International Mathematics Research Notices 1991, No. 7

ABC IMPLIES MORDELL[1]

NOAM D. ELKIES

Introduction: the ABC and Mordell conjectures. The *ABC conjecture* over $\mathbb{Q}$ (see [Oe], [La], and [Vol, p. 71]) asserts that, for any relatively prime nonzero A, B, $C \in \mathbb{Z}$ such that $A + B + C = 0$,

$$N(A, B, C) \gg_\varepsilon H(A, B, C)^{1-\varepsilon}. \tag{1}$$

Here, the *conductor*[2] $N(A, B, C)$ and the [naïve exponential] *height* $H(A, B, C)$ are defined by

$$N(A, B, C) = \prod_{p|ABC} p, \qquad H(A, B, C) = \max(|A|, |B|, |C|) \tag{2}$$

(the product being taken *without* multiplicity), and (1) is to hold for all positive ε, with the constant implied in $\gg$ depending on ε but not on A, B, C.

We can remove the condition that $A, B, C \in \mathbb{Q}^*$ be coprime integers by redefining the height and conductor:

$$H(A, B, C) = \prod_v \max(\|A\|_v, \|B\|_v, \|C\|_v), \tag{3}$$

v ranging over all normalized valuations of $\mathbb{Q}$ and

$$N(A, B, C) = \prod_{p \in I} p, \qquad \text{where}$$

$$I = \{p \text{ prime: } \max(\|A\|_p, \|B\|_p, \|C\|_p) > \min(\|A\|_p, \|B\|_p, \|C\|_p)\}. \tag{4}$$

Note that (3, 4) are finite products whose values are unchanged if A, B, C are replaced by λA, λB, λC for any $\lambda \in \mathbb{Q}^*$, and that they agree with (2) when A, B, C are coprime integers; so the ABC conjecture over $\mathbb{Q}$ is equivalent to the inequality (1) for any nonzero rational numbers A, B, C such that $A + B + C = 0$ with these new definitions (3, 4) of H and N.

Received 30 October 1991.
Communicated by Barry Mazur.

[1] Don Zagier notes the amusing equivalent formulation: "Mordell is as easy as ABC!"

[2] So called because, up to a bounded power-of-2 factor, it is the conductor of the elliptic curve $y^2 = x(x - A)(x + B)$ associated to (A, B, C) by Frey [Fr].

We can now state the *ABC conjecture over an arbitrary number field K* (see [Vo1, p. 84]): for each $\varepsilon > 0$ the inequality (1) holds for all nonzero $A, B, C \in K$ such that $A + B + C = 0$ with the constant implied in $\ll$ now depending on K as well as ε, but not on A, B, C; here, $H(A, B, C)$ is defined again by (3), and $N(A, B, C)$ is the product of the absolute norms of all the finite primes of K at which $\max(\|A\|, \|B\|, \|C\|)$ strictly exceeds $\min(\|A\|, \|B\|, \|C\|)$.

Since $H(A, B, C)$ and $N(A, B, C)$ are scaling invariant, they both depend only on the ratio $(-A/B) = r$, say, with $r \in K - \{0, 1\}$.[3] Indeed, $H(A, B, C)$ is just $\prod_v \max(1, \|r\|_v)$ times a factor bounded between 1 and $2^{r_1+r_2}$ (where r_1 and r_2 are the numbers of real and complex embeddings of K), i.e., the naïve height of r times $\exp O(1)$; and $N(A, B, C)$ is the product of the absolute norms of all the finite primes of K at which r, $1/r$, or $r - 1$ has a positive valuation. Thus, the ABC conjecture over K asserts that this product is at least as large as the $(1 - \varepsilon)$ power of the naïve height of r, for all but finitely many $r \in K - \{0, 1\}$. We abuse notation slightly by writing $H(r)$ for the naïve height $\prod_v \max(1, \|r\|_v)$ and abbreviating $N(r, -1, 1, -r)$ by $N(r)$; we also factor $N(r)$ as the product of $N_0(r)$, $N_1(r)$, and $N_\infty(r)$, these being the products of the absolute norms of the prime ideals containing r, $r - 1$, $1/r$ respectively.

[In the analogous case of a function field $K = k(X)$, r is a rational function on some fixed curve X of genus g over the field k, and $h(r) = \log H(r)$ is just the degree of r. Also, $n(r) = \log N(r)$ becomes the number of distinct points (over the closure of the ground field, and counted without multiplicity) at which r attains one of the values 0, 1, ∞. In this case it has been shown that the corresponding conjecture $n(r) > (1 - \varepsilon)h(r) + C_\varepsilon$ is true provided that the differential dr is not identically zero on X, i.e., provided the covering $r: X \to \mathbb{P}^1$ is separable. Indeed, in that case the more precise bound $n(r) \geqslant h(r) + 2 - 2g$ can be obtained by bounding the total degree of the divisor of dr, which is known to be $2 - 2g$; see [Ma1].[4] The condition $dr \not\equiv 0$ is essential when k has positive characteristic p: for any r, $h(r^p) = ph(r)$ and $n(r^p) = n(r)$, so that $n(r^{p^\alpha}) = o(h(r^{p^\alpha}))$ as $\alpha \to \infty$ for any fixed r of positive degree; of course, $d(r^{p^\alpha}) = 0$ once $\alpha \geqslant 1$. These results constitute the strongest evidence to date for the ABC conjecture.]

Mordell's conjecture (see [Se]) asserts that any curve of genus at least 2 over a number field K has only finitely many K-rational points. Several different proofs have recently been given for this conjecture [Fa1, Fa2, Vo2, Bo], but they are all "ineffective", in that they do not give an upper bound on the size ("height") of these points, nor do they give any other procedure for provably finding all K-rational points on such a curve.

In this note we show that the truth of the ABC conjecture in any number field K implies Mordell's conjecture for any curve C over K. At present, this is of little use: Mordell's conjecture is now proved, and in several different ways, while we do not

[3] More symmetrically, $r \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ here and later.

[4] This idea was first borrowed from the value-distribution theory of analytic functions at least as early as 1956 in the last problem of that year's W. L. Putnam exam; see [GGK, pp. 47 and 431].

yet know how to prove ABC, even with $K = \mathbb{Q}$ and the exponent $1 - \varepsilon$ of (1) replaced by the weaker $\kappa - \varepsilon$ for some $\kappa > 0$. But the result is still interesting because the implication is considerably easier than any of the known proofs of Mordell's conjecture, and more importantly because our proof shows that an *effective* version of the ABC conjecture would imply Mordell's conjecture with an effective height bound, which is at present still out of reach.

We also show that our argument can easily be modified to obtain finiteness results on integral points assuming the ABC conjecture (though this is somewhat less interesting because effective methods are already available [Ba, BC]) and indicate how our construction behaves in the case of an elliptic curve or a rational curve punctured at two points. Curiously, all these ideas apply to curves over number fields but *not* to curves over function fields, because we make essential use of Belyi's theorem on unramified covers of the thrice-punctured projective line.

Motivation and proof. Our proof generalizes the known implication "effective ABC $\Rightarrow$ eventual Fermat" which was the original motivation for the ABC conjecture (see [Oe, p. 4], [La, pp. 42–43]); we begin by reviewing the proof of that implication and rephrasing it to suit our purposes. Thus, if $n > 3$ and x, y, z are nonzero integers such that $x^n + y^n + z^n = 0$, we may eliminate common factors to make x, y, z relatively prime and may take

$$(A, B, C) = (x^n, y^n, z^n) \tag{5}$$

in (1); then

$$N(A, B, C) \leqslant |xyz| < H(A, B, C)^{3/n}, \tag{6}$$

contradicting (1) with any $\varepsilon < 1 - (3/n)$ once $H(A, B, C)$ is large enough.

Now of course this $(x:y:z)$ is a rational point on the nth Fermat curve F_n, and $H(A, B, C)$ is just n times its naïve height relative to its standard degree-n embedding in the projective plane. In the formalism of [Vo1], the ABC conjecture is regarded as a bound on the "ramification" of the rational number $r = (-A/B)$ above 0, 1, and ∞; and the basic observation here is that r is the value at $(x:y:z)$ of the rational function $f = -(x/y)^n$ on F_n and that the bound (6) on $N(A, B, C)$ reflects the ramification of this function f above 0, 1, ∞. Indeed, f has degree n^2, but it attains each of these three values at only n distinct points of $F_n(\overline{\mathbb{Q}})$; so each of A, C, B contributes only $O(H(A, B, C)^{n/n^2})$ to $N(A, B, C)$, whence the inequality (6). As it happens, 0, 1, ∞ are the only ramified values of f (as may be checked by direct computation or from the Riemann-Hurwitz formula), but all we use here is that the cardinality of $f^{-1}(\{0, 1, \infty\})$ is less than the degree of f. So we can expect that the argument will generalize to any curve C over an arbitrary number field K, provided we can find a rational function $f \in K(C)$ such that

$$\#\{P \in C(\overline{\mathbb{Q}}): f(P) \in \{0, 1, \infty\}\} < \deg(f). \tag{7}$$

If the curve C has genus 0 or 1, then the existence of such $f \in K(C)$ is ruled out by the Riemann-Hurwitz formula (i.e., by Mason's proof [Ma1] of the ABC conjecture for function fields) because the left-hand side of (7) is

$$3 \deg(f) - \sum_{\substack{P \in C(\bar{\mathbb{Q}}) \\ f(P) \in \{0,1,\infty\}}} b_f(P), \tag{8}$$

$b_f(P)$ being the branch number (multiplicity minus 1) of f at P, and the sum in (8) is bounded above by the total branch number $2 \deg(f) - \chi(C) \leqslant 2 \deg(f)$ of f. (This is as it should be, because a curve of genus $\leqslant 1$ can have points of unbounded height over a number field!) But once C has genus $g \geqslant 2$ we can find f satisfying (7): Belyi's theorem ([Be], [Se, pp. 70–73]) provides a rational function $f \in K(C)$ ramified only above 0, 1, ∞; for this f, the sum in (8) accounts for all of the ramification of f and thus by Riemann-Hurwitz equals $2 \deg(f) + 2g - 2$, whence the left-hand side of (7) is $\deg(f) + 2 - 2g < \deg(f)$ as required. For future reference note that Belyi actually shows that for any finite subset S of $\mathbb{P}^1(\bar{\mathbb{Q}})$ there exists a rational function $\phi \in \mathbb{Q}(\mathbb{P}^1)$ ramified only above 0, 1, ∞ such that $\phi^{-1}(\{0, 1, \infty\}) \supseteq S$ (from which f is constructed by letting S contain the ramified points of an arbitrary nonconstant rational function on C and composing that function with ϕ); also note that the proof of Belyi's theorem gives an effective procedure for obtaining ϕ and f.

So fix $f \in K(C)$ satisfying (7) and let $d = \deg(f)$ and

$$m = \#\{P \in C(\bar{\mathbb{Q}}) : f(P) \in \{0, 1, \infty\}\} < d. \tag{9}$$

(We have seen that for Belyi's f we get $m = d + 2 - 2g$, but we need only the inequality $m < d$.) For any K-rational point $P \in C(K)$ not in the finite set $f^{-1}(\{0, 1, \infty\})$, we shall show that $H_P = H(f(P))$ and $N_P = N(f(P))$ satisfy

$$\boxed{\log N_P < \frac{m}{d} \log H_P + O(\sqrt{\log H_P} + 1)} \tag{10}$$

with the implied O-constant effective and depending on K, C, f but not on P; so $f(P)$ gives a counterexample to the ABC conjecture over K for $\varepsilon > 1 - (m/d)$ once H_P is large enough, i.e., for all but finitely many P. In fact, we shall show the following proposition.

PROPOSITION. *Let C be any curve over K and $f \in K(C)$ be a rational function of degree d. Then for any K-rational point $P \in C(K) - f^{-1}(0)$ we have*

$$\log N_0(f(P)) < \left(1 - \frac{b_f(0)}{d}\right) \log H_P + O(\sqrt{\log H_P} + 1) \tag{11}$$

with the implied constant effective and depending on K, C, f but not on P.

Given this estimate, we can replace f by $f-1$ and $1/f$ to obtain also (since $H(r)=H(1/r)=H(r-1)+O(1)$ for all $r\in K^*$)

$$\log N_1(f(P)) < \left(1-\frac{b_f(1)}{d}\right)\log H_P + O(\sqrt{\log H_P}+1),$$
$$\log N_\infty(f(P)) < \left(1-\frac{b_f(\infty)}{d}\right)\log H_P + O(\sqrt{\log H_P}+1); \tag{12}$$

adding these to (11), we shall then recover the inequality (10) since

$$\left(1-\frac{b_f(0)}{d}\right)+\left(1-\frac{b_f(1)}{d}\right)+\left(1-\frac{b_f(\infty)}{d}\right)$$
$$=\frac{\#(f^{-1}(0))}{d}+\frac{\#(f^{-1}(1))}{d}+\frac{\#(f^{-1}(\infty))}{d}=\frac{m}{d}. \tag{13}$$

Proof of the proposition. Note that when C is of genus zero, the proposition is elementary. For then we may identify the point P with a nonzero $z\in K\cup\{\infty\}$, and $f(P)$ is a rational function of z of degree d. Then

$$\log H_P = \log H(f(z)) = d\log H(z)+O(1). \tag{14}$$

Write f in homogeneous coordinates as a quotient $F(X,Y)/G(X,Y)$ of homogeneous polynomials of degree d and factor F over K:

$$F(X,Y)=w\prod_k F_k(X,Y)^{m_k} \tag{15}$$

where $w\in K^*$ and the F_k are irreducible polynomials of degrees (say) d_k; so $d=\sum_k m_k d_k$ and $b_f(0)=d-\sum_k d_k$. We can write $z=x/y$ with x, y algebraic integers of K of height $O(H(x))$. But then

$$\log N_0(f(P)) = \log N_0(F(x,y))+O(1)$$
$$\leqslant \sum_k \log H(F_k(x,y))+O(1) \leqslant \sum_k d_k \log H(z)+O(1), \tag{16}$$

which together with (14) yields (11), and with the error term reduced to $O(1)$ to boot.

For arbitrary C and f we generally no longer have a factorization (15), so that we use instead the theory of heights on algebraic curves (see, for instance, [Se, Ch. 2, 3]); the facts we need are the decomposition of the height as a sum of local terms and upper bounds on the height relative to a divisor of degree zero. For any divisor or divisor class c on C let $h_c(\cdot)$ be a (logarithmic) height function relative to c,

which is well defined up to $O(1)$. Let D be the zero divisor of f and write

$$D = \sum_k m_k D_k \tag{17}$$

where D_k are distinct irreducible divisors of degrees (say) d_k occurring with multiplicities m_k in D. Thus again

$$d = \sum_k m_k d_k \qquad \text{and} \qquad b_f(0) = d - \sum_k d_k = \deg D' \tag{18}$$

where D' is the divisor $\sum_{f(P)=0}(P)$, i.e., D_0 with all multiplicities removed. We then have

$$\log H_P = h_D(P) + O(1) = \sum_k m_k h_{D_k}(P) + O(1). \tag{19}$$

Except for finitely many primes of K (the primes of bad reduction of C and the primes of good reduction at which f reduces to the identically zero function), a prime occurs in $N_0(f(P))$ if and only if it contributes to $h_{D_k}(P)$ for some k. Since the contribution of any prime, finite or infinite, to the height relative to a given effective divisor is bounded below, we thus obtain

$$\log N_0(f(P)) < \sum_k h_{D_k}(P) + O(1) = h_{D'}(P) + O(1) \tag{20}$$

with $<$ accounting for finite primes at which P and D' may meet nontransversally and infinite places at which P may come close to the support of D'. So it remains to prove that

$$h_{D'}(P) = \frac{\deg D'}{\deg D} + O(\sqrt{\log H_P} + O(1)) \tag{21}$$

or equivalently that

$$h_\Delta(P) = O(\sqrt{\log H_P} + 1) \tag{22}$$

where Δ is the degree-zero divisor

$$\Delta = (\deg D)D' - (\deg D')D = d(D - D') - b_f(0)D. \tag{23}$$

But that is known for any degree-zero divisor Δ by a theorem of Néron [Se, p. 45]; so the proof of the proposition and thus also of (10) is complete.

Remarks on error terms. The proof of estimate (22) uses the Cauchy-Schwarz inequality and requires the use of canonical ("normalized" in [Se, Ch. 3]) heights.

For our purposes it suffices to have

$$h_\Delta(P) < \varepsilon \log H_P + O_\varepsilon(1) \tag{24}$$

for all positive ε, provided the O_ε is effective, and this can be done without invoking canonical heights [Se, p. 26]. When C has genus 0, any Δ of degree 0 is linearly equivalent to zero; so we again recover the improved estimate $h_\Delta(P) = O(1)$. (That all degree-zero divisors are principal is of course equivalent to the existence of the factorization (15) for all F; so the two arguments in the genus-zero curve are essentially the same.) The $\sqrt{\log H_P}$ part of the error term can be dropped in one additional case: if C is of genus 1 and $f \in K(C)$ is ramified only above 0, 1, ∞ (so $b_f(0) + b_f(1) + b_f(\infty) = 2 \deg(f)$), then

$$\log N_P < \log H_P + O(1), \qquad \text{i.e., } N_P \ll H_P. \tag{25}$$

To prove this, note that for any Belyi function f on a curve C, the divisor obtained by summing the points of $f^{-1}(\{0, 1, \infty\})$ without multiplicity is linearly equivalent to $D - \omega$, where ω is the canonical divisor on C—indeed, it is equal to $D[=(f)_0]$ minus the divisor of the differential form $df/(f-1)$. In the case of an elliptic curve the canonical divisor ω vanishes; thus, the sum of the Δ's occurring in (22) is a principal divisor, the $h_\Delta(P)$'s therefore sum to $O(1)$, and (25) follows.

We can also adapt these ideas to show that the ABC conjecture implies an effective form of Siegel's theorem ([Si], [Se, Ch. 7]) on the finiteness of integral (or S-integral) points. Indeed, the proof of Belyi's theorem allows us to include the points at infinity among the ramified points of f; then if P is integral, the contribution of any D_k at infinity towards $\log N_0(f(P))$ is bounded, so that we can improve (20) to $\log N_0(f(P)) < h_{D''}(P) + O(1)$, where D'' is the divisor D' with points at infinity removed, and likewise for the estimates on N_1 and N_∞. We thus obtain (10) with m replaced by $m - m_\infty$, where m_∞ is the number of distinct $\overline{K}$-points at infinity, and since we can take $m = d + 2 - 2g$, this contradicts the ABC conjecture if H_P is sufficiently large, provided $m_\infty > 2 - 2g$. One can also relax the condition of integrality to obtain some further results (assuming ABC) on Diophantine approximation; for instance, one can readily adapt our method to show that the ABC conjecture over a number field K implies Vojta's conjectured K-analogue of the Second Main Theorem of Nevanlinna theory: for any polynomial $P \in K(x)$ without repeated roots

$$N_0(P(r)) \gg_\varepsilon H(r)^{\deg(P)-2-\varepsilon} \tag{26}$$

for all $r \in K$, with the implied constant depending on K, P, ε, but not r.

Finally, we note that in [Mo1, §7] it is shown that if one could prove, for the single hyperelliptic curve C: $y^2 + y = x^5$, a strong form of Mordell's conjecture (called "Mordell Effectif" there and elsewhere) with bounds for all number fields K on the height of a K-rational point on C, then ABC conjecture (1) would follow, albeit with an exponent worse than $1 - \varepsilon$. In the preface to the Astérisque volume containing

this article, it is announced that the same result has been shown with C replaced by an arbitrary curve of genus $\geqslant 2$. Now the proof in [Mo1] uses a putative counterexample $r \in K$ to the weakened ABC conjecture to construct a point $(x, y) \in C(K')$ (for some extension K' of K of bounded degree) with $-4x^5 = r$; a contradiction is then obtained by estimating the height of (x, y) and the discriminant of K'. But $-4x^5$ is a degree-10 Belyi function on C, and so the argument of [Mo1] resembles the argument of the present paper in reverse, using the Belyi function to get from an ABC counterexample to a point on the curve rather than the other way around. Indeed, L. Moret-Bailly confirms [Mo2] that the proof, due to him and L. Szpiro, that C may be replaced by any curve of genus $\geqslant 2$ uses Belyi functions in the same manner.

(*Added in proof.* See [Sz2].)

ABC "near-misses" parametrized by elliptic curves and Fermat-Pell equations. Suppose we perform our construction with an elliptic curve C of positive K-rank. Then from (25) we obtain an infinite family of $r \in K$ such that $N(r) \ll H(r)$, i.e., such that $N(r)$ is almost as small as it is allowed to be by the ABC conjecture. Indeed, we can find subfamilies in which $N(r)$ is an arbitrarily small multiple of $H(r)$, for instance, by forcing $(S \cdot P)_v \to \infty$ for some fixed section S in the support of $D_0 + D_1 + D_\infty$ and (finite or infinite) place v of K.

Just as (10) was a generalization of a known result with Fermat curves, this construction is a generalization of a known idea [Sz1] of using (twists of) the Fermat cubic and semiquartic curves to produce families of $r \in \mathbb{Q}$ with $N(r) \ll H(r)$. Thus, we may fix $M \in \mathbb{Q}^*$ such that the elliptic curve $x^3 + y^3 + Mz^3 = 0$ has positive rank (say $M = 6$) and associate to a rational point $(x:y:z)$ the number $r = -(x/y)^3$ with $H(r) \ll N(r)$, and likewise for $x^4 - y^4 = Mz^2$ (say with $M = 5$) and $r = (x/y)^4$. Observe that in each case r is the value of a rational function (here of degree 3 or 4) on the elliptic curve ramified only above 0, 1, ∞. Another known method for constructing such r is to solve a Fermat-Pell equation $x^2 - My^2 = 1$ (for some fixed positive $M \in \mathbb{Z}$ not a perfect square) and let r be the integer x^2. Here $(x:y)$ is a point of that conic which is integral relative to the pair of points at infinity, and r is the value at (x, y) of a rational function of degree 4, ramified only above 0, 1, ∞, with the branch points including both of the points at infinity. Thus this approach also falls under the rubric of the ideas of the previous section. Finally and most simply, one can take r to be an S-unit for a fixed finite set S of rational primes, when $N_0(r)$ and $N_\infty(r)$ are both bounded—which is the starting point of several constructions of families of $r \in \mathbb{Q}$ with $N(r) = o(H(r))$ ([Ma2, ST]; see also [La, pp. 40–41]). This is tantamount to taking for f the identity function $\mathrm{id}: \mathbb{P}^1 \to \mathbb{P}^1$, whose (empty!) set of ramification points is contained in $\mathrm{id}^{-1}(\{0, 1, \infty\})$, and taking r to be S-integral relative to $\{0, \infty\} \subset \mathrm{id}^{-1}(\{0, 1, \infty\})$; so we can regard this method too as an application of the inequality $\log N_P < ((m - m_\infty)/d) \log H_P + O(1)$, albeit a trivial one since here $m - m_\infty = d = 1$.

We can thus expect to obtain new families of $r \in \mathbb{Q}$ by using different Belyi functions f. Such is in fact the case; we give two related examples, one of an elliptic family and one of a Fermat-Pell family.

First, let C be the elliptic curve $y^2 = x^3 + 5x + 10$ of $\mathbb{Q}$-rank 1,[5] and let f be the degree-5 function $(x - 5)y$ ramified only above ∞ and ± 16. (The origin of C is the quintuple pole, and f attains the value ± 16 with multiplicity 4 at the generators $\pm P_0 = (1, \mp 4)$ of the Mordell-Weil group.) Thus, $r = (f(P) + 16)/32$ satisfies $N(r) \ll H(r)$ for rational points $P \in C(\mathbb{Q})$ other than the preimages $\mathbf{0}$, $\pm P_0$, $\pm 4P_0$ of $\{0, 1, \infty\}$. For example, evaluating f at the 11th multiple of (1, 4) and clearing common factors in $(f + 16) = (f - 16) + 32$, we find

$$3931396791184375 + 12341487070149132 - 16272883861333507 = 0 \quad (27)$$

or in factored form

$$(5^5)(43^4)(53^2)(131) + (2^2)(3)(7^4)(809^4) - (1747^5) = 0 \quad (28)$$

which, thanks to the extra repeated factors of 5 and 53, gives an ABC ratio of

$$\frac{\log N}{\log H} = \frac{32.115\ldots}{37.328\ldots} = .8603\ldots . \quad (29)$$

Second, let C be the rational curve $y^2 = 3x^2 + 6$, which has infinitely many integral points starting with $(x, y) = (\pm 1, \pm 3)$, and let f be the degree-4 function $(x - 4)y$ ramified only above ∞ and ± 9. (The two points at infinity are double poles, and f attains the value ± 9 with multiplicity 3 at $(x, y) = (1, \mp 3)$.) Thus, $r = (f(P) + 9)/18$ satisfies $N(r) \ll H(r)$ for integral (x, y) with $x \neq 1, 5$. For instance, the 17th positive integral solution $(x, y) = (1934726305, 3351044259)$ yields, after clearing common factors,

$$360186303539019775 + 1 - 360186303539019776 = 0 \quad (30)$$

or in factored form

$$(5^2)(19)(29)(67^3)(443^3) + 1 - (2^{15})(7^3)(13)(37)(73)(97^3) = 0, \quad (31)$$

and again the extra repeated factors improve the ABC ratio, this time to

$$\frac{\log N}{\log H} = \frac{35.899\ldots}{40.425\ldots} = .8880\ldots . \quad (32)$$

[5] This curve of conductor 400, labeled 400-H1 in Cremona's tables [Cr], was also singled out in [MSD, p. 17] in a rather different context: numerical computations suggest that its modular parametrization has a multiple branch point at $i/20$.

Computing elliptic curves and Fermat-Pell equations that admit such Belyi functions of low degree and determining when they are defined over $\mathbb{Q}$ (which involves the "rigidity" methods of [Ma3] in a context other than the inverse Galois problem) are topics of quite a different flavor that we hope to treat more fully elsewhere.

Acknowledgements. Thanks to Jean-François Burnol and Benedict Gross for valuable suggestions for simplifying the proofs and improving the exposition, to Jean-François Mestre for directing me to L. Szpiro's *Séminaire sur les pinceaux de courbes elliptiques* (Astérisque # 183) from which the references [Ma2, Mo1, Sz] are taken, and to Henri Darmon and Joe Silverman for comments and corrections on an earlier version of the manuscript.

The computations in the last section used the computer packages MAC-SYMA and PARI.

I am grateful to the National Science Foundation for partial support during the preparation of this work.

References

[Ba] A. Baker, *Contributions to the theory of Diophantine equations, I: On the representation of integers by binary forms*, Philos. Trans. Roy. Soc. London Ser. A **263** (1968), 173–191.

[BC] A. Baker and J. Coates, *Integer points on curves of genus 1*, Proc. Cambridge Philos. Soc. **67** (1970), 595–602.

[Be] G. V. Belyi, *On the Galois extensions of the maximal cyclotomic field*, in Russian, Izv. Akad. Nauk SSSR **43** (1979), 267–276.

[Bo] E. Bombieri, *The Mordell conjecture revisited*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), 615–640.

[Cr] J. E. Cremona, *Computation of modular elliptic curves and the Birch–Swinnerton Dyer conjecture*, preprint, 1990–91.

[Fa1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[Fa2] ———, *Diophantine approximation on Abelian varieties*, preprint, 1989–90.

[Fr] G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), 1–40.

[GGK] A. M. Gleason, R. E. Greenwood, and L. M. Kelly, *The William Lowell Putnam Mathematical Competition—Problems and Solutions: 1938–1964*, Math. Assoc. of Amer., Washington D.C., 1980.

[La] S. Lang, *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. **23** (1990), 37–75.

[Ma1] R. C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. **96**, Cambridge Univ. Press, Cambridge, 1984. See also *Number Theory, Noordwijkerhout, 1983*, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, 149–157.

[Ma2] D. W. Masser, *Note on a conjecture of Szpiro*, Astérisque **183** (1990), 19–24.

[Ma3] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math. **1284**, Springer, Berlin, 1987.

[Mo1] L. Moret-Bailly, *Hauteurs et classes de Chern sur les surfaces arithmétiques*, Astérisque **183** (1990), 37–58.

[Mo2] ———, private communication, electronic mail, 20 September 1991.

[MSD] B. Mazur and H. P. F. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[Oe] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat, Sém. Bourbaki, Volume 1987/88, exposé #694*, Astérisque **161–162** (1988), 165–186.

[Se] J.-P. SERRE, *Lectures on the Mordell-Weil Theorem*, trans. by M. Brown, Aspects of Math. E **15**, Vieweg und Sohn, Braunschweig, 1989.

[Si] C. L. SIEGEL, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. (1929); *Gesamelte Abhandlungen, Volume I*, Springer, Berlin, 1966, 209–266.

[ST] C. L. STEWART AND R. TIJDEMAN, *On the Oesterlé-Masser conjecture*, Monats. Math. **102** (1986), 251–257.

[Sz1] L. SZPIRO, *Discriminant et conducteur des courbes elliptiques*, Astérisque **183** (1990), 7–18.

[Sz2] ———, *Remarques sur la taille des solutions de certaines équations algébriques*, preprint, 1991.

[Vo1] P. VOJTA, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math. **1239**, Springer, Berlin, 1987.

[Vo2] ———, *Siegel's theorem in the compact case*, Ann. of Math. **133** (1991), 509–548.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138; elkies@zariski.harvard.edu (uucp) or ELKIES@ZARISKI (bitnet)