Acta Math., 189 (2002), 161–177

Rational solutions of certain equations involving norms

by

ROGER HEATH-BROWN and ALEXEI SKOROBOGATOV

University of Oxford
Oxford, England, U.K.

Imperial College
London, England, U.K.

1. Introduction

Let k be a number field, and K an extension of degree n. We shall write $N(x_1,...,x_n)$ for the norm form $N_{K/k}(\omega_1 x_1+...+\omega_n x_n)$, where $\{\omega_1,...,\omega_n\}$ is a basis of K as a vector space over k. Let $P(t)$ be a polynomial with coefficients in k. In this paper we are interested in the Hasse principle and the density of solutions in k of the following Diophantine equation:

$$P(t)=N(x_1,...,x_n). \tag{1}$$

Let $\bar{k}$ be an algebraic closure of k. In the case when $P(t)$ has at most one root in $\bar{k}$, the open subset of the affine variety (1) given by $P(t)\neq 0$ is a principal homogeneous space under an algebraic k-torus. In this case it is well known that the Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation on any smooth projective model of this variety (Colliot-Thélène and Sansuc [CSan1]). In this paper we prove the same result when $P(t)$ has exactly two roots in k and no other roots in $\bar{k}$, and k is the field of rational numbers $\mathbf{Q}$. An immediate change of variables then reduces (1) to the equation

$$t^{a_0}(1-t)^{a_1}=\alpha N(x_1,...,x_n), \tag{2}$$

where $\alpha\in k^*$, and a_0 and a_1 are positive integers. We can assume without loss of generality that a_i satisfy $0<a_i<n$.

A remarkable feature of our work is that it combines the method of descent with the Hardy–Littlewood circle method. It appears that this is the first time such an approach has been used.([1]) One consequence of this is that we are able to handle an equation

([1]) The second author learnt the idea that the circle method can be used for proving the Hasse principle and weak approximation for varieties appearing after descent from Per Salberger (see the survey [C, p. 331]).

of degree n in as few as $n+1$ variables. Normal applications of the circle method are restricted to equations in $2n$ variables, at the very least.

The affine variety X given by (2) contains two obvious rational points given by $x_i=0$ for all $i=1,...,n$, $t=0$ or $t=1$. The point corresponding to $t=0$ (resp. $t=1$) is smooth if and only if $a_0=1$ (resp. $a_1=1$). So if one of these conditions is satisfied, the smooth Hasse problem is trivial, but it is not clear how to find more rational points (see also the Remark in §2). When $n=2$ the existence of a smooth k-point on the quadric X implies the rationality of X. When $n=3$ and $a_0+a_1\leqslant 3$, the existence of a smooth k-point on the cubic X implies the unirationality of X (see e.g. [CSal, Proposition 1.3]). However, for general n no method ensuring that there are other k-rational points seems to be known.([2]) Another phenomenon appearing in the cubic case is the existence of counterexamples to weak approximation. For example, when $a_0=a_1=1$, $k=\mathbf{Q}$ and $K=\mathbf{Q}(\theta)$, where θ is a root of $x^3-7x^2+14x-7=0$, the set $X(\mathbf{Q})$ is not dense in $X(\mathbf{Q}_7)$ (D. Coray, see [CSal, (8.2)]). In the cubic case Colliot-Thélène and Salberger proved that the failure of weak approximation is always accounted for by the Brauer–Manin obstruction ([CSal, Theorem 6.2]. The non-trivial case here is when $a_0=a_1=1$, because otherwise X is rational over k, see [CSal, Lemma 6.1]).

Our main result is the following theorem.

THEOREM 1.1. *Let k be the field of rational numbers $\mathbf{Q}$. If $(a_0,a_1,n)=1$, then the Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation on any smooth and projective model of the variety X given by* (2). *If there is no Brauer–Manin obstruction to the Hasse principle on such a model, then the $\mathbf{Q}$-rational points are Zariski dense in X.*

Note that the projection to the coordinate t equips an appropriate smooth and projective model of X with a morphism to $\mathbf{P}^1_k$ such that at most three fibres are not geometrically integral (the fibres at 0, 1 and ∞). The known methods (descent and fibration) apply well to the case of at most two "bad" fibres, but the general case of three bad fibres remains open (see, however, [CSal], [CSk, Theorem B] and the ensuing comments for a discussion of known cases). Note also that the smooth k-fibres of the projection of X to the coordinate t are principal homogeneous spaces under the norm torus, and in general satisfy neither the Hasse principle nor weak approximation. (If each bad fibre were to contain an irreducible component of multiplicity 1 which splits into two over an algebraic closure of the residue field, then we would be able to apply the results of [HS].)

([2]) When K is a cyclic extension of an arbitrary number field k, and $P(t)$ is a separable polynomial of *any* degree, it is proved in [CSS, Theorem 1.1 and Example 1.6], that under Schinzel's hypothesis (H) the conclusions of our Theorem 1.1 still hold.

Our proof is a combination of descent and the circle method, whence the restriction on the ground field. We need the validity of the Hasse principle and weak approximation on a certain variety obtained after descent. This is a smooth affine variety $Y \subset \mathbf{A}_k^{2n}$ given by the equation

$$r_0 N(y_1, ..., y_n) + r_1 N(z_1, ..., z_n) = 1, \tag{3}$$

where $r_0, r_1 \in k^*$. When $k = \mathbf{Q}$ the Hasse principle for (3) follows from an asymptotic lower bound for the number of solutions of the homogenized form of (3) in a large box, obtained by Birch, Davenport and Lewis using the circle method [BDL]. In this paper the method of [BDL] is extended to prove that Y satisfies weak approximation.

It is quite likely that the theorem still holds when $(a_0, a_1, n) \neq 1$, but the proof of this would be much more technical and is not discussed here.([3])

2. Universal torsors

In this section k is any field of characteristic zero with algebraic closure $\bar{k}$, $\Gamma_k = \mathrm{Gal}(\bar{k}/k)$. When X is a k-variety we write $\overline{X} = X \times_k \bar{k}$.

Let a_0, a_1 and n be positive integers such that $(a_0, a_1, n) = 1$. For $\alpha \in k^*$ let X be the subvariety of $\mathbf{A}_k^{n+1}$ given by (2).

LEMMA 2.1. *There exists a positive integer a_1', coprime to a_0, such that X is birationally equivalent to the affine variety* (2) *with a_1 replaced by a_1'.*

Proof. Let $d = (a_1, n)$. Then $(a_0, d) = 1$. By the theorem on primes in an arithmetic progression there exist a positive integer m and a prime number p not dividing a_0, such that $dp = a_1 + mn$. Let $a_1' = dp$. The desired birational map is given by $x_i = (1-t)^{-m} x_i'$, $i = 1, ..., n$. □

Without loss of generality now we assume that $(a_0, a_1) = 1$.

Remark. When a_0, a_1 or $a_0 + a_1$ is coprime to n, it can be shown, using an appropriate base change and the Lang–Nishimura lemma ([L], [N]), that every proper model of X has a k-rational point. (Extracting a root of a local parameter one finds a smooth k-point on the covering variety. When $(a_0, n) = 1$ choose b such that $a_0 b \equiv 1 \bmod n$, then write $t = t_1^b$. The resulting variety is birationally equivalent to the variety given by $t_1(1 - t_1^b)^{a_1} = \alpha N(z_1, ..., z_n)$, and the point $t_1 = z_1 = ... = z_n = 0$ is smooth. When $(a_1, n) = 1$ one needs to extract a root of $t - 1$, and when $(a_0 + a_1, n) = 1$ one extracts a root from t^{-1}, a local parameter at ∞. Now the Lang–Nishimura lemma says that if $X_1 \to X_2$ is a

([3]) See the forthcoming paper by J.-L. Colliot-Thélène, D. Harari and the second author for the proof of this result.

rational map of integral varieties over any field k, X_1 has a smooth k-point, and X_2 is proper, then X_2 has a k-point.) This is not true when $a_0=a_1=2$, $n=4$, and K is a totally imaginary number field: then the open subset $t^2(t-1)^2=-N(z_1,z_2,z_3,z_4)\neq 0$ has no real points, hence there are no real points on any smooth and proper model.

The main result of this section is the following theorem.

THEOREM 2.2. *Let $X'=X_{\mathrm{smooth}}$ be the smooth locus of X. Universal X'-torsors exist, and any such torsor is birationally equivalent to the affine variety* (3) *for some $r_0, r_1\in k^*$.*

Proof. The $\bar{k}$-variety $\overline{X}$ can be given by the equation

$$t^{a_0}(1-t)^{a_1}=u_1\dots u_n.$$

A straightforward computation shows that X' can be described as follows. The morphism $X\to\mathbf{A}^1_k$ given by projection to the coordinate t has exactly two geometrically reducible fibres, X_0 over $t=0$ and X_1 over $t=1$. Let $i\in\{0,1\}$. If $a_i=1$, we let Z_i be empty; otherwise let Z_i be the closed subset of the fibre X_i consisting of points which belong to two or more irreducible components of $\overline{X}_i$, that is, such that $u_j=u_{j'}=0$ for some $j\neq j'$. Geometrically, $X_i\setminus Z_i$ is the smooth locus of X_i. Then we have $X'=X\setminus(Z_0\cup Z_1)$. In particular, $X'=X$ when $a_0=a_1=1$. The morphism $X'\to\mathbf{A}^1_k$ is always surjective. Let D^0_i, $i=1,\dots,n$, be the divisor on $\overline{X}'$ given by $t=u_i=0$. Similarly, let D^1_i, $i=1,\dots,n$, be given by $1-t=u_i=0$. Note that

$$\operatorname{div}(t)=\sum_{i=1}^{n}D^0_i,\quad \operatorname{div}(1-t)=\sum_{i=1}^{n}D^1_i,\quad \operatorname{div}(u_i)=a_0D^0_i+a_1D^1_i,\quad i=1,\dots,n. \tag{4}$$

We now check that $\bar{k}[X']^*=\bar{k}^*$. Indeed, the generic fibre of $\overline{X}'\to\mathbf{A}^1_k$ is $\mathbf{G}^{n-1}_{m,\bar{k}(t)}$. Hence any invertible regular function ψ on $\overline{X}'$ can be written as $\psi=f(t)\prod_{i=1}^n u_i^{m_i}$. Computing $\operatorname{div}(\psi)$ we see that ψ must be a constant.

Consider the open subset $U\subset X'$ given by $t(1-t)\neq 0$. We have

$$\overline{U}\simeq(\mathbf{A}^1_{\bar{k}}\setminus\{0,1\})\times\mathbf{G}^{n-1}_{m,\bar{k}},$$

hence $\operatorname{Pic}\overline{U}=0$. The descent theory now tells us that universal X'-torsors exist if and only if the following exact sequence of Γ_k-modules is split:

$$1\to\bar{k}^*\to\bar{k}[U]^*\to\bar{k}[U]^*/\bar{k}^*\to 1$$

([CSan2, Proposition 2.3.4], or [S, Corollary 2.3.10]). The group $\bar{k}[U]^*/\bar{k}^*$ is generated by the classes of the functions t, $1-t$ and u_i. Every relation satisfied by these classes is

a multiple of $a_0[t]+a_1[1-t]-\sum_{i=1}^{n}[u_i]=0$. The displayed exact sequence of Γ_k-modules is split if and only if there exists a Galois equivariant lifting of these classes to $\bar{k}[U]^*$. Every such lifting has the form

$$[t]\mapsto \varrho_0 t, \quad [1-t]\mapsto \varrho_1(1-t), \quad [u_i]\mapsto \xi_i u_i, \quad i=1,\dots,n,$$

where $\varrho_0,\varrho_1\in k^*$, and the conjugate elements $\xi_1,\dots,\xi_n\in\bar{k}^*$ are the images of an element $\xi\in K^*$ with respect to all n embeddings $K\to\bar{k}$, such that $\varrho_0^{a_0}\varrho_1^{a_1}=\alpha N_{K/k}(\xi)$. In particular, the above sequence is split if and only if $\alpha\in N_{K/k}(K^*)k^{*a_0}k^{*a_1}$. This is clearly true in our case since $(a_0,a_1)=1$.

Let $\mathcal{T}\to X'$ be a universal torsor. We now describe the restriction $\mathcal{T}_U$ of $\mathcal{T}$ to $U\subset X'$.

The abelian group $\mathrm{Div}_{\overline{X}'\setminus\bar{U}}\,\overline{X}'$ is freely generated by the D_i^0 and the D_i^1; the Galois group Γ_k acts on these divisors by permutations of subscripts. We have an exact sequence of Γ_k-modules:

$$1=\bar{k}[X]^*/\bar{k}^*\to\bar{k}[U]^*/\bar{k}^*\to\mathrm{Div}_{\overline{X}'\setminus\bar{U}}\,\overline{X}'\to\mathrm{Pic}\,\overline{X}'\to\mathrm{Pic}\,\overline{U}=0, \tag{5}$$

where the second arrow is $\psi\mapsto\mathrm{div}(\psi)$. It is clear from (4) and (5) that the condition $(a_0,a_1)=1$ implies that $\mathrm{Pic}\,\overline{X}'$ has no torsion.

Consider the exact sequence of k-tori which is dual to (5):

$$1\to S\to R_{K/k}(\mathbf{G}_{m,K})^2\to T\to 1.$$

Recall that $R_{K/k}(\mathbf{G}_{m,K})$ is a k-torus defined as the Weil descent of the multiplicative group $\mathbf{G}_{m,K}$. This exact sequence equips $R_{K/k}(\mathbf{G}_{m,K})^2$ with the structure of a T-torsor under S. By the local description of torsors ([CSan2, Theorem 2.3.1, Proposition 2.3.4], or [S, Theorem 4.3.1]) there exists a homomorphism of Γ_k-modules $\phi:\widehat{T}=\bar{k}[U]^*/\bar{k}^*\to\bar{k}[U]^*$ which is a section of the obvious surjective map, such that $\mathcal{T}_U$ is the pullback of this torsor to U with respect to the natural morphism $U\to T$ defined by (the inverse of) ϕ. Let $\mathbf{y}$ and $\mathbf{z}$ be the K-coordinates on $R_{K/k}(\mathbf{G}_{m,K})^2$. The torus T is naturally a subtorus of $\mathbf{G}_{m,k}^2\times R_{K/k}(\mathbf{G}_{m,K})$ given by $t_0^{a_0}t_1^{a_1}=N(\mathbf{x})$, and the composed map $R_{K/k}(\mathbf{G}_{m,K})^2\to T\to\mathbf{G}_{m,k}^2$ is given by $(N(\mathbf{y}),N(\mathbf{z}))$. From the explicit form of ϕ displayed above, it is clear that a point $(t,\mathbf{x})$ of U goes to $(\varrho_0^{-1}t,\varrho_1^{-1}(1-t),\xi^{-1}\mathbf{x})$. Thus the image of U in T is given by the equation $\varrho_0 t_0+\varrho_1 t_1=1$. Hence $\mathcal{T}_U\subset R_{K/k}(\mathbf{G}_{m,K})^2$ is given by $\varrho_0 N(\mathbf{y})+\varrho_1 N(\mathbf{z})=1$. □

When $a_0+a_1\equiv 0 \bmod n$ the k-variety X is birationally equivalent to a principal homogeneous space of a k-torus. (By a change of variables as in the proof of Lemma 2.1 the equation of X is reduced to $T^{a_0}=\alpha N(\mathbf{x})$, where $T=t/(1-t)$.) In this case Theorem 1.1 is a particular case of a general result [CSan1].

3. Weak approximation on universal torsors

Our approach to proving weak approximation on the universal torsor will use the Hardy–Littlewood circle method. Good general descriptions of the method are given by Davenport [D] and Vaughan [V], to which we refer the reader unfamiliar with these techniques. In fact the present problem is not difficult by today's standards, and requires only a mild adaptation of an existing argument due to Birch, Davenport and Lewis [BDL]. However, we shall give reasonably full details.

We wish to prove a weak approximation result for the homogeneous equation

$$aN(\mathbf{x})+bN(\mathbf{y})=z^n, \tag{6}$$

where a and b are non-zero integers, and $N(*)$ is a norm form defined for a number field K of degree n over $\mathbf{Q}$. Suppose that the equation (6) has a solution $\mathbf{x}^{(\mathbf{R})}, \mathbf{y}^{(\mathbf{R})}, z^{(\mathbf{R})}$ over $\mathbf{R}$ and a solution $\mathbf{x}^{(M)}, \mathbf{y}^{(M)}, z^{(M)}$ to some modulus M. Then for a given $\eta>0$, we will want our solution of (6) to satisfy

$$\max|x_i-Px_i^{(\mathbf{R})}|<\eta P, \quad \max|y_i-Py_i^{(\mathbf{R})}|<\eta P, \quad |z-Pz^{(\mathbf{R})}|<\eta P, \tag{7}$$

for some positive real P, and also

$$x_i\equiv x_i^{(M)}, \quad y_i\equiv y_i^{(M)}, \quad z\equiv z^{(M)} \mod M. \tag{8}$$

For a weak approximation result it is clearly sufficient to assume that each of $\mathbf{x}^{(\mathbf{R})}$, $\mathbf{y}^{(\mathbf{R})}, z^{(\mathbf{R})}$ is non-zero. In particular, we shall suppose that $z^{(\mathbf{R})}>0$. Moreover it also suffices to assume that η is sufficiently small. Thus we may suppose that none of $\mathbf{x}=\mathbf{0}$, $\mathbf{y}=\mathbf{0}$ and $z=0$ satisfy the constraints (7), so that

$$\eta<z^{(\mathbf{R})}. \tag{9}$$

Henceforth we shall regard $\mathbf{x}^{(\mathbf{R})}, \mathbf{y}^{(\mathbf{R})}, z^{(\mathbf{R})}, \mathbf{x}^{(M)}, \mathbf{y}^{(M)}, z^{(M)}, M, \eta$ and the norm form N as fixed, and allow the constants implied by the notations $\ll$, $\gg$ and $O(\cdot)$ to depend on them.

We now define

$$S_1(\alpha)=\sum_{\mathbf{x}} e(\alpha aN(\mathbf{x})), \quad \alpha\in\mathbf{R},$$

where $\mathbf{x}$ runs over integer vectors satisfying the constraints (7) and (8), and $e(x)$ is defined as $\exp(2\pi ix)$. Similarly we write

$$S_2(\alpha)=\sum_{\mathbf{y}} e(\alpha bN(\mathbf{y}))$$

and

$$S_3(\alpha)=\sum_z e(\alpha z^n),$$

where again the variables are restricted by (7) and (8).

The number of solutions of (6), subject to (7) and (8), is then

$$\int_0^1 S_1(\alpha)S_2(\alpha)S_3(-\alpha)\,d\alpha = M(P),$$

say, and we aim to show that

$$M(P)\gg P^{n+1}$$

as P tends to infinity. This is clearly sufficient.

For integers h,q satisfying

$$(h,q)=1,\quad 1\leqslant q\leqslant P^{\delta},$$

we shall define intervals $I_{h,q}$ by the inequalities

$$\left|\alpha-\frac{h}{q}\right|<P^{-n+\delta}.$$

Here $\delta\in(0,1)$ is a parameter to be chosen in due course, see (21). We begin by considering the values of α which fall in none of the intervals $I_{h,q}$. Here our starting point is Weyl's inequality in the form given by Vaughan ([V, Lemma 2.4]), for example.

LEMMA 3.1. *Let $f(x)=\beta x^n+\ldots$ be a polynomial of degree $n\geqslant 2$ with real coefficients, and suppose that β has a rational approximation a/q such that*

$$\left|\beta-\frac{a}{q}\right|\leqslant\frac{1}{q^2},\tag{10}$$

where $q\geqslant 1$ and $(a,q)=1$. Let

$$S(f)=\sum_{m=1}^{N} e(f(m)).$$

Let $K=2^{n-1}$ and $\varepsilon>0$. Then

$$|S(f)|\ll N^{1+\varepsilon}(N^{-1}+q^{-1}+N^{-n}q)^{1/K},\tag{11}$$

where the implied constant depends on n and ε.

From now on all the constants implied by the notations $\ll$, $\gg$ and $O(\cdot)$ will be allowed to depend on ε.

To apply Lemma 3.1 we write $z=Mw+z^{(M)}$, so that the interval (7) for z becomes $A<w<A+2\eta P/M$, say. If we now set $w=k+[A]$ we find that k runs over a range $1\leqslant k\leqslant N$, say, with $N\ll P$. The sum $S_3(\alpha)$ now takes the form $S(f)$ required for Lemma 3.1, with $\beta=M^n\alpha$. According to Dirichlet's approximation theorem, for any $Q\geqslant 1$ we can find coprime integers a and q, with $1\leqslant q\leqslant Q$, such that

$$\left|M^n\alpha-\frac{a}{q}\right|<\frac{1}{qQ}.$$

Thus (10) is automatically satisfied. If we take $Q=P^{n-\delta}$ then

$$\left|\alpha-\frac{a}{M^nq}\right|<\frac{1}{M^nqQ}\leqslant\frac{1}{Q}=P^{-n+\delta}.$$

We may write the fraction $a/(M^nq)$ in lowest terms with denominator

$$\frac{M^nq}{(a,M^nq)}.$$

If we assume that α belongs to none of the intervals $I_{u,v}$ we deduce that

$$\frac{M^nq}{(a,M^nq)}>P^{\delta},$$

whence $q\gg P^{\delta}$. In view of the bounds $P^{\delta}\ll q\leqslant Q=P^{n-\delta}$ we now conclude from (11) that

$$|S_3(\alpha)|\ll P^{1-\delta/K+\varepsilon}. \tag{12}$$

Lemma 1 of Birch, Davenport and Lewis [BDL] still holds, since it hinges on an upper bound for the number of solutions of the equation $N(\mathbf{x})=N(\mathbf{x}')$ in the box described by (7). In our situation there is an additional congruence restriction on $\mathbf{x}$ and $\mathbf{x}'$, but this does not affect the validity of the upper bound. Thus we have

$$\int_0^1|S_1(\alpha)|^2\,d\alpha\ll P^{n+\varepsilon} \tag{13}$$

and

$$\int_0^1|S_1(\alpha)S_2(\alpha)|\,d\alpha\ll P^{n+\varepsilon},$$

for any $\varepsilon>0$. We may combine this with the bound (12) to deduce that

$$\int_m|S_1(\alpha)S_2(\alpha)S_3(-\alpha)|\,d\alpha\ll P^{n+1-\delta/K+2\varepsilon},$$

where m denotes the complement in the unit interval of the union of the intervals $I_{h,q}$. Since a positive δ is to be specified, see (21), and ε is arbitrary, we may conclude that

$$M(P)=\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}\int_{I_{h,q}}S_1(\alpha)S_2(\alpha)S_3(-\alpha)\,d\alpha+o(P^{n+1}), \tag{14}$$

on noting that the intervals $I_{h,q}$ are necessarily disjoint.

We now have to approximate $S_1(\alpha)S_2(\alpha)S_3(-\alpha)$ on the interval $I_{h,q}$. It will be convenient to establish a general result.

LEMMA 3.2. *Let F be an integer polynomial in r variables, of total degree n. Let $N_1, ..., N_r$ be positive integers with $N_i \ll P$. For any $a \in \mathbf{Z}$ and $q \in \mathbf{N}$ with $q \leqslant P^{\delta}$, write*

$$S(a,q) = \sum_{1 \leqslant k_i \leqslant q} e\left(\frac{a}{q} F(k_1, ..., k_r)\right),$$

and for any real μ write

$$I(\mu) = \int_{0 \leqslant t_i \leqslant N_i} e(\mu F(t_1, ..., t_r))\, dt_1 ... dt_r.$$

Then if

$$S(\alpha) = \sum_{1 \leqslant k_i \leqslant N_i} e(\alpha F(k_1, ..., k_r))$$

and $|\mu| \leqslant P^{-n+\delta}$, we have

$$S(a/q+\mu) = q^{-r} S(a,q) I(\mu) + O(P^{r-1+2\delta}). \tag{15}$$

Proof. We split the sum $S(a/q+\mu)$ according to the residue class of $\mathbf{k}$ modulo q, writing $\mathbf{k} = \mathbf{m} + q\mathbf{s}$, to give

$$\begin{aligned} S(a/q+\mu) &= \sum_{\mathbf{m} \pmod q} \sum_{\mathbf{s} \in \mathcal{S}} e((a/q+\mu) F(\mathbf{m}+q\mathbf{s})) \\ &= \sum_{\mathbf{m} \pmod q} e\left(\frac{a}{q} F(\mathbf{m})\right) \sum_{\mathbf{s}} e(\mu F(\mathbf{m}+q\mathbf{s})), \end{aligned} \tag{16}$$

where $\mathbf{s}$ runs over the range $\mathcal{S}$ given by

$$\frac{1-m_i}{q} \leqslant s_i \leqslant \frac{N_i - m_i}{q}, \quad 1 \leqslant i \leqslant r.$$

Now if $0 \leqslant v_i \leqslant 1$ for $1 \leqslant i \leqslant r$, then

$$F(\mathbf{m}+q\mathbf{s}) = F(\mathbf{m}+q(\mathbf{s}+\mathbf{v})) + O(qP^{n-1}),$$

the implied constant in the error term depending on F. Thus

$$\mu F(\mathbf{m}+q\mathbf{s}) = \mu F(\mathbf{m}+q(\mathbf{s}+\mathbf{v})) + O(qP^{-1+\delta}),$$

so that

$$e(\mu F(\mathbf{m}+q\mathbf{s})) = e(\mu F(\mathbf{m}+q(\mathbf{s}+\mathbf{v}))) + O(qP^{-1+\delta}).$$

If we average this over $\mathbf{v}$ we find that

$$e(\mu F(\mathbf{m}+q\mathbf{s})) = \int_{\mathbf{v}} e(\mu F(\mathbf{m}+q(\mathbf{s}+\mathbf{v}))) \, dv_1 \dots dv_r + O(qP^{-1+\delta})$$
$$= q^{-r} \int_{\mathbf{t}} e(\mu F(\mathbf{t})) \, dt_1 \dots dt_r + O(qP^{-1+\delta}),$$

where $\mathbf{t}$ runs over the box

$$m_i + qs_i \leqslant t_i \leqslant m_i + q(s_i+1).$$

It follows that

$$\sum_{\mathbf{s}} e(\mu F(\mathbf{m}+q\mathbf{s})) = q^{-r} \int_{\mathbf{t}\in\mathcal{T}} e(\mu F(\mathbf{t})) \, dt_1 \dots dt_r + O(qP^{-1+\delta} \# \mathcal{S}),$$

in which $\mathcal{T}$ is a box $A_i \leqslant t_i \leqslant B_i$ with $A_i = O(q)$ and $B_i = N_i + O(q)$. Thus $\mathcal{T}$ differs from $\prod [0, N_i]$ by a set of measure $O(qP^{r-1})$, so that

$$\sum_{\mathbf{s}} e(\mu F(\mathbf{m}+q\mathbf{s})) = q^{-r} I(\mu) + O(q^{1-r} P^{r-1}) + O(qP^{-1+\delta} \# \mathcal{S}).$$

Moreover $\# \mathcal{S} \ll (P/q+1)^r \ll P^r q^{-r}$, whence

$$\sum_{\mathbf{s}} e(\mu F(\mathbf{m}+q\mathbf{s})) = q^{-r} I(\mu) + O(q^{1-r} P^{r-1+\delta}).$$

We may now insert this into (16) to deduce (15). □

We shall apply Lemma 3.2 to the product $S_1(\alpha) S_2(\alpha) S_3(-\alpha)$ taking $r = 2n+1$. If we write $x_i = x_i^{(M)} + Mu_i$, then the interval $|x_i - Px_i^{(\mathbf{R})}| < \eta P$ can be interpreted as a range $A_i < u_i \leqslant B_i$ for certain integers A_i, B_i such that $B_i = A_i + 2\eta P M^{-1} + O(1)$. We then set

$$k_i = u_i - A_i, \quad c_i = x_i^{(M)} + MA_i, \quad N_i = B_i - A_i.$$

We follow an analogous procedure for the variables y_i and z, to put $S_1(\alpha) S_2(\alpha) S_3(-\alpha)$ into the shape required for Lemma 3.2 with

$$F(k_1, \dots, k_{2n+1}) = aN(c_1 + Mk_1, \dots, c_k + Mk_n) \\ + bN(c_{n+1} + Mk_{n+1}, \dots, c_{2n} + Mk_{2n}) - (c_{2n+1} + Mk_{2n+1})^n. \tag{17}$$

We conclude that

$$S_1(\alpha) S_2(\alpha) S_3(-\alpha) = q^{-2n-1} S(h, q) I(\alpha - h/q) + O(P^{2n+2\delta})$$

on the interval $I_{h,q}$. Since

$$\sum_{q\leqslant P^{\delta}}\sum_{1\leqslant h\leqslant q}\operatorname{meas}(I_{h,q})\ll P^{-n+3\delta},$$

we deduce from (14) that

$$M(P)=\Sigma\mathcal{I}+O(P^{n+5\delta})+o(P^{n+1}), \tag{18}$$

where

$$\Sigma=\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n-1}S(h,q) \tag{19}$$

and

$$\mathcal{I}=\int_{-P^{-n+\delta}}^{P^{-n+\delta}}I(\mu)\,d\mu. \tag{20}$$

In view of (18) we shall take

$$\delta=\tfrac{1}{6}. \tag{21}$$

We deal first with $\mathcal{I}$. If we write $c_i+Mt_i=v_i$ in the definition of $I(\mu)$, we see that $\mathbf{v}$ runs over a box $\mathcal{V}$, say, defined by constraints

$$-V_i^{(-)}\leqslant v_i-Px_i^{(\mathbf{R})}\leqslant V_i^{(+)},\quad 1\leqslant i\leqslant n,$$

and similarly for $n+1\leqslant i\leqslant 2n+1$, with $V_i^{(-)},V_i^{(+)}=\eta P+O(1)$. We then have

$$I(\mu)=M^{-2n-1}\int_{\mathbf{v}}e(\mu\{aN(v_1,\dots,v_n)+bN(v_{n+1},\dots,v_{2n})-v_{2n+1}^n\})\,dv_1\dots dv_{2n+1}.$$

Since $\mathcal{V}$ differs from the original region (7) by a set of measure $O(P^{2n})$, it follows that

$$I(\mu)=M^{-2n-1}\int_{\mathbf{t}}e(\mu\{aN(t_1,\dots,t_n)+bN(t_{n+1},\dots,t_{2n})-t_{2n+1}^n\})\,dt_1\dots dt_{2n+1}+O(P^{2n}),$$

the integral being over the region (7). If we now set $\mathbf{t}=P\mathbf{w}$ we find that

$$I(\mu)=M^{-2n-1}P^{2n+1}J(P^n\mu)+O(P^{2n}),$$

where

$$J(\gamma)=\int_{\mathbf{w}}e(\gamma\{aN(w_1,\dots,w_n)+bN(w_{n+1},\dots,w_{2n})-w_{2n+1}^n\})\,dw_1\dots dw_{2n+1},$$

the integral being over the set

$$\begin{aligned} &\max|w_i - x_i^{(\mathbf{R})}| \leqslant \eta, \quad 1 \leqslant i \leqslant n, \\ &\max|w_i - y_{i+n}^{(\mathbf{R})}| \leqslant \eta, \quad n+1 \leqslant i \leqslant 2n, \\ &|w_{2n+1} - z^{(\mathbf{R})}| \leqslant \eta. \end{aligned} \tag{22}$$

Thus (20) becomes

$$\mathcal{I} = M^{-2n-2} P^{n+1} \int_{-P^\delta}^{P^\delta} J(\gamma) + O(P^{n+\delta}).$$

Since $N(\mathbf{x})$ is homogeneous, the partial derivatives

$$\frac{\partial}{\partial w_j} N(w_1, ..., w_n)$$

can only vanish simultaneously at a point for which $N(w_1, ..., w_n) = 0$. Thus, if we take our original η to be sufficiently small, we can ensure that there is some index j for which

$$\left| \frac{\partial}{\partial w_j} N(w_1, ..., w_n) \right| \gg 1$$

on the range (22). Without loss of generality we may take $j = 1$. We now substitute

$$t = aN(w_1, ..., w_n) + bN(w_{n+1}, ..., w_{2n}) - w_{2n+1}^n \tag{23}$$

for w_1, giving

$$J(\gamma) = \int_{-\infty}^{\infty} \psi(t) e(\gamma t)\, dt$$

with

$$\psi(t) = a^{-1} \int ... \int \left| \frac{\partial}{\partial w_1} N(w_1, ..., w_n) \right|^{-1} dw_2 ... dw_{2n+1},$$

with w_1 being given implicitly by (23). In this final integral, the range is restricted by the constraints (22). The function $\psi(t)$ is a continuous function of bounded variation, whence the Fourier inversion theorem shows that

$$\lim_{T \to \infty} \int_{-T}^{T} J(\gamma)\, d\gamma = \psi(0).$$

Moreover the integrand of $\psi(t)$ is positive, and the region of integration contains a non-empty open set. It follows that $\psi(0)$ is positive. This enables us to conclude that

$$\mathcal{I} \sim M^{-2n-2} P^{n+1} \psi(0), \quad P \to \infty.$$

It remains to consider the sum Σ given by (19). We first show, following Birch, Davenport and Lewis ([BDL, Section 6]), that the sum

$$\mathfrak{S}=\sum_{q=1}^{\infty}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}} q^{-2n-1}S(h,q)$$

is absolutely convergent. We shall write

$$S_1(h,q)=\sum_{1\leqslant k_1,\dots,k_n\leqslant q} e\Big(\frac{h}{q}F_1(k_1,\dots,k_n)\Big),$$

where

$$F_1(k_1,\dots,k_n)=aN(c_1+Mk_1,\dots,c_n+Mk_n).$$

We define $S_2(h,q)$ analogously, and set

$$S_3(h,q)=\sum_{1\leqslant n\leqslant q} e\Big(\frac{-h}{q}(c_{2n+1}+Mn)^n\Big),$$

whence

$$S(h,q)=S_1(h,q)S_2(h,q)S_3(h,q).$$

We now repeat our analysis of the major arcs, but working with

$$\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}\int_{I_{h,q}}|S_1(\alpha)|^2\,d\alpha$$

in place of

$$\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}\int_{I_{h,q}}S_1(\alpha)S_2(\alpha)S_3(-\alpha)\,d\alpha.$$

In this way we find that

$$\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}\int_{I_{h,q}}|S_1(\alpha)|^2\,d\alpha=\Sigma_1\mathcal{I}_1+O(P^{n-1+5\delta}),$$

where

$$\Sigma_1=\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}} q^{-2n}|S_1(h,q)|^2$$

and

$$\mathcal{I}_1\sim CP^n,$$

for a certain positive constant C. However,

$$\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}\int_{I_{h,q}}|S_1(\alpha)|^2\,d\alpha\leqslant\int_0^1|S_1(\alpha)|^2\,d\alpha\ll P^{n+\varepsilon},\tag{24}$$

by (13), whence

$$\Sigma_1=\sum_{q\leqslant P^{\delta}}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n}|S_1(h,q)|^2\ll P^{\varepsilon}.$$

Recall here that $\delta=\frac{1}{6}$, by (21).

The above estimate holds for any $P\geqslant 1$, and for any $\varepsilon>0$. Moreover the sum $S_1(h,q)$ depends on neither P nor ε. It therefore follows from (24), on choosing $P=R^6$ and $\varepsilon=\frac{1}{6}\varpi$, that

$$\sum_{q\leqslant R}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n}|S_1(h,q)|^2\ll R^{\varpi},\tag{25}$$

for any $R\geqslant 1$, and any $\varpi>0$. An entirely analogous argument shows that

$$\sum_{q\leqslant R}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n}|S_2(h,q)|^2\ll R^{\varpi}.\tag{26}$$

We now examine the sum

$$\mathfrak{S}_R=\sum_{R/2<q\leqslant R}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n-1}S(h,q)=\sum_{R/2<q\leqslant R}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n-1}S_1(h,q)S_2(h,q)S_3(h,q).$$

The bounds (25) and (26) show that

$$\sum_{R/2<q\leqslant R}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n}|S_j(h,q)|^2\ll R^{\varpi},\quad j=1,2,$$

whence Cauchy's inequality yields

$$\sum_{R/2<q\leqslant R}\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}}q^{-2n}|S_1(h,q)S_2(h,q)|\ll R^{\varpi}.$$

To bound $S_3(h,q)$ we may apply Lemma 3.1, taking $N=q$, and reducing the fraction M^nh/q to lowest terms to produce a new denominator q', say, with $q\ll q'\ll q$. This shows that

$$S_3(h,q)\ll q^{1-1/K+\varepsilon},$$

so that

$$\mathfrak{S}_R \ll R^{\varpi-1/K+\varepsilon} \ll R^{-1/(2K)},$$

on choosing $\varpi=\varepsilon=1/(4K)$. It follows that the sum for $\mathfrak{S}$ is absolutely convergent.

We can now conclude that

$$M(P)=\mathfrak{S}M^{-2n-2}P^{n+1}\psi(0)+o(P^{n+1})$$

as P tends to infinity, and it remains to show that the constant $\mathfrak{S}$ is positive. An elementary argument reveals that the function

$$f(q)=\sum_{\substack{1\leqslant h\leqslant q\\(h,q)=1}} q^{-2n-1}S(h,q)$$

is multiplicative. In view of the absolute convergence it therefore suffices to show that

$$\sum_{e=0}^{\infty} f(p^e)$$

is positive for each prime p. However, standard arguments show that

$$\sum_{e=0}^{E} f(p^e)=p^{-2nE}\#\{(k_1,\dots,k_{2n+1}) \pmod{p^E} : F(k_1,\dots,k_{2n+1})\equiv 0 \pmod{p^E}\},$$

with F being the polynomial (17). Thus it suffices to show that the number on the right above is bounded below. Using Hensel's lemma we then see that it is enough for $F(\mathbf{k})=0$ to have a p-adic integer solution $\mathbf{k}$ in which some partial derivative

$$\frac{\partial F}{\partial k_i}(\mathbf{k})$$

is non-zero. This yields the following conclusion.

THEOREM 3.3. *Suppose that, for every prime p, there is a non-singular p-adic integral solution of* (6) *satisfying* (8). *Then the equation* (6) *has an integer solution satisfying* (7) *and* (8), *for every sufficiently large real P.*

4. Proof of the main theorem

Let X be a variety of a field k. Recall that $\mathrm{Br}_0 X=\mathrm{Im}[\mathrm{Br}\,k\to\mathrm{Br}\,X]$ and $\mathrm{Br}_1 X=\mathrm{Ker}[\mathrm{Br}\,X\to\mathrm{Br}\,\overline{X}]$. Now let $k=\mathbf{Q}$, and $\mathbf{A}_\mathbf{Q}$ be the adèle ring of $\mathbf{Q}$. Recall that $X(\mathbf{A}_\mathbf{Q})^{\mathrm{Br}}$ (resp. $X(\mathbf{A}_\mathbf{Q})^{\mathrm{Br}_1 X}$) is the set of adelic points orthogonal to $\mathrm{Br}\,X$ (resp. to $\mathrm{Br}_1 X$) with respect to the pairing defined by evaluation and taking the sum of all local invariants. By definition, there is no Brauer–Manin obstruction to the Hasse principle on X if and only if $X(\mathbf{A}_\mathbf{Q})^{\mathrm{Br}}\neq\varnothing$.

Proof of Theorem 1.1. Using Lemma 2.1 we arrange that $(a_0, a_1)=1$. Let Z be a smooth compactification of X' (it exists by Hironaka's theorem). The condition $(a_0, a_1)=1$ implies that $\operatorname{Pic}\overline{X}'$ has no torsion, hence $\operatorname{Br}_1 X'/\operatorname{Br}_0 X'=H^1(\Gamma_{\mathbf{Q}}, \operatorname{Pic}\overline{X}')$ is finite. By Proposition 1.1 of [CSk] (based on D. Harari's "formal lemma") the set $X'(\mathbf{A_Q})^{\operatorname{Br}_1 X'}$ is dense in the closed subset $Z(\mathbf{A_Q})^{\operatorname{Br}}$ of $Z(\mathbf{A_Q})$. (Note that Z is a smooth, proper, rational variety, hence $\operatorname{Br}\overline{Z}=0$.) We want to approximate an adelic point in $Z(\mathbf{A_Q})^{\operatorname{Br}}$ by a $\mathbf{Q}$-rational point R, but we first approximate it by an adelic point $\{R_v\}\in X'(\mathbf{A_Q})^{\operatorname{Br}_1 X'}$. Since Z is proper, the topological space $Z(\mathbf{A_Q})$ is $\prod_v Z(\mathbf{Q}_v)$, and so we just need to ensure that R is close to R_v for v in a given finite set S of places of $\mathbf{Q}$. We can assume that S contains the infinite place. By the main theorem of the descent theory ([S, Theorem 6.1.2]) $\{R_v\}$ lifts to an adelic point $\{Q_v\}$ on some universal X'-torsor Y'. By Theorem 2.2 this torsor Y' is a dense open subset of Y given by (3) for some $r_0, r_1\in\mathbf{Q}^*$. We need to find $Q\in Y'(\mathbf{Q})$ which is arbitrarily close to Q_v for $v\in S$. The points Q_v give rise to integral p-adic points on the homogeneous affine variety (6), and to a real point $(\mathbf{x}^{(\mathbf{R})}, \mathbf{y}^{(\mathbf{R})}, z^{(\mathbf{R})})$ with $z^{(\mathbf{R})}=1$. By the Chinese remainder theorem approximating p-adic integers for $p\in S$ amounts to solving congruences of the form (8), where M is the product of sufficiently high powers of primes in S. Let $(\mathbf{x}, \mathbf{y}, z)$ be an integral solution of (6) provided by Theorem 3.3 for some small $\eta>0$, when P is sufficiently large. In particular, $z>0$. Then $Q=(\mathbf{x}/z, \mathbf{y}/z)$ is a $\mathbf{Q}$-rational point on Y' which is as close as we wish to Q_v for $v\in S$. Now $R=f(Q)$ is the desired $\mathbf{Q}$-rational point on X.

By the p-adic implicit function theorem we can choose the local points R_v away from any given closed subset of X. Thus the resulting $\mathbf{Q}$-rational points are Zariski dense in X. This completes the proof. □

Note that this proof does not work when a_0 and a_1 are not coprime. In this case X' is "too small" in the sense that $\operatorname{Pic}\overline{X}'$ contains torsion, whereas $\operatorname{Pic}\overline{Z}$ contains none, thus $\operatorname{Br} X'/\operatorname{Br} Z$ is infinite.

References

[BDL] BIRCH, B. J. & DAVENPORT, H. & LEWIS, D. J., The addition of norm forms. *Mathematika*, 9 (1962), 75–82.

[C] COLLIOT-THÉLÈNE, J.-L., L'arithmétique des variétés rationnelles. *Ann. Fac. Sci. Toulouse Math.* (*6*), 1 (1992), 295–336.

[CSal] COLLIOT-THÉLÈNE, J.-L. & SALBERGER, P., Arithmetic on some singular cubic hypersurfaces. *Proc. London Math. Soc.* (*3*), 58 (1989), 519–549.

[CSan1] COLLIOT-THÉLÈNE, J.-L. & SANSUC, J.-J., La R-équivalence sur les tores. *Ann. Sci. École Norm. Sup.* (*4*), 10 (1977), 175–229.

[CSan2] — La descente sur les variétés rationnelles, II. *Duke Math. J.*, 54 (1987), 375–492.

[CSk] COLLIOT-THÉLÈNE, J.-L. & SKOROBOGATOV, A. N., Descent on fibrations over $\mathbf{P}^1_k$ revisited. *Math. Proc. Cambridge Philos. Soc.*, 128 (2000), 383–393.

[CSS] COLLIOT-THÉLÈNE, J.-L., SKOROBOGATOV, A. N. & SWINNERTON-DYER, SIR P., Rational points and zero-cycles on fibred varieties: Schinzel's hypothesis and Salberger's device. *J. Reine Angew. Math.*, 495 (1998), 1–28.

[D] DAVENPORT, H., *Analytic Methods for Diophantine Equations and Diophantine Inequalities*. Ann Arbor Publishers, Ann Arbor, MI, 1963.

[HS] HARARI, D. & SKOROBOGATOV, A. N., The Brauer group of torsors and its arithmetic applications. Preprint 02-33, Max-Planck-Institut, 2002.

[L] LANG, S., Some applications of the local uniformization theorem. *Amer. J. Math.*, 76 (1954), 362–374.

[N] NISHIMURA, H., Some remark on rational points. *Mem. Coll. Sci. Univ. Kyoto Ser. A Math.*, 29 (1955), 189–192.

[S] SKOROBOGATOV, A. N., *Torsors and Rational Points*. Cambridge Tracts in Math., 144. Cambridge Univ. Press, Cambridge, 2001.

[V] VAUGHAN, R. C., *The Hardy–Littlewood Method*, 2nd edition. Cambridge Tracts in Math., 125. Cambridge Univ. Press, Cambridge, 1997.

ROGER HEATH-BROWN
Mathematical Institute
University of Oxford
24–29 St. Giles'
Oxford OX1 3LB
England, U.K.
rhb@maths.ox.ac.uk

ALEXEI SKOROBOGATOV
Department of Mathematics
The Huxley Building
Imperial College
180 Queen's Gate
London SW7 2BZ
England, U.K.
a.skorobogatov@ic.ac.uk

Received July 18, 2001