DENSITY RESULTS ON FAMILIES OF DIOPHANTINE EQUATIONS WITH FINITELY MANY SOLUTIONS

Autor(en): **Ribenboim, P.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **39 (1993)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-60411

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'Enseignement Mathématique, t. 39 (1993), p. 3-23

p 74 771 Sect. 2

ETH-BIBLIOTHEK ZÜRICH Sto.

DENSITY RESULTS ON FAMILIES OF DIOPHANTINE EQUATIONS WITH FINITELY MANY SOLUTIONS

by P. RIBENBOIM

In this paper, we shall consider families of diophantine equations, each having only finitely many solutions. Due to relations between the solutions of these equations, it is possible to deduce density results.

For the convenience of the reader, we first gather the required facts concerning uniform density and asymptotic density of sets of natural numbers.

The second section consists of applications of Faltings' theorem. We work with families of homogeneous polynomials satisfying very mild conditions, which imply that the associated plane homogeneous curves are smooth. The key for the application is an easy lemma by Filaseta. The density results obtained are interpreted and discussed in special cases, which concern differences and sums of powers.

The final section is about applications of a theorem of Schinzel and Tijdeman. We discuss the density results obtained, in face of Erdös' conjecture that there do not exist three consecutive powerful numbers.

1. In this first section we explain the concept of uniform density, following very closely, for the convenience of the reader, the recent paper of Brown and Freedman [B-F].

For $t, k \in \mathbf{N}$, $t > 0$, let $I_{k,t} = \{m \in \mathbf{N} \mid k + 1 \leqslant m \leqslant k + t\}$ and let $\mathscr{I}_t = \{I_{k,t} \mid k \in \mathbf{N}\}$.

For each subset E of $\mathbf{N}_{>0}$ and $t \in \mathbf{N}_{>0}$, let $\bar{\sigma}_t(E)$ (resp. $\underline{\sigma}_t(E)$) be the largest (resp. smallest) integer s such that there exist infinitely many $k \in \mathbf{N}$ for which $\#(E \cap I_{k,t}) = s$.

So
$$\bar{\sigma}_t(E) = \limsup_k \#(E \cap I_{k,t}) ,$$
$$\underline{\sigma}_t(E) = \liminf_k \#(E \cap I_{k,t}) .$$

Thus $0 \leqslant \underline{\sigma}_t(E) \leqslant \bar{\sigma}_t(E) \leqslant t$.

Also, if $0 < t < u$, then $\underline{\sigma}_t(E) \leqslant \underline{\sigma}_u(E)$ and $\bar{\sigma}_t(E) \leqslant \bar{\sigma}_u(E)$. For $0 < t, 0 < u$, we have

$$\underline{\sigma}_{t+u}(E) \geqslant \underline{\sigma}_t(E) + \underline{\sigma}_u(E) ,$$
$$\bar{\sigma}_{t+u}(E) \leqslant \bar{\sigma}_t(E) + \bar{\sigma}_u(E) ,$$

the proof being easy.

It follows that $\lim_{t\to\infty} \dfrac{\underline{\sigma}_t(E)}{t}$ exists; it is denoted by $\underline{\mu}(E)$ and called the *lower uniform density* of E.

We give the proof since it is less obvious. Let $t, u > 0$; we write $t = qu + r$, with $0 \leqslant r < u$. Then $t \geqslant qu$, hence by the facts quoted, $\underline{\sigma}_t(E) \geqslant \underline{\sigma}_{qu}(E) \geqslant q\,\underline{\sigma}_u(E)$.

So

$$\frac{\underline{\sigma}_t(E)}{t} \geqslant \frac{q\,\underline{\sigma}_u(E)}{(q+1)u} .$$

Then

$$\liminf_{1\to\infty} \frac{\underline{\sigma}_t(E)}{t} \geqslant \liminf_{q\to\infty} \frac{q}{q+1} \cdot \frac{\underline{\sigma}_u(E)}{u} = \frac{\underline{\sigma}_u(E)}{u} .$$

Since this holds of every $u > 0$, then

$$\liminf_{t} \frac{\underline{\sigma}_t(E)}{t} \geqslant \limsup_{u} \frac{\underline{\sigma}_u(E)}{u}$$

and the limit exists.

Similarly, $\lim_{t\to\infty} \dfrac{\bar{\sigma}_t(E)}{t}$ exists; it is denoted by $\bar{\mu}(E)$ and called the *upper uniform density* of E.

Clearly $0 \leqslant \underline{\mu}(E) \leqslant \bar{\mu}(E) \leqslant 1$. If $\underline{\mu}(E) = \bar{\mu}(E)$, this number is denoted by $\mu(E)$ and called the *uniform density* of E.

The *lower asymptotic density* of E is

$$\delta(E) = \liminf_{t\to\infty} \frac{\#(E \cap I_{0,t})}{t} ,$$

the *upper asymptotic density* of E is

$$\bar{\delta}(E) = \limsup \frac{\#(E \cap I_{0,t})}{t} .$$

We have $\underline{\mu}(E) \leqslant \underline{\delta}(E) \leqslant \bar{\delta}(E) \leqslant \bar{\mu}(E)$.

If $\underline{\delta}(E) = \bar{\delta}(E)$, this number is denoted by $\delta(E)$ and called the *asymptotic density* of E.

It follows that if E has uniform density $\mu(E)$, then it has asymptotic density, and they are equal: $\mu(E) = \delta(E)$.

The following example illustrates the fact that a set E may have asymptotic density, but not uniform density.

Let $E = \bigcup_{n=0}^{\infty} I_{(2n+i)^2, 4n+3}$. Then, an easy calculation gives $\underline{\mu}(E) = 0$, $\bar{\mu}(E) = 1$, while $\delta(E) = \frac{1}{2}$.

If E' is the complement of E in $\mathbf{N}_{>0}$, that is $E' = \bigcup_{n=0}^{\infty} I_{(2n)^2, 4n+1}$, then $\underline{\mu}(E') = 0$, $\underline{\mu}(E') = 1$, $\delta(E') = \frac{1}{2}$.

Thus, it is possible to have a set E and its complement with $\underline{\mu}(E) = \underline{\mu}(E') = 0$, or also $\bar{\mu}(E) = \bar{\mu}(E') = 1$.

Since $\bar{\sigma}_t(E) = t - \underline{\sigma}_t(E')$, then $\mu(E) = 1$ if and only if $\mu(E') = 0$.

It is also easy to see that if E has asymptotic density, so does E', and $\delta(E) + \delta(E') = 1$.

Still following Brown and Freedman, we indicate some easy properties:

1) If $E \subseteq F$ and $\nu \in \{\underline{\mu}, \bar{\mu}, \underline{\delta}, \bar{\delta}, \mu, \delta\}$ then $\nu(E) \leqslant \nu(F)$.

2) For any sets $E, F \subseteq \mathbf{N}_{>0}$ and $\nu \in \{\bar{\mu}, \bar{\delta}, \mu, \delta\}$, we have

$$\nu(E \cup F) \leqslant \nu(E) + \nu(F) .$$

e) Suppose that the arithmetic progressions $A_i = \{a_i + kd_i \mid k \geqslant 0\}$ (for $i = 1, 2, \ldots, n$) are disjoint subsets of $\mathbf{N}_{>0}$. Then $A = \bigcup_{i=0}^{n} A_i$ has uniform density

$$\mu(A) = \sum_{i=1}^{n} \frac{1}{d_i} .$$

The following lemmas from [B-F] will be used:

LEMMA 1. *Let P be a finite set of prime numbers and N_P the set of natural numbers not divisible by any $p \in P$. Then N_P has uniform density*

$$\mu(N_P) = \prod_{p \in P} \left(1 - \frac{1}{p}\right) .$$

For the proof, see [B-F].

If $n > 0$ and $E \subseteq \mathbf{N}_{>0}$, let $E_n = \{m \in E \mid n \text{ divides } m\}$.

LEMMA 2. *Let E be a subset of $\mathbf{N}_{>0}$.*

i) *If P is a finite set of primes, such that $\mu(E_p) = 0$ for every $p \in P$, then* $\bar{\mu}(E) \leqslant \prod_{p \in P} \left(1 - \frac{1}{p}\right)$;

ii) *If $P = \{p \text{ prime} \mid n_0 < p\}$ (for some integer n_0, and $\mu(E_p) = 0$ for every $p \in P$, then $\mu(E) = 0$.*

Proof. For the convenience of the reader, we repeat the proof given by [B-F].

i) Since $E \subseteq \bigcup_{p \in P} E_p \cup N_P$, then $\bar{\mu}(E) \leqslant \bar{\mu}\left(\bigcup_{p \in P} E_p \cup N_P\right) \leqslant \sum_{p \in P} \bar{\mu}(E_p) + \bar{\mu}(N_P) = \bar{\mu}(N_P) = \prod_{p \in P} \left(1 - \frac{1}{p}\right)$.

ii) Let $\varepsilon > 0$. As it is known, there exists s such that if $P = \{p \text{ prime} \mid n_0 \leqslant p < s\}$ then $\prod_{p \in P} \left(1 - \frac{1}{p}\right) < \varepsilon$. By (i), $\bar{\mu}(E) < \varepsilon$. This shows that $\mu(E) = 0$. □

We shall also consider asymptotic densities of subsets S of $\mathbf{N}^m$ (where $m \geqslant 2$). The *lower* (respectively *upper*) *asymptotic density* of S are defined as follows:

$$\underline{\delta}(S) = \liminf_{M \to \infty} \frac{\# S(M)}{M^m},$$

$$\bar{\delta}(S) = \limsup_{M \to \infty} \frac{\# S(M)}{M^m},$$

where $S(M) = \{(s_1, \ldots, s_m) \in S \mid 1 \leqslant s_i \leqslant M \text{ for each } i = 1, \ldots, m\}$.

Clearly $\underline{\delta}(S) \leqslant \bar{\delta}(S)$. If $\underline{\delta}(S) = \bar{\delta}(S)$, this number is called the *asymptotic density* of S and denoted by $\delta(S)$.

At the end of this paper, we shall use a density relative to a sequence of natural numbers; the densities considered up to now are relative to the sequence $\{1, 2, 3, \ldots\}$.

Let $0 < \omega(1) < \omega(2) < \cdots$ be a sequence of natural numbers, let $E \subseteq \mathbf{N}_{>0}$. If $t \geqslant 1$, let

$$\underline{\sigma}_{t,\omega}(E) = \liminf_k \# (E \cap \{\omega(k+1), \omega(k+2), \ldots, \omega(k+t)\}),$$

$$\bar{\sigma}_{t,\omega}(E) = \limsup_k \# (E \cap \{\omega(k+1), \omega(k+2), \ldots, \omega(k+t)\}).$$

The following limits exist

$$\underline{\mu}_\omega(E) = \lim_{t\to\infty} \frac{\underline{\sigma}_{t,\omega}(E)}{t}, \qquad \bar{\mu}_\omega(E) = \lim_{t\to\infty} \frac{\bar{\sigma}_{t,\omega}(E)}{t}$$

and are called respectively, the *lower* (upper) *uniform density of E, relative to* ω. If $\underline{\mu}_\omega(E) = \bar{\mu}_\omega(E)$, this number is denoted by $\mu_\omega(E)$ and called the *uniform density of E relative to* ω.

The relative densities satisfy the same properties indicated for the densities. In particular, we note that if E' is the complement of E in $\mathbf{N}_{>0}$, then $\mu_\omega(E) = 1$ if and only if $\mu_\omega(E') = 0$.

If p is any prime number, let $E_{p,\omega} = E \cap \{\omega(pn) \mid n \geqslant 1\}$ and if P is a finite set of distinct primes, let $N_{P,\omega} = \mathbf{N}_{>0} \setminus \bigcup_{p\in P} \{\omega(pn) \mid n \geqslant 1\}$. Then

$$\mu_\omega(N_{P,\omega}) = \prod_{p\in P}\left(1 - \frac{1}{p}\right).$$

Finally, we shall also need:

If $\mu_\omega(E_{p,\omega}) = 0$ for every prime p, then $\mu_\omega(E) = 0$.

We leave to the reader the verification that the density relative to ω satisfies indeed these properties.

The following lemma is well-known and very simple to prove (see [P-R] which has a proof of a special case):

LEMMA 3. *Let* P *be a set of* $t \geqslant 1$ *pairwise relatively prime positive integers, let* $m \geqslant 1, M > 1$ *and let* $R_{P,M,m} = \{(k_1, k_2, \ldots, k_m) \mid 1 \leqslant k_i \leqslant M$ *for every* i, *and there exists* $n \in P$ *such that* $n \mid k_1, n \mid k_2, \ldots, n \mid k_m\}$. *Then*

$$\#(R_{P,M,m}) \geqslant M^m\left[1 - \prod_{n\in P}\left(1 - \frac{1}{n^m}\right)\right] - mM^{m-1} \times 2^t.$$

2. In this section we shall use the theorem of Faltings. Appealing to a clever idea of Filaseta [F], we obtain an extension of previous results (which were also derived using Filaseta's argument) by Granville [G1], Heath-Brown [H-B], Powell and Ribenboim [P-R] and Brown and Freedman [B-F].

Let $f \in \mathbf{Z}[X, Y, Z]$ be a non-constant homogeneous polynomial, denote by $C(f)$ the curve of zeroes of f in $\mathbf{P}_2(\mathbf{C})$.

For every $n \geqslant 1$, let $f_n(X, Y, Z) = f(X^n, Y^n, Z^n)$.

The following lemma – which I acknowledge gratefully to J. Top – holds:

LEMMA 4. *If the curve* $C(f)$ *is smooth, the following conditions are equivalent:*

1) *For every* $n \geqslant 2$, *the curve* $C(f_n)$ *is smooth.*

2) *There exists* $n \geqslant 2$ *such that* $C(f_n)$ *is smooth.*

3) *Conditions (a) and (b) are satisfied:*

   (a) $C(f)$ *contains no point with two coordinates equal to* 0;

   (b) *at each point of* $C(f)$ *with one coordinate equal to* 0, *each one of the partial derivatives relative to the other coordinates does not vanish.*

The proof, which is a simple exercise, is omitted.

Note also that if $C(f)$ is smooth, then f is absolutely irreducible. Indeed, if $f = gh$, with g, h non-constant polynomials in $\mathbf{C}[X, Y, Z]$, the plane curves $C(g)$, $C(h)$ must have at least one point of intersection, and at that point, the partial derivatives of $f = gh$ would all vanish.

Let $f \in \mathbf{Z}[X, Y, Z]$ be a non-constant homogeneous polynomial such that the curve $C(f)$ is smooth and satisfies conditions (a), (b) of the above lemma.

$$\text{Let } n_0 = \begin{cases} 1 \text{ if } \deg(f) > 1 \\ 3 \text{ if } \deg(f) = 1 \end{cases}.$$

If $n > n_0$, the genus of the curve $C(f_n)$ is equal to

$$\frac{[n \deg(f) - 1]\,[n \deg(f) - 2]}{2} > 1 .$$

Here is the lemma of Filaseta:

LEMMA 5. *Under the above hypotheses and notations, if* $n > n_0$ *there exists an integer* $N(n) > 1$ *such that if* $k > N(n)$, $l, m \geqslant 1$ *and* $f(x^{kn}, y^{ln}, z^{mn}) = 0$, *with* x, y, z *relatively prime, then* $|x| \leqslant 1$.

Proof. Since $n > n_0$, the curve $C(f_n)$, which is smooth, has genus greater than 1. By Faltings' theorem, there exist only finitely many triples of relatively prime integers (x_i, y_i, z_i), such that $f_n(x_i, y_i, z_i) = 0$. Let $N(n) = \max_i \{|x_i|, |y_i|, |z_i|\}$.

If x, y, z are relatively prime integers such that $f(x^{kn}, y^{ln}, z^{mn}) = 0$, then $f_n(x^k, y^l, z^m) = 0$. Hence there exists i such that $x^k = x_i, y^l = y_i, z^m = z_i$, and so $|x|^k \leqslant N(n) < k$. This implies that $|x| \leqslant 1$. □

In particular, if it is assumed that $k > N(n)$ and $l > N(n)$, then $|xy| \leqslant 1$. Similarly, if $k, l, m > N(n)$, then $|xyz| \leqslant 1$.

Let

$$F = \{k \geqslant 1 \mid \text{if } x, y, z \text{ are relatively prime integers such that } f(x^k, y^k, z^k) = 0, \text{ then } |xyz| \leqslant 1\}.$$

PROPOSITION 1. *The set* F *has uniform density* $\mu(F) = 1$.

Proof. Let F' be the complement of F in $\mathbf{N}_{>0}$; we show that $\mu(F') = 0$.

For each prime $p > n_0$, the set $F'_p = \{k \in F' \mid p \text{ divides } k\}$ is finite. Indeed, if $k = np$, where $n > N(p)$, by lemma 5, $k \in F$, so $k \notin F'$.

By Lemma 2, $\mu(F') = 0$, and by a previous remark, $\mu(F) = 1$. □

In particular, F has asymptotic density $\delta(F) = 1$. The proposition may be applied to many polynomials, and was known in special cases.

1°) The proposition is applicable to $f = aX + bY - cZ$, where a, b, c are non-zero integers.

In particular, if $a = b = c = 1$, the proposition concerns Fermat's last theorem. Noting that if $f = X + Y - Z$, then $f(x^k, y^k, z^k) \neq 0$ when $k \geqslant 3$, $xyz \neq 0$ and $|x|, |y|$ or $|z|$ is equal to 1, then proposition 1, in this particular case was given by Brown and Freedman. The proof that $\delta(F) = 1$ was given, independently, by Granville [G1] and Heath-Brown [H-B].

2°) $f = X^2 + Y^2 + Z^2 + XY + YZ + XZ$. It is easy to verify that the proposition is applicable.

3°) $f = X^3 + Y^3 + Z^3 - aXYZ$, where $a \neq 3, -1$. Again $C(f)$ is smooth and satisfies the conditions (a), (b) of the lemma 1, and the proposition holds.

4°) More generally, let $g \in \mathbf{Z}[Y, Z]$ be a homogeneous polynomial of degree $d \geqslant 1$, $g(Y, Z) = a_0 Y^d + a_1 Y^{d-1} Z + \cdots + a_{d-1} YZ^{d-1} + a_d Z^d$. Assume $a_0 a_d \neq 0$ and also that the polynomial $Z^d g\left(\frac{Y}{Z}\right)$ is irreducible; hence $Y^d g\left(\frac{Z}{Y}\right)$ is also irreducible. Let $f = cX^d - g(Y, Z)$ (with $c \in \mathbf{Z}, c \neq 0$), so f is a non-constant homogeneous polynomial. In view of the above hypotheses, the curve of f is smooth and the conditions (a), (b) are satisfied, so the proposition is applicable.

We shall now indicate other density results. For every $k \geqslant 1$, let $D_k = \{(l, m) \mid 1 \leqslant l, m;$ if x, y, z are relatively prime integers such that $f(x^k, y^l, z^m) = 0$, then $|x| \leqslant 1\}$.

We note at once that $F \subseteq \{k \mid D_k \neq \varnothing\}$; indeed, if $k \in F$, then $(k, k) \in D_k$. By proposition 1, the set $\{k \mid D_k \neq \varnothing\}$ has uniform density 1.

We are tempted to believe that the subset $\{k \mid \delta(D_k) = 1\}$ has also uniform density 1. However, we can only prove weaker results. For each $\alpha, 0 \leqslant \alpha < 1$, let $H_\alpha = \{k \mid \underline{\delta}(D_k) \leqslant \alpha\}$ and $P_\alpha = \{p \text{ prime} \mid \alpha < 1/p^2\}$.

PROPOSITION 2. *If* $0 \leqslant \alpha < 1$, *then for each* $\varepsilon > 0$

$$\bar{\mu}(H_\alpha) \leqslant \prod_{n_0 < p \in P_{\alpha+\varepsilon}} \left(1 - \frac{1}{p}\right).$$

In particular, the set $H_0 = \{k \mid \underline{\delta}(D_k) = 0\}$ *has uniform density* $\mu(H_0) = 0$.

Proof. We show that if $p \in P_{\alpha+\varepsilon}$ and $n_0 < p$, then $\mu((H_\alpha)_p) = 0$; by lemma 2, this implies that $\bar{\mu}(H_\alpha) \leqslant \prod_{n_0 < p \in P_{\alpha+\varepsilon}} \left(1 - \frac{1}{p}\right)$.

It suffices to show that if $n_0 < p \in P_{\alpha+\varepsilon}$ and if $k > N(p)$ (as defined in lemma 5), then $kp \notin H_\alpha$; thus $(H_\alpha)_p$ is finite and therefore $\mu((H_\alpha)_p) = 0$.

So, we show that if $n_0 < p \in P_{\alpha+\varepsilon}$ and $k > N(p)$, then $\underline{\delta}(D_{kp}) > \alpha$. Let L_0 be sufficiently large, say $\left(\frac{L_0}{L_0+1}\right)^2 \geqslant \frac{2\alpha+\varepsilon}{2(\alpha+\varepsilon)}$. If $k > N(p)$ and $pL \leqslant M < p(L+1)$, where $L_0 \leqslant L$, for every $l, m \geqslant 1$, if x, y, z are relatively prime integers and $f(x^{kp}, y^{lp}, z^{mp}) = 0$, then $|x| \leqslant 1$; thus $(lp, mp) \in D_{kp}$. Hence $\# D_{kp}(M) \geqslant \left[\frac{M}{p}\right]^2 \geqslant L^2$. So

$$\frac{\# D_{kp}(M)}{M^2} \geqslant \frac{L^2}{p^2(L+1)^2} \geqslant \frac{1}{p^2}\left(\frac{L_0}{L_0+1}\right)^2 \geqslant \frac{2\alpha+\varepsilon}{2p^2(\alpha+\varepsilon)} \geqslant \alpha + \frac{\varepsilon}{2}.$$

Thus, $\underline{\delta}(D_{kp}) > \alpha$. Since $\lim_{\varepsilon \to 0} \prod_{n_0 < p \in P_\varepsilon} \left(1 - \frac{1}{p}\right) = 0$, then $\mu(H_0) = 0$. □

We may also state the last assertion as follows: the set $H_0' = \{k \geqslant 1 \mid \underline{\delta}(D_k) > 0\}$ has uniform density equal to 1.

We give explicitly some applications.

First, let $f = X - Y + Z$. Now $D_k = \{(l, m) \mid$ no difference $y^l - z^m$, with non-zero relatively prime integers y, z is equal to a k^{th} power (different from

$0, \pm 1)\}$. Then, with uniform density equal to 1, we have $\underline{\delta}(D_k) > 0$.

Here it should be recalled that according to Tijdeman's theorem [T], there exists an effectively computable constant T, such that if $1 = y^l - z^m$ (with $y, z \geqslant 1, l, m \geqslant 2$), then $y, z, l, m \leqslant T$.

If $f = X - Y - Z$, then $D_k = \{(l, m) \mid$ no sum $y^l + z^m$, with non-zero y, z relatively prime, is equal to a k^{th} power$\}$. Then, with uniform density 1, we have $\underline{\delta}(D_k) > 0$.

We continue with density results for other sets. For $l, m \geqslant 1$, let $E_{(l,m)} = \{k \geqslant 1 \mid$ if x, y, z are relatively prime integers such that $f(x^k, y^l, z^m) = 0$, then $|yz| \leqslant 1\}$.

Let

$$I = \{(l, m) \mid 1 \leqslant l, m \quad \text{and} \quad \underline{\delta}(E_{(l,m)}) > 0\}.$$

We note that the set F, previously defined satisfies the inclusion

$$F \subseteq \bigcup_{1 \leqslant l, m} E_{(l,m)} .$$

Indeed, if $k \in F$, then $k \in E_{(k,k)}$.

Let

$$h^{(2)} = \begin{cases} \dfrac{25}{18} & \text{if } \deg(f) = 1 \\ 1 & \text{if } \deg(f) \geqslant 2 . \end{cases}$$

As usual, $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ is the sequence of primes.

PROPOSITION 3. *With above hypotheses and notations,*

$$\underline{\delta}\ (I) \geqslant 1 - \frac{6h^{(2)}}{\pi^2} > 0 .$$

Proof. Let $s \geqslant 3$ and

$$P_s = \begin{cases} \{4, 9, p_3, \ldots, p_s\} & \text{if } \deg(f) = 1 , \\ \{2, 3, p_3, \ldots, p_s\} & \text{if } \deg(f) \geqslant 2 . \end{cases}$$

For each $n \in P_s$, let $N(n)$ be defined as in lemma 5; let

$$N_s = \max\{nN(n) \mid n \in P_s\} \text{ and let } M > N_s .$$

We consider the sets: $R_{s,M} = R = \{(l, m) \mid 1 \leqslant l, m \leqslant M$ and there exists $n \in P_s$ such that $n \mid l$ and $n \mid m\}$, $S_{s,M} = S = \{(l, m) \in R \mid N_s < l, m\}$, $T_{s,M} = T = \{(l, m) \mid 1 \leqslant l, m \leqslant M$ and $\min\{l, m\} \leqslant N_s\}$.

Clearly $\#(T) = M^2 - (M - N_s)^2 \leqslant 2MN_s$.

Now we show that $S \subseteq I(M)$. Let $(l, m) \in S$, let $n \in P_s$ be such that n divides l and m, so $l = nl', m = nm'$. We have $nN(n) \leqslant N_s < l, m$, hence $N(n) < l', m'$. We wish to show that $\underline{\delta}(E_{(l,m)}) > 0$, thus $(l, m) \in I(M)$.

For this purpose, let $u = lcm(l, m)$, hence n divides u. Let r_0 be sufficiently large, let $r_0 u \leqslant t$, so there exists r such that $r_0 \leqslant r$ and $ru \leqslant t < (r+1)u$.

If $1 \leqslant k$ we write $ku = k'n$. If x, y, z are relatively prime integers such that $f(x^{ku}, y^l, z^m) = 0$ then $f(x^{k'n}, y^{l'n}, z^{m'n}) = 0$. By lemma 5, $|yz| \leqslant 1$. This shows that $ku \in E_{(l,m)}$ for each $k \geqslant 1$. Hence

$$\frac{\# E_{(l,m)}(t)}{t^2} \geqslant \frac{r^2}{(r+1)^2 u^2} \geqslant \frac{r_0^2}{(r_0+1)^2 u^2} > 0$$

for every $t \geqslant r_0 u$. Hence $\underline{\delta}(E_{(l,m)}) > 0$ and $(l, m) \in I(M)$.

So $\# R \leqslant \# S + \# T \leqslant \# I(M) + 2MN_s$. By lemma 3,

$$\# R \geqslant M^2 \left[1 - \prod_{n \in P_s} \left(1 - \frac{1}{n^2}\right)\right] - 2^{s+1} M .$$

Therefore

$$\frac{\# I(M)}{M^2} \geqslant 1 - \prod_{n \in P_s} \left(1 - \frac{1}{n^2}\right) - \frac{2N_s + 2^{s+1}}{M}$$

$$= 1 - h^{(2)} \prod_{i=1}^{s} \left(1 - \frac{1}{p_i^2}\right) - \frac{2(N_s + 2^s)}{M} ,$$

because

$$\frac{25}{18} \times \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) = \left(1 - \frac{1}{4^2}\right)\left(1 - \frac{1}{9^2}\right) .$$

We recall that

$$\prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^2}\right) = \frac{6}{\pi^2} .$$

Given $\varepsilon > 0$, we choose s sufficiently large, so that

$$\frac{6h^{(2)}}{\pi^2} < h^{(2)} \prod_{i=1}^{s} \left(1 - \frac{1}{p_i^2}\right) + \frac{1}{p_s} < \frac{6h^{(2)}}{\pi^2} + \varepsilon .$$

Let $M > 2N_s(N_s + 2^s)$, hence

$$\frac{2(N_s + 2^s)}{M} < \frac{1}{N_s} \leqslant \frac{1}{p_s} .$$

Finally

$$\frac{\# I(M)}{M^2} > 1 - \frac{6h^{(2)}}{\pi^2} - \varepsilon, \text{ for every } \varepsilon > 0 .$$

Hence $\underline{\delta}(I) \geqslant 1 - \dfrac{6h^{(2)}}{\pi^2} > 0.$ □

With the same method, we can prove a similar density result.

Let $C = \{(k, l, m) \mid 1 \leqslant k, l, m$ and if x, y, z are relatively prime integers such that $f(x^k, y^l, z^m) = 0$, then $|xyz| \leqslant 1\}$.

Let

$$h^{(3)} = \begin{cases} \dfrac{7}{6} \text{ if } \deg(f) = 1 , \\ 1 \text{ if } \deg(f) \geqslant 2 . \end{cases}$$

Let $\zeta(3) = \sum_{n=1}^{\infty} \dfrac{1}{n^3}$.

PROPOSITION 4. *With above hypotheses and notations,*

$$\underline{\delta}(C) \geqslant 1 - \frac{h^{(3)}}{\zeta(3)} > 0 .$$

Proof. We proceed as in the preceding proposition. Let $s \geqslant 3$, let

$$P_s = \{p_j \mid 1 \leqslant j \leqslant s\} , \text{ if } \deg(f) \geqslant 2 ,$$
$$\text{or } P_s = \{4, 9, p_3, \ldots, p_s\} , \text{ if } \deg(f) = 1 .$$

For every $n \in P_s$ there exists $N(n) > 0$ as in lemma 5.

Let $N_s = \max\{nN(n) \mid n \in P_s\}$ and let $M > N_s$.

Consider the sets:

$R = \{(k, l, m) \mid 1 \leqslant k, l, m \leqslant M$ and there exists $n \in P_s$ such that $n \mid k, n \mid l, n \mid m\}$.

$S = \{(k, l, m) \in R \mid N_s < k, l, m\}$.

$T = \{(k, l, m) \mid 1 \leqslant k, l, m \leqslant M$ and $\min\{k, l, m\} \leqslant N_s\}$.

Then $R \subseteq S \cup T$ and $\# T = M^3 - (M - N_s)^3 \leqslant 3M^2N_s$.

We show that $S \subseteq C(M)$. Assume that $(k, l, m) \in S$, let $n \in P_s$ be such that $k = nk', l = nl', m = nm'$; since $k, l, m > N_s = nN(n)$ then $k', l', m' > N(n)$ and by lemma 5, $f(x^k, y^l, z^m) = f(x^{k'n}, y^{l'n}, z^{m'n}) = 0$ with x, y, z relatively prime; then $|xyz| \leqslant 1$, thus $(k, l, m) \in C(M)$.

Hence

$$\frac{\#R}{M^3} \leqslant \frac{\#S}{M^3} + \frac{\#T}{M^3} \leqslant \frac{\#C(M)}{M^3} + \frac{3N_s}{M}.$$

On the other hand, by lemma 3,

$$\frac{\#R}{M^3} \geqslant 1 - \prod_{n \in P_s} \left(1 - \frac{1}{n^3}\right) - \frac{3 \times 2^s}{M}.$$

Given $\varepsilon > 0$, choose s such that

$$\frac{h^{(3)}}{\zeta(3)} < h^{(3)} \prod_{j=1}^{s} \left(1 - \frac{1}{p_j^3}\right) + \frac{1}{p_s} < \frac{h^{(3)}}{\zeta(3)} + \varepsilon;$$

Let $M > N_s(3 \times 2^s + 3N_s)$, hence

$$\frac{3 \times 2^s + 3N_s}{M} < \frac{1}{N_s} \leqslant \frac{1}{p_s},$$

and finally

$$\frac{\#C(M)}{M^3} \geqslant \frac{\#R}{M^3} - \frac{3N_s}{M} \geqslant 1 - \prod_{n \in P_s} \left(1 - \frac{1}{n^3}\right) - \frac{3[2^s + N_s]}{M}$$

$$> 1 - h^{(3)} \prod_{j=1}^{s} \left(1 - \frac{1}{p_j^3}\right) - \frac{1}{p_s} > 1 - \frac{h^{(3)}}{\zeta(3)} - \varepsilon.$$

This shows that $\underline{\delta}(C) \geqslant 1 - \dfrac{h^{(3)}}{\zeta(3)}$. □

The particular case where $f(X) = aX + bY - cZ$ (with $a, b, c \neq 0$) was established by Powell and Ribenboim [P-R].

3. The aim in this section is to establish the following density result. For the proof we acknowledge gratefully a useful suggestion by Andrew Granville.

PROPOSITION 5. *Let* $d \geqslant 1$, *let* $\mathscr{P} = \mathscr{P}_d$ *be the set of all homogeneous polynomials* $f \in \mathbf{Z}[X, Y, Z]$ *of degree* d, *satisfying the following conditions:*

a) *There is no triple* $(x, y, z) \in \mathbf{C}^3, (x, y, z) \neq (0, 0, 0)$, *with two coordinates equal to* 0, *such that* $f(x, y, z) = 0$.

b) *There is no triple* $(x, y, z) \in \mathbf{C}^3, (x, y, z) \neq (0, 0, 0)$, *with exactly one coordinate equal to* 0, *such that* $f(x, y, z) = 0$ *and the partial derivative of* f *with respect to another coordinate vanishes at* (x, y, z).

c) *There is no triple* $(x, y, z) \in \mathbf{C}^3, (x, y, z) \neq (0, 0, 0)$, *such that* $\dfrac{\partial f}{\partial X}, \dfrac{\partial f}{\partial Y}$ *and* $\dfrac{\partial f}{\partial Z}$ *vanish at* (x, y, z).

Then the set $\mathscr{P}$ *has asymptotic density equal to* 1.

Proof. Before the proof of this proposition, it is convenient to introduce notations.

Let $\mathscr{H} = \mathscr{H}_d$ be the set of all homogeneous polynomials $f \in \mathbf{Z}[x, Y, Z]$ having degree d.

Let $\mathscr{P}^{(a)} = \{f \in \mathscr{H}_d \mid f$ satisfies condition (a)$\}$. Define $\mathscr{P}^{(b)}$, $\mathscr{P}^{(c)}$ similarly, so $\mathscr{P} = \mathscr{P}^{(a)} \cap \mathscr{P}^{(b)} \cap \mathscr{P}^{(c)}$.

Let $\mathscr{B} = \mathscr{H} \setminus \mathscr{P}$, $\mathscr{B}^{(a)} = \mathscr{H} \setminus \mathscr{P}^{(a)}$ and define $\mathscr{B}^{(b)}$, $\mathscr{B}^{(c)}$ similarly. Thus $\mathscr{B} = \mathscr{B}^{(a)} \cup \mathscr{B}^{(b)} \cup \mathscr{B}^{(c)}$.

For each subset S of $\mathscr{H}$ and integer $N > 0$, let $S(N) = \{f \in S \mid$ the absolute value of each coefficient of f is at most equal to $N\}$.

Let $I_d = I = \{(i, j, k) \mid 0 \leqslant i, j, k, i + j + k = d\}$. So $\# I = \binom{d+2}{2}$ is the number of monomials $X^i Y^j Z^k$, of total degree d. It follows that

$$\# \mathscr{H}(N) = (2N + 1)^{\binom{d+2}{2}} - 1$$

(since the zero polynomial is not in $\mathscr{H}$).

To prove that $\lim_{N \to \infty} \dfrac{\# \mathscr{P}(N)}{\# \mathscr{H}(N)} = 1$ is equivalent to prove that $\lim_{N \to \infty} \dfrac{\# \mathscr{B}(N)}{\# \mathscr{H}(N)} = 0$.

For this purpose, it suffices to show:

1°) $\lim_{N\to\infty} \dfrac{\#\mathscr{B}^{(a)}(N)}{\#\mathscr{H}(N)} = 0,$

2°) $\lim \dfrac{\#(\mathscr{B}^{(b)}\setminus \mathscr{B}^{(a)})(N)}{\#\mathscr{H}(N)} = 0$ and

3°) $\lim \dfrac{\#(\mathscr{B}^{(c)}\setminus(\mathscr{B}^{(a)}\cup \mathscr{B}^{(b)}))(N)}{\#\mathscr{H}(N)} = 0.$

Each polynomial $f \in \mathscr{H}$ may be written as $f = \sum_I a_{ijk}X^iY^jZ^k$ with $a_{ijk} \in \mathbf{Z}$.

Proof of (1°). Let $\mathscr{B}^{(a)}_{Y,Z} = \{f \in \mathscr{H} \mid f(1,0,0) = 0\} = \{f \in \mathscr{H} \mid a_{100} = 0\}$. Define similarly $\mathscr{B}^{(a)}_{X,Z}$, $\mathscr{B}^{(a)}_{X,Y}$, so $\mathscr{B}^{(a)} = \mathscr{B}^{(a)}_{X,Y} \cup \mathscr{B}^{(a)}_{X,Z} \cup \mathscr{B}^{(a)}_{Y,Z}$.

Since $\#\mathscr{B}^{(a)}_{X,Y}(N) = \#\mathscr{B}^{(a)}_{X,Z}(N) = \#\mathscr{B}^{(a)}_{Y,Z} = (2N+1)^{\binom{d+2}{2}-1} - 1$, then $\#\mathscr{B}^{(a)}(N) \leqslant 3(2N+1)^{\binom{d+2}{2}-1}$ and $\lim_{N\to\infty} \dfrac{\#\mathscr{B}^{(a)}(N)}{\#\mathscr{H}(N)} = 0.$

Proof of (2°). Let $\mathscr{B}^{(b)}_{X,Y} = \{f \in \mathscr{H} \mid f(x,y,0) = 0$ and $\dfrac{\partial f}{\partial X}(x,y,0) = 0$ for some non-zero $x, y \in \mathbf{C}\}$, $\mathscr{B}^{(b)}_{Y,X} = \{f \in \mathscr{H} \mid f(x,y,0) = 0$ and $\dfrac{\partial f}{\partial Y}(x,y,0) = 0$ for some non-zero $x, y \in \mathbf{C}\}$. Define similarly $\mathscr{B}^{(b)}_{X,Z}$, $\mathscr{B}^{(b)}_{Z,X}$, $\mathscr{B}^{(b)}_{Y,Z}$, $\mathscr{B}^{(b)}_{Z,Y}$. So $\mathscr{B}^{(b)}\setminus \mathscr{B}^{(a)} \subseteq \mathscr{B}^{(b)}_{X,Y} \cup \mathscr{B}^{(b)}_{Y,X} \cup \mathscr{B}^{(b)}_{X,Z} \cup \mathscr{B}^{(b)}_{Y,Z} \cup \mathscr{B}^{(b)}_{Y,Z} \cup \mathscr{B}^{(b)}_{Z,Y}$.

Now observe that $\#\mathscr{B}^{(b)}_{X,Y}(N) \leqslant (2N+1)^{\binom{d+2}{2}-2}$.

Indeed, let $f \in \mathscr{B}^{(b)}_{X,Y}(N)$, so there exist $x, y \in \mathbf{C}$, $x, y \neq 0$, with

$$\begin{cases} a_{d00}x^d + a_{d-1,10}x^{d-1}y + \cdots + a_{1,d-1,0}xy^{d-1} + a_{0d0}y^d = 0 \\ da_{d00}x^{d-1} + (d-1)a_{d-1,10}x^{d-2}y + \cdots + a_{1,d-1,0}y^{d-1} = 0 \end{cases}$$

Let $J = I\setminus\{(d,0,0), (d-1,1,0)\}$ and consider the mapping

$$\varphi : f \mapsto (a_{ijk})_{(i,j,k)\in J}.$$

Since the matrix

$$\begin{pmatrix} x^d & x^{d-1}y \\ dx^{d-1} & (d-1)x^{d-2}y \end{pmatrix}$$

has rank 2, then φ is injective. Hence

$$\#\mathscr{B}^{(b)}_{X,Y} \leqslant (2N+1)^{\binom{d+2}{2}-2}.$$

This implies at once that

$$\#(\mathscr{B}^{(b)} \setminus \mathscr{B}^{(a)})(N) \leqslant 6(2N+1)^{\binom{d+2}{2}-2}$$

and $\lim_{N\to\infty} \dfrac{\#(\mathscr{B}^{(b)} \setminus \mathscr{B}^{(a)})(N)}{\#\mathscr{H}(N)} = 0.$

Preliminaries to the proof of (3°). For the convenience of the reader, we begin recalling facts about the resultant of two polynomials.

Let A be an integral domain, let $m, n > 0$, let

$$f = a_0X^m + a_1X^{m-1} + \cdots + a_m \in A[X],$$
$$g = b_0X^n + b_1X^{n-1} + \cdots + b_n \in A[X],$$

with $a_0b_0 \neq 0$. By definition, the resultant of f, g is

$$\mathrm{Res}(f,g) = \det \begin{pmatrix} a_0 & a_1 & \dots & \dots & a_m & 0 & \dots & \dots & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{m-1} & a_m & \dots & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_0 & b_1 & \dots & \dots & \dots & b_n & 0 & \dots & \dots & 0 \\ 0 & b_0 & b_1 & \dots & \dots & b_{n-1} & b_n & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

(the square matrix has n rows with the coefficients a_i of f and m rows with the coefficients b_j of g).

This definition is completed by putting $\mathrm{Res}(f, b_0) = b_0^m$ (when $m > 0$), $\mathrm{Res}(a_0, g) = a_0^n$ (when $n > 0$).

We shall require the following fundamental property of the resultant:

If f, g are non-constant polynomials, then f, g have a common zero in some field containing the field of quotients of A, if and only if $\mathrm{Res}(f, g) = 0$.

If the coefficients of f, g are in $A = \mathbf{Z}[Y, Z]$ it is easy to estimate the degree in Y, Z of $\mathrm{Res}(f, g)$. These and similar considerations follow without difficulty from the very definition of the resultant.

Let $(\alpha_{ijk})_{(i,j,k)\in I}$ be a family of indeterminates, let $F = \sum_I \alpha_{ijk}X^iY^jZ^k$ be the generic homogeneous polynomial of degree d. Let $F_1 = \dfrac{\partial F}{\partial X}$, $F_2 = \dfrac{\partial F}{\partial Y}$, $F_3 = \dfrac{\partial F}{\partial Z}$; they are homogeneous polynomials of total degree and

also separate degree $d-1$ in X, Y, Z with coefficients in $\mathbf{Z}[\alpha_{ijk}]_{(i,j,k)\in I}$.

Considering F_1, F_2, F_3 as polynomials in X, of degree $d-1$, with coefficients in $A = \mathbf{Z}[\alpha_{ijk}]_I[Y, Z]$, let $G_i = \mathrm{Res}(F_j, F_k)$ where $\{i, j, k\} = \{1, 2, 3\}$. So $G_i \in A$ and more precisely $G_i = \sum G_{r,s}^{(i)} Y^r Z^s$ (sum for $0 \leqslant r, s, r+s = (d-1)^2$) where $G_{r,s}^{(i)} \in \mathbf{Z}[\alpha_{l,m,n}]_{(l,m,m)\in I}$, each $G_{r,s}^{(i)}$ being homogeneous of degree $2(d-1)$.

Viewing G_1, G_2, G_3 as elements of $B[Y]$ of degree $(d-1)^2$ where $B = \mathbf{Z}[\alpha_{ijk}][Z]$, let $H_i = \mathrm{Res}(G_j, G_k)$, where $\{i, j, k\} = \{1, 2, 3\}$. Then $H_i = H_r^{(i)} Z^r$ with $r = (d-1)^4$ and $H_r^{(i)} \in \mathbf{Z}[\alpha_{l,m,n}]$. It should be noted that $H_r^{(i)}$ is not identically zero; in fact, $H_r^{(i)}$ is a homogeneous polynomial in the indeterminates α_{lmn} of degree $4(d-1)^3$.

We shall also use the following notation. If $P \in \mathbf{Z}[\alpha_{lmn}][X, Y, Z]$, if $\bar{a} = (a_{lmn})_I$, let $P(\bar{a}) \in \mathbf{Z}[X, Y, Z]$ be obtained by substituting a_{lmn} for α_{lmn}.

Proof of (3°). The set $\mathscr{B}^{(c)} \setminus (\mathscr{B}^{(a)} \cup \mathscr{B}^{(b)})$ is identified with the set

$$\mathscr{E} = \{\bar{a} = (a_{lmn}) \in \mathbf{Z}^{\#(I)} \mid \text{there exist } x, y, z, \in \mathbf{C},$$

x, y, z not all equal to 0, such that $F_i(\bar{a})(x, y, z) = 0$ for $i = 1, 2, 3\}$.

Let

$$\mathscr{E}' = \{\bar{a} = (a_{lmn}) \in \mathbf{Z}^{\#(I)} \mid \text{there exist } y, z \in \mathbf{C},$$

not both equal to 0, such that $G_i(\bar{a})(y, z) = 0$ for $i = 1, 2, 3\}$.

Again, let

$$\mathscr{E}'' = \{\bar{a} = (a_{lmn}) \in \mathbf{Z}^{\#(I)} \mid \text{there exist } z \in \mathbf{C},$$

$$z \neq 0 \text{ such that } H_i(\bar{a})(z) = 0 \text{ for } i = 1, 2, 3\}.$$

Note that $\mathscr{E}''$ is identified with

$$\mathscr{E}_0'' = \{\bar{a} = (a_{lmn}) \in \mathbf{Z}^{\#(I)} \mid H_i(\bar{a}) = 0 \text{ for } i = 1, 2, 3\}.$$

If S is any subset of $\mathbf{Z}^{\#(I)}$, if $N > 0$, let $S(N) = \{(a_{lmn}) \in \mathbf{Z}^{\#(I)} \mid |a_{lmn}| \leqslant N$ for each $(l, m, n) \in I\}$. By the fundamental property of the resultant, $\mathscr{E} \subseteq \mathscr{E}' \subseteq \mathscr{E}''$, hence also $\mathscr{E}(N) \subseteq \mathscr{E}'(N) \subseteq \mathscr{E}''(N)$, so $\#(\mathscr{B}^{(c)} \setminus (\mathscr{B}^{(a)} \cup \mathscr{B}^{(b)}))(N) \leqslant \# \mathscr{E}_0''(N)$.

Since the polynomials H_1, H_2, H_3 are not identically zero, some indeterminate $\alpha_{i_0 j_0 k_0}$ appears in the polynomial $H_1 H_2 H_3$. Let $J = I \setminus \{(i_0, j_0, k_0)\}$. Given arbitrarily any family $(a_{lmn})_{(l,m,n)\in J}$ with $a_{lmn} \in \mathbf{Z}$, $|a_{lmn}| \leqslant N$, there exist at most $4(d-1)^3$ integers a_{i_0, j_0, k_0}, with $|a_{i_0 j_0 k_0}| \leqslant N$, such that the family $\bar{a} = (a_{ijk})$ is a common zero of

H_1, H_2, H_3. Thus $\# \mathscr{E}_0''(N) \leqslant 4(d-1)^3(2N+1)^{\binom{d+2}{2}-1}$.

Hence

$$\lim_{N \to \infty} \frac{\# (\mathscr{B}^{(c)} \setminus (\mathscr{B}^{(a)} \cup \mathscr{B}^{(b)}))(N)}{\# \mathscr{H}(N)} = 0 .$$

This concludes the proof of the proposition. □

4. In this section, we shall apply the following theorem of Schinzel and Tijdeman [S-T]:

Let $f \in \mathbf{Q}[X]$ with at least three simple zeroes (resp. two simple zeroes). Then there exists an effectively computable constant $T(f) > 0$, such that if x, y, z are integers, $|y| \geqslant 2$, $z \geqslant 2$ (resp. $|y| \geqslant 2$, $z \geqslant 3$) and $f(x) = y^z$, then $|x|, |y|, z \leqslant T(f)$.

Let $f \in \mathbf{Q}[X]$, let $a \geqslant 2$ and for every $h \geqslant 1$, consider the polynomial $f_h = \frac{1}{a^h} f \in \mathbf{Q}[X]$. Next, consider the exponential diophantine equations (for $h \geqslant 1$):

$$(E_h) \qquad f(X) = a^h Y^Z .$$

Let $z \geqslant 2$ when f has at least three simple zeroes, or $z \geqslant 3$ when f has exactly two simple zeroes. Define $D^{(z)}_{a,f} = \{h \geqslant 1 \mid$ there do not exist integers x, y, with $y \geqslant 2$, such that $f(x) = a^h y^z\}$.

LEMMA 6. *Given f, a, z satisfying the above hypotheses. For every $h \geqslant 1$ there exists an effectively computable integer $e = e(f, a, z, h) > 0$ such that if $h' \geqslant e$, then $h'h \in D^{(z)}_{a,f}$.*

Proof. For each $h \geqslant 1$, let $T_h = T(f_h) > 0$ be the effectively computable constant associated to f_h by the theorem of Schinzel and Tijdeman. Let $e = e(f, a, z, h)$ be sufficiently large, namely

$$e = \left(\left[\frac{\log \bar{T}_{z,h}}{h \log a} \right] + 1 \right) z ,$$

where $\bar{T}_{z,h} = \max\{T_{rh} \mid 0 < r \leqslant z\}$.

Let $h' > e$. If there exist integers x, y such that $y \geqslant 2$ and $f(x) = a^{hh'} y^z$, let $h' = lz + r$, with $0 < r \leqslant z$. So $f(x) = a^{rh}(a^{lh} y)^z$ and therefore

$$a^{lh} \leqslant a^{lh} |y| \leqslant T_{rh} \leqslant \bar{T}_{z,h} ;$$

so $l \leqslant \left[\frac{\log \bar{T}_{z,h}}{h \log a}\right]$. Then

$$h' = lz + r \leqslant (l+1)z \leqslant \left(\left[\frac{\log \bar{T}_{z,h}}{h \log a}\right] + 1\right) z = e .$$

Hence, if $h' > e$ then $h'h \in D^{(z)}_{a,f}$. □

PROPOSITION 6. *For every* $a \geqslant 2, z \geqslant 2$ *(if* f *has at least three simple zeroes) or* $z \geqslant 3$ *(if* f *has exactly two simple zeroes),* $\mu(D^{(z)}_{a,f}) = 1$.

Proof. Let D' be the complement in $\mathbf{N}_{>0}$ of the set $D^{(z)}_{a,f}$. Let p be any prime, let $e = e(f, a, z, p) > 0$ (as given in the preceding lemma). If $h' > e$ then $h'p \in D^{(z)}_{a,f}$, hence $h'p \notin D'$. Therefore the set D'_p is finite, hence $\mu(D'_p) = 0$. By lemma 2, $\mu(D') = 0$ and we conclude that $\mu(D^{(z)}_{a,f}) = 1$. □

In particular, $\delta(D^{(z)}_{a,f}) = 1$.

The above result may be applied for the polynomials $X^m - 1$, when $m \geqslant 2$; it sharpens what was proved in [R 1] about the polynomial $X^2 - 1$.

To conclude, we wish to discuss Erdös conjecture about powerful numbers.

We recall that a natural number $n = \prod_{i=1}^{r} p_i^{e_i}$ (with distinct primes p_i and $e_i \geqslant 1$) is a *powerful number* when each $e_i \geqslant 2$. It is equivalent to say that $n = a^2 b^3$, where $a \geqslant 1, b \geqslant 1$ (and a, b are not necessarily relatively prime).

Erdös conjectured (see [G2], [R 1]):

(E) There do not exist three consecutive powerful numbers.

This conjecture implies the following conjecture:

(E_1) For every $m \geqslant 2$ and even $x \geqslant 2$, the integer $x^{2m} - 1$ is not powerful.

Indeed, if $x^{2m} - 1 = (x^m + 1)(x^m - 1)$ is powerful, since $\gcd(x^m + 1, x^m - 1) = 1$, then $x^m + 1$, $x^m - 1$ are powerful, and so is x^m.

It is noteworthy that Granville [G2] showed how to derive from (E_1) the difficult theorem of Adleman, Heath-Brown and Fouvry (see also [R 3]):

There exist infinitely many prime exponents p *for which the first case of Fermat's last theorem is true (if* $x, y, z \neq 0, x^p + y^p = z^p, \gcd(x, y, z) = 1$, *then* p *divides* xyz*).*

Let $f_m(X) = 2^{2m} X^{2m} - 1$; for simplicity denote $D^{(z)}_{a,m} = D^{(z)}_{a,f_m}$.

The conjecture (E_1) may be rewritten as follows:

For every $m \geqslant 2, 3 \in \bigcap_{a \geqslant 2} D^{(2)}_{a,m}$.

By proposition 6, we have seen that $\mu(D^{(2)}_{a,m}) = 1$ for each $a \geqslant 2$, $m \geqslant 2$.

For each $a \geqslant 2$, let $Q_a = \{m \geqslant 2 \mid 3 \in D^{(2)}_{a,m}\}$.

For each $m \geqslant 2$, let $R_m = \{a \geqslant 2 \mid 3 \in D^{(2)}_{a,m}\}$.

Supporting the conjecture (E_1), I note that from the theorem of Schinzel and Tijdeman it follows that $\mu(Q_a) = 1$, because $Q'_a \cap \mathbf{N}p$ is finite for every prime $p \geqslant 3$ (Q'_a denotes the complement of Q_a).

Concerning the sets R_m, we can prove the following proposition about relative density:

PROPOSITION 7. *Let* $\omega(n) = n^2$ *for every* $n \geqslant 1$. *Then, for every* $m \geqslant 2$, *the uniform density of* R_m *relative to* ω *is equal to* 1.

Proof. Let R'_m denote the complement of R_m in $\mathbf{N}_{>0}$. We shall show that $\mu_\omega(R'_m) = 0$.

It suffices to prove that, for every prime p, the set

$$(R'_m)_{p,\omega} = R'_m \cap \{\omega(pn) \mid n \geqslant 1\}$$

has relative density equal to 0. In fact, we show that $(R'_m)_{p,\omega}$ is finite.

Given p, let $T(p^2, m) > 0$ be such that if $x, y,$ are integers $x, y \geqslant 2$, and $(2x)^{2m} - 1 = (p^2)^3 y^2$ then $x, y < T(p^2, m)$. Let n be such that $T(p^2, m) < n^3$. If $\omega(pn) \in R'_m$, then $3 \notin D^{(2)}_{\omega(pn),m}$, which means that there exist integers $x, y \geqslant 2$ satisfying $(2x)^{2m} - 1 = (p^2n^2)^3 y^2 = (p^2)^3 (n^3 y)^2$. So $n^3 y \leqslant T(p^2, m) < n^3$, hence $|y| \leqslant 1$ which is contrary to the hypothesis.

This shows indeed that $\mu_\omega(R'_m)_{p,\omega} = 0$ for every prime. So, $\mu_\omega(R'_m) = 0$, hence $\mu_\omega(R_m) = 1$. □

5. In this final section, we give yet another application of the theorem of Schinzel and Tijdeman, using the same method.

Let $f \in \mathbf{Q}[X]$ be a polynomial of degree $d \geqslant 1$; assume:

1) $f(0), f(1), f(-1)$ are not proper powers.

2) f has some simple zero $t \in \mathbf{C}$, $t \neq 0$.

For each $m \geqslant 1$, let $f_m(X) = f(X^m)$. Thus, if $t_1, \ldots, t_m \in \mathbf{C}$ are the m^{th} roots of t, then f_m has at least m simple roots.

Let

$$(E_m) \quad f_m(X) = Y^Z .$$

For convenience, we say that a triple of integers (x, y, z) with $y \geqslant 2$, $z \geqslant 2$ if $m \geqslant 3$ or $z \geqslant 3$ if $m = 2$, is a non-trivial solution of (E_m) if $f(x^m) = y^z$.

According to the theorem of Schinzel and Tijdeman, for every $m \geqslant 2$ there exists $C_m > 0$ (and effectively computable) such that if (x, y, z) is a non-trivial solution of (E_m), then $|x|, y, z < C_m$.

LEMMA 7. *With above hypotheses, if* $m \geqslant 2$ *and* $k > C_m$, *then* (E_{km}) *has only trivial solutions.*

Proof. Let $k > C_m$, let (x, y, z) be a non-trivial solution of (E_{km}). So $f(x^{km}) = y^z$, thus (x^k, y, z) is a non-trivial solution of (E_m). Hence $|x^k| < C_m < k$. Then $|x| \leqslant 1$ and therefore $f(0)$, $f(1)$ or $f(-1)$ is a proper power, which is contrary to the hypothesis. □

Let $F = \{m \geqslant 2 \mid (E_m) \text{ has only trivial solutions}\}$.

PROPOSITION 8. $\mu(F) = 1$.

Proof. Let F' be the complement of the set F; it suffices to show that $\mu(F') = 0$.

For each prime p, $kp \in F$ for each $k > C_p$, according to lemma 7. So $\mathbf{N}p \cap F'$ is finite. By lemma 2, $\mu(F') = 0$. □

Actually, the complement of F is finite, if f has at least two simple zeroes.

We note the following interesting application. Let a, b, c be non-zero integers, such that $-\frac{c}{b}$ and $\pm\frac{a}{b} - \frac{c}{b}$ are not zero, nor 1, nor proper powers.

Let $f = \frac{a}{b}X - \frac{c}{b}$. The above result is applicable to the polynomial f and yields:

The set of $m \geqslant 3$ *such that there exist integers* $n \geqslant 2$, *and* x, y, *with* $y \geqslant 2$, *satisfying* $ax^m - by^n = c$, *has uniform density equal to zero.*

BIBLIOGRAPHY

[B-F] BROWN, T.C. and A.R. FREEDMAN. The uniform density of sets of integers and Fermat's last theorem. *C. R. Math. Rep. Acad. Sci. Canada 12* (1990), 1-6.

[F] FILASETA, M. An application of Faltings' theorem to Fermat's last theorem. *C. R. Math. Rep. Acad. Sci. Canada 6* (1984), 31-32.

[G1] GRANVILLE, A. The set of exponents, for which Fermat's last theorem is true, has density one. *C. R. Math. Rep. Acad. Sci. Canada 7* (1985), 55-60.

[G2] —— Powerful numbers and Fermat's last theorem. *C. R. Math. Rep. Acad. Sci. Canada 8* (1986), 215-218.

[H-B] HEATH-BROWN, D.R. Fermat's last theorem for "almost all" primes. *Bull. London Math. Soc. 17* (1985), 15-16.

[P-R] POWELL, B. and P. RIBENBOIM. Note on a paper by M. Filaseta regarding Fermat's last theorem. *Ann. Univ. Turkuensis 187* (1985), 3-22.

[R1] RIBENBOIM, P. Remarks on exponential congruences and powerful numbers. *J. Nb. Th. 29* (1988), 251-263.

[R2] —— A note on Catalan's equation. *J. Nb. Th. 24* (1986), 245-248.

[R3] —— Recent results on Fermat's last theorem. *Expo. Math. 5* (1987), 75-90.

[S-T] SCHINZEL, A. and R. TIJDEMAN. On the equation $y^m = P(x)$. *Acta Arithm. 31* (1976), 199-204.

[T] TIJDEMAN, R. On the equation of Catalan. *Acta Arithm. 29* (1976), 197-209.

(Reçu le 28 janvier 1992)

Paulo Ribenboim

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
Canada K7L, 3N6

vide-leer-empty