ACTA ARITHMETICA
LX.3 (1992)

Finding integers k for which a given Diophantine equation has no solution in kth powers of integers

by

Andrew Granville* (Princeton, N.J.)

1. Introduction. For a given polynomial $f(X_1, X_2, \dots, X_n) \in \mathbb{Z}[X_1, X_2, \dots, X_n]$ we shall investigate the set $T(f)$ of exponents k for which the Diophantine equation

$$f(x_1^k, x_2^k, \dots, x_n^k) = 0 \tag{1}$$

has solutions in non-zero integers $x_1, x_2, \dots, x_n$. For homogeneous diagonal f of degree one, Davenport and Lewis [DL] showed that $k \in T(f)$ whenever $(n-1)^{1/2} \geq k \geq 18$; however, Ankeny and Erdős [AE] showed that $T(f)$ has zero density in the set of all positive integers provided that all distinct subsets of the set of coefficients of f have different sums. For general polynomials f, Ribenboim [Ri] showed that certain values of k cannot belong to $T(f)$, and the result of Ankeny and Erdős shows that $T(f)$ has zero density, under the same conditions on its coefficients as above (this may be seen by replacing the jth monomial in f by a new variable Y_j to get a new homogeneous polynomial of degree 1).

In the next section we shall introduce a technical condition on polynomials that we call *admissibility*. All polynomials with distinct coefficient sums (as above) are admissible, as well as many others—for example, $f(X, Y, Z) = X + 2Y^2 + 3Z^2$. We shall prove

Theorem 1. *Suppose that $f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ is an admissible polynomial. The Diophantine equation $f(x_1^k, \dots, x_n^k) = 0$ has solutions in non-zero integers $x_1, \dots, x_n$ for $o(x)$ exponents $k \leq x$.*

Remark. The bound $o(x)$, in Theorem 1, may be improved to $O(x/\log^c x)$ for some fixed $c > 0$.

The proof is based on that of Ankeny and Erdős, though its roots lie in much earlier work of Sophie Germain. There are a number of innovations

* The author is supported, in part, by the National Science Foundation (grant number DMS-8610730).

here: In particular, we use a result of Conway and Jones [CJ] to obtain all sets $\zeta_1, \zeta_2, \dots, \zeta_n$ of roots of unity, such that

$$f(\zeta_1, \zeta_2, \dots, \zeta_n) = 0\,. \tag{2}$$

In the special case that f is homogeneous in three variables, Faltings' Theorem [Fa] tells us that (1) has only finitely many non-trivial, coprime solutions, for all sufficiently large k. Then we can prove that $T(f)$ has zero density by using the arguments of [G3] or [HB].

In [AHB], Adleman and Heath-Brown showed how to obtain results (in a related example) for prime exponents k. Their method gives

THEOREM 2. *If f is an admissible, homogeneous polynomial in three variables then the Diophantine equation $f(x_1^p, x_2^p, x_3^p) = 0$ has no solution in non-zero integers x_1, x_2, x_3 for $\gg x^{2/3}$ primes $p \le x$.*

It is possible to extend our results to arbitrary number fields; the necessary modifications in the proofs are straightforward. In the ring of polynomials, much better results have been obtained: First note that a 'non-trivial' solution of (1) with each $x_j \in \mathbb{C}[t]$ generates a 'non-trivial' solution of

$$z_1^k + z_2^k + \ldots + z_r^k = 0$$

with each $z_j \in \mathbb{C}[t]$, where r is the number of monomials of f. Newman and Slater [NS] showed that this equation has no 'non-trivial' solutions for $k \ge 8r^2$; and this may be improved to $k \ge (r-1)^2$, by an immediate application of the main result of [BM]. On the other hand, 'non-trivial' solutions can be constructed whenever $k \le (r^2 - r)/4$. We are thus close to determining precisely for which values of k and r this equation has a non-trivial solution.

Acknowledgments. The main ideas of this paper were part of the author's doctoral thesis, completed under the supervision of Dr. Paulo Ribenboim at Queen's University in the summer of 1987. I would also like to thank Professor Bombieri for a few suggestions.

2. Notation and definitions. Throughout we shall assume that the polynomial f is written in the form

$$f(X_1, X_2, \dots, X_n) = \sum_{i=1}^{r} a_i f_i(X_1, X_2, \dots, X_n)$$

where each a_i is a non-zero integer (or a complex number in Section 6), and each f_i takes the form

$$f_i(X_1, X_2, \dots, X_n) = X_1^{e_{i,1}} X_2^{e_{i,2}} \dots X_n^{e_{i,n}}\,,$$

with each $e_{i,j}$ a non-negative integer. For any subset I of $\{1, 2, \dots, r\}$ define

$$f_I(X_1, X_2, \dots, X_n) := \sum_{i \in I} a_i f_i(X_1, X_2, \dots, X_n)\,.$$

We define f to be *admissible* if the largest power of t that divides the polynomial $f(x_1, \dots, x_n)$ equals the minimum of the degrees of the $f_i(x_1, \dots, x_n)$, whenever each x_j equals $\pm$ a non-negative power of the variable t. The admissibility of a given f can be determined as follows:

We start by defining $R(f)$ to be the set of subsets I of $\{1, 2, \dots, r\}$ for which there exist non-negative integers $d_1, d_2, \dots, d_n$ such that

$$\sum_{j=1}^{n} e_{i,j} d_j \quad = d \text{ (if } i \in I)\,, \quad > d \text{ (otherwise)}\,. \tag{3}$$

In the 1820s Fourier outlined a method that allows one to compute whether a solution to such a system exists (see p. 241 of [Ch]). A more efficient (and modern) method would be to re-express (3) as a linear programming problem and then apply the simplex algorithm to the associated auxiliary problem ([Ch], p. 39) to determine whether feasible values of d_j exist. Thus the set $R(f)$ may be constructed.

From here we simply need to test whether $f_I(x_1, \dots, x_n) = 0$ for some $I \in R(f)$ and some choice of the x_i's as -1 or 1; as there are only 2^n possible choices for the x_i's and $R(f)$ is already determined, we thus have a finite algorithm to determine admissibility.

Finally, we define $A(f) := \sum_{i=1}^{r} |a_i|$, and $N(f) := n - 1$ if f is homogeneous, n otherwise.

3. The main results. The main result that we shall prove is

PROPOSITION 1. *For any polynomial f with integer coefficients, there exists a finite set of integers $B(f)$ with the following property: If m is a positive integer that is not divisible by any element of $B(f)$, then the Diophantine equation $f(x_1^k, \dots, x_n^k) = 0$ has no solutions in non-zero integers $x_1, \dots, x_n$, whenever $q := mk + 1$ is a sufficiently large prime.*

Remark. The exceptional primes q in Proposition 1 all belong to a set, $Q(f, m)$, which we obtain explicitly in the proof.

Proposition 1 improves results from [AE] and [Ri] (it holds for more polynomials than the analogous result in [AE]; and for more values of m than the analogous result in [Ri]). It is based on the following, famous result of Sophie Germain:

If m is a positive integer not divisible by 3, *then there are no solutions in integers x, y, z to $x^k + y^k = z^k$ with* $\gcd(k, xyz) = 1$, *whenever $q := mk + 1$ is a sufficiently large prime.*

Again the exceptional primes q may be obtained explicitly—they are the set of prime divisors of norms of sums of three mth roots of unity—compare this with the definition of $Q(f,m)$ below.

It seems likely that for any admissible f, (1) has no non-zero solutions for all sufficiently large k. This is equivalent to (1) having no non-zero solutions for all sufficiently large prime powers k. By a method similar to Proposition 1 we can obtain

THEOREM 3. *For any polynomial f with integer coefficients, there exists a finite set of integers $B(f)$ with the following property: If p is a prime that does not divide $a_1a_2\dots a_r$ and such that $p-1$ is not divisible by any element of $B(f)$, then* (1) *has no solutions in non-zero integers $x_1,x_2,\dots,x_n$ for $k=p^t$, whenever $t\ge \log A(f)\phi(p-1)/\log p$.*

Remark. The set $B(f)$, of the two results above, is constructed below. It turns out that f is admissible if and only if neither 1 nor 2 belong to $B(f)$—thus Proposition 1 and Theorem 3 are both uninteresting for inadmissible polynomials.

The proofs of both of these results rely on the following proposition, which we shall prove in Section 5:

PROPOSITION 2. *For any polynomial f with integer coefficients, there exists a finite set of integers $\beta(f)$ with the following property: There exist m-th roots of unity $\zeta_1,\zeta_2,\dots,\zeta_n$ satisfying $f(\zeta_1,\zeta_2,\dots,\zeta_n)=0$ if and only if m is divisible by some element of $\beta(f)$.*

Moreover, we can explicitly compute the set $\beta(f)$.

From this we can present the

Proof of Proposition 1. Let $B(f)$ be the union of the $\beta(f_I)$, taken over all $I\in R(f)$. For each positive integer m, let $Q(f,m)$ be the set of prime divisors of $a_1a_2\dots a_r$ together with the set of prime power divisors of the norms (over $\mathbb{Q}(\zeta_m)|\mathbb{Q}$) of all algebraic numbers of the form

$$f_I(\zeta_1,\zeta_2,\dots,\zeta_n) \tag{4}$$

where $\zeta_1,\zeta_2,\dots,\zeta_n$ are mth roots of unity, and $I\in R(f)$.

We see that $Q(f,m)$ can be determined from computing a finite list of norms, and so is finite if and only if each such norm is non-zero. However, a norm is zero only when some $f_I(\zeta_1,\zeta_2,\dots,\zeta_n)$ equals zero, and this happens only for $m\in B(f)$ by Proposition 2.

We will suppose that m and q are chosen as in the hypothesis so that m is not divisible by any element of $B(f)$, and q $(:=mk+1)$ is a prime not in the set $Q(f,m)$.

Now assume that there exists a solution of (1) in non-negative integers $x_1,x_2,\dots,x_n$.

Let q^d be the largest power of q dividing every $f_i(x_1,\dots,x_n)$, and let I be the set of values of i for which $f_i(x_1,\dots,x_n)$ is divisible by q^d but not q^{d+1}. By writing each x_j in the form $q^{d_j}z_j$, where q does not divide z_j, we see that $I \in R(f)$ (from (3)). Moreover, as q does not divide $a_1a_2\dots a_r$, and as $f_i(x_1^k,\dots,x_n^k) = f_i(x_1,\dots,x_n)^k$ for each i, we see that

$$\begin{aligned} q^{dk}f_I(z_1^k,z_2^k,\dots,z_n^k) &= f_I(x_1^k,x_2^k,\dots,x_n^k) \\ &\equiv f(x_1^k,x_2^k,\dots,x_n^k) = 0 \pmod{q^{dk+1}}, \end{aligned}$$

and so

$$q \text{ divides } f_I(z_1^k,z_2^k,\dots,z_n^k) \text{ but not } z_1,z_2,\dots,z_n\,. \tag{5}$$

Let ζ be a primitive mth root of unity, and let g be an integer that has order m modulo q. By Fermat's little theorem we know that each z_j^k is an mth root of 1 $(\mathrm{mod}\, q)$, and so there exist integers $l_1,\dots,l_n$ such that $z_j^k \equiv g^{l_j} \pmod q$ for each j. But then, by (5),

$$\begin{aligned} f_I(\zeta^{l_1},\dots,\zeta^{l_n}) &\equiv f_I(g^{l_1},\dots,g^{l_n}) \\ &\equiv f_I(z_1^k,\dots,z_n^k) \equiv 0 \pmod{(q,g-\zeta)}, \end{aligned}$$

where $(q,g-\zeta)$ is the ideal of $\mathbb{Q}(\zeta)$ generated by q and $g-\zeta$. Thus the norm of $f_I(\zeta^{l_1},\dots,\zeta^{l_n})$ (which we will denote by N) belongs to the ideal $(q,g-\zeta)$. However, N is an integer and so must also belong to each conjugate of the ideal $(q,g-\zeta)$. It is easily seen that any two such conjugate ideals are coprime, and so N must belong to their product, $(q,\phi_m(g))$ (where $\phi_m(g)$ is the mth cyclotomic polynomial). However, q evidently divides $\phi_m(g)$ (by the definition of g), and so q divides N. Therefore q must belong to the set $Q(f,m)$ (by definition), which gives a contradiction.

A sketch of the proof of Theorem 3. Suppose that there is a solution of (1) in non-zero integers $x_1,\dots,x_n$ for $k = p^t$, with $t \geq \log A(f)\phi(p-1)/\log p$. As in the proof above we can show that

$$f_I(z_1^{p^t},z_2^{p^t},\dots,z_n^{p^t}) \equiv 0 \pmod q,$$

for some $I \in R(f)$, where $q = p^{t+1}$ and each z_j is the largest divisor of x_j that is not divisible by p. Then, as each $z_j^{p^t}$ is a $(p-1)$th root of 1 $(\mathrm{mod}\, q)$ by Euler's generalization of Fermat's little theorem, we can show that q belongs to the set $Q(f,p-1)$ (as in the proof above). Now $Q(f,p-1)$ is finite (as $p-1$ is not divisible by any element of $B(f)$), and its elements either divide one of $a_1,\dots,a_r$ (and so are certainly less than $A(f)$) or divide some norm of an algebraic number of the form (4). However, an algebraic number of the form (4) has magnitude $\leq A(f_I) \leq A(f)$ (as each monomial $f_i(\zeta_1,\dots,\zeta_n)$ has absolute value 1); thus its norm has magnitude $\leq A(f)^{\phi(p-1)}$, as the

norm is the product of $\phi(p-1)$ algebraic numbers of the form (4). But then

$$t < \log q/\log p \le \log A(f)\phi(p-1)/\log p$$

contradicting the hypothesis.

The argument at the end of the proof of Theorem 3 may be extended to any non-zero norm of an algebraic number of the form (4); thus any such norm is of magnitude $\le A(f)^{\phi(m)}$. Moreover, if we multiply together all algebraic numbers of the form (4) then we get an integer (by Newton's Law of Symmetric Polynomials) that is $\le A(f)^{m^n}$, and so $Q(f,m)$ contains $\ll_f m^n$ elements. If f is homogeneous then the elements of $Q(f,m)$ each divide the product of all algebraic numbers of the form (4) with ζ_1 fixed to be 1: this follows as the norm of $f_I(\zeta_1,\zeta_2,\dots,\zeta_n)$ equals the norm of $f_I(1,\zeta_2\zeta_1^{-1},\dots,\zeta_n\zeta_1^{-1})$. Therefore $Q(f,m)$ contains $\ll_f m^{n-1}$ elements. To summarize we have proved

Lemma 1. *For any given polynomial f and integer m not divisible by any element of $B(f)$, the set $Q(f,m)$ has $\ll_f m^{N(f)}$ elements, and each of these elements is $\le A(f)^{\phi(m)}$.*

4. Analytic results. The proofs of Theorems 1 and 2

A sketch of the proof of Theorem 1. Given any constant $c>0$ and any finite set of integers B, each ≥ 3, define K to be the set of integers k, free of prime factors $\le \log\log k$, for which there exists a prime $q \equiv 1 \pmod k$, with $q \le ck\log k$ and $(q-1)/k$ not divisible by any element of B. In the proof of Theorem 2 in [AE] it is shown that, for $B=\{4\}$, the set of multiples of elements of K has density one in the set of integers; a proof of this result for an arbitrary set B presents no additional difficulties.

Now, for a given admissible polynomial f, let $c = 2/\log A(f)$ and $B = B(f)$. For any given $k \in K$, define $m=(q-1)/k$, where q is as in the paragraph above. By Lemma 1 we see that the hypothesis of Proposition 1 is satisfied and so (1) has no non-zero solutions for exponent k, nor for any exponent which is an integer multiple of k. Theorem 1 then follows from the result quoted in the paragraph above.

A sketch of the proof of Theorem 2. In [G2] (Theorem 5(ii)) we proved the following generalization of the main result of [AHB]:

Lemma 2. *Suppose that the polynomial f is given. Suppose further that there exists a value of θ in the range $1-1/(N(f)+1) < \theta < 1$ for which there are $\gg \pi(x)$ prime pairs p,q with $q \equiv 1 \pmod p$, $x^\theta < p < q \le x$ and with $q-1$ not divisible by any element of $B(f)$. Then there are $\gg x^\theta$ primes $k \le x$ for which (1) has no non-zero integer solutions.*

In [Fo], Fouvry established such an estimate for $\theta = 0.6687$ and $B = \{3\}$, which allowed Adleman and Heath-Brown [AHB] to prove that the first case of Fermat's Last Theorem is true for infinitely many prime exponents. The proof in [Fo] should allow us to establish such an estimate for $\theta = 0.6687$ and all finite sets B that do not contain either 1 or 2. Theorem 2 then follows from Lemma 2.

5. Solving Diophantine equations using only roots of unity. Define $e(x) := e^{2i\pi x}$ and, for any given polynomial f, let R be the product of the primes $\le r$. By using a result in [CJ] we shall indicate how to find all solutions of (2) in roots of unity; Proposition 2 then follows easily.

PROPOSITION 3. *Given $f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ we may construct all solutions of* (2) *in roots of unity $\zeta_1, \dots, \zeta_n$. More precisely, every solution of* (2) *is part of a parametric family of the form*

$$\zeta_i = e(b_i + L_i(p_1, p_2, \dots, p_r, t_1, t_2, \dots, t_n)), \quad i = 1, 2, \dots, n\,, \tag{6}$$

where all possibilities for the rationals $b_1, \dots, b_n$ and the linear functions $L_1, \dots, L_n$ may be computed, and $p_1, \dots, p_r$ are arbitrary integer parameters, $t_1, \dots, t_n$ are arbitrary rational parameters.

Proof. In [CJ] Theorem 3 it is shown that any solution of

$$a_1 e(\theta_1) + a_2 e(\theta_2) + \ldots + a_r e(\theta_r) = 0\,, \tag{7}$$

with each θ_j rational, is contained in one of the parametric families

$$\theta_i = p_i + q_{u(i)} + v(i)/R\,, \quad i = 1, 2, \dots, r\,, \tag{8}$$

where $p_1, \dots, p_r$ are arbitrary integer parameters, $q_1, \dots, q_r$ are arbitrary rational parameters and u and v are a pair of functions satisfying

$$u:\ \{1, 2, \dots, r\} \to \{1, 2, \dots, r\}\,, \quad v : \{1, 2, \dots, r\} \to \{0, 1, 2, \dots, R-1\}\,.$$

Moreover, for each $k = 1, 2, \dots, r$,

$$\sum_{u(i)=k} a_i e(v(i)/R) = 0\,.$$

Such a condition is easily verified computationally, so that all possible pairs u, v may be determined.

Now suppose that $\zeta_1, \zeta_2, \dots, \zeta_n$ satisfy (2) where each $\zeta_j = e(\phi_j)$ for some rational ϕ_j. Then

$$\theta_i = \sum_{j=1}^{n} e_{i,j}\phi_j\,, \quad i = 1, 2, \dots, r\,,$$

provides a solution of (7) and, by substituting this into any one of the possibilities for (8) and then solving the resulting system of linear equations,

we find that either there are no solutions or

$$\phi_j = b_j + K_j(p_1, \dots, p_r, q_1, \dots, q_r, s_1, \dots, s_n)$$

for each j, where the K_j are some computable linear forms with $s_1, \dots, s_n$ some arbitrary rational parameters. Finally, note that the rational parameters may certainly be re-parametrized in terms of $\le n$ rational parameters as there are only n forms, and so we obtain (6).

The proof of Proposition 2. Define T to be the least common multiple of the denominators of all the b_i and of all the coefficients of L_i over every possibility in (6): This may be computed by Proposition 3. We shall obtain, from any solution of (2) in mth roots of unity, a solution of (2) in gth roots of unity where $g = \gcd(m, T)$. Thus, by observing that any bth root of unity is also an mth root of unity if b divides m, we see that one can take $\beta(f)$ to be simply the set of divisors b of T for which (2) has a solution in bth roots of unity. This set can be found explicitly, for instance, by simply trying out all sets of Tth roots of unity $\zeta_1, \zeta_2, \dots, \zeta_n$ in (2).

So suppose that we have a solution of (2) with $\zeta_i = e(c_i/m)$ where each c_i is an integer. Let $m = gd$ where $g = \gcd(m, T)$ and so, by Proposition 3,

$$Tb_i + TL_i(p_1, \dots, p_r, t_1, \dots, t_n) = \frac{T}{g}\frac{c_i}{d} \quad \text{for } i = 1, 2, \dots, n$$

for certain choices of integers $p_1, \dots, p_r$ and rationals $t_1, \dots, t_n$. We now select an integer y such that $y \equiv 0 \pmod d$ and $y \equiv 1 \pmod{T/g}$. (This is possible, by the Chinese Remainder Theorem, as $(d, T/g) = 1$.) Then taking $q_i = yp_i$ and $u_j = yt_j$ for each i and j we have another choice of parameters, giving

$$\begin{aligned} Tb_i + TL_i(q_1, \dots, q_r, u_1, \dots, u_n) &= Tb_i + yTL_i(p_1, \dots, p_r, t_1, \dots, t_n) \\ &= k_i(T/g) \end{aligned}$$

where k_i is the integer $c_i(y/d) - Tb_i((y-1)/(T/g))$. But by Proposition 3 this provides a solution to (2) (where $\zeta_i = e(k_i/g)$ for each i) in gth roots of unity.

Remark. A rather more pedestrian proof of Proposition 2 appeared in my thesis [G1]. We also gave there a different, non-constructive proof:

Let M $(= M(f))$ be the set of integers m for which there exist mth roots of unity $\zeta_1, \zeta_2, \dots, \zeta_n$ satisfying (2). Call $B \subset M$ a *basis* for M if every element of M is divisible by an element of B. Again, by noting that any bth root of unity is an mth root of unity whenever b divides m, we see that M is precisely the set of multiples of elements of B.

Our proof comes in two steps. First we use elementary facts about roots of unity (see, for instance, (2.2) and (2.3) of [L] or Corollary 1.1 of [M]) to observe that if $a_1, a_2, \dots, a_r$ are integers and $\zeta_1, \zeta_2, \dots, \zeta_r$ are roots of unity

such that

$$a_1\zeta_1 + a_2\zeta_2 + \ldots + a_r\zeta_r = 0\,,$$

then

$$a_1\zeta_1^p + a_2\zeta_2^p + \ldots + a_r\zeta_r^p = 0$$

for each prime $p > r$. Therefore if $\zeta_1, \zeta_2, \ldots, \zeta_n$ are mth roots of unity satisfying (2) then $\zeta_1^{m/b}, \zeta_2^{m/b}, \ldots, \zeta_n^{m/b}$ are bth roots of unity satisfying (2), where b is the largest divisor of m that is free of prime factors $> r$. Thus C, the subset of integers in M that have only prime factors that are $\le r$, forms a basis for M. We now use an old result of Mann [M] to show that C, and so M, has a finite basis:

If C does not have a finite basis then it contains an infinite sequence of integers $c_1, c_2, \ldots$ such that c_i does not divide c_j whenever $i \ne j$. We construct a vector v_i from each c_i, the jth component of which is the exact power of p_j dividing c_i, where p_j is the jth smallest prime (note that the number of components of v_i is just k, the number of primes $\le r$). We thus obtain an infinite sequence $v_1, v_2, \ldots$ of k-dimensional vectors of non-negative integers, such that some component of v_i is larger than the corresponding component of v_j, and some other component of v_i in less than the corresponding component of v_j, whenever $i \ne j$. However, Mann ([M], Theorem 2) showed that this is impossible.

6. Concluding remarks. In a further paper, [G2], we investigate the consequences, for Fermat's Last Theorem, of assuming a variety of plausible conjectures in analytic number theory. The key tool is the aforementioned theorem of Sophie Germain. We also indicate there that our methods apply equally well to all admissible polynomials, by using Proposition 1 (from here) in place of Sophie Germain's theorem. For instance, we prove that if the least prime in all arithmetic progressions $a \pmod d$ with $(a, d) = 1$ is $\ll \phi(d)\log^3 d$, then $T(f)$ contains $\ll \log^{10} x$ elements $\le x$. Also if a certain uniform quantitative version of the prime k-tuplets conjecture holds (analogous to the Siegel–Walfisz Theorem), then $T(f)$ contains $o(\pi(x))$ primes $\le x$. Further, we prove results corresponding to each of those in [AHB] (one of which appears as Lemma 2 above).

References

[AHB] L. M. Adleman and D. R. Heath-Brown, *The first case of Fermat's last theorem*, Invent. Math. 79 (1985), 409–416.

[An] N. C. Ankeny, *The insolubility of sets of Diophantine equations in the rational numbers*, Proc. Nat. Acad. Sci. U.S.A. 38 (1952), 880–884.

[AE] N. C. Ankeny and P. Erdős, *The insolubility of classes of Diophantine equations*, Amer. J. Math. 76 (1954), 488–496.

[BM] W. D. Brownawell and D. W. Masser, *Vanishing sums in function fields*, Math. Proc. Cambridge Philos. Soc. 100 (1986), 427–434.

[Ch] V. Chvátal, *Linear Programming*, Freeman, New York 1983.

[CJ] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations* (*On vanishing sums of roots of unity*), Acta Arith. 30 (1976), 229–240.

[DL] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Royal Soc. Ser. A 274 (1963), 443–460.

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366, Erratum, ibid. 75 (1984), 381.

[Fo] E. Fouvry, *Théorème de Brun–Titchmarsh*; *application au théorème de Fermat*, ibid. 79 (1985), 383–407.

[G1] A. Granville, *Diophantine equations with varying exponents* (*with special reference to Fermat's Last Theorem*), Doctoral thesis, Queen's University, Kingston, Ontario, 1987, 209 pp.

[G2] —, *Some conjectures in Analytic Number Theory and their connection with Fermat's Last Theorem*, in: Analytic Number Theory, B. C. Brendt, H. G. Diamond, H. Halberstam, A. Hildebrand (eds.) Birkhäuser, Boston 1990, 311–326.

[G3] —, *The set of exponents for which Fermat's Last Theorem is true*, *has density one*, C. R. Math. Acad. Sci. Canada 7 (1985), 55–60.

[HB] D. R. Heath-Brown, *Fermat's Last Theorem for "almost all" exponents*, Bull. London Math. Soc. 17 (1985), 15–16.

[L] H. W. Lenstra, Jr., *Vanishing sums of roots of unity*, in: Proc. Bicentennial Cong. Wiskundig Genootschap, Vrije Univ., Amsterdam 1978, 249–268.

[M] H. B. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), 107–117.

[NS] D. J. Newman and M. Slater, *Waring's problem for the ring of polynomials*, J. Number Theory 11 (1979), 477–487.

[Ri] P. Ribenboim, *An extension of Sophie Germain's method to a wide class of diophantine equations*, J. Reine Angew. Math. 356 (1985), 49–66.

[V] H. S. Vandiver, *On classes of Diophantine equations of higher degrees which have no solutions*, Proc. Nat. Acad. Sci., U.S.A. 32 (1946), 101–106.

SCHOOL OF MATHEMATICS
INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY 08540, U.S.A.

Current address
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GEORGIA
ATHENS
GEORGIA 30602, U.S.A.

Received on 23.3.1990
and in revised form on 29.3.1991 (2020)