ACTA ARITHMETICA
167.2 (2015)

Random Thue and Fermat equations

by

Rainer Dietmann (London) and Oscar Marmon (Göttingen)

1. Introduction. Let $F(X_1,\dots,X_s)\in\mathbb{Z}[X_1,\dots,X_s]$. If $F(x_1,\dots,x_s) = 0$ for some $\mathbf{x}\in\mathbb{Z}^s$, then trivially the equation $F(x_1,\dots,x_s)=0$ also has solutions over $\mathbb{R}$ and over all local rings $\mathbb{Z}_p$. If the opposite is true as well, then we say that F satisfies the *Hasse principle*. For homogeneous polynomials F, always $F(0,\dots,0)=0$, so one then naturally asks for nontrivial solutions. The Hasse principle for example holds true for quadratic forms, but fails for cubic forms: one famous counterexample (see [17]) is given by the cubic form

$$F(X_1,X_2,X_3)=3X_1^3+4X_2^3+5X_3^3. \tag{1}$$

In recent years questions about the frequency of such failures of the Hasse principle were addressed for different classes of Diophantine equations (see for example [1], [2], [3], [5], [6], [16]). For hyperelliptic curves, Bhargava [1] has recently shown that asymptotically, as their genus tends to infinity, their probability to satisfy the Hasse principle, given that there are local solutions, tends to zero.

In this note we focus on curves as well, namely those that are given by Fermat equations such as (1), or given by Thue equations. This way we provide families of curves which satisfy the Hasse principle with probability zero, and already for fixed small degree rather than asymptotically for the degree tending to infinity, but on the other hand our results, like those in a related earlier paper [8], are conditional on the *abc-conjecture* (see [14]), which we briefly recall: if $a+b=c$ with $a,b,c\in\mathbb{Z}$ where $abc\neq 0$, $(a,b,c)=1$, and

$$P=\prod_{p\mid abc} p,$$

2010 *Mathematics Subject Classification*: Primary 11D45; Secondary 11D41, 11E76, 11G35, 11G50, 14G05.

Key words and phrases: Thue equations, Fermat equations, random Diophantine equations, Hasse principle, *abc*-conjecture.

DOI: 10.4064/aa167-2-6

the product being taken over all primes p dividing abc, then

$$\max\{|a|,|b|,|c|\} \ll_\varepsilon P^{1+\varepsilon}.$$

Assuming the abc-conjecture, we are able to show that a 'random' Thue equation of degree at least three has an integer solution with probability 0, even if it is locally soluble everywhere.

To be more precise, let

$$N_{k,\mathrm{loc}}(H) = \#\{a,b \in \mathbb{Z} : 0 < |a|,|b| \le H \text{ and } ax^k + by^k = 1 \\ \text{has solutions over all local rings } \mathbb{Z}_p \text{ and over } \mathbb{R}\}$$

and

$$N_{k,\mathrm{glob}}(H) = \#\{a,b \in \mathbb{Z} : 0 < |a|,|b| \le H \text{ and } ax^k + by^k = 1 \\ \text{has a solution } (x,y) \in \mathbb{Z}^2\}.$$

We can now state our main result on random Thue equations.

Theorem 1. *Let $k \ge 3$, and assume the truth of the abc-conjecture. Then*

$$\frac{N_{k,\mathrm{glob}}(H)}{N_{k,\mathrm{loc}}(H)} \to 0 \quad (H \to \infty).$$

In particular, assuming the abc-conjecture, for any fixed degree at least three there are infinitely many Thue equations violating the Hasse principle, and a 'random' Thue equation of degree at least three that is locally soluble everywhere has an integer solution with probability 0. Theorem 1 follows immediately from Lemmas 4 and 6, whose proofs will be given in Sections 2 and 3, respectively. Our strategy roughly follows that laid out in [6], reversing the roles of linear variables and kth powers when dealing with equations on average, though the details are simpler here. With a little bit more work also more general Thue equations of the form $ax^k + by^k = c$ should be doable, though we refrained from treating them and concentrated on the special case $c = 1$ in order to keep the exposition simple.

In a similar way one can establish results for homogenized Thue equations, i.e. Fermat equations. Let

$$M_{k,\mathrm{loc}}(H) = \#\{a,b,c \in \mathbb{Z} : 0 < |a|,|b|,|c| \le H \text{ and } ax^k + by^k + cz^k = 0 \\ \text{has non-trivial solutions over all local rings } \mathbb{Z}_p \text{ and over } \mathbb{R}\}$$

and

$$M_{k,\mathrm{glob}}(H) = \#\{a,b,c \in \mathbb{Z} : 0 < |a|,|b|,|c| \le H \text{ and } ax^k + by^k + cz^k = 0 \\ \text{has a solution } (x,y,z) \in \mathbb{Z}^3 \setminus \{\mathbf{0}\}\}.$$

The following result is a homogeneous analogue of Theorem 1.

THEOREM 2. *Let $k \geq 6$, and assume the truth of the abc-conjecture. Then*

$$\frac{M_{k,\mathrm{glob}}(H)}{M_{k,\mathrm{loc}}(H)} \to 0 \quad (H \to \infty).$$

Again, Theorem 2 follows immediately from Lemmas 5 and 7, to be proved in Sections 2 and 3, respectively.

2. Local considerations. To get a better understanding of $N_{k,\mathrm{loc}}$ we need the following two well known results, which we state for the convenience of the reader.

LEMMA 1. *Let $k \in \mathbb{N}$, let p be a rational prime exceeding $k^2(k+1)^2$, and let $a_1, a_2, a_3 \in \mathbb{Z}$ be coprime to p. Then the congruence*

$$a_1 x_1^k + a_2 x_2^k + a_3 \equiv 0 \pmod{p}$$

has at least one solution.

Proof. See [15, formula (1.17)]. ■

LEMMA 2. *Let $f(X_1, \ldots, X_s) \in \mathbb{Z}[X_1, \ldots, X_s]$ and let p be a rational prime. Suppose that for some $x_1, \ldots, x_s \in \mathbb{Z}$ and some non-negative integer n we have*

$$f(x_1, \ldots, x_s) \equiv 0 \pmod{p^{2n+1}} \quad \textit{and} \quad p^n \| \nabla f(x_1, \ldots, x_s).$$

Then there exist $y_1, \ldots, y_n \in \mathbb{Z}_p$ such that

$$y_i \equiv x_i \pmod{p^{n+1}} \quad (1 \leq i \leq s)$$

and $f(y_1, \ldots, y_s) = 0$.

Proof. This is a version of Hensel's lemma (see for example [9, p. 64]). ■

LEMMA 3. *Let p be an odd prime and $a \in \mathbb{Z}$ with $(a/p) = 1$. Further, let $k \in \mathbb{N}$ be such that $p \equiv -1 \pmod{k}$. Then the congruence $x^k \equiv a \pmod{p}$ has a solution.*

Proof. Let G be the multiplicative group of non-zero residue classes modulo p, and let $\varphi : G \to G$ be the map given by $\varphi(x) = x^k$ for $x \in G$. If k is odd, then $p \equiv -1 \pmod{k}$ implies that $(p-1, k) = 1$, so φ is surjective and the conclusion immediately follows. If k is even, then $(p-1, k) = 2$ by $p \equiv -1 \pmod{k}$, so $\varphi(G)$ is a subgroup of G of index 2. Since G is cyclic, the only such subgroup is the group of quadratic residues modulo p, and as $(a/p) = 1$, the conclusion follows again. ■

We are now in a position to derive a lower bound for $N_{k,\mathrm{loc}}$. Note that in the following all the implied O-constants are allowed to depend on k.

Lemma 4. *We have*

$$N_{k,\mathrm{loc}}(H) \gg \left(\frac{H}{\log H}\right)^2.$$

Proof. For each rational prime p, define α_p by $p^{\alpha_p} \parallel k$, and let

$$m = \prod_{p \le k^2(k+1)^2} p^{2\alpha_p+2}. \tag{2}$$

By the Siegel–Walfisz Theorem (see for example [13, Corollary 5.29]), there are

$$\gg_k \left(\frac{H}{\log H}\right)^2$$

pairs of primes q, r such that $k^2(k+1)^2 < q, r \le H$, $q \ne r$ and $q \equiv r \equiv -1 \pmod{m}$. In particular, we then have $q \equiv r \equiv -1 \pmod{k}$ and $q \equiv r \equiv 3 \pmod{4}$, so by the law of quadratic reciprocity, for each such pair (q, r),

$$\text{either} \quad \left(\frac{q}{r}\right) = 1 = -\left(\frac{r}{q}\right) \quad \text{or} \quad \left(\frac{r}{q}\right) = 1 = -\left(\frac{q}{r}\right). \tag{3}$$

By interchanging the roles of q and r if necessary, we may assume without loss of generality that there are $\gg (H/\log H)^2$ such pairs (q, r) as above for which the first alternative in (3) holds true. It is then enough to show that for each such fixed pair (q, r) the Thue equation

$$qx^k - ry^k = 1 \tag{4}$$

has local solutions everywhere.

Since $q, r > 0$, there clearly are real solutions, so let us focus on p-adic solubility for any given rational prime p. Let us first discuss the case that $p \le k^2(k+1)^2$. In particular, p is then coprime to r. So in order to find a solution of (4) in $\mathbb{Z}_p$, by Lemma 2 it suffices to find a solution of the congruence

$$qx^k - ry^k \equiv 1 \pmod{p^{2\alpha_p+1}} \tag{5}$$

with p not dividing y. As $r \equiv -1 \pmod{m}$, by (2) also $r \equiv -1 \pmod{p^{2\alpha_p+1}}$, hence $x = 0$, $y = 1$ is such a solution. Next, let us assume that $p > k^2(k+1)^2$. Then $(p, k) = 1$, so $\alpha_p = 0$. If p is different from q and r, then Lemma 1 provides a non-singular solution of (5), which again, by Lemma 2, can be lifted to a solution of (4) over $\mathbb{Z}_p$. Finally, it remains to discuss the two cases $p = q$ and $p = r$. In both cases, $\alpha_p = 0$. For $p = q$, as above we need to find a solution of the congruence

$$-ry^k \equiv 1 \pmod{q}. \tag{6}$$

Now $q \equiv -1 \pmod{k}$, so by Lemma 3 this can be done provided that $(-r/q) = 1$, and the latter condition follows from $q \equiv 3 \pmod{4}$ and (3).

For $p = r$, we need to solve

$$qx^k \equiv 1 \pmod{r}.$$

Again, $r \equiv -1 \pmod{k}$, equation (3) and Lemma 3 provide a solution of the latter congruence. This finishes the proof of Lemma 4. ∎

Lemma 5. *We have*

$$M_{k,\mathrm{loc}}(H) \gg \left(\frac{H}{\log H}\right)^3.$$

Proof. The proof is similar to that of Lemma 4. We call a triple (p_1, p_2, p_3) of distinct primes p_i with $p_i \equiv 3 \pmod{4}$ $(1 \le i \le 3)$ *good* if there exists $i \in \{1, 2, 3\}$ such that

$$\left(\frac{p_i}{p_j}\right) = \left(\frac{p_i}{p_k}\right),$$

where $\{i, j, k\} = \{1, 2, 3\}$. Clearly, for any given quadruple (p_1, p_2, p_3, p_4) of distinct primes p_i with $p_i \equiv 3 \pmod{4}$ $(1 \le i \le 4)$, we can find three amongst them, say p_1, p_2, p_3, such that (p_1, p_2, p_3) is a good triple. Now define m by (2). Then by the Siegel–Walfisz Theorem, and the observation above, we can find

$$\gg_k \left(\frac{H}{\log H}\right)^3$$

triples of distinct primes q, r, s such that $k^2(k+1)^2 < q, r, s \le H$, $q \equiv r \equiv s \equiv -1 \pmod{m}$ and

$$\left(\frac{s}{q}\right) = \left(\frac{s}{r}\right). \tag{7}$$

Note that automatically $q \equiv r \equiv s \equiv -1 \pmod{k}$ and $q \equiv r \equiv s \equiv 3 \pmod{4}$. Now fix any such triple (q, r, s). Using (7), $q \equiv r \equiv s \equiv 3 \pmod{4}$ and the law of quadratic reciprocity, we find that either

$$\left(\frac{-rs}{q}\right) = \left(\frac{qs}{r}\right) = 1 \tag{8}$$

or

$$\left(\frac{-rs}{q}\right) = \left(\frac{qs}{r}\right) = -1. \tag{9}$$

In the first case, let us consider the equation

$$qx^k - ry^k - sz^k = 0. \tag{10}$$

There clearly are non-trivial real solutions, and for $p \le k^2(k+1)^2$ we can follow the argument from the proof of Lemma 4 to show that there are non-trivial p-adic zeros: As $q \equiv r \pmod{m}$, also $q \equiv r \pmod{p^{2\alpha_p+1}}$, so

$(x, y, z) = (1, 1, 0)$ is a solution of

$$qx^k - ry^k - sz^k \equiv 0 \pmod{p^{2\alpha_p+1}}, \tag{11}$$

which by Lemma 2 can be lifted to a non-trivial solution of (10) over $\mathbb{Z}_p$. If $p > k^2(k+1)^2$, then $\alpha_p = 0$. If in addition p is different from q, r, s, then we can set $z = 1$ and use Lemma 1 to find a non-singular solution of (11), which again by Lemma 2 lifts to a non-trivial solution of (10) over $\mathbb{Z}_p$, so it remains to discuss the case $p \in \{q, r, s\}$. Then $\alpha_p = 0$, so by Lemma 2 it suffices to find a non-singular solution of

$$qx^k - ry^k - sz^k \equiv 0 \pmod{p}.$$

If k is odd, this is easy, since the map $x \mapsto x^k$ is surjective modulo p, as $q \equiv r \equiv s \equiv -1 \pmod{k}$. For even k, by Lemma 3, it is enough to show that there exists a non-singular solution of

$$qx^2 - ry^2 - sz^2 \equiv 0 \pmod{p}. \tag{12}$$

For $p \in \{q, r\}$ this immediately follows from (8). For $p = s$, note that (7) and $q \equiv r \equiv s \equiv 3 \pmod{4}$ imply that

$$\left(\frac{qr}{s}\right) = 1,$$

again showing that (12) has a non-singular solution. (In fact, by the Hasse principle for ternary quadratic forms (see for example [18, Corollary 3, p. 43]), as we had already shown non-trivial local solubility of $qx^2 - ry^2 - sz^2 = 0$ over $\mathbb{R}$ and all local fields except possibly $\mathbb{Q}_s$, the existence of a non-trivial solution over $\mathbb{Q}_s$ would have followed automatically, but we preferred to show it directly.)

Let us briefly discuss the second case (9). Instead of (10), we now consider the equation

$$qx^k - ry^k + sz^k = 0.$$

The only slight difference then is the argument for $p \in \{q, r, s\}$ and even k. Again, we need to make sure that

$$qx^2 - ry^2 + sz^2 \equiv 0 \pmod{p}$$

has a non-singular solution, which reduces to checking that

$$\left(\frac{rs}{q}\right) = \left(\frac{-qs}{r}\right) = \left(\frac{qr}{s}\right) = 1,$$

and again these properties follow from $q \equiv r \equiv s \equiv 3 \pmod{4}$, (7) and (9). This finishes the proof of Lemma 5. ■

Regarding upper bounds, note that an application of the large sieve gives

$$M_{k,\mathrm{loc}}(H) \ll \frac{H^3}{(\log H)^{\Psi(k)}}$$

where

$$\Psi(k) = \frac{3}{\phi(k)}\left(1 - \frac{1}{k}\right)$$

and ϕ denotes Euler's totient function (see [5, Theorem 1.1]; for composite k, the bound could be improved somewhat). It would be interesting to decide what is the true order of magnitude for this quantity. In this direction, for $k = 2$, Hooley [12] and independently Guo [10] obtained the sharp bound $M_{2,\mathrm{loc}}(H) \gg H^3/(\log H)^{3/2}$.

3. The density of soluble Thue equations. To prove Theorem 1, it remains to bound the quantity $N_{k,\mathrm{glob}}(H)$ from above, assuming the truth of the *abc*-conjecture. To this end, in the case $k = 3$, we shall use the results of [7], whereas for larger k, an elementary argument will suffice. We shall prove the following result.

Lemma 6. *Assume the truth of the abc-conjecture. Then*

$$N_{k,\mathrm{glob}}(H) \ll \begin{cases} H^{47/27+\varepsilon} & \textit{for } k = 3, \\ H^{1+\varepsilon} & \textit{for } k \geq 4. \end{cases}$$

Proof. We begin with the following observation: let $a, b, x, y \in \mathbb{Z}$ where $0 < \max\{|a|, |b|\} \leq H$. Suppose that

$$ax^k + by^k = 1.$$

There are only $O(H)$ such equations where $xy = 0$ is possible, so in the following we may assume that $xy \neq 0$. If the *abc*-conjecture holds true, then

$$\max\{|ax^k|, |by^k|\} \ll \Bigl(\prod_{p \mid abx^ky^k} p\Bigr)^{1+\varepsilon} \ll |abxy|^{1+\varepsilon}. \tag{13}$$

By symmetry, without loss of generality, we can assume that $|y| \geq |x|$. Then

$$|y^k| \ll H^{1+\varepsilon}|x|^{1+\varepsilon}|y|^{1+\varepsilon} \ll H^{1+\varepsilon}|y|^{2+\varepsilon},$$

so

$$|y| \ll H^{1/(k-2)+\varepsilon}, \quad \text{whence also} \quad |x| \ll H^{1/(k-2)+\varepsilon}. \tag{14}$$

Next, let us recall the result from [7] that we will use. Let $N(X, Y, Z)$ be the number of quadruples $(a, b, x, y) \in \mathbb{N}^4$ satisfying

$$\begin{gathered} ax^k - by^k = 1, \\ X < x \leq 2X, \quad Y < y \leq 2Y \quad \text{and} \quad Z < by^k \leq 2Z. \end{gathered} \tag{15}$$

The following proposition summarizes the main technical result in [7]. Its proof relies on a recent version of the approximate determinant method by Heath-Brown (see [11]).

Proposition 1. *Suppose that $X \le Y \ll Z^{1/k} \ll XY$. Let M be a natural number satisfying*

$$\log Z \ge \log M \ge \max\left\{\frac{9}{2}(1+\delta)\frac{\log(ZX^{-k})\log Y}{\log Z}, \log Y\right\} \tag{16}$$

for a given $\delta > 0$. Then we have the estimate

$$N(X,Y,Z) \ll_{\delta,\varepsilon} Z^{\varepsilon}(XM^{1/2}+Y). \tag{17}$$

If instead $X \ge Y$, then the same holds with the roles of X and Y interchanged in (16) *and* (17).

Proposition 1 is valid for all $k \ge 3$, but in fact we shall only need it for $k = 3$. Indeed, if $k \ge 4$, then by (14) we immediately have

$$\begin{aligned} &N_{k,\mathrm{glob}}(H)\\ &\quad \le \#\{a,b,x,y \in \mathbb{Z} : 0 < |a|,|b| \le H,\ |x|,|y| \ll H^{1/2+\varepsilon},\ ax^k + by^k = 1\}\\ &\quad = \sum_{\substack{|x|,|y| \ll H^{1/2+\varepsilon}\\ (x,y)=1}} \#\{a,b \in \mathbb{Z} : 0 < |a|,|b| \le H,\ ax^k + by^k = 1\}\\ &\quad \ll \sum_{|x|,|y| \ll H^{1/2+\varepsilon}} \left(1 + \frac{H}{\max\{|x|^k, |y|^k\}}\right) \ll H^{1+\varepsilon}, \end{aligned}$$

as asserted in Lemma 6.

We continue the proof of the lemma. In view of Proposition 1, it will now be more convenient to study the quantity

$$\begin{aligned} N^{+}_{k,\mathrm{glob}}(H) = \#\{a,b \in \mathbb{N} : a,b \le H \text{ and } ax^k - by^k = 1\\ \text{has a solution } (x,y) \in \mathbb{N}^2\}. \end{aligned}$$

We certainly have $N_{k,\mathrm{glob}}(H) \ll N^{+}_{k,\mathrm{glob}}(H)$. From now on, we let $k = 3$. Again, by (14) we have

$$\begin{aligned} N^{+}_{3,\mathrm{glob}}(H) &\le \#\{a,b,x,y \in \mathbb{N} : a,b \le H,\ x,y \ll H^{1+\varepsilon},\ ax^3 - by^3 = 1\}\\ &= \sum_{x,y \ll H^{1+\varepsilon}} \#\{a,b \in \mathbb{N} : a,b \le H,\ ax^3 - by^3 = 1\}. \end{aligned}$$

For a parameter Q to be specified at a later stage, we shall estimate separately the contributions to $N^{+}_{3,\mathrm{glob}}(H)$ from terms with $xy \le Q$ and terms with $xy > Q$. The contribution from the first range is

$$\ll \sum_{xy \le Q} \left(1 + \frac{H}{\max\{x^3, y^3\}}\right) \ll Q\log Q + H. \tag{18}$$

For the remaining range, we shall use Proposition 1. Indeed, partitioning the ranges for x, y and by^k into dyadic intervals, we obtain

$$\sum_{x,y\ll H^{1+\varepsilon}} \#\{a,b\in\mathbb{N} : a,b\le H,\ ax^3-by^3=1\} \ll H^{\varepsilon} \max_{X,Y,Z} N(X,Y,Z),$$

where the maximum is taken over X,Y,Z satisfying the conditions

$$Z\ll H^{4+\varepsilon},\quad X,Y\ll H^{1+\varepsilon},\quad XY\gg Q.$$

Thus, let X,Y,Z as above be fixed such that $N(X,Y,Z)$ is maximal. Without loss of generality, we may assume that $X\le Y\ll Z^{1/3}$, so if we require $Q\gg H^{4/3+\varepsilon}$, then Proposition 1 is applicable. Let us write $Z=H^{\tau}$, where $\tau\le 4+\varepsilon$. If $Q=H^{\gamma}$, then we may further write $X\approx Z^{\alpha}$ and $Y\approx Z^{\beta}$, where

$$\alpha\le\beta\le\min\{1/3,1/\tau\},\qquad \alpha+\beta\ge\gamma/\tau. \tag{19}$$

In view of (16), we choose δ, depending on ε, such that

$$\frac{9}{2}\delta(1-3\alpha)\beta\le\varepsilon,$$

and we take $M\in\mathbb{N}$ to satisfy

$$\max\{Z^{9(1+\delta)(1-3\alpha)\beta/2},Z^{\beta}\}\le M\ll\max\{Z^{9(1+\delta)(1-3\alpha)\beta/2},Z^{\beta}\}. \tag{20}$$

Provided that $M\le Z$, the estimate (17) then yields

$$\begin{aligned} N(X,Y,Z) &\ll Z^{\varepsilon}(Z^{\alpha+9(1-3\alpha)\beta/4}+Z^{\alpha+\beta/2}+Z^{\beta})\\ &\ll H^{\varepsilon}(H^{u+9(1-3u/4)v/4}+H^{u+v/2}+H^{v}),\end{aligned}$$

where we have put $u=\tau\alpha$ and $v=\tau\beta$ and used $\tau\le 4+\varepsilon$. For u and v, we have the restrictions

$$u\le v\le 1,\qquad u+v\ge\gamma. \tag{21}$$

The two terms $H^{u+v/2}$ and H^{v} now obviously give negligible contributions to $N^{+}_{3,\mathrm{glob}}(H)$. Moreover, for u,v satisfying the inequalities (21), the function

$$\Psi(u,v)=u+\frac{9}{4}\left(1-\frac{3}{4}u\right)v$$

appearing in the exponent of the remaining term satisfies

$$\Psi(u,v)\le\Psi(u,1)=\frac{9}{4}-\frac{11}{16}u\le\frac{9}{4}-\frac{11}{16}(\gamma-1)=\frac{47-11\gamma}{16}.$$

In view of the estimate (18), we optimize by equating the rightmost expression to γ, taking $\gamma=47/27$. To establish the estimate $N_{3,\mathrm{glob}}(H)\ll H^{47/27+\varepsilon}$, it only remains to justify the assumption $M\le Z$. To this end, we analyze the quantity

$$\Phi(\alpha,\beta)=\frac{9}{2}(1-3\alpha)\beta$$

appearing in (20). Note that the assumptions (19) imply $\alpha \geq (\gamma - 1)/\tau = 20/(27\tau)$, so that

$$\varPhi(\alpha, \beta) \leq \frac{9}{2\tau}(1 - 3\alpha) \leq \frac{9}{2\tau}\left(1 - \frac{20}{9\tau}\right) = g\left(\frac{1}{\tau}\right),$$

say, where $g(t) = \frac{9}{2}t\bigl(1 - \frac{20}{9}t\bigr)$. As the quadratic function g is decreasing for $t \geq 9/40$, we have

$$\varPhi(\alpha, \beta) \leq g(1/(4+\varepsilon)) \leq g(9/40) = 81/160 < 1,$$

so we may certainly ensure that $M \leq Z$ by choosing δ small enough. This finishes the proof of Lemma 6. ■

4. The density of soluble Fermat equations. As in Section 3, to prove Theorem 2, it remains to establish an upper bound for $M_{k,\mathrm{glob}}(H)$ as given in the following result.

LEMMA 7. *Let $k \geq 6$, and assume the truth of the abc-conjecture. Then*

$$M_{k,\mathrm{glob}}(H) \ll H^{2+\varepsilon}.$$

Proof. For technical reasons, it is easier to first deal with the quantity

$$M_{k,\mathrm{glob,prim}}(H) = \#\{a, b, c \in \mathbb{Z} : (a, b, c) = 1,\ 0 < |a|, |b|, |c| \leq H \text{ and } ax^k + by^k + cz^k = 0 \text{ has a solution } (x, y, z) \in \mathbb{Z}^3 \setminus \{\mathbf{0}\}\}$$

focusing on Fermat equations $ax^k + by^k + cz^k = 0$ with primitive coefficient vector (a, b, c). Under the assumptions of Lemma 7, we will show that

$$M_{k,\mathrm{glob,prim}}(H) \ll H^{2+\varepsilon}. \tag{22}$$

Now the equation $ax^k + by^k + cz^k = 0$ has a non-trivial integer solution (x, y, z) if and only if the equation

$$\frac{a}{\gamma}x^k + \frac{b}{\gamma}y^k + \frac{c}{\gamma}z^k = 0$$

has one, where $\gamma = (a, b, c)$. Therefore, it is easy to deduce Lemma 7 from (22) via

$$M_{k,\mathrm{glob}}(H) \leq \sum_{\gamma \leq H} M_{k,\mathrm{glob,prim}}\left(\frac{H}{\gamma}\right) \ll \sum_{\gamma \leq H}\left(\frac{H}{\gamma}\right)^{2+\varepsilon} \ll H^{2+\varepsilon}.$$

Thus it remains to prove (22), so suppose that $ax^k + by^k + cz^k = 0$ has a solution $(x, y, z) \in \mathbb{Z}^3 \setminus \{\mathbf{0}\}$. Since the equation is homogeneous, we can assume without loss of generality that $(x, y, z) = 1$. If $xyz = 0$, then $\max\{|x|, |y|, |z|\} \ll H^{1/k}$, otherwise put $u = ax^k$, $v = by^k$, $w = cz^k$, and let γ be the greatest common divisor of u, v, w. Now if $p^g \| \gamma$ for some prime power p^g, then p^g must divide one of a, b, c, because $(x, y, z) = 1$. Therefore, γ divides abc, so

$$\prod_{p \mid u/\gamma \cdot v/\gamma \cdot w/\gamma} p \leq \prod_{p \mid abc/\gamma} p \cdot \prod_{p \mid x^k y^k z^k} p \leq \frac{|abcxyz|}{\gamma}.$$

Let us now assume without loss of generality that $|x| \geq |y|$ and $|x| \geq |z|$. As $u/\gamma + v/\gamma + w/\gamma = 0$, by the *abc*-conjecture we obtain

$$\frac{|u|}{\gamma} \ll \left(\frac{|abcxyz|}{\gamma}\right)^{1+\varepsilon},$$

so

$$\max\{|x|, |y|, |z|\} \ll H^{2/(k-3)+\varepsilon}.$$

Consequently,

$$\begin{aligned} M_{k,\mathrm{glob,prim}}(H) \leq \#\{&a, b, c, x, y, z \in \mathbb{Z} : (a, b, c) = (x, y, z) = 1, \\ &|a|, |b|, |c| \leq H,\ |x|, |y|, |z| \ll H^{2/(k-3)+\varepsilon},\ \text{and } ax^k + by^k + cz^k = 0\}. \end{aligned}$$

Now for fixed x, y, z with $(x, y, z) = 1$, the integer solutions (a, b, c) of the equation $ax^k + by^k + cz^k = 0$ lie on a two-dimensional lattice Γ of determinant

$$\Delta_{x,y,z} \gg \max\{|x|^k, |y|^k, |z|^k\} \tag{23}$$

(see [4, Lemma 4.4]), and by [4, Lemma 4.5], the number of such primitive solutions (a, b, c) with $|a|, |b|, |c| \leq H$ is at most of the order of magnitude

$$1 + H^2/\Delta_{x,y,z}. \tag{24}$$

Hence the contribution to $M_{k,\mathrm{glob,prim}}(H)$ coming from those x, y, z giving $\Delta_{x,y,z} \geq H^2$ is at most the order of magnitude $O(H^{6/(k-3)+\varepsilon})$ of all permissible (x, y, z) stemming from the bound $|x|, |y|, |z| \leq H^{2/(k-3)+\varepsilon}$. Since $k \geq 6$, this is compatible with (22). Let us now bound the contribution from smaller $\Delta_{x,y,z}$. To this end, fix $A \in [1, H^2]$. By (23), the number of $x, y, z \in \mathbb{Z}$ such that $A \leq \Delta_{x,y,z} \leq 2A$ is at most $O(A^{3/k})$, and for such fixed x, y, z, by (24), there are at most $O(H^2/A)$ corresponding (a, b, c). The total contribution from $A \leq \Delta \leq 2A$ is therefore $O(H^2 A^{3/k-1})$. A dyadic summation over the range of A, keeping in mind that $k \geq 6$, therefore again gives the bound $O(H^{2+\varepsilon})$ as claimed in (22). This finishes the proof of Lemma 7. ■

References

[1] M. Bhargava, *Most hyperelliptic curves over $\mathbb{Q}$ have no rational points*, arXiv: 1308.0395 (2013).

[2] M. Bhargava, *A positive proportion of plane cubics fail the Hasse principle*, arXiv: 1402.1131 (2014).

[3] R. de la Bretèche and T. D. Browning, *Density of Châtelet surfaces failing the Hasse principle*, Proc. London Math. Soc. (3) 108 (2014), 1030–1078.

[4] T. D. Browning, *Quantitative Arithmetic of Projective Varieties*, Progr. Math. 277, Birkhäuser, Basel, 2009.

[5] T. D. Browning and R. Dietmann, *Solubility of Fermat equations*, in: Quadratic Forms—Algebra, Arithmetic, and Geometry, Contemp. Math. 493, Amer. Math. Soc., Providence, RI, 2009, 99–106.

[6] J. Brüdern and R. Dietmann, *Random Diophantine equations, I*, Adv. Math. 256 (2014), 18–45.

[7] R. Dietmann and O. Marmon, *The density of twins of k-free numbers*, Bull. London Math. Soc. 46 (2014), 818–826.

[8] A. Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*, Int. Math. Res. Notices 2007, no. 8, art. ID 027, 24 pp.

[9] M. J. Greenberg, *Lectures on Forms in Many Variables*, W. A. Benjamin, New York, 1969.

[10] C. R. Guo, *On solvability of ternary quadratic forms*, Proc. London Math. Soc. (3) 70 (1995), 241–263.

[11] D. R. Heath-Brown, *Square-free values of $n^2 + 1$*, Acta Arith. 155 (2012), 1–13.

[12] C. Hooley, *On ternary quadratic forms that represent zero*, Glasgow Math. J. 35 (1993), 13–23.

[13] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[14] D. W. Masser, *Open problems*, in: W. W. L. Chen (ed.), Proc. Sympos. on Analytic Number Theory, Imperial College, London, 1985.

[15] L. J. Mordell, *The number of solutions of some congruences in two variables*, Math. Z. 37 (1933), 193–209.

[16] B. Poonen and J. F. Voloch, *Random Diophantine equations*, in: Arithmetic of Higher-Dimensional Algebraic Varieties (Palo Alto, CA, 2002), Progr. Math. 226, Birkhäuser Boston, Boston, MA, 2004, 175–184.

[17] E. S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. 85 (1951), 203–362.

[18] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, New York, 1973.

Rainer Dietmann
Department of Mathematics
Royal Holloway, University of London
Egham TW20 0EX, UK
E-mail: Rainer.Dietmann@rhul.ac.uk

Oscar Marmon
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen, Germany
E-mail: omarmon@uni-math.gwdg.de

Received on 14.8.2014 (7898)