PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 11, Pages 3141–3150
S 0002-9939(02)06589-9
Article electronically published on April 17, 2002

ON *abc* AND DISCRIMINANTS

D. W. MASSER

(Communicated by David E. Rohrlich)

ABSTRACT. We modify the *abc*-conjecture for number fields K in order to make the support (like the height) well-behaved under field extensions. We show further that the exponent $\mu > 1$ of the absolute value D_K of the discriminant cannot be replaced by $\mu = 1$, and even that an arbitrarily large power of $\log D_K$ must be present.

1. INTRODUCTION

The *abc*-conjecture states that for each $\lambda > 1$ there is a constant $C(\lambda)$ such that if a, b, c are any non-zero rational integers, coprime with zero sum, then

$$H \leq C(\lambda) S^{\lambda}. \tag{1.1}$$

Here

$$H = H(a, b, c) = \max\{|a|, |b|, |c|\} \tag{1.2}$$

is the "height" and

$$S = S(a, b, c) = \prod_{p|abc} p \tag{1.3}$$

is the "support" or "squarefree kernel" or "radical", in which p denotes a positive rational prime.

It is well known that this conjecture becomes false for $\lambda = 1$, and in 1986 Stewart and Tijdeman [ST] proved that it fails quite badly (see also von Frankenhuysen [Fra] for a numerical improvement of their result).

There have been several proposals for generalizing (1.1) to algebraic number fields K. The term H is then classically defined, and even in a projective sense (see below). In 1987 Vojta [V], after some considerations in a much broader setting, suggested a definition of the term S and conjectured (p. 84) a version of (1.1). See also [L2] (pp. 63–67). In 1991 Elkies [E] adjusted the definition to make it projective (p. 99) and conjectured (1.1) with $C(\lambda)$ replaced by a constant $C_K(\lambda)$ depending also on K. This too becomes false with $\lambda = 1$, whatever the number field K.

In fact the falsity holds for relatively trivial reasons, because the support as defined by Vojta and Elkies does not have good behaviour under field extensions. In this note we show how to modify the definition to obtain good behaviour. The

Received by the editors June 4, 2001.
2000 *Mathematics Subject Classification.* Primary 11D61, 11P99, 11S99.

new "ramified support" can be strictly larger than the old support; nevertheless the corresponding modification of (1.1) remains false for $\lambda = 1$.

Another interesting approach for number fields K was proposed in 1993 by Smirnov [Sm]. However, it turns out that his Conjecture A (p. 363) requires minor modifications, even when K is the rational field $\mathbf{Q}$. We discuss this briefly in an Appendix.

But the main purpose of this note is to examine more closely the dependence of $C_K(\lambda)$ on the number field K. In Vojta's work (see also Frey [Fre], p. 529) this is conjectured to have the form

$$C_K(\lambda) \leq C(\mu, \lambda) D_K^{\mu}, \tag{1.4}$$

where D_K is the absolute value of the discriminant of K. Here $C(\mu, \lambda)$ should depend, at least when the degree n of K is fixed, on μ and λ. In general possibly C (and even μ) should depend on this degree. However, by analogy with the function field case one might expect any $\mu > 1$ to be admissible (see also Granville and Stark [GS], p. 510).

We will prove that for each fixed $n \geq 2$ the *abc*-conjecture resulting from (1.1) and (1.4) is false with $\mu = 1$, whatever the value of λ, even with the possibly larger ramified support. Now this ramified support, by virtue of its good behaviour under field extensions, extends to a support $\overline{S}$ over the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, just as the height H extends to a height $\overline{H}$ over $\overline{\mathbf{Q}}$. It follows from our main result that there can be no "absolute *abc*-conjecture" of the shape

$$\overline{H} \leq C(\omega) \overline{S}^{\omega} \tag{1.5}$$

for non-zero a, b, c in $\overline{\mathbf{Q}}$ with zero sum, whatever the value of ω. This last conclusion also follows (on a suitable Riemann Hypothesis) from the constructions in [GS] (see p. 511) with modular functions.

We show further that the conjecture with $\mu = 1$ fails quite badly as in the work of Stewart and Tijdeman. We do this by going through the proof in [ST] and persuading their support S over $\mathbf{Q}$ to play the part of our discriminant D_K over K.

We now state our result in precise terms. For a number field K we construct valuations v in the usual way such that the "finite" valuations correspond to prime ideals $\mathcal{P}$ of the ring of integers $\mathcal{O}_K$ and the "infinite" valuations correspond to the embeddings σ of K into the field $\mathbf{C}$ of complex numbers. We normalize the finite valuations by

$$|\xi|_v = (N\mathcal{P})^{-e}$$

where $N\mathcal{P} = [\mathcal{O}_K : \mathcal{P}]$ and $e = \operatorname{ord}_{\mathcal{P}} \xi$ is the exact exponent of $\mathcal{P}$ dividing the ideal $\xi \mathcal{O}_K$. We normalize the infinite valuations so that the product formula

$$\prod_v |\xi|_v = 1 \tag{1.6}$$

holds for every non-zero ξ in K.

Now let a, b, c be non-zero elements in K. We define the height in the standard way by

$$H_K(a, b, c) = \prod_v \max\{|a|_v, |b|_v, |c|_v\}. \tag{1.7}$$

By (1.6) this makes sense on projective space $\mathbf{P}_2(K)$.

If a, b, c happen to be in $\mathbf{Q}$, then it is well-known that

$$H_K(a,b,c) = H_{\mathbf{Q}}(a,b,c)^n \tag{1.8}$$

for $n = [K : \mathbf{Q}]$; this is the "good behaviour" referred to above. And if further a, b, c are coprime in the ring $\mathbf{Z}$ of rational integers, then

$$H_{\mathbf{Q}}(a,b,c) = H(a,b,c) \tag{1.9}$$

as in (1.2).

Return now to a, b, c in K. The support as defined by Elkies is

$$\underline{S}_K(a,b,c) = \prod_v N\mathcal{P}, \tag{1.10}$$

where the product is over all finite v such that $|a|_v, |b|_v, |c|_v$ are not all equal. If there are no such v we take $\underline{S}_K = 1$. Again this makes sense projectively.

But now the analogue of (1.8) is not always true. For example, let p be a positive rational prime and let $K = \mathbf{Q}(\sqrt{p})$. Then $\underline{S}_K(1,1,p) = p$ because the only prime $\mathcal{P}$ in question is that with $\mathcal{P}^2 = p\mathcal{O}_K$, and $N\mathcal{P} = p$. But also $\underline{S}_{\mathbf{Q}}(1,1,p) = p$, so that the exponent $n = 2$ is missing.

To correct this situation we define the ramified support by the modified product

$$S_K(a,b,c) = \prod_v (N\mathcal{P})^{e(\mathcal{P})}, \tag{1.11}$$

over the same v as before, but with the ramification index $e(\mathcal{P}) = \operatorname{ord}_{\mathcal{P}} p$ for $p\mathbf{Z} = \mathcal{P} \cap \mathbf{Z}$. Again the empty product is interpreted as 1. In the example above $S_K(1,1,p) = p^2$.

The two definitions are closely related; thus one has

$$\underline{S}_K \le S_K \le D_K \underline{S}_K. \tag{1.12}$$

The left-hand inequality is obvious. To prove the right-hand inequality we note that the order $d(\mathcal{P}) = \operatorname{ord}_{\mathcal{P}} \mathcal{D}_K$ of the different $\mathcal{D}_K$ at any prime $\mathcal{P}$ satisfies $d(\mathcal{P}) \ge e(\mathcal{P}) - 1$ (see for example [Se1], Proposition 1, p. 326). Thus

$$D_K = N\mathcal{D}_K \ge \prod_{\mathcal{P}} (N\mathcal{P})^{e(\mathcal{P})-1} \ge S_K/\underline{S}_K.$$

But now there is the required good behaviour under field extensions; thus if a, b, c are in $\mathbf{Q}$ we have

$$S_K(a,b,c) = S_{\mathbf{Q}}(a,b,c)^n. \tag{1.13}$$

For when $\mathcal{P}|p$ then a, b, c have the same orders at $\mathcal{P}$ if and only if they have the same orders at p. So the left-hand side of (1.13) is

$$\prod_p \prod_{\mathcal{P}|p} (N\mathcal{P})^{e(\mathcal{P})} = \prod_p p^n$$

because $N\mathcal{P} = p^{f(\mathcal{P})}$ with $n = \sum_{\mathcal{P}|p} e(\mathcal{P}) f(\mathcal{P})$.

Further, $S_{\mathbf{Q}}(a,b,c) = \underline{S}_{\mathbf{Q}}(a,b,c)$, and if a, b, c are coprime in $\mathbf{Z}$, then

$$S_{\mathbf{Q}}(a,b,c) = S(a,b,c) \tag{1.14}$$

as in (1.3).

These equations already show that $\lambda = 1$ is impossible in the analogue of (1.1); more precisely for any C and any number field K there are non-zero a, b, c in K, with zero sum, such that

$$H_K > CS_K. \tag{1.15}$$

For example, [ST] delivers a, b, c in $\mathbf{Z}$, coprime with zero sum, such that $H > C^{1/n}S$. Now (1.15) follows from this using (1.8), (1.9), (1.13) and (1.14).

The right-hand inequality in (1.12) suggests the possibility that the conjecture $H_K \le C(\mu, \lambda)D_K^{\mu}(\underline{S}_K)^{\lambda}$ arising from (1.1) and (1.4) might be strengthened to an "absolute version"

$$H_K \le C(\omega)S_K^{\omega} \tag{1.16}$$

in which the discriminant does not appear. Our main result implies that (1.16) is false, and even that the discriminant must occur with exponent at least 1. The full result uses the functions

$$\varphi_\nu(x) = \exp\{(\log x)^\nu / \log\log x\}$$

already occurring in [ST] with $\nu = 1/2$. When $\nu > 0$ these grow faster than any power of $\log x$.

Theorem. *For any integer $n \ge 2$, any real $\lambda \ge 1$, any real $\nu < 1/(\lambda n + 1)$, and any real C there is a number field K of degree n containing non-zero a, b, c with zero sum such that*

$$H_K > CD_K\varphi_\nu(D_K)S_K^{\lambda}$$

where

$$H_K = H_K(a, b, c), \qquad S_K = S_K(a, b, c).$$

Thus for example the conjecture

$$H_K \le 10^{100}D_K(\log D_K)^{100}S_K^{100}$$

fails for some cubic field K. But the conjecture

$$H_K \le C(\omega)(D_K S_K)^{\omega} \tag{1.17}$$

is not yet disproved for any fixed $\omega > 1$.

Finally suppose a, b, c are in any subfield L of a number field K. It is well known that

$$H_K(a, b, c) = H_L(a, b, c)^{[K:L]}$$

generalizing (1.8); and it is just as easy to prove

$$S_K(a, b, c) = S_L(a, b, c)^{[K:L]}$$

generalizing (1.13). These make it possible to define

$$\overline{H}(a, b, c) = H_K(a, b, c)^{1/n}, \qquad \overline{S}(a, b, c) = S_K(a, b, c)^{1/n}$$

for any a, b, c in $\overline{\mathbf{Q}}$ simply by choosing a field K of degree n containing them. The Theorem above implies that there can be no "absolute *abc*-conjecture" of the form (1.5), even for number fields of fixed degree $n \ge 2$.

The remaining sections are devoted to a proof of the Theorem. In section 2 we record some preliminaries about irreducibility, and it is a pleasure to thank Andrzej Schinzel and Umberto Zannier for valuable information and references

about this topic. Then in section 3 we construct the number fields K using essentially the arguments of Stewart and Tijdeman together with some observations about discriminants.

Note. After this paper was submitted, we came across Browkin's survey article [B], in which a similar but different support (let us call it S'_K) was proposed (p. 89) with the same good behaviour under field extensions. In fact $S'_K \geq S_K$ and so our Theorem implies no analogous result involving S'_K. Thus it fails to disprove Browkin's own absolute *abc*-conjecture (p. 90).

We are also grateful to him for remarking that our (1.5) can be disproved in a very simple way. For example it suffices to take a large rational integer d and a root of $a(a-1)(a-d)=1$ and check $\overline{H} > d^{1/3}, \overline{S}=1$ for $b=1-a$ and $c=-1$.

2. Irreducibility

To establish the existence of certain number fields of given degree we need to prove that certain polynomials are irreducible. There are several ways of proceeding, but the laziest is through Hilbert's Theorem, or rather a quantitative version that controls the "exceptional set" of rational values of the parameter. In general the sharpest conclusion to be expected is that the number of exceptional values of height at most B is of order at most B (as opposed to the trivial upper bound of order B^2). See for example [Se2] (pp. 132, 133). But because the values $t = u/\tilde{u}$ that turn up in our proof are already much sparser, we need a correspondingly sharper conclusion. This we can secure with a hypothesis that is slightly stronger than usual.

Proposition. *Suppose $P(X,T)$ in $\mathbf{Q}[X,T]$ is such that $P(X,T^e)$ is irreducible over $\mathbf{C}(T)$ for all positive integers e. Then there is a positive integer f such that $P(X,t^f)$ is irreducible over $\mathbf{Q}$ for all but finitely many t in $\mathbf{Q}$.*

Proof. We modify Siegel's proof as given for example in [L1] (pp. 226–229), using a special case of Néron's trick to make the genus g at least 2 instead of 1; then we can appeal to Faltings's Theorem (Mordell's Conjecture) instead of Siegel's Theorem.

Let n be the degree of $P(X,S)$ with respect to X. We can assume without loss of generality that the coefficient of X^n is 1. For each integer m with $0 < m < n$ consider a formal factorization

(2.1)
$$P(X,S) = (X^m + U_1X^{m-1} + \cdots + U_m)(X^{n-m} + V_1X^{n-m-1} + \cdots + V_{n-m}).$$

Comparing coefficients gives equations that define a certain curve $\mathcal{C}_{P,m}$ depending on P and m. This curve might not be irreducible; let $\mathcal{C}$ be any absolutely irreducible component. So $\mathcal{C}$ is defined over some number field. It is not difficult to see that if f is a sufficiently large prime, the additional equation $S = T^f$ defines an absolutely irreducible covering $\mathcal{C}^{(f)}$ of $\mathcal{C}$ of degree f, defined over the same number field. We claim that the genus satisfies

(2.2)
$$g(\mathcal{C}^{(f)}) \geq 2$$

for all sufficiently large f. This suffices to prove the Proposition, because a nontrivial factorization of $P(X,t^f)$ over $\mathbf{Q}$ gives a point defined over $\mathbf{Q}$ (with coordinate $T=t$) on some $\mathcal{C}^{(f)}$.

To check (2.2) we use of course the Hurwitz Formula. We get

$$2g(\mathcal{C}^{(f)}) - 2 = (2g-2)f + \sum_{\pi}(e(\pi)-1) \tag{2.3}$$

with $g = g(\mathcal{C})$, where the sum is taken over all points π of $\mathcal{C}^{(f)}$ and $e(\pi)$ denotes the ramification.

The easiest case is when $g \geq 2$; then the right-hand side of (2.3) tends to infinity with f.

In case $g = 1$ it suffices to note that there is ramification with $e(\pi) = f$ above each zero or pole of S on $\mathcal{C}$, at least if f is a sufficiently large prime. So the right-hand side still tends to infinity.

Finally if $g = 0$ this remains true unless S has zero or poles at only one or two points of $\mathcal{C}$. But the latter possibility cannot happen. For write the function field of $\mathcal{C}$ over $\mathbf{C}$ as $\mathbf{C}(w)$ and express S as a rational function of w. Then it must have the form $S(w) = ((\alpha w+\beta)/(\gamma w+\delta))^e$ for $\alpha, \beta, \gamma, \delta$ in $\mathbf{C}$ and a positive integer e. It follows from (2.1) that $P(X, S(w))$ becomes reducible over $\mathbf{C}(w)$. Thus $P(X, T^e)$ is reducible over $\mathbf{C}(T)$, contradicting the hypothesis. This completes the proof of the Proposition.

The example $P(X,T) = X^2 - T$ shows that the hypothesis cannot be weakened to just $e = 1$, and the example $P(X,T) = X^2 - X - T$ shows that the conclusion cannot be strengthened to just $f = 1$.

Because we use Faltings's Theorem, the exceptional set of t in the Proposition is not effectively computable. But the exponent f is easily computable for any given polynomial. In section 3 we will use the example

$$P(X,T) = X^n - nX + (n-1)T^n. \tag{2.4}$$

It is not hard to see that $P(X, T^e)$ is always irreducible over $\mathbf{C}(T)$. Namely, Gauss's Lemma enables us to work over $\mathbf{C}[T]$, and now comparing coefficients of X^1 and X^0 in a factorization (2.1) with $S = T^e$ forces either U_m or V_{n-m} to be cT^{ne} ($0 \neq c$ in $\mathbf{C}$). In both cases looking at degrees with respect to T shows that one factor must be independent of T, an obvious impossibility.

For this example Zannier has verified that $\mathcal{C}_{P,m}$ is absolutely irreducible with genus

$$g = 1 + (1/2)\binom{n}{m}\{m(n-m) - 2\}. \tag{2.5}$$

We do not exhibit the calculations here—they can be carried out following Schinzel [Sc2], especially pp. 14–20.

If $n \geq 4$, then (2.5) is at least 3, and so we can take $f = 1$.

And if $n = 3$ we can take $f = 2$ to give genus 4. The choice $f = 1$ gives genus 1, but the finiteness fails because the elliptic curve $X^3 - 3X + 2T^3 = 0$ has positive rank over $\mathbf{Q}$.

Finally if $n = 2$ we should take $f = 3$ to give genus 2, but we can also take $f = 2$ because the elliptic curve $X^2 - 2X + T^4 = 0$ has zero rank. Again $f = 1$ is not possible.

Given a finite set of rational numbers not 0 or 1, there exists a positive integer h such that none of them is a perfect hth power in $\mathbf{Q}$. Increasing the exponent f to hf in the Proposition, we see that the exceptional set of t can be reduced to $\{0, 1\}$ at most. But the new exponent is probably no longer effective.

The Proposition can be strengthened in another way by assuming only that each $P(X, T^e)$ is irreducible over $\mathbf{Q}(T)$, not $\mathbf{C}(T)$. We do not supply the details of the proof, which is more or less standard following for example Schinzel [Sc1] (sections 16 and 22).

3. Proof of the Theorem

We shall need one technical estimate. For real $y \geq 0$ write as usual $\theta(y) = \sum_{p \leq y} \log p$, and for real $x \geq 0$ and a positive integer q write $\psi_q(x, y)$ for the number of positive integers not exceeding x composed only of primes p with $q < p \leq y$.

Lemma. *Suppose q, η, ζ are fixed with $0 < \zeta < \eta \leq 1/2$. Then with $\Lambda = 1/\eta - 1$ and $y = (\log x)^\eta$ the quotient*

$$\exp\{-\Lambda\theta(y)\}\psi_q(x, y)/\varphi_\zeta(x) \tag{3.1}$$

tends to infinity with x.

Proof. If $\psi(x, y) = \psi_1(x, y)$ denotes the more standard counting function, then we have the estimates

$$\psi(x, y) = \exp\{\pi(y) \log\log x - y + O(y/L^2)\} \tag{3.2}$$

with $L = \log(y + 2)$ and

$$\pi(y) = y/L + y/L^2 + O(y/L^3), \qquad \theta(y) = y + O(y/L^2);$$

see for example [N], p. 25; or alternatively the elementary method explained in [ST] gives directly a lower bound which suffices for our purposes. Now the result for (3.1) with $q = 1$ follows after a short calculation.

To generalize to arbitrary q, note that every integer counted by $\psi(x, y)$ has the form rs with r composed only of primes $p \leq q$ and s composed only of primes p with $q < p \leq y$. Since $r \leq x$ and $s \leq x$, it follows that $\psi(x, y) \leq \psi(x, q)\psi_q(x, y)$. Finally (3.2) implies that $\psi(x, q)$ is bounded by a fixed power of $\log x$, and the Lemma follows in general.

We can now prove our Theorem. Given $n \geq 2$ define $P(X, T)$ as in (2.4). We already checked the irreducibility hypothesis of the Proposition. So there is a positive integer f and a finite set $\mathcal{T}$ in $\mathbf{Q}$ such that $P(X, t^f)$ is irreducible over $\mathbf{Q}$ for all rational t not in $\mathcal{T}$.

Let $q > n$ be an upper bound for all primes appearing in the numerator and denominator of all elements of $\mathcal{T}$. Choose $\Lambda = n\lambda$ and $\eta = 1/(\Lambda + 1) \leq 1/2$. For large x and $y = (\log x)^\eta$ there are then $\psi_q(x, y) > 2$ positive integers not exceeding x composed only of primes p with $q < p \leq y$. Defining the positive integer d by

$$2^d < \psi_q(x, y) \leq 2^{d+1} \tag{3.4}$$

we find from the Box Principle two such integers $u, \tilde{u}$ with

$$0 < u < \tilde{u} \leq x, \qquad u \equiv \tilde{u} \pmod{2^d}. \tag{3.5}$$

Dividing by common factors (which by $q \geq 2$ are necessarily odd) we can assume that u and $\tilde{u}$ are coprime.

Consider now any solution ξ of the equation

$$\xi^n - n\tilde{u}^{(n-1)f}\xi + (n - 1)u^{nf} = 0. \tag{3.6}$$

This is $P(\xi/\tilde{u}^f, t^f) = 0$ for $t = u/\tilde{u}$. By choice of q, this t cannot lie in the exceptional set $\mathcal{T}$. This means that $P(X, t^f)$ is irreducible over $\mathbf{Q}$, and therefore $K = \mathbf{Q}(\xi)$ is a number field of degree exactly n.

We define

$$a = \xi^n, \quad b = -n\tilde{u}^{(n-1)f}\xi, \quad c = (n-1)u^{nf}$$

which by (3.6) have zero sum; and we proceed to estimate H_K, S_K and D_K.

To begin with, ξ is an algebraic integer, and the algebraic integers b/ξ and $c/\xi = -\xi^{n-1} + n\tilde{u}^{(n-1)f}$ have no common prime ideal factor, otherwise this would divide $b/\xi = -n\tilde{u}^{(n-1)f}$ and c; whereas these are coprime by construction and because $q > n$. It follows that $H_K(a/\xi, b/\xi, c/\xi)$ is

$$\prod_v \max\{|\sigma(a/\xi)|, |\sigma(b/\xi)|, |\sigma(c/\xi)|\} \geq \prod_v |\sigma(b/\xi)|$$

over just the infinite valuations. By projectivity this gives

$$H_K \geq n^n \tilde{u}^{n(n-1)f}. \tag{3.7}$$

Next, if v corresponds to a prime $\mathcal{P}$ dividing $p > y$, then $|c|_v = 1$ so $|\xi|_v = 1$ so $|a|_v = |b|_v = |c|_v = 1$. It follows that

$$S_K \leq \prod_{p \leq y} \prod_{\mathcal{P}|p} (N\mathcal{P})^{e(\mathcal{P})} = \prod_{p \leq y} p^n = \exp\{n\theta(y)\}. \tag{3.8}$$

Finally D_K divides the discriminant of the polynomial in (3.6) defining ξ. Now the discriminant of $X^n + \widetilde{U}X - U$ is up to sign $(n-1)^{n-1}\widetilde{U}^n + n^n U^{n-1}$ (see for example [GKZ], p. 406, or [M]). It follows that D_K divides $D = hE$ with $h = (n-1)^{n-1}n^n$ and

$$E = \tilde{u}^{n(n-1)f} - u^{n(n-1)f}.$$

But in fact D_K must be a lot smaller than D. This is because the exponent e of 2 dividing D_K is bounded solely in terms of n, thanks to a result of Hensel; see for example [Se1], Corollaire p. 328, which gives the explicit bound

$$e \leq n - 1 + n(\log n)/(\log 2).$$

By (3.5) E is divisible by 2^d, and it follows that

$$D_K \leq 2^{e-d} D \leq 2^{e-d} h \tilde{u}^{n(n-1)f}. \tag{3.9}$$

Now using (3.4), (3.7), (3.8) and (3.9) we get

$$H_K/(D_K S_K^\lambda) \geq 2^d \delta \exp\{-\Lambda\theta(y)\} \geq (1/2)\delta \exp\{-\Lambda\theta(y)\}\psi_q(x, y) \tag{3.10}$$

with

$$\delta = 2^{-e}(n-1)^{-(n-1)} \geq 2^{1-n}/h.$$

If $\nu < \eta$ is as in the Theorem, there is ζ between ν and η and we can apply the Lemma to the right-hand side of (3.10). Finally putting $\tilde{u} \leq x$ in (3.9) shows that $\varphi_\zeta(x)/\varphi_\nu(D_K)$ tends to infinity with x, and this completes the proof of the Theorem.

In fact it can be shown that D_K itself tends to infinity with x; thus we get infinitely many different fields K with this construction. For the quotient D/D_K is $\pm z^2$ for z in $\mathbf{Z}$, and so we obtain an equation $h\tilde{u}^{n(n-1)f} - hu^{n(n-1)f} = \pm D_K z^2$. By Theorem 2 (p. 515) of Darmon and Granville [DG], this equation has for each D_K only finitely many solutions in rational integers $u, \tilde{u}, z$ with u and $\tilde{u}$ coprime,

provided $n(n-1)f \geq 5$. On the other hand we know that $\tilde{u} - u$ is divisible by 2^d which tends to infinity with x.

Appendix

To see that some modification of Smirnov's Conjecture A is required, apply it to $f = m/n$ in the notation of section 3.6 (p. 363) of [Sm]. Throwing away the quantity $\delta_2 \geq 0$ we find after a short calculation that

$$\log(m-n) \leq \log S + 1 + R_1(m/n) \tag{A.1}$$

for any coprime rational integers m, n with $m > n > 0$, where $S = S(a,b,c)$ is the support in (1.3) above for $a = n, b = m-n, c = -m$.

The function $R_1(x)$ is not precisely specified in [Sm], except that it must be continuous on the set $\mathbf{R}^*$ of non-zero real numbers, satisfy $R_1(x) = R_1(-x) = R_1(1/x)$ and not grow too fast as x goes to infinity. Anyway, if we restrict $x > 1$ to a compact set $\mathcal{X}$ in $\mathbf{R}^*$, then $R_1(x)$ is bounded above. Also since for our $x = m/n$ we have $m - n = m(1-1/x)$ and $m = H = H(a,b,c)$, the equation (A.1) now reads

$$H \leq CS \tag{A.2}$$

for some constant C depending only on $\mathcal{X}$.

Of course (A.2) fails in general—see just after (1.15) above—but we need a counterexample $a + b + c = 0$ with $a > 0, b > 0$ and $x = |c|/a$ restricted to the set $\mathcal{X}$. In fact it is not difficult to produce a class of counterexamples with x dense in the interval $[1, \infty)$; perhaps the simplest method is the following.

Fix a positive integer d with

$$2^d > 30C, \tag{A.3}$$

and then fix positive integers k, ℓ such that

$$3^k \equiv 5^\ell \equiv 1 \pmod{2^d}.$$

For any positive integers r, s with $3^{rk} > 5^{s\ell}$ the numbers $c = -3^{rk}$ and $a = 5^{s\ell}$ satisfy $a + c \equiv 0 \pmod{2^d}$, and therefore $b = -a - c > 0$ has the form $2^d b'$ with b' in $\mathbf{Z}$. Clearly a, b, c are coprime with

$$S \leq 30b' = 30b/2^d \leq 30H/2^d,$$

so using (A.3) we see that (A.2) is indeed contradicted. Further our $x = |c|/a$ satisfies $\log x = (r\gamma - s)\log(5^\ell)$ with $\gamma = \log(3^k)/\log(5^\ell)$, and now the irrationality of γ allows us to conclude that the $r\gamma - s$ are dense in $[0, \infty)$. Therefore x is dense in $[1, \infty)$ as required.

References

[B] J. Browkin, *The abc-conjecture*, Number Theory (eds. R. P. Bambah, V. C. Dumir, R. J. Hans-Gill), Trends in Mathematics, Birkhäuser, 2000, 75–105. MR **2001f:**11053

[DG] H. Darmon and A. Granville, *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513–543. MR **96e:**11042

[E] N. Elkies, *ABC implies Mordell*, Int. Math. Res. Notices **7** (1991), 99–109. MR **93d:**11064

[Fra] M. von Frankenhuysen, *A lower bound in the abc Conjecture*, J. Number Theory **82** (2000), 91–95. MR **2001m:**11109

[Fre] G. Frey, *On ternary equations of Fermat type and relations with elliptic curves*, Modular forms and Fermat's last theorem (eds. G. Cornell, J. H. Silverman, G. Stevens), Springer, 1997, 527–548. MR **99k:**11004

[GKZ] I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky, *Discriminants, resultants and multidimensional determinants*, Birkhäuser, 1994. MR **95e:**14045

[GS] A. Granville and H. M. Stark, *ABC implies no "Siegel zeros" for L-functions of characters with negative discriminant*, Invent. Math. **139** (2000), 509–523. MR **2002b:**11114

[L1] S. Lang, *Fundamentals of diophantine geometry*, Springer, 1983. MR **85j:**11005

[L2] S. Lang, *Number theory* III, Encyclopaedia of Mathematical Sciences, Vol. 60, Springer, 1991. MR **93a:**11048

[M] D. W. Masser, *The discriminants of special equations*, Mathematical Gazette **372** (1966), 158–160.

[N] K. K. Norton, *Numbers with small prime factors, and the least kth power non-residue*, Mem. Amer. Math. Soc. **106** (1971). MR **44:**3948

[Sc1] A. Schinzel, *Selected topics on polynomials*, University of Michigan, 1982. MR **84k:**12010

[Sc2] A. Schinzel, *On reducible trinomials*, Dissertationes Math. **CCCXXIX** (1993). MR **95d:**11146

[Se1] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Pub. Math. I.H.E.S. **54** (1981), 323–401. MR **83k:**12011

[Se2] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, Aspects of Math. E15, Vieweg, 1990. MR **90e:**11086

[Sm] A. L. Smirnov, *Hurwitz inequalities for number fields*, St. Petersburg Math. J. **4** (1993), 357–375. MR **93h:**11065

[ST] C. L. Stewart and R. Tijdeman, *On the Oesterlé-Masser conjecture*, Monatshefte Math. **102** (1986), 251–257. MR **87k:**11077

[V] P. Vojta, *Diophantine approximations and value-distribution theory*, Lecture Notes 1239, Springer, 1987. MR **91k:**11049

Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland

E-mail address: masser@math.unibas.ch