.*

Proof: Each point of $s_{m'P} \cap s_0$ is also a point of intersection of s_{mP} with s_0, to at least the same multiplicity. Hence $s_{m'P} \cdot s_0 \leq s_{mP} \cdot s_0$, so

$$h(m'P) = 2s_{m'P} \cdot s_0 \leq 2s_{mP} \cdot s_0 = h(mP)$$

as claimed. □

Remarks:

1. We could also state the result as: The naïve height of a point is less than or equal to the naïve height of any of its multiples that is not the zero point. This is a more natural formulation (the first point does not have to be written as $m'P$), but less convenient for our purposes.
2. In the proof, "at least the same multiplicity" can be strengthened to "exactly the same multiplicity" in our characteristic-zero setting. In general $h(mP)$ may strictly exceed $h(m'P)$ because $s_{mP} \cap s_0$ may also contain points where $m'P$ reduces to a nontrivial (m/m')-torsion point.

The naïve height satisfies further inequalities along the lines of Lemma 1, for instance

$$h(6P) + h(P) \geq h(2P) + h(3P). \tag{11}$$

Lemma 1 suffices for the proofs of Theorems 1–3 in the genus-zero case, but inequalities such as (11) are sometimes needed to exclude possible configurations with positive g, as we shall see for $d = 24$. The strongest such inequality we found is:

Lemma 2. *Let P be a point on an elliptic curve over $k(C)$, and let m be any integer such that $mP \neq 0$. Then*

$$\sum_{m'|m} \mu(m/m')\, h(m'P) \geq 0. \tag{12}$$

Proof: The left-hand side can be interpreted as twice the number of points of C, counted with multiplicity, at which $mP = 0$ but $m'P \neq 0$ for each proper factor m' of m. □

Inequality (11) is the special case $m = 6$ of this Lemma. The sum in (12) may be considered as an analogue of the formula $\prod_{m'|m}(x^{m'} - 1)^{\mu(m/m')}$ for the m-th cyclotomic polynomial. We recover Lemma 1 by summing the inequality (12) over all factors of m, including m itself but not 1, to obtain $h(mP) \geq h(P)$, which is equivalent to Lemma 1 by the first Remark above.

2.2 Local invariants, and Shioda's inequality. To go from the naïve to the canonical height we must use the minimal model of E for the elliptic surface $\mathcal{E}$. We next describe this model, collect some known facts on the singular fibers of $\mathcal{E}$, and give Shioda's lower bound on the conductor degree.

Whereas a naïve height could be defined for any model of E,[3] the canonical height requires the Néron minimal model. It is known that there exists a minimal line bundle $\mathcal{L}$ on C with the following property: let D be a divisor on C such that $O(D) \cong \mathcal{L}$; then E is isomorphic to a curve with an extended Weierstrass equation (4) whose coefficients a_i are global sections of iD. In characteristic zero we can easily obtain D and $\mathcal{L}$ by putting E in narrow Weierstrass form $Y^2 = X^3 + a_4X + a_6$. Then D is the smallest divisor such that $(a_4) + 4D \geq 0$ and $(a_6) + 6D \geq 0$. In other words, we can regard a_4, a_6 as global sections of $\mathcal{L}^{\otimes 4}, \mathcal{L}^{\otimes 6}$ such that there is no point of C where a_4 and a_6 vanish to order at least 4 and 6 respectively. Once we have $a_i \in \Gamma(\mathcal{L}^{\otimes i})$, we can regard the Weierstrass equation (4) as a surface in the plane bundle $\mathcal{L}^{\otimes 2} \oplus \mathcal{L}^{\otimes 3}$ over C. If all the roots of the discriminant $\Delta \in \Gamma(\mathcal{L}^{\otimes 12})$ are distinct then this surface is smooth and is the minimal model of E. Otherwise it has isolated singularities, which we blow up as many times as needed (we may follow Tate's algorithm [16]) to obtain the minimal model $\mathcal{E}$. This is a smooth algebraic surface of arithmetic genus $n = \deg \mathcal{L}$, equipped with a map to C with generic fiber E and $\omega_{\mathcal{E}/C} \cong \mathcal{L}$. See for instance [1, pp.149ff.].

We shall need much information about the singular fibers that can arise for the elliptic fibration $\mathcal{E} \to C$. We extract from Tate's table [16, p.46] the following local data for each possible Kodaira type of a singular fiber E_v: the discriminant degree d_v, the conductor degree N_v, and the structure of the group $E_v/(E_v)_0$ of multiplicity-1 components. We also list in each case the root lattice L_v that E_v contributes to the Néron-Severi lattice $\mathrm{NS}(\mathcal{E})$ of $\mathcal{E}$. In each case, L_v has rank $d_v - N_v$, and $E_v/(E_v)_0 \cong L_v^*/L_v$ where $L_v^* \subset L_v \otimes \mathbf{Q}$ is the dual lattice. The lattice "A_0" that appears for Kodaira types I_1 and II is the trivial lattice of rank zero. For Kodaira type I_ν^*, the group $E_v/(E_v)_0$ always has order 4, and has exponent 2 or 4 according as ν is even or odd. For positive ν of either parity, a fiber of type I_ν^* has a distinguished multiplicity-1 component of order 2 in $E_v/(E_v)_0$, namely

[3] Two models may yield different heights h, h', but $h' = h + O(1)$ holds for any pair of naïve heights on the same curve. It also follows that the property $\hat{h} = h + O(1)$ of the canonical height does not depend on the choice of naïve height h.

the one closest to the identity component. In the L_v picture, the distinguished component corresponds to the nontrivial coset of $D_{4+\nu}$ in $\mathbf{Z}^{4+\nu}$. When $\nu = 0$ there is no distinguished component: all three non-identity components of multiplicity 1 are equivalent, as are all three nontrivial cosets due to the triality of D_4.

Kodaira type	$\mathrm{I}_\nu (\nu > 0)$	II	III	IV	I_ν^*	IV*	III*	II*
d_v	ν	2	3	4	$6+\nu$	8	9	10
N_v	1	2	2	2	2	2	2	2
$E_v/(E_v)_0$	$\mathbf{Z}/\nu\mathbf{Z}$	$\{0\}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$	$D_{4+\nu}^*/D_{4+\nu}$	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$	$\{0\}$
root lattice	$A_{\nu-1}$	A_0	A_1	A_2	$D_{4+\nu}$	E_6	E_7	E_8

The discriminant and conductor degrees d, N of $\mathcal{E}$ are sums of the discriminant and conductor degrees of the singular fibers:

$$12n = d = \sum_v d_v, \qquad N = \sum_v N_v. \tag{13}$$

Hence $d - N = \sum_v (d_v - N_v) = \sum_v \operatorname{rk} L_v$ is the rank of the subgroup $\oplus_v L_v$ of $\mathrm{NS}(\mathcal{E})$ due to the singular fibers. Shioda used this to prove [9, Cor. 2.7 (p.30)]:

Proposition 1. *Let E be a nonconstant elliptic curve over a function field $K = k(C)$ of genus g, with discriminant and conductor degrees $d = 12n$ and N. Then*

$$N \geq 2n + (2 - 2g) + r, \tag{14}$$

where r is the rank of the Mordell-Weil group $E(K)$.

Proof: Let $T \subseteq \mathrm{NS}(\mathcal{E})$ be the subgroup spanned by s_0, the generic fiber, and $\oplus_v L_v$. Then we have a short exact sequence (see for instance [10, Thm. 1.3]):

$$0 \to T \to \mathrm{NS}(\mathcal{E}) \to E(K) \to 0, \tag{15}$$

where the map $\mathrm{NS}(\mathcal{E}) \to E(K)$ is the sum on the generic fiber. Taking ranks, we find

$$\operatorname{rk} \mathrm{NS}(\mathcal{E}) = \operatorname{rk} T + \operatorname{rk} E(K) = 2 + (d - N) + r. \tag{16}$$

But $\mathrm{NS}(\mathcal{E})$ embeds into $H^{1,1}(\mathcal{E}, \mathbf{Z})$, a group of rank $h^{1,1}(\mathcal{E}) = 10n + 2g$. Hence $\operatorname{rk} \mathrm{NS}(\mathcal{E}) \leq 10n + 2g$. Therefore

$$N \geq (d + 2 + r) - (10n + 2g) = 2n + (2 - 2g) + r,$$

as claimed. ∎

Remarks:

1. Since $r \geq 0$ it follows that

$$N \geq 2n + (2 - 2g) = (d/6) + \chi \tag{17}$$

for any nonconstant elliptic surface. This weaker inequality is sufficient for most of our purposes, even though we are interested in curves with a non-torsion point, for which the strict inequality $N > (d/6) + \chi$ holds because $r > 0$.

2. The inequality (17) is now usually known as the "Szpiro inequality", but Shioda's paper [9] predates Szpiro's [15] by almost two decades (see also [12, p.114]). It is by now well-known that (17) can be proved by elementary means via Mason's theorem [5] (the ABC inequality for function fields). Can one also give an elementary proof of Shioda's inequality, or even of its consequence that $r = 0$ if $N = (d/6) + \chi$?
3. The requirement that E not be a constant curve is essential. There is an analogous statement for constant curves but many details must change. Suppose E is such a curve, that is, $\mathcal{E} = C \times E_0$ for some elliptic curve E_0/k. Then $E(K)$ is not finitely generated, because it contains a copy of $E_0(k)$. Still, $E(K)/E_0(k)$ is finitely generated, and identified with the group $\mathrm{NS}(\mathcal{E})/T$. Again we call the rank of this group r. Since $n = d = N = 0$ in this setting, we obtain the inequality $r + 2 \le h^{1,1}(C \times E_0) - 2$. But for a constant curve, $h^{1,1}(C \times E_0) = 2g + 2$, instead of the $2g$ that one would expect from the $10n + 2g$ formula. Hence $r \le 2g$. This can also be proved using the identification of $E(K)/E_0(k)$ with $\mathrm{End}(\mathrm{Jac}(C), E_0)$, an approach that also yields the equality condition: clearly $r = 2g$ if $g = 0$; if $g > 0$ then $r = 2g$ if and only if E_0 has complex multiplication and $\mathrm{Jac}(C)$ is isogenous with E_0^g. See for instance [2].
4. The hypothesis of characteristic zero, too, is essential here. In positive characteristic, one cannot decompose the second Betti number $b_2(\mathcal{E})$ as $h^{2,0} + h^{1,1} + h^{0,2}$, so one has only the weaker upper bound $b_2(\mathcal{E})$ on $\mathrm{rk}(\mathrm{NS}(\mathcal{E}))$. This upper bound exceeds the characteristic-zero bound by $2g$ for a constant curve and $2(n + g - 1)$ for a nonconstant one. For instance, a constant curve $C \times E_0$ has $r \le 4g$, with equality if and only if either $g = 0$ or E_0 and $\mathrm{Jac}(C)$ are both supersingular. In general $\mathcal{E}$ is said to be "supersingular" if $NS(\mathcal{E}) \cong \mathbf{Z}^{b_2(\mathcal{E})}$; such surfaces were studied and used in [10,2].

2.3 Local height corrections. We next list the local height corrections $\lambda_v(mP)$ for each of the Kodaira types. For convenience we abuse notation by using mP to refer also to the section s_{mP}.

– If mP is on the identity component of E_v then

$$\lambda_v(mP) = d_v/6. \tag{18}$$

In particular this covers fibers of type II or II*.

– If E_v is of type I_ν and P passes through component $a \in \mathbf{Z}/\nu\mathbf{Z}$, let $x = \bar{a}/\nu$ for any lift $\bar{a}$ of a to $\mathbf{Z}$; then

$$\lambda_v(mP) = \nu B(mx), \tag{19}$$

where $B(\cdot)$ is the second Bernoulli function $B(z) := \sum_{n=1}^{\infty} \cos(2\pi n)/(\pi n)^2$. Since B is $\mathbf{Z}$-periodic, the choice of $\bar{a}$ does not matter. Likewise, since

$B(z) = B(-z)$ it does not matter that a cannot be canonically distinguished from $-a$. We have

$$B(z) = z^2 - z + \frac{1}{6} \tag{20}$$

for all $z \in [0, 1]$, so in particular $B(0) = 1/6$. Hence $\lambda_v(mP) = \nu/6$ if mP passes through the identity component of E_v, as also asserted by (18) in that case.

- If E_v is of type III, IV, I_0^*, III^*, or IV^*, and mP passes through a non-identity component of E_v, then $\lambda_v(mP) = 0$.
- Finally, suppose E_v is of type I_ν^* $(\nu > 0)$ and that mP passes through a non-identity component. If that component is the distinguished one of order 2 then $\lambda_v(mP) = \nu/6$. Otherwise $\lambda_v(mP) = -\nu/12$. (We could have also allowed $\nu = 0$, when there is no distinction among the three non-identity components, but $\lambda_v(mP) = \nu/6 = -\nu/12 = 0$ for all of them.)

We record two applications of these formulas for future use:

Lemma 3. *Let E be an elliptic curve of discriminant degree $12n$ over a function field K, and P any nonzero point of $E(K)$. Then*

$$-n \leq \hat{h}(P) - h(P) \leq 2n. \tag{21}$$

Proof: For each v we have $-d_v/12 \leq \lambda_v \leq d_v/6$. Summing over v yields (21). □

Lemma 4. *Let E be an elliptic curve of discriminant degree $12n$ over a function field K, and P any point of $E(K)$. If for some integer m the multiple mP is a nonzero integral point then $\hat{h}(mP) \leq 2n/m^2$.*

Proof: By our formulas for λ_v we have $\lambda_v(mP) \leq d_v/6$ for all v. Hence

$$m^2 \hat{h}(P) = \hat{h}(mP) = h(mP) + \sum_v \lambda_v(mP) \leq h(mP) + \sum_v d_v/6. \tag{22}$$

But $h(mP) = 0$ since mP is integral, and $\sum_v d_v/6 = d/6 = 2n$. Hence $m^2 \hat{h}(P) \leq 2n$, and the Lemma follows. □

2.4 Reduction to the semistable case. Recall that an elliptic curve is said to be *semistable* if all its singular fibers are of type I_ν for some ν. Suppose E/K is semistable and P is a nontorsion point in $E(K)$. We associate to (E, P) an element γ of the abelian group $\mathbf{G}$ of formal $\mathbf{Z}$-linear combinations of orbits of $\mathbf{Q}$ under the infinite dihedral group D_∞ generated by $z \mapsto z + 1$ and $z \leftrightarrow 1 - z$. We denote by $[z]$ the generator of $\mathbf{G}$ corresponding to the orbit of z. Then γ is defined as a sum of local contributions $\gamma_v \in \mathbf{G}$ that record the types $\nu(v)$ of the singular fibers E_v and the component $c_v = a(v) \in \mathbf{Z}/(\nu(v))\mathbf{Z}$ of each fiber that contains P, as follows:

$$\gamma_v := \sum_v \gcd(a(v), \nu(v)) \cdot \left[\frac{a(v)}{\nu(v)}\right]. \tag{23}$$

Then each of the height corrections $\hat{h}(mP) - h(mP)$, as well as the discriminant degree, are images of γ under homomorphisms $\boldsymbol{\lambda}_m, \mathbf{d}$ from $\mathbf{G}$ to $\mathbf{Q}$ or $\mathbf{Z}$, and the conductor is bounded above by the image of a homomorphism $\mathbf{N} : \mathbf{G} \to \mathbf{Z}$. We define these homomorphisms on the generators of $\mathbf{G}$ and extend by linearity. Suppose $\mathbf{Q} \ni z = a/b$ with $b > 0$ and $\gcd(a, b) = 1$. Note that b is an invariant of the action of D_∞. Then we set

$$\boldsymbol{\lambda}_m([z]) := b\, B_2(mz), \qquad \mathbf{d}([z]) := b, \qquad \mathbf{N}([z]) := 1. \tag{24}$$

Then our formulas (19,13) yield the identities

$$\hat{h}(mP) = h(mP) + \boldsymbol{\lambda}_m(\gamma) \quad (m = 1, 2, 3, \ldots), \qquad 12n = d = \mathbf{d}(\gamma) \tag{25}$$

and the estimate

$$N \le \mathbf{N}(\gamma). \tag{26}$$

(This last is an upper bound rather than an identity because each v contributes 1 to N and $\gcd(a(v), \nu(v)) \ge 1$ to $\mathbf{N}(\gamma)$.) It follows that

$$\mathbf{N}(\gamma) \ge N \ge (d/6) + (2 - 2g) + r \ge \frac{1}{6}\mathbf{d}(\gamma) + 3 - 2g. \tag{27}$$

The second step is Shioda's inequality (Prop. 1), and the third step uses the positivity of r, which follows from our hypothesis that P is nontorsion.

To generalize these formulas to curves that may not be semistable, it might seem that we would have to extend $\mathbf{G}$ with generators that correspond to Kodaira types other than I_ν. But we can associate to any additive fiber E_v an element of $\mathbf{G}$ whose images under $\boldsymbol{\lambda}_m$ and $\mathbf{d}$ coincide with $\lambda_v(mP)$ and d_v, and whose image under $\mathbf{N}$ is $\ge N_v$. (Note that we already did this for multiplicative fibers with $f = \gcd(a(v), \nu(v)) > 1$, replacing them in effect by f fibers with a, ν coprime and the same value of a/ν.) As in the multiplicative case, this element is positive, in the sense that it is a nonzero formal linear combination of elements of $\mathbf{Q}/D_\infty$ with nonnegative coefficients. Specifically, we have:

Proposition 2. *Let E be an elliptic curve over a function field K of genus g, and $P \in E(K)$ a nontorsion point. Define for each singular fiber E_v a positive $\gamma_v \in \mathbf{G}$, depending on (E_v, c_v) as follows:*

- *If E_v is multiplicative, γ_v is defined by (23).*
- *If c_v is the identity component then $\gamma_v := d_v\,[0]$.*
- *If c_v is a non-identity component of a fiber E_v of type III, IV, IV*, or III* then γ_v is respectively*

$$[1/2] + [0], \quad [1/3] + [0], \quad 2 \cdot [1/2] + 2 \cdot [0], \quad 3 \cdot [1/3] + 3 \cdot [0].$$

- *If c_v is a distinguished component of a fiber E_v of type I_ν^* then*

$$\gamma_v := 2\,[1/2] + (\nu + 2)\,[0].$$

– *If c_v is a non-distinguished, non-identity component of a fiber E_v of type I_ν^* then*

$$\gamma_v := (\mu+2)\,[1/2] + 2\,[0]$$

if $\nu = 2\mu$, and

$$\gamma_v := [1/4] + (\mu+1)\,[1/2] + [0]$$

if $\nu = 2\mu+1$ for some integer μ.

Then:

i) $\lambda_v(mP) = \boldsymbol{\lambda}_m(\gamma_v)$ for each $m = 1, 2, 3, \ldots$;
ii) $d_v = \mathbf{d}(\gamma_v)$; and
iii) $N_v \le \mathbf{N}(\gamma_v)$.

Thus (25,26,27) hold for $\gamma := \sum_v \gamma_v$. Equality in (iii) holds if and only if E_v is either a multiplicative fiber with $\gcd(a, \nu) = 1$, a fiber of type III or IV with c_v a non-identity component, or a fiber of type II.

[Note that, as was true for the λ_v formulas, the first two formulas in Prop. 2 overlap in the case of a multiplicative fiber with $a(v) = 0$, but give the same answer in this case. Here both prescriptions yield $\gamma_v = \nu(v) \cdot [0]$ for such v.]

Proof: The multiplicative case was seen already. For each of the other Kodaira types, it is straightforward to verify that $\lambda_v(mP) = \boldsymbol{\lambda}_m(\gamma_v)$ for each nonnegative m less than the exponent of the finite group $E_v/(E_v)_0$ (which is at most 4), and to check that $d_v = \mathbf{d}(\gamma_v)$, and that $N_v \le \mathbf{N}(\gamma_v)$, with strict inequality except in the three cases listed. We recover (25,26,27) by summing over v. ∎

3. The values of $\hat{h}_{\min}(0, 12n)$ for $n = 1, 2, 3$, and consecutive integral multiples.

For each n we can use the formulas and results above to obtain a lower bound on $\hat{h}_{\min}(g, 12n)$. When $g = 0$ and $n = 1, 2, 3$ we also show that this bound is attained if and only if mP is integral for $m \le M = 6, 8, 9$, and verify that the (E, P) exhibited in Theorem n satisfy those conditions.

Suppose E is an elliptic curve over $\mathbf{C}(T)$ with discriminant degree $12n$. Let P be a nontorsion rational point on E, and γ the associated element of $\mathbf{G}$. From γ and $\hat{h}(P)$ we can recover all the naïve heights $h(mP)$ from the first formula in (25): $h(mP) = m^2\hat{h}(P) - \boldsymbol{\lambda}_m(\gamma)$. Given n and an upper bound H on $\hat{h}(P)$, there are only finitely many candidates for the pair $(\gamma, \hat{h}(P))$: there are finitely many $\gamma > 0$ with $\mathbf{d}(\gamma) = 12n$, and for each one there are only finitely many possible choices for $h(P)$ consistent with $h(P) + \boldsymbol{\lambda}_1(\gamma) = \hat{h}(P) \in (0, H]$. For each candidate $(\gamma, \hat{h}(P))$ we can check the condition $m'|m \Rightarrow h(mP) \ge h(m'P) \ge 0$. Only finitely many m need be checked for each $(\gamma, \hat{h}(P))$: by Lemma 3 we know that $h(mP) \ge 0$ once $m^2\hat{h}(P) \ge n$, and $h(mP) \ge h(m'P)$ for each $m'|m$ once $m^2\hat{h}(P) \ge 4n$. The minimal $\hat{h}(P)$ among the $(\gamma, \hat{h}(P))$ that pass these tests is then our lower bound on $\hat{h}_{\min}(g, 12n)$. [We could also test the more complicated inequality of Lemma 2, which may further improve the bound; instead we checked that inequality after the fact when necessary.]

We wrote a GP program to compute this bound by exhaustive search, and ran it with $H = 2n/M^2$ for $n = 1, 2, 3$. We chose this upper bound H to ensure that, by Lemma 4, we would also find all feasible $(\gamma, \hat{h}(P))$ such that $h(mP) = 0$ for each $m = 1, 2, 3, \ldots, M$. For $n = 1$, we found that the minimum occurs for

$$\gamma = [1/5] + [1/3] + [1/2] + 2\,[0], \qquad \hat{h}(P) = 1/30, \tag{28}$$

and is the unique $(\gamma, \hat{h}(P))$ such that $h(mP) = 0$ for each $m \leq 6$. For $n = 2$, we found that the minimum occurs for

$$\gamma = [1/11] + 2\,[2/5] + [1/3], \qquad \hat{h}(P) = 4/165; \tag{29}$$

but this is not feasible because $h(mP) = 0, 2, 2, 2$ for $m = 2, 4, 6, 12$, so inequality (11) is violated when $m = 2$. Our lower bound on $\hat{h}_{\min}(g, 24)$ is thus the next-smallest value, which occurs for

$$\gamma = [1/7] + [2/5] + [1/4] + [1/3] + [1/2] + 3\,[0], \qquad \hat{h}(P) = 11/420, \tag{30}$$

and is the unique $(\gamma, \hat{h}(P))$ such that $h(mP) = 0$ for each $m \leq 8$.

On the other hand, the $(\gamma, \hat{h}(P))$ pairs of (28,30) are also those associated with the curves and points E, P exhibited in (1,2). Hence those E, P attain our lower bounds 1/30, 11/420 on $\hat{h}_{\min}(12)$, $\hat{h}_{\min}(24)$, as well as the upper bounds 6 and 8 on the number of consecutive integral multiples for $n = 1$ and $n = 2$. This proves all of Theorems 1 and 2 except for the claims that every (E, P) attaining those bounds is isomorphic with some $E_1(q)$ or $E_2(u)$.

For $n = 3$, we find that there is a unique $(\gamma, \hat{h}(P))$ such that $h(mP) = 0$ for each $m \leq 9$, namely

$$\gamma = [1/8] + [3/7] + [1/5] + [1/4] + 2\,[1/3] + [1/2] + 4\,[0], \quad \hat{h}(P) = 23/840. \tag{31}$$

Again these are the γ and $\hat{h}(P)$ for the (E, P) exhibited in the Introduction (formula (3)). But we do not claim that $\hat{h}_{\min}(36) = 23/840$: Lemma 2 eliminates the second-smallest pair

$$(\gamma, \hat{h}(P)) = ([1/13] + [3/8] + [3/7] + [1/5] + [1/3],\ 229/10920)$$

(which violates the inequality (11) in the same way that (29) did), but not several other possibilities with $\hat{h}(P) < 23/840$. We next list all these possibilities, in order of increasing $\hat{h}(P)$:

γ	$\hat{h}(P)$
$[1/13] + [3/11] + [3/8] + 2\,[1/2]$	$23/1144 \approx .02010$
$[1/13] + [3/8] + [2/7] + [1/4] + 2\,[1/2]$	$17/728 \approx .02335$
$[1/11] + [4/9] + [2/7] + [1/4] + [1/3] + 2\,[0]$	$65/2772 \approx .02345$
$[1/12] + [3/11] + [3/8] + 2\,[1/2] + [0]$	$7/264 \approx .02652$
$[1/11] + [3/7] + 2\,[1/5] + [1/4] + 2\,[1/2]$	$41/1540 \approx .02662$

(32)

(For comparison, $229/10920 \approx .02097$ and $23/840 \approx .02738$.) We have $\mathbf{d}(\gamma) \leq 7$ for each entry in the table (32); therefore by Prop. 1 none of them can occur for an elliptic curve over $\mathbf{P}^1$. (Even the weaker inequality (17) would suffice here; either of those inequalities also excludes (29) for $n = 2$, and would thus be enough to obtain $\hat{h}_{\min}(0, 24)$, but the determination of $\hat{h}_{\min}(24)$ required a further argument.) Thus $\hat{h}_{\min}(0, 36) = 23/840$, proving Theorem 3 except for the claim that every (E, P) satisfying conditions (a) and (b) is of the form $E_3(A)$ for some A.

Acknowledgements. I thank J. Silverman and T. Shioda for helpful correspondence concerning their papers and related issues, and M. Watkins for carefully reading a draft of this paper. This work was made possible in part by funding from the Packard Foundation and the National Science Foundation.

References

1. Barth, W., Peters, C., Van de Ven, A.: *Compact Complex Surfaces*. Berlin: Springer, 1984.
2. Elkies, N.D.: Mordell-Weil lattices in characteristic 2, I: Construction and first properties. *International Math. Research Notices* 1994 #8, 343–361.
3. Hindry, M., Silverman, J.H.: The canonical height and integral points on elliptic curves, *Invent. Math.* **93** (1988), 419–450.
4. Lang, S.: *Elliptic Curves: Diophantine Analysis.* Berlin: Springer, 1978.
5. Mason, R.C.: *Diophantine Equations over Function Fields*, London Math. Soc. Lect. Note Ser. **96**, Cambridge Univ. Press 1984. See also pp.149–157 in Springer LNM **1068** (1984) [=proceedings of Journées Arithmétiques 1983 (Noordwijkerhout), H. Jager, ed.].
6. Nishiyama, K.-i.: The minimal height of Jacobian fibrations on K3 surfaces, *Tohoku Math. J.* (2) **48** (1996), 501–517.
7. Oguiso, K., Shioda, T.: The Mordell-Weil lattice of a rational elliptic surface, *Comment. Math. Univ. St. Pauli* **40** (1991), 83–99.
8. PARI/GP, versions `2.1.1–4`, Bordeaux, 2000–4, http://pari.math.u-bordeaux.fr .
9. Shioda, T.: Elliptic Modular Surfaces, *J. Math. Soc. Japan* **24** (1972), 20–59.
10. Shioda, T.: On the Mordell-Weil lattices. *Comment. Math. Univ. St. Pauli* **39** (1990), 211–240.
11. Shioda, T.: Existence of a Rational Elliptic Surface with a Given Mordell-Weil Lattice, *Proc. Japan Acad. (Ser. A)* **68** (1992), 251–255.
12. Shioda, T.: Some remarks on elliptic curves over function fields, *Astérisque* **209** (1992) [=proceedings of Journées Arithmétiques 1991 (Genève), D.F. Coray and Y.-F. S. Pétermann, eds.], 99–114.
13. Silverman, J.H.: Computing Heights on Elliptic Curves, *Math. of Computation* **51** #183 (July 1988), 339–358.
14. Silverman, J.H.: A lower bound for the canonical height on elliptic curves over abelian extensions, *J. Number Theory* **104** (2005), 353–372.
15. Szpiro, L.: Discriminant et conducteur des courbes elliptiques. *Astérisque* **183** (1990) [=*Séminaire sur les Pinceaux de Courbes Elliptiques*, Paris 1988], 7–18.
16. Tate, J.: Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil. Pages 33–52 in *Modular Functions of One Variable IV* (Lect. Notes in Math. **476** (1975); Birch, B.J., Kuyk, W., eds.).