Rendiconti
del
Seminario Matematico
della
Università di Padova

A. Schinzel
U. Zannier

Distribution of solutions of diophantine equations $f_1(x_1)f_2(x_2) = f_3(x_3)$, where f_i are polynomials

Rendiconti del Seminario Matematico della Università di Padova, tome 87 (1992), p. 39-68

<http://www.numdam.org/item?id=RSMUP_1992__87__39_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 87 (1992)

Distribution of Solutions of Diophantine Equations $f_1(x_1)f_2(x_2) = f_3(x_3)$, where f_i are Polynomials.

A. SCHINZEL - U. ZANNIER (*)

Introduction and statement of results.

At the meeting on Analytic Number Theory of Oberwolfach 1988 P.T. Bateman presented the following question sent to the American Mathematical Monthly by W. R. Utz:

«Is the density of positive integers z such that the equation

$$\binom{z+1}{2} = \binom{x+1}{2}\binom{y+1}{2}$$

is soluble in integers x, y greater than 1, equal to zero?»

The only correct solution of this problem sent to the American Math. Monthly, due to F. Dodd and L. Mattics [4] gives for the number $N(Z)$ of such $z \leq Z$ the estimate

$$N(Z) = O(Z^{3/4}).$$

We shall consider here a more general problem; namely, given three polynomials with integer coefficients f_i $(i = 1, 2, 3)$, the distribution of integers x_3 such that $|x_3| \leq x$ and the equation

$$f_3(x_3) = f_1(x_1)f_2(x_2) \tag{1}$$

is soluble in integers x_1, x_2.

(*) Indirizzo degli AA.: A. SCHINZEL: Mathematical Institute P.A.N., P.O.Box 137, 00 950 Warsaw, Poland; U. ZANNIER: D.S.T.R., Ist. Univ. di Architettura, S. Croce 191, 30135 Venezia, Italy.

The equation in question may have an infinite sequence of integer solutions with $f_i(x_i) = a$ for an $i \leqslant 2$ and $x_{3-i} = p(x_3)$ for a suitable polynomial $p \in \mathbb{Q}[x_3] \setminus \mathbb{Q}$. Such solutions will be called trivial.

Let $N(x)$ be the number of x_3 with $|x_3| \leqslant x$ for wich (1) has non-trivial solutions.

Let f_i have the degree $d_i > 0$, the discriminant Δ_i and the leading coefficient a_i. We shall assume throughout that $a_i > 0$ for all $i \leqslant 3$; indeed if two of the a_i's are negative one may change the signs of both relevant polynomials f_i without affecting the equation and if exactly one of the a_i's is negative the problem reduces to finitely many equations in two variables which are dealt with by known methods.

We have the following general result.

THEOREM 1. If $\Delta_3 \neq 0$, then for all $\varepsilon > 0$

$$N(x) \ll x^{c+\varepsilon}$$

where

$$c = \max\left\{\frac{d_3}{d_1 + d_2},\ \frac{1}{d_1} + \frac{1}{d_2} - \frac{1}{d_1 d_2},\ \min\left\{\frac{1}{2},\ \frac{(d_1, d_3)}{d_1}\right\},\ \min\left\{\frac{1}{2},\ \frac{(d_2, d_3)}{d_2}\right\}\right\}.$$

(The implied constant depends on the f_i's as well as on ε.)

Some information about trivial solutions is contained in the following.

THEOREM 2. Assume that f_1 has at least two distinct zeros. There exists at most one positive number A such that

$$f_3(t) = m f_1(p(t)) \qquad p \in \mathbb{C}[t],\ m \in \mathbb{C}$$

and $|m| = A$.

For the special case of quadratic polynomials the following more precise theorem holds.

THEOREM 3. Let $d_i = 2$ $(i \leqslant 3)$. Assume that at most one of the Δ_i's is 0 and let $\Delta_0 = a_3^2 \Delta_1 \Delta_2 + 4a_1 a_2 a_3 \Delta_3$. We have

$$N(x) \ll x^{1/2} \qquad \text{if } \sqrt{\frac{\Delta_0}{\Delta_3}} \notin \mathbb{Q} \text{ and } \sqrt{\frac{\Delta_3}{\Delta_i}} \notin \mathbb{Q} \quad (i = 1, 2),$$

$$N(x) \ll x^{1/2} \log x \qquad \text{if either } \sqrt{\frac{\Delta_0}{\Delta_3}} \notin \mathbb{Q} \text{ or } \sqrt{\frac{\Delta_3}{\Delta_i}} \notin \mathbb{Q} \quad (i = i, 2),$$

$$N(x) \ll x^{1/2} \log^2 x \qquad \text{always},$$

where, by convention, $1/0 \notin \mathbb{Q}$.

In some cases it is possible to give a much sharper estimate for $N(x)$.

THEOREM 4. Let $d_i = 2$, $a_i = 1$ $(i \leqslant 3)$. Assume that $\Delta_i \in \{0, 1, 4, 16\}$ $(i = 1, 2)$, $\sqrt{\Delta_3} \notin \mathbb{Q}$. Then

$$N(x) \ll \log x \qquad \text{if } \Delta_1 \Delta_2 = 0,$$

$$N(x) \ll (\log x)^c \qquad \text{if } \Delta_1 \Delta_2 \neq 0, \quad 32\Delta_3 \equiv 0 \bmod \Delta_1 \Delta_2$$

and $2^c > 5 + 4/(c-1)$.

As to lower bounds for $N(x)$ we have two results for the quadratic case.

THEOREM 5. If $d_i = 2$ $(i \leqslant 3)$, if each of the polynomials f_i $(i \leqslant 3)$ has an integer zero and if at most one of these is double then

$$N(x) \gg x^{c_0}$$

for some positive c_0 (depending on the f_i's) if $\sqrt{a_1 a_2 a_3} \in \mathbb{Q}$ and

$$N(x) \gg \exp_2\left(\frac{\log 2 \cdot \log_2 x}{\log_3 x}\right) \qquad \text{for } x > x_0$$

always.

The symbols $\exp_k$ and $\log_k$ denote, here and in the sequel, the k-th iterate of the exponential and the logarithmic functions respectively.

The numbers $c_1, c_2, \ldots$ depend only on polynomials f_i.

In some cases, where $d_i = 2$ $(i \leqslant 3)$, $\sqrt{a_1 a_2 a_3} \in \mathbb{Q}$, it is possible to give an asymptotic formula for $N(x)$. We work out one such example at the end of the paper. If $d_i = 2$ $(i \leqslant 3)$, $\sqrt{a_1 a_2 a_3} \notin \mathbb{Q}$ we conjecture that $N(x) \ll x^{\varepsilon}$ for every $\varepsilon > 0$.

1. Proof of Theorem 1.

Throughout this section constants involved in the symbol $\ll$ will depend on the f_i's ($i = 1, 2, 3$) and possibly on other specified parameters. We may also assume $d_1, d_2, d_3 \geqslant 2$. Indeed if $d_i = 1$ ($i = 1$ or 2) all solutions of (1) with $f_3(x_3) \neq 0$ are trivial, thus $N(x) \leqslant d_3$; if $d_3 = 1$ then trivially

$$N(x) \ll x^{1/\min\{d_1, d_2\}}.$$

For $a \in \mathbb{Z}$ and $i = 1$ or 2 define $N^{(i)}(a, x) = \#\{x_3 \mid |x_3| \leqslant x$ and (1) has a non-trivial solution with $x_i = a\}$.

We shall use a strong recent result due to E. Bombieri and J. Pila ([1], Th. 5), which we state as

LEMMA 1. Let C be an absolutely irreducible curve of degree $\mathcal{D} \geqslant 2$ and let $N \geqslant \exp(\mathcal{D}^c)$. Then the number of integral points on C and inside a square of side N does not exceed

$$N^{1/\mathcal{D}} \exp\left(12\sqrt{\mathcal{D} \log N \log_2 N}\right).$$

This lemma implies

LEMMA 2. For every a we have

$$N^{(1)}(a, x) \ll x^{\gamma + \varepsilon},$$

where

$$\gamma = \min\left\{\frac{1}{2}, \frac{(d_2, d_3)}{d_2}\right\}.$$

PROOF. If $f_1(a) = 0$ then clearly $N^{(1)}(a, x) \leqslant d_3$. If $f_1(a) \neq 0$ we consider the curve Γ defined by

$$f_3(x_3) - f_1(a) f_2(x_2) = 0.$$

Clearly $N^{(1)}(a, x)$ does not exceed the number $M(x)$ of integral points on Γ with $|x_3| \leqslant x$ and with the further condition $x_2 \neq p(x_3)$ in case there exists an identity

$$f_3(t) = f_1(a) f_2(p(t)), \qquad p \in \mathbb{Q}[t] \setminus \mathbb{Q}.$$

Let

(2) $$f_3(x_3) - f_1(a) f_2(x_2) = \prod_{\mu=1}^{m} F_\mu(x_2, x_3)^{e_\mu}$$

be a decomposition into powers of absolutely irreducible factors F_μ, relatively prime in pairs, corresponding to irreducible curves Γ_μ. Defining $M_\mu(x)$ for Γ_μ as $M(x)$ is defined for Γ we obtain

(3) $$N^{(1)}(a, x) \leq M(x) \leq \sum_{\mu=1}^{m} M_\mu(x).$$

If $\deg_{x_2} F_\mu = 1$ we have on Γ_μ $x_2 = p(x_3)$, $p \in \mathbb{C}[x_3]$, thus by the definition of M_μ

(4) $M_\mu(x) = 0$ if $p \in \mathbb{Q}[x_3]$, $\quad M_\mu(x) \leq \deg_{x_3} F_\mu$ if $p \notin \mathbb{Q}[x_3]$.

In general, if x_2, x_3 are given weight d_3, d_2 respectively, the polynomial on the left hand side of (2) has the highest isobaric part

$$a_3 x_3^{d_3} - f_1(a) a_2 x_2^{d_2}.$$

This is the product of the highest isobaric parts of the polynomials $F_\mu(x_2, x_3)^{e_\mu}$, hence

$$\frac{\deg_{x_3} F_\mu}{\deg_{x_2} F_\mu} = \frac{d_3}{d_2} \qquad (1 \leq \mu \leq m).$$

It follows that

$$\deg_{x_2} F_\mu \geq \frac{d_2}{(d_2, d_3)}$$

thus either (4) holds or

$$\deg_{x_2} F_\mu \geq \gamma^{-1}, \qquad \deg_{x_3} F_\mu \geq \gamma^{-1} \frac{d_3}{d_2}.$$

Observe also that if (x_2, x_3) is a point on Γ with $|x_3| \leq x$ then

$$|f_2(x_2)| \leq |f_3(x_3)| \ll |x_3^{d_3}| \leq x^{d_3},$$

whence $|x_2| \ll x^{d_3/d_2}$.

Let $\mathscr{D}_\mu$ be the degree of the curve Γ_μ. Two cases occur

1) $d_2 > d_3$, $\mathscr{D}_\mu = \deg_{x_2} F_\mu$. Now for large x the integral points on Γ_μ

with $|x_3| \leq x$ lie in a square of side $2x$. Application of Lemma 1 gives

$$M_\mu(x) \ll_\varepsilon x^{1/\mathcal{D}_\mu + \varepsilon} \leq x^{\gamma + \varepsilon}.$$

2) $d_3 \geq d_2$, $\mathcal{D}_\mu = \deg_{x_3} F_\mu$. In this case for large x the integral points in question lie in a square of side $\ll x^{d_3/d_2}$ and the application of Lemma 1 gives

$$M_\mu(x) \ll_\varepsilon (x^{d_3/d_2})^{1/\mathcal{D}_\mu + \varepsilon} \leq x^{\gamma + \varepsilon}.$$

Hence by (3)

$$N^{(1)}(a, x) \ll_\varepsilon x^{\gamma + \varepsilon}.$$

Observe that in view of the strong uniformity in Lemma 1 the constant in the symbol $\ll$ is independent of a.

LEMMA 3. *Under the assumptions of Theorem 1 the number of integers a such that the curve $f_3(x) = f_1(a) f_2(x_2)$ is reducible over $\mathbb{C}$ is finite.*

PROOF. By E. Noether's theorem (see [11], Theorem 15) the set V of $\lambda \in \mathbb{C}$ such that the curve in question is reducible over $\mathbb{C}$ is an affine algebraic variety (note that $0 \in V$ since $d_3 \geq 2$). If $\dim V = 0$, $\operatorname{card} V < \infty$ and the assertion of the lemma follows. If $\dim V = 1$, $V = \mathbb{C}$ and by Bertini's theorem (see [11], Theorem 18) we have

$$f_3(x_3) - \lambda f_2(x_2) = \sum_{i=0}^{n} a_i(\lambda)\, \varphi^{n-i} \psi^i, \tag{5}$$

where $n \geq 2$, $a_i \in \mathbb{C}[\lambda]$, $\varphi, \psi \in \mathbb{C}[x_2, x_3]$. It follows that

$$f_3(x_3) = \sum_{i=0}^{n} a_i(0)\, \varphi^{n-i} \psi^i. \tag{6}$$

Let

$$\sum_{i=0}^{n} a_i(0)\, t^{n-i} = a_m(0) \prod_{j=1}^{m} (t - \zeta_j), \qquad \zeta_j \in \mathbb{C}.$$

It follows from (6) that

$$\varphi - \zeta_j \psi \in \mathbb{C}[x_3] \quad (1 \leq j \leq m), \quad \psi^{n-m} \in \mathbb{C}[x_3].$$

Hence if either $n > m$ or at least two ζ_j $(1 \leq j \leq m)$ are distinct we obtain $\varphi, \psi \in \mathbb{C}[x_3]$ and by (5) $f_2(x_2) \in \mathbb{C}[x_3]$, a contradiction. If $n = m$ and all ζ_j are equal we obtain

$$f_3(x_3) = a_n(0)(\varphi - \zeta_1 \psi)^n,$$

contrary to the assumption that f_3 has no multiple zeros.

Proof of Theorem 1. Set $q = d_3/(d_1 + d_2)$ and observe that (1) implies that at least one of the inequalities

$$|x_i| \leqslant c_1 |x_3|^q, \qquad i = 1, 2$$

holds. Thus

$$N(x) \leqslant N^{(1)}(x) + N^{(2)}(x) \tag{7}$$

where

$$N^{(i)}(x) = \sum_{|a| \leqslant c_1 x^q} N^{(i)}(a, x).$$

In order to estimate $N^{(1)}(x)$ we shall follow different arguments depending on the magnitude of a.

Clearly, if $f_1(a) = 0$ then $N^{(1)}(a, x) \leqslant d_3$, while if $f_1(a) \neq 0$, as we shall assume from now on,

$$N^{(1)}(a, x) \leqslant \# \{x_3 \mid |x_3| \leqslant x,\ f_3(x_3) \equiv 0 \bmod f_1(a)\}$$
$$\leqslant \rho(f_1(a)) \left\{ \frac{x}{|f_1(a)|} + 1 \right\},$$

where $\rho(M)$ is the number of solutions of the congruence

$$f_3(t) \equiv 0 \bmod M.$$

Since $\Delta_3 \neq 0$ we have by the theorem of Sándor [9] and Huxley [5]

$$\rho(M) \leqslant |\Delta_3|^{1/2} d_3^{\omega(M)},$$

where $\omega(M)$ is the number of distinct prime factors of M. For our purpose the weaker estimate

$$\rho(M) \ll_\varepsilon M^\varepsilon \qquad \text{for all } \varepsilon > 0$$

suffices. Since

$$|f_1(a)| \asymp |a|^{d_1} \qquad \text{for } af_1(a) \neq 0$$

we obtain

$$N^{(1)}(a, x) \ll_\varepsilon \frac{x}{|a|^{d_1 - \varepsilon}} + |a|^\varepsilon .$$

Using this estimate for $|a| \geq x^\delta$, $\delta = 1/d_1 - 1/d_1 d_2$ we easily obtain

$$\sum_{x^\delta \leq |a| \leq c_1 x^q} N^{(1)}(a, x) \ll_\varepsilon x^{1/d_1 + 1/d_2 - 1/d_1 d_2 + \varepsilon} + x^{q + \varepsilon} \tag{8}$$

for all $\varepsilon > 0$. (Of course the sum may be empty).

If $|a| < x^\delta$ and $f_3(x_3) - f_1(a) f_2(x_2)$ is irreducible over $\mathbb{C}$ we apply Lemma 1 to the square $|x_3| \leq x$ if $d_3 < d_2$ or to the square $|x_2| \ll x^{d_3/d_2}$ if $d_3 \geq d_2$, as in the proof of Lemma 2 and similarly obtain

$$N^{(1)}(a, x) \ll_\varepsilon x^{1/d_2 + \varepsilon} .$$

This gives

$$\sum{}^{*} N^{(1)}(a, x) \ll_\varepsilon x^{1/d_1 + 1/d_2 - 1/d_1 d_2 + \varepsilon} \tag{9}$$

where $\sum^{*}$ is taken over all integers a with $|a| \leq x^\delta$ such that $f_3(x_3) - - f_1(a) f_2(x_2)$ is irreducible over $\mathbb{C}$.

By Lemma 3 and Lemma 2

$$\sum_{|a| \leq x^\delta} N^{(1)}(a, x) - \sum{}^{*} N^{(1)}(a, x) \ll_\varepsilon x^{\gamma + \varepsilon} . \tag{10}$$

Combining the estimates (8), (9), (10) we obtain

$$N^{(1)}(x) \ll_\varepsilon x^{c + \varepsilon} .$$

In view of symmetry the same estimate holds for $N^{(2)}(x)$ and the theorem follows by virtue of (7).

REMARK 1. If f_3 has multiple zeros with maximal multiplicity m a similar, but more complicated argument shows that

$$N(x) \ll_\varepsilon x^{c_0 + \varepsilon}$$

where

$$c_0 = \max\left\{\frac{d_3}{d_1+d_2},\ \frac{m}{\min\{d_1,d_2\}} + \frac{1}{\max\{d_1,d_2\}} - \frac{m}{d_1 d_2},\right.$$
$$\left.\min\left\{\frac{1}{2},\ \frac{(d_1,d_3)}{d_1}\right\},\ \min\left\{\frac{1}{2},\ \frac{(d_2,d_3)}{d_2}\right\}\right\}$$

provided f_i $(i = 1, 2)$ has at least two zeros of multiplicity not divisible by p for every prime p such that both f_3 and f_{3-i} are p-th powers in $\mathbb{C}[x]$. The above estimate is not trivial only if $d_i > m$ $(i = 1, 2)$.

REMARK. 2. Another proof of Theorem 1, but with a worse estimate for c (which, however, remains < 1 provided $q < 1$, $d_1, d_2 \geq 2$ and dependent only on d_1, d_2, d_3) may be given without appealing to Bombieri-Pila's theorem. Instead one may follow one of classical proofs of the Hilbert Irreducibility Theorem (namely the one based on a certain theorem of Dörge, as given in [11], § 22) to bound the number of integers $x_3 \leq x$ such that the equation

$$f_3(x_3) = \lambda f_2(x_2)$$

has a solution $x_2 \in \mathbb{Z}$ (here λ is a real parameter, $|\lambda| \geq 1$). The only modifications with respect to the mentioned method come from the fact that one needs uniformity with respect to λ.

2. Proof of Theorem 2.

Suppose that

$$f_3(t) = m_i f_1(p_i(t)) \qquad i = 1, 2. \tag{11}$$

It follows that

$$\mathbb{C}(p_1(t)) \cap \mathbb{C}(p_2(t)) \neq \mathbb{C},$$

hence, by a theorem of Engstrom (see [11], Theorem 5),

$$\mathbb{C}(p_1(t)) \cap \mathbb{C}(p_2(t)) = \mathbb{C}(p_0(t))$$

where $p_0 \in \mathbb{C}[t]$ and $\deg p_0 = [\deg p_1, \deg p_2]$.

However, by (11), $\deg p_1 = \deg p_2$, hence $\deg p_0 = \deg p_i$ $(i = 1, 2)$ and we obtain

$$p_i = a_i p_0 + b_i, \qquad a_i, b_i \in \mathbb{C}.$$

Therefore $p_2 = \alpha p_1 + \beta$ and by (11)

$$m_2 f_1(\alpha t + \beta) = m_1 f_1(t) \qquad \alpha, \beta \in \mathbb{C}. \tag{12}$$

Let Z be the set of zeros of f_1, $\rho =$ diameter of Z.
By the assumption $\rho > 0$ and by (12) we get

$$|\alpha|\,\rho = \rho, \qquad \text{hence } |\alpha| = 1.$$

By (11) again we gave $|m_1| = |m_2|$.

3. Proof of Theorem 3.

LEMMA. 4. Let d, $q = 2^\alpha m$, m odd, be non-zero integers without a common square factor greater than 1. The total number $M_0(d, q)$ of essentially distinct representations of q by a complete system of inequivalent integral binary quadratic forms with discriminant $4d$ equals

$$c(d, \alpha) \sum_{\mu \mid m} \left(\frac{d}{\mu}\right),$$

where

$$c(d, \alpha) = \begin{cases} 2\alpha - 1 & \text{if } d \equiv 1 \bmod 8, \ \alpha > 0, \\ 3 & \text{if } d \equiv 5 \bmod 8, \ \alpha > 0 \text{ even}, \\ 2 & \text{otherwise}. \end{cases}$$

If two representations are not essentially distinct they differ by proper automorph of the relevant form.

REMARK 3. This lemma generalizes the classical result of Dirichlet ([3], § 91) in which it is assumed that $(q, 2d) = 1$. A generalization to the case where q and $4d$ have no common square factor greater than 1 given as Theorem 55 of [6] is false. It fails e.g. for $d = p$, $q = p^2$, p an odd prime. Dirichlet proved also a related result concerning forms with odd discriminant d (in modern terminology). In this case the extended formula is the same as the original one

$$\sum_{\mu \mid q} \left(\frac{d}{\mu}\right).$$

PROOF. Let $M(d, q)$ be total number of essentially different proper representations of q by a complete system of quadratic forms in question. By Theorem 53 of [6] $M(d, q)$ is the number of distinct solutions of the congruence

$$x^2 \equiv d \bmod q.$$

(Note that our d is denoted by $-d$ in [6]), hence it is a multiplicative function of q. On the other hand

$$M_0(d, q) = \sum_{r^2 \mid q} M(d, q/r^2), \tag{13}$$

hence $M_0(d, p)$ is also a multiplicative function of q and it suffices to evaluate it for $q = p^\alpha$, p a prime. By Theorem 54 of [6]

$$M(d, 2^\alpha) = \begin{cases} 1 & \text{if } \alpha < 2, \\ 2 & \text{if } \alpha = 2 \text{ and } d \equiv 1 \bmod 4, \\ 4 & \text{if } \alpha \geqslant 3 \text{ and } d \equiv 1 \bmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

Using (13) we find by a little tedious calculation

$$M_0(d, 2^\alpha) = c(d, \alpha).$$

If $p > 2$, $p \mid d$ we have by Theorem 54 of [6]

$$M(d, p^\alpha) = \begin{cases} 1 & \text{if } \alpha \leqslant 1, \\ 0 & \text{otherwise,} \end{cases}$$

hence by (13) we obtain

$$M_0(d, p^\alpha) = 1 = \sum_{\mu \mid p^\alpha} \left(\frac{d}{\mu}\right).$$

If $p > 2$, $p \nmid d$ we have by Theorem 54 of [6]

$$M(d, p^\alpha) = 1 + \left(\frac{d}{p}\right), \qquad (\alpha > 0)$$

hence by (13) we obtain

$$M_0(d, p^\alpha) = \sum_{\mu \mid p^\alpha} \left(\frac{d}{\mu}\right).$$

Since $\sum_{\mu \mid m} (d/\mu) = \prod_{p^\alpha \| m} \sum_{\mu \mid p^\alpha} (d/\mu)$ the lemma follows.

LEMMA 5. Let a polynomial $F \in \mathbb{Z}[x]$ have no multiple zeros and

$\rho(p)$ be the number of solutions of the congruence

$$F(x) \equiv 0 \mod p.$$

Let f be a multiplicative function such that for all prime powers p^l

$$0 \leqslant f(p^l) \leqslant Al^B, \qquad A,\ B \text{ constants.}$$

We have

$$\sum_{\substack{n \leqslant x \\ F(n) \neq 0}} f(|F(n)|) \ll x \exp S(x),$$

where

$$S(x) = \int_{p \leqslant x} \frac{\rho(p)}{p}(f(p) - 1).$$

PROOF. The sequence $\{|F(n)|\}$ $(F(n) \neq 0)$ and the function f satisfy the assumption of Wolke's Theorem 1 ([12], p. 55) except possibly the second part of the assumption (A_2) the inequality $\rho(p) < p$, which may fail for finitely many primes p. If such exceptional primes exist the function $P(x)$ occuring in Lemma 2 of [12] has to be redefined as $\prod_{p \leqslant x,\ \rho(p) < p} (1 - \rho(p)/p)$, but otherwise only minor modifications of the proof are needed.

PROOF OF THEOREM 3. We shall give the proof first for the principal case $\Delta_1\Delta_2\Delta_3 \neq 0$ and then indicate briefly the changes needed if $\Delta_1\Delta_2\Delta_3 = 0$. On completing the squares we obtain

(14) $$N(x) \leqslant 2N_1(x) + 2N_2(x) + O(1),$$

where $N_i(x)$ is the number of positive integers $y_3 \leqslant 2a_3 x$ such that

(15) $$a_3(y_1^2 - \Delta_1)(y_2^2 - \Delta_2) = 4a_1 a_2(y_3^2 - \Delta_3)$$

is soluble in integers y_1, y_2 satisfying $0 \leqslant y_i \leqslant y_{3-i}$ and

$$y_i^2 - \Delta_i \neq \frac{4a_1 a_2 \Delta_3}{a_3 \Delta_{3-i}}$$

(the equality corresponds to trivial solutions).

If $0 \leqslant y_1 \leqslant y_2$ the equation (15) implies

$$y_1 \leqslant c_2 \sqrt{y_3} \leqslant c_3 \sqrt{x},$$

hence

$$N_1(x) \leqslant \sum_{0 \leqslant y_1 \leqslant c_3 \sqrt{x}}^{*} N(y_1, x), \tag{16}$$

where $N(y_1, x)$ is the number of solutions of the equation (15) in non-negative integers y_2, y_3 with $y_3 \leqslant 2a_3 x$ and the star signifies the condition

$$y_1 \neq \sqrt{\Delta_1 + \frac{4a_1 a_2 \Delta_3}{a_3 \Delta_2}} \tag{17}$$

for y_1 in the range of summation.

The equation (15) can be rewritten in the form

$$a_3 (y_1^2 - \Delta_1) y_2^2 - 4a_1 a_2 y_3^2 = a_3 (y_1^2 - \Delta_1) \Delta_2 - 4a_1 a_2 \Delta_3 = p(y_1) \tag{18}$$

where in view of (17) $p(y_1) \neq 0$.

Let

$$m_1 = (a_3 (y_1^2 - \Delta_1), 4a_1 a_2),$$

m_2^2 be the maximal square dividing $\left(\dfrac{4a_1 a_2}{m_1}, \Delta_2 \right)$,

m_3^2 be the maximal square dividing $\left(\dfrac{a_3 (y_1^2 - \Delta_1)}{m_1}, \Delta_3 \right)$.

It follows from (18) that $m_i \mid y_i$ $(i = 2, 3)$, $y_i = m_i z_i$ $(z_i \in \mathbb{Z})$,

$$\frac{a_3 (y_1^2 - \Delta_1)}{m_1 m_3^2} z_2^2 - \frac{4a_1 a_2}{m_1 m_2^2} z_3^2 = \frac{p(y_1)}{m_1 m_2^2 m_3^2} = q(y_1). \tag{19}$$

Let

$$d(y_1) = \frac{4a_1 a_2 a_3 (y_1^2 - \Delta_1)}{m_1^2 m_2^2 m_3^2}.$$

We infer that $(d(y_1), q(y_1))$ is squarefree.

Since the quadratic form on the left hand side of (19) is primitive all its proper automorphs are given by the formulae

$$z_2' = tz_2 + \frac{4a_1 a_2}{m_1 m_2^2} u z_3, \qquad z_3' = \frac{a_3(y_1^2 - \Delta_1)}{m_1 m_3^2} u z_2 + t z_3,$$

where the integers t, u satisfy the Pell equation

$$t^2 - d(y_1) u^2 = 1$$

(see [6], Theorem 50). These formulae imply

$$\sqrt{\frac{a_3(y_1^2-\Delta_1)}{m_1 m_3^2}} z_2' + \sqrt{\frac{4a_1 a_2}{m_1 m_2^2}} z_3' =$$

$$= \left(\sqrt{\frac{a_3(y_1^2-\Delta_1)}{m_1 m_3^2}} z_2 + \sqrt{\frac{4a_1 a_2}{m_1 m_2^2}} z_3\right)(t + u\sqrt{d(y_1)}).$$

The condition $m_3 z_3 = y_3 \leqslant 2a_3 x$ together with (19) implies

$$\left|\sqrt{\frac{a_3(y_1^2-\Delta_1)}{m_1 m_3^2}} z_2 + \sqrt{\frac{4a_1 a_2}{m_1 m_2^2}} z_3\right| \leqslant c_4 x,$$

on the other hand the conditions $z_i \geqslant 0$, $z_i' \geqslant 0$ $(i = 2, 3)$ restrict the signs of t, u. Hence we obtain

$$N(y_1, x) \leqslant M_0(d(y_1), q(y_1)) \cdot$$

$$\cdot \begin{cases} 1 + \left[\dfrac{\log c_4 x}{\log \eta(y_1)}\right] & \text{if } d(y_1) > 0 \text{ is not a square,} \\ 1 & \text{otherwise,} \end{cases}$$

where $\eta(y_1)$ is the fundamental totally positive unit of $\mathbb{Z}[\sqrt{d(y_1)}]$.

If $d(y_1) > 0$ is not a square we have

$$d(y_1) \geqslant \left|\frac{a_3(y_1^2-\Delta_1)}{4a_1 a_2 \Delta_3}\right|.$$

Since $\eta(y_1) \geqslant 2\sqrt{d(y_1)}$ we obtain

$$N(y_1, x) \leqslant \frac{c_5 \log x}{\log(y_1+2)} M_0(d(y_1), q(y_1)) \tag{20}$$

and it remains to estimate $M_0(d(y_1), q(y_1))$. By Lemma 4

$$M_0(d(y_1), q(y_1)) \leqslant 3 \sum_{\mu | q(y_1)}^{**} \left(\frac{d(y_1)}{\mu}\right),$$

where $\sum^{**}$ signifies that μ in the range of summation is restricted to odd integers unless $d(y_1) \equiv 1 \bmod 8$.

We have for all d, e, q different from 0

$$\sum_{\mu|q}^{**}\left(\frac{d}{\mu}\right) \leqslant \sum_{\mu|(q,e^2)}^{**}\left(\frac{d}{\mu}\right) \cdot \sum_{\mu|q/(q,e^2)}^{**}\left(\frac{d}{\mu}\right). \tag{21}$$

This can be verified for q equal to a prime power and the follows by multiplicativity of both sides with respect to q.

Taking $d = d(y_1)$, $e = \Delta_2$, $q = q(y_1)$ we obtain

$$M_0(d(y_1), q(y_1)) \leqslant c_6 \sum_{\mu|q(y_1)/(q(y_1),\Delta_2^2)}^{**} \left(\frac{d(y_1)}{\mu}\right) \leqslant 3c_6 \sum_{\mu|q(y_1)/(q(y_1),\Delta_2^2)}^{***} \left(\frac{d(y_1)}{\mu}\right),$$

where $\sum^{***}$ signifies that μ in the range of summation is restricted to odd integers unless $d(y_1) \equiv 1 \bmod 8$ and $q(y_1)/(q(y_1), \Delta_2^2) \equiv 0 \bmod 8$.

Since

$$\left(\frac{q(y_1)}{(q(y_1), \Delta_2^2)}, \frac{\Delta_2^2}{(q(y_1), \Delta_2)^2}\right) = 1$$

we have for all odd $\mu | q(y_1)/(q(y_1), \Delta_2^2)$

$$\left(\frac{d(y_1)}{\mu}\right) = \left(\frac{d(y_1)a^2}{\mu}\right), \qquad a = \frac{\Delta_2}{(q(y_1), \Delta_2)},$$

also if $q(y_1)/(q(y_1), \Delta_2^2)$ is even $d(y_1) \equiv d(y_1)a^2 \bmod 8$.

On the other hand, by (19)

$$d(y_1)\Delta_2^2 = \Delta_2 \cdot \frac{4a_1a_2}{m_1} \cdot \frac{a_3(y_1^2 - \Delta_1)\Delta_2}{m_1 m_2^2 m_3^2} \equiv \Delta_2\Delta_3\left(\frac{4a_1a_2}{m_1m_2m_3}\right)^2 \bmod \Delta_2 q(y_1)$$

hence

$$d(y_1)a^2 \equiv \Delta_2\Delta_3 b(y_1)^2 \bmod \frac{\Delta_2 q(y_1)}{(q(y_1), \Delta_2)^2},$$

where

$$b(y_1) = \frac{4a_1 a_2}{m_1 m_2 m_3 (q(y_1), \Delta_2)}.$$

Since

$$\frac{q(y_1)}{(q(y_1), \Delta_2^2)} \Bigg| \frac{\Delta_2 q(y_1)}{(q(y_1), \Delta_2)^2}$$

it follows that

$$\left(\frac{d(y_1)}{\mu}\right) = \left(\frac{\Delta_2 \Delta_3 b(y_1)^2}{\mu}\right)$$

for all odd $\mu | q(y_1)/(q(y_1), \Delta_2^2)$ and for all $\mu | q(y_1)/(q(y_1), \Delta_2^2)$ if

$$\frac{q(y_1)}{(q(y_1), \Delta_2^2)} \equiv 0 \bmod 8.$$

Thus finally

$$\text{(22)} \qquad M_0(d(y_1), q(y_1)) \leqslant 3c_6 \sum_{\mu | q(y_1)/(q(y_1), \Delta_2^2)}^{***} \left(\frac{\Delta_2 \Delta_3 b(y_1)^2}{\mu}\right)$$

$$\leqslant 3c_6 \sum_{\mu | q(y_1)/(q(y_1), \Delta_2^2)}^{**} \left(\frac{\Delta_2 \Delta_3 b(y_1)^2}{\mu}\right).$$

The ratio

$$\frac{p(y_1)}{q(y_1)} = m_1 m_2^2 m_3^2 \, | 4a_1 a_2 \Delta_2 \Delta_3$$

depends only upon the residue class of $y_1 \bmod 4a_1 a_2 \Delta_3$ while $(q(y_1), \Delta_2^2)$ and $b(y_1)$ depend only upon the residue class of $y_1 \bmod 4a_1 a_2 \Delta_2^3 \Delta_3$.

For every residue $r \bmod 4a_1 a_2 \Delta_2^3 \Delta_3$, we have

$$F_r(t) = \frac{q(4a_1 a_2 \Delta_2^3 \Delta_3 t + r)}{(q(r), \Delta_2^2)} \in \mathbb{Z}[t]$$

and F_r has a multiple zero if and only if $\Delta_0 = 0$. Moreover if $\Delta_0 \neq 0$ the number $\rho_r(p)$ of solutions of the congruence

$$F_r(n) \equiv 0 \bmod p$$

satisfies for sufficiently large primes p

$$\rho_r(p) = 1 + \left(\frac{\Delta_0 \Delta_2}{p}\right). \tag{23}$$

Taking

$$f_r(m) = \sum_{\mu \mid m}{}^{**} \left(\frac{\Delta_2 \Delta_3 b(r)^2}{\mu}\right)$$

we find that f_r is multiplicative,

$$\begin{cases} f_r(2) = 2 & \text{if } \Delta_2 \Delta_3 b(r)^2 \equiv 1 \bmod 8, \ 1 \text{ otherwise} \\ f_r(p) = 1 + \left(\dfrac{\Delta_2 \Delta_3 b(r)^2}{p}\right) & \text{for } p > 2, \\ f_r(p^l) \leqslant l + 1, \end{cases} \tag{24}$$

hence if $\Delta_0 \neq 0$ the polynomial F_r and the function f_r satisfy the assumptions of Lemma 5 and we obtain

$$\sum_{\substack{y_1 \leqslant c_4 \sqrt{x} \\ y_1 \equiv r \bmod 4a_1 a_2 \Delta_2^3 \Delta_3}} M_0(d(y_1), q(y_1)) \ll x^{1/2} \exp S_r(x), \tag{25}$$

where

$$S_r(x) = \sum_{p \leqslant c_7 \sqrt{x}} \frac{\rho_r(p)}{p} (f(p) - 1) \qquad (0 \leqslant r < 4a_1 a_2 \Delta_2^3 \Delta_3).$$

Using (23), (24) and the classical formula for characters χ

$$\sum_{p \leqslant x} \frac{\chi(p)}{p} = \begin{cases} \log \log x + O(1) & \text{if } \chi \text{ is principal,} \\ O(1) & \text{otherwise,} \end{cases}$$

we obtain

$$S_r(x) = O(1) \quad \text{if } \sqrt{\frac{\Delta_0}{\Delta_3}} \notin \mathbb{Q} \text{ and } \sqrt{\frac{\Delta_3}{\Delta_2}} \notin \mathbb{Q},$$

$$S_r(x) = 2 \log \log x + O(1) \quad \text{if } \sqrt{\frac{\Delta_0}{\Delta_3}} \in \mathbb{Q} \text{ and } \sqrt{\frac{\Delta_3}{\Delta_2}} \in \mathbb{Q},$$

$$S_r(x) = \log \log x + O(1), \quad \text{otherwise}.$$

This gives in views of (25)

$$\sum_{0\le y_1\le c_3\sqrt{x}} M_0(d(y_1),\, q(y_1)) \ll$$

$$\ll \begin{cases} x^{1/2} & \text{if } \sqrt{\dfrac{\Delta_0}{\Delta_3}} \notin \mathbb{Q} \text{ and } \sqrt{\dfrac{\Delta_3}{\Delta_2}} \notin \mathbb{Q}, \\ x^{1/2}\log x & \text{if either } \sqrt{\dfrac{\Delta_0}{\Delta_3}} \notin \mathbb{Q} \text{ or } \sqrt{\dfrac{\Delta_3}{\Delta_2}} \notin \mathbb{Q}, \\ x^{1/2}\log^2 x & \text{always.} \end{cases}$$

Using (20) we obtain by partial summation the same estimate for the $\sum^*_{0\le y_1\le c_3\sqrt{x}} N(y_1, x) = N_1(x)$.

In view of the symmetry between y_1 and y_2 we obtain for $N_2(x)$ a similar estimate with Δ_2 replaced by Δ_1. In view of (14) this gives the theorem for the case $\Delta_0 \ne 0$.

If $\Delta_0 = 0$, we have

$$F_r = A_r G_r^2, \qquad \text{where } A_r \in \mathbb{Z},\ G_r \in \mathbb{Z}[t],$$

and G_r is of degree 1. By (21) applied with

$$d = \Delta_2\Delta_3 b(r)^2, \qquad e = G_r(t), \qquad q = F_r(t)$$

and by (22) we obtain in this case

$$M_0(d(4a_1a_2\Delta_2^3\Delta_3 t + r),\, q(4a_1a_2\Delta_2^3\Delta_3 t + r)) \ll \sum^{**}_{\mu\mid G_r(t)^2} \left(\frac{\Delta_2\Delta_3 b(r)^2}{\mu}\right).$$

Taking

$$g_r(m) = \sum^{**}_{\mu\mid m^2} \left(\frac{\Delta_2\Delta_3 b(r)^2}{\mu}\right)$$

we find that g is a multiplicative function and

$g_r(2) = 3 \quad$ if $\Delta_2\Delta_3 b(r)^2 \equiv 1 \bmod 8$, 1 otherwise,

$g_r(p) = 2 + \left(\dfrac{\Delta_2\Delta_3 b(r)^2}{p}\right) \quad$ if $p \nmid \Delta_2\Delta_3 b(r)^2$, 1 otherwise $(p > 2)$,

$g_r(p^l) \le 2l + 1$.

Applying Lemma 4 to the polynomial G_r and the function g_r we find by a computation similar to that made before that

$$N_1(x) \ll x^{1/2} \log x \quad \text{if } \sqrt{\frac{\Delta_3}{\Delta_2}} \notin \mathbb{Q},$$
$$N_1(x) \ll x^{1/2} \log^2 x \quad \text{always}.$$

In view of the symmetry between y_1 and y_2 we obtain for $N_2(x)$ a similar estimate with Δ_2 replaced by Δ_1. In view of (14) this completes the proof.

Assume now that $\Delta_1 = 0$, $\Delta_2 \Delta_3 \neq 0$. Then $\Delta_0 \neq 0$, but the symmetry between $N_1(x)$ and $N_2(x)$ is lost. $N_1(x)$ can be estimated as above, i.e.

$$N_1(x) \ll \begin{cases} x^{1/2} & \text{if } \sqrt{\dfrac{\Delta_0}{\Delta_3}} \notin \mathbb{Q} \text{ and } \sqrt{\dfrac{\Delta_3}{\Delta_2}} \notin \mathbb{Q}, \\ x^{1/2} \log x & \text{if either } \sqrt{\dfrac{\Delta_0}{\Delta_3}} \notin \mathbb{Q} \text{ or } \sqrt{\dfrac{\Delta_3}{\Delta_2}} \notin \mathbb{Q}, \\ x^{1/2} \log^2 x & \text{always}. \end{cases}$$

If we reverse the roles of y_1 and y_2 we find that

$$q(y_2) \mid 4a_1 a_2 \Delta_3$$

hence by Lemma 4

$$M(d(y_2), q(y_2)) \ll 1$$

(16) and (20) give by partial summation

$$N_2(x) \ll x^{1/2}$$

and the theorem follows from (14). A similar argument works if $\Delta_2 = 0$, $\Delta_1 \Delta_3 \neq 0$.

Finally assume that $\Delta_3 = 0$, $\Delta_1 \Delta_2 \neq 0$. Then $\Delta_0 \neq 0$ and there is a symmetry between $N_1(x)$ and $N_2(x)$. However, the lower estimate for $d(y_1)$ is not valid and hence instead of (20) we have only

$$N(y_1, x) \leqslant c_8 \log x M_0(d(y_1), q(y_2)).$$

On the other hand,

$$q(y_1) = \frac{a_3(y_1^2 - \Delta_1)\Delta_2}{m_1 m_2^2 m_3^2}$$

hence

$$\frac{q(y_1)}{(q(y_1),\, d(y_1))} \leqslant m_1 \Delta_2 \leqslant 4a_1 a_2 \Delta_2$$

and by Lemma 4

$$M(d(y_1),\, q(y_1)) \ll 1.$$

It follows by (16) that $N_1(x) \ll x^{1/2} \log x$, by symmetry the same estimate holds for $N_2(x)$ and by (14) the theorem follows.

REMARK 4. The established estimate for $N(x)$ is valid also for the number of all non-trivial integer solutions of (1) satisfying $|x_3| \leqslant x$.

REMARK 5. If $\Delta_i = \Delta_3 = 0$ for $i = 1$ or 2, all solutions of (1) with $f_3(x_3) \neq 0$ are trivial thus $N(x) \leqslant 2$.

If $\Delta_1 = \Delta_2 = 0$, $\Delta_3 \neq 0$ the equation (18) gives

$$a_3 (y_1 y_2)^2 - 4a_1 a_2 y_3^2 = -4a_1 a_2 \Delta_3,$$

hence $N_1(x) = N_2(x) \ll \log x$ and $N(x) \ll \log x$.

4. Proof of Theorem 4.

If $\Delta_1 = \Delta_2 = 0$ the theorem holds by Remark 5. Therefore we may assume that $\Delta_1 + \Delta_2 > 0$ and in view of symmetry that $\Delta_2 > 0$.

If $\Delta_1 = 0$ we multiply the equation (1) by $16/\Delta_2$ and obtain

$$g_3(y_3) = f_1(x_1) g_2(y_2)$$

where

$$g_i(x) = \frac{16}{\Delta_2} f_i\left(x \frac{\sqrt{\Delta_2}}{4}\right); \qquad y_i = x_i \frac{4}{\sqrt{\Delta_2}} \qquad (i = 2, 3).$$

If $\Delta_1 > 0$ we multiply the equation (1) by $256/\Delta_1 \Delta_2$ and obtain

$$g_3(y_3) = g_1(y_1) g_2(y_2),$$

where

$$g_i(x) = \frac{16}{\Delta_i} f_i\left(x \frac{\sqrt{\Delta_i}}{4}\right), \qquad y_i = x_i \frac{4}{\sqrt{\Delta_i}} \qquad (i = 1, 2)$$

$$g_3(x) = \frac{256}{\Delta_1 \Delta_2} f_i\left(x \frac{\sqrt{\Delta_1 \Delta_2}}{16}\right), \qquad y_3 = x_3 \frac{16}{\sqrt{\Delta_1 \Delta_2}}.$$

In both cases the leading coefficients of g_i are equal to 1.

If $\Delta_1 = 0$ the discriminant of g_2 is 16, if $\Delta_1 > 0$ the discriminants of g_1, g_2 are equal to 16 and the discriminant of g_3 is equal to $256\Delta_3/\Delta_1\Delta_2$. Therefore it is enough to prove the theorem for the cases

1) $\Delta_1 = 0,\ \Delta_2 = 16,\ \sqrt{\Delta_3} \notin \mathbb{Q}$,

2) $\Delta_1 = \Delta_2 = 16,\ \Delta_3 \equiv 0 \bmod 8,\ \sqrt{\Delta_3} \notin \mathbb{Q}$.

In the case 1) on completing the squares we obtain

$$N(x) \leqslant 2N_1(x) + O(1),$$

where $N_1(x)$ is the number of nonnegative integers $y_3 \leqslant x$ for which

$$y_3^2 - \Delta_3 = y_1^2(y_2^2 - 4) \tag{26}$$

is soluble in integer y_1, y_2. For each $y_2 \leqslant |\Delta_3| + 3$ the equation (26) has only $O(\log x)$ solution with $y_3 \leqslant x$ (see the proof of Theorem 3) and for $y_2 > |\Delta_3| + 3$ the equation (26) has no solutions. Indeed, then $|\Delta_3| < \sqrt{y_2^2 - 4}$ and by Theorem 12 of Chapter II of [7] for every solution y_3/y_1 must be a convergent of the continued fraction for $\sqrt{y_2^2 - 4}$. Now the continued fraction expansions of $\sqrt{y^2 - 4}$ are known:

$$\sqrt{y^2 - 4} = \left[y - 1,\ \overline{1,\ \frac{1}{2}(y-4),\ 1,\ 2y - 2}\right] \quad \text{if } y \equiv 0 \bmod 2,\ y > 4,$$

$$\sqrt{y^2 - 4} = \left[y - 1,\ \overline{1,\ \frac{1}{2}(y-3),\ 2,\ \frac{1}{2}(y-3),\ 1,\ 2y - 2}\right]$$

$$\text{if } y \equiv 1 \bmod 2,\ y > 3,$$

(see, e.g. [10], p. 411). It follows that

$$\frac{\Delta_3}{(y_1, y_3)^2} = 1,\ 4,\ -(2y_2 - 5) \text{ or } -(y_2 - 2),$$

which contradicts the assumption $\sqrt{\Delta_3} \notin \mathbb{Q}$.

In the case 2) on completing the squares we obtain

$$N(x) \leqslant 2N_1(x) + O(1) \tag{27}$$

where $N_1(x)$ is the number of nonnegative integers $y_3 \leqslant x$ such that

$$y_3^2 - \frac{\Delta_3}{4} = (y_1^2 - 4)(y_2^2 - 4) \tag{28}$$

is soluble in integers y_1, y_2. This equation can be written in the form

$$y_3^2 - (y_1^2 - 4)y_2^2 = \frac{\Delta_3}{4} - 4(y_1^2 - 4). \tag{29}$$

If $\langle y_1, y_2, y_3 \rangle$ is an integer solution of (29) then by the assumption $\Delta_3 \equiv 0 \bmod 8$ it follows that

$$y_3 \equiv y_1 y_2 \bmod 2.$$

Hence the numbers $y_2^{\pm}$, $y_3^{\pm}$ defined by the formula

$$y_3^{\pm} + \sqrt{y_1^2 - 4}\,y_2^{\pm} = (y_3 + \sqrt{y_1^2 - 4}\,y_2)\left(\frac{y_1 + \sqrt{y_1^2 - 4}}{2}\right)^{\pm 1}$$

are integers and it is easily seen that $\langle y_1, y_2^{\pm}, y_3^{\pm} \rangle$ is a solution of (29).

Let us assign two solutions of (29) is nonnegative integers $\langle y_1, y_2', y_3' \rangle$ and $\langle y_1, y_2'', y_3'' \rangle$ to the same class if there exist numbers $\varepsilon = \pm 1$, $\eta = \pm 1$ and an integer n such that

$$y_3'' + \sqrt{y_1^2 - 4}\,y_2'' = (\varepsilon y_3' + \eta\sqrt{y_1^2 - 4}\,y_2')\,\zeta^n, \qquad \zeta = \frac{y_1 + \sqrt{y_1^2 - 4}}{2}.$$

Let us denote the family of all such classes by $\mathcal{F}(y_1)$.

Any two solutions of (29) differing by an automorph of the quadratic form $x^2 - (y_1^2 - 4)y^2$ belong to the same class since the fundamental solution of the Pell equation $x^2 - (y_1^2 - 4)y^2 = 1$ is given by ζ^2 for y_1 even and by ζ^3 for y_1 odd, Hence $\mathcal{F}(y_1)$ is finite for each y_1 such that

$$y_1^2 - 4 \neq 0, \qquad \frac{\Delta_3}{4} - 4(y_1^2 - 4) \neq 0.$$

If $y_1^2 - 4 = 0$ the equation (29) has no solutions, since $\sqrt{\Delta_3} \notin \mathbb{Q}$.

If $\Delta_3/4 - 4(y_1^2 - 4) = 0$ the equation (29) has only one solution, namely $y_2 = y_3 = 0$, since then $y_3^2 - (\Delta_3/16)y_2^2 = 0$. Thus

$$N_2(y_1) = \operatorname{card}\mathcal{F}(y_1) < \infty \qquad \text{for all } y_1.$$

Given a class $C \in \mathcal{F}(y_1)$ let $A(x, y_1, C)$, $B(y, y_1, C)$ be the number of solutions of (29) belonging to C and such that $y_3 \leqslant x$ or $y_2 \leqslant y$, respectively.

A simple calculation shows that for all $C \in \mathcal{F}(y_1)$, $x \geqslant 2$, $x \geqslant 3$

$$A(x, y_1, C) \leqslant$$

$$\leqslant \frac{2 \log\left(x + \sqrt{x^2 + 4(y_1^2 - 4) - \frac{\Delta_3}{4}}\right) - \log\left(4(y_1^2 - 4) - \frac{\Delta_3}{4}\right)}{\log \zeta} + 1,$$

$$B(y, y_1, C) \leqslant$$

$$\leqslant \frac{2 \log\left(\sqrt{(y_1^2 - 4)(y^2 - 4) + \frac{\Delta_3}{4}} + y\sqrt{y_1^2 - 4}\right) - \log\left(4(y_1^2 - 4) - \frac{\Delta_3}{4}\right)}{\log \zeta} + 1,$$

if $y_1 > \sqrt{4 + |\Delta_3|/16}$, and

$$A(x, y_1, C) \leqslant a(y_1) \log x, \qquad B(y, y_1, C) \leqslant b(y_1) \log y \tag{30}$$

always.

For y_1 sufficiently large, say $y_1 > c_9 > \sqrt{1 + |\Delta_3|/16}$ we obtain

$$\begin{cases} A(x, y_1, C) \leqslant \dfrac{2 \log(2x + c_{10})}{\log(y_1 - 1)} & \text{if } y_1^2 - 4 \leqslant \sqrt{x^2 - \dfrac{\Delta_3}{4}}, \\ B(y, y_1, C) \leqslant \dfrac{2 \log 2y}{\log(y_1 - 1)}. \end{cases} \tag{31}$$

In view of symmetry of the equation (28) with respect to y_1, y_2 we may assume that $y_1 \leqslant y_2$ and hence we have

$$\begin{cases} y_1^2 - 4 \leqslant \sqrt{x^2 - \dfrac{\Delta_3}{4}}, \qquad y_1 \leqslant \sqrt{x} + c_{11}, \\ N_1(x) \leqslant \displaystyle\sum_{\substack{y_1 \leqslant \sqrt{x} + c_{11} \\ C \in F(y_1)}} A(x, y_1, C) = \sum_{\substack{y_1 \leqslant c_9 \\ C \in F(y_1)}} A(x, y_1, C) + \\ \qquad + \displaystyle\sum_{\substack{c_9 < y_1 < \sqrt{x} + c_{11} \\ C \in F(y_1)}} A(x, y_1, C) = O(\log x) + \\ \qquad + \displaystyle\sum_{c_9 < y_1 < \sqrt{x} + c_{11}} N_2(y_1) \frac{2 \log(2x + c_{10})}{\log(y_1 - 1)}. \end{cases} \tag{32}$$

Given a solution $\langle y_1, y_2^0, y_3^0\rangle$ in a class $C \in \mathcal{F}(y_1)$ we choose n such that

$$\sqrt{4(y_1^2-4)\frac{\Delta_3}{4}}\,\zeta^{-1/2} \leqslant (y_3^0 + \sqrt{y_1^2 - 4y_2^0})\,\zeta^n < \sqrt{4(y_1^2-4) - \frac{\Delta_3}{4}}\,\zeta^{1/2}$$

and then obtain from (29)

$$\sqrt{4(y_1^2-4)\frac{\Delta_3}{4}}\,\zeta^{-1/2} < (-y_3^0 + \sqrt{y_1^0 - 4y_2^0})\,\zeta^{-n} \leqslant \sqrt{4(y_1^2-4) - \frac{\Delta_3}{4}}\,\zeta^{1/2}.$$

Setting

$$y_3 + \sqrt{y_1^2 - 4y_2} = (y_3^0 + \sqrt{y_1^2 - 4y_2^0})\,\zeta^n$$

we have $\langle y_1, |y_2|, |y_3|\rangle \in C$ and

$$(33)\qquad 0 < y_2 < \sqrt{4 - \frac{\Delta_3}{4(y_1^2-4)}}\,\zeta^{1/2} < 2\sqrt{y_1} + 1 \qquad (y_1 > c_{12} \geqslant 3).$$

Thus for $y_1 > c_{12}$ every class $C \in \mathcal{F}(y_1)$ contains a solution $\langle y_1, y_2, y_3\rangle$ of (29) satisfying (33). In view of symmetry of (28) with respect to y_1, y_2 we obtain

$$\sum_{c_{12} < y_1 \leqslant y} N_2(y_1) \leqslant \sum_{\substack{y_2 < 2\sqrt{y}+1 \\ C \in F(y_2)}} B(y, y_2, C)$$

and further by (29) and (30)

$$(34)\qquad \sum_{c_{12} < y_1 \leqslant y} N_2(y_1) \leqslant \left(\sum_{y_2 \leqslant c_{13}} b(y_2) N(y_2)\right) \log y + \sum_{c_{12} < y_2 < 2\sqrt{y}+1} N_2(y_2) \frac{2\log 2y}{\log(y_2 - 1)},$$

where $c_{13} = \max\{c_9, c_{12}\}$.

Since $2^c > 5 + 4/(c-1)$ there exists a $c_{14} \geqslant 8$ such that for $y > c_{14}$

$$(35)\qquad \log y + 5(\log 2\sqrt{y})^c + \frac{2\log 2y}{c-1}(\log 2\sqrt{y})^{c-1} < (\log(y-1))^c.$$

We choose a c_{15} such that

$$(36)\qquad c_{15} \geqslant \sum_{y_2 \leqslant c_{13}} b(y_2) N_2(y_2)$$

and

$$\sum_{y \geqslant y_1 < c_{12}} N_2(y_1) \leqslant c_{15}(\log(y-1))^c \tag{37}$$

for all $y \leqslant c_{14}$, $y \geqslant 3$. We shall show by induction on y that the inequality (37) holds for all integers $y \geqslant 3$. Suppose that $y > c_{14} \geqslant 8$ and that (37) holds with y replaced by an arbitrary integer $z < y$, $z \geqslant 3$. Then it holds also with y replaced by an arbitrary real $z \leqslant y-1$, $z \geqslant 3$ and since $2\sqrt{y}+1 \leqslant y-1$, by an arbitrary real $z \leqslant 2\sqrt{y}+1$, $z \geqslant 3$. Using (34), (36), partial summation, the inductive assumption and (35) we obtain

$$\sum_{y \geqslant y_1 > c_{12}} N_2(y_1) \leqslant c_{15}\log y + c_{15}(\log 2\sqrt{y})^c\left(\frac{2\log 2y}{\log 2\sqrt{y}}+1\right)+$$

$$+\int_{c_{12}}^{2\sqrt{y}+1} c_{15}(\log(t-1))^c \frac{2\log 2y}{(t-1)\log^2(t-1)}\,dt \leqslant$$

$$\leqslant c_{15}\left(\log y + 5(\log 2\sqrt{y})^c + \frac{2\log 2y}{c-1}(\log 2\sqrt{y})^{c-1}\right) < c_{15}(\log(y-1))^c$$

which completes the inductive proof of (37). Substituting (37) into (32) and using partial summation again we obtain $N_1(x) \ll (\log x)^c$. The theorem follows by (27).

REMARK 6. The method of proof should extend to the case, where $\Delta_i \in \{0, 1, 4, -4, 16, -16\}$ $(i=1,2)$ however the details become complicated.

REMARK 7. Let us call a polynomial solution every solution of (1) which comes from an identity

$$f_3(p_3(t)) = f_1(p_1(t))f_2(p_2(t)), \tag{38}$$

where $p_1, p_2, p_3 \in \mathbb{Q}[t]$ are polynomials not all constant (thus trivial solutions are polynomial, but in general not vice versa). Then the method of proof of Theorem 4 gives

1) If $a_1 = a_2 = a_3 = 1$, $\Delta_i \in \{1, 4, 16\}$ $(i=1,2)$, $32\Delta_3 \equiv 0 \bmod \Delta_1\Delta_2$ the number of non-polynomial solutions of (1) with $|x_3| \leqslant x$ is $O((\log x)^c)$ for every c with $2^c > 5 + 4/(c-1)$.

2) The number of solutions of (38) in polynomials p_1, p_2, p_3 satisfying the three conditions: $\deg p_3 \leqslant d$, $\mathbb{Q}(p_1, p_2, p_3) = \mathbb{Q}(t)$, p_3 has the

leading coefficient 1 and the second coefficient 0, is finite for every d, in fact less than d^c for a suitable c.

If $a_1 = a_2 = a_3 = 1$, $\sqrt{\Delta_i} \in \mathbb{Q}$ $(i = 1, 2, 3)$ there exist polynomial solutions, see the proof of Theorem 5. The above two facts indicate the way of finding the asymptotic formula for $N(x)$ in the case $a_1 = a_2 = a_3 = 1$, $\Delta_i \in \{1, 4, 16\}$ $(i = 1, 2)$, $32\Delta_3 \equiv 0 (\text{mod } \Delta_1 \Delta_2)$, $\sqrt{\Delta_3} \in \mathbb{Q}$ however many details have to be settled in order to prove such a formula. If $\Delta_1 \in \{1, 4, 16\}$, $\Delta_2 = 0$ the situation is simpler and an example is worked out at the end of the paper.

5. Proof of Theorem 5.

Let $f_i(x) = a_i x^2 + b_i x + c_i$ and $\Delta_i = d_i^2$, $d_i \in \mathbb{Z}$, $d_i \equiv b_i \bmod 2a_i$. On completing the squares we obtain

$$N(x) \geqslant N_0(x) + O(1),$$

where $N_0(x)$ is the number of integers y_3 such that

$$|y_3| \leqslant 2a_3 x, \tag{39}$$

$$y_3 \equiv d_3 \bmod 2a_3 \tag{40}$$

and (15) holds for some integers y_i satisfying

$$y_i \equiv d_i \bmod 2a_i \qquad (i = 1, 2), \tag{41}$$

$$y_i^2 - d_i^2 \neq \frac{4a_1 a_2 d_3^2}{a_3 d_{3-i}^2} \qquad (i = 1, 2). \tag{42}$$

We distinguish two cases

1) $a_1 a_2 a_3$ is a perfect square,

2) $a_1 a_2 a_3$ is not a perfect square.

In the case 1) we assume without loss of generality that $d_1 \neq 0$, set $a = \sqrt{a_1 a_2 a_3}$ and for an integer parameter $t \equiv 1 \bmod 2a_1/(2a_1, d_1)$, $t > 1$ put

$$u_n(t) = \frac{(t + \sqrt{t^2 - 1})^n - (t - \sqrt{t^2 - 1})^n}{2\sqrt{t^2 - 1}}.$$

By Euler's theorem for the field $\mathbb{Q}(\sqrt{t^2-1})$ there exist positive integers n such that

$$u_n(t) \equiv 0 \bmod \frac{ad_1}{(a, d_1)}.$$

Let $n(t)$ be the least positive integer n with this property and $m = \min n(t)$, the minimum being taken over all t in question, $T = \{t\colon n(t) = m\}$. T is a union of arithmetic progressions.

For all $t \in T$ we set

$$y_1 = d_1 t,$$
$$y_2 = d_2 + 2d_2(t^2-1)u_m^2(t) + \frac{2a_1a_2d_3}{ad_1}u_{2m}(t),$$
$$y_3 = d_3 + 2d_3(t^2-1)u_m^2(t) + \frac{a_3d_1d_2}{a}(t^2-1)u_{2m}(t)$$

and verify that the conditions (15), (40), (41) and (42) are satisfied except for $O(1)$ values of t. The number of values of $t \in T$ such that (20) holds is $\gg x^{1/(2m+1)}$ (even $\gg x^{1/2m}$ if $d_2 = 0$) and the same y_3 can correspond to a most $2m+1$ such values. Hence

$$N_0(x) \ll \begin{cases} x^{1/2m} & \text{if } d_2 = 0, \\ x^{1/(2m+1)} & \text{always}. \end{cases}$$

In the case 2) we take the fundamental solution $\langle p_0, q_0 \rangle$ of the Pell equation

$$p^2 - 4a_1^3a_2a_3q^2 = 1$$

and set

$$\alpha = p_0 + 2a_1\sqrt{a_1a_2a_3}\,q_0, \qquad \beta = p_0 - 2a_1\sqrt{a_1a_2a_3}\,q_0,$$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Postponing for a moment the choice of n we take for t an arbitrary divisor of $(1/2)\,u_{2n}$ and put

$$\text{(43)}\qquad \begin{cases} s = 1 + 8a_1^3 a_2 a_3 u_n^2 + 4a_1^2 a_2 a_3 d_1 u_{2n} t\,, \\ y_1 = d_1 + 8a_1^3 a_2 a_3 u_n^2 + \dfrac{a_1 u_{2n}}{t}\,, \\ y_2 = d_2 s + 4a_1^2 a_2 d_3 t\,, \\ y_3 = d_3 s + a_3 d_2 (y_1^2 - d_1^2)\, t\,. \end{cases}$$

The numbers y_1, y_2, y_3 satisfy the condition (15), (40), (41) and (42) except for at most 4 values of t. The condition (39) will be satisfied provided

$$\text{(44)}\qquad n \leqslant \frac{\log x}{6 \log \alpha} - c_{16}\,.$$

Take for n the maximal product of initial consecutive odd primes satisfying (44). Denoting the i-th prime by p_i ($p_i = 2$) we obtain

$$\text{(45)}\qquad \prod_{j=2}^{k} p_j > \frac{\log x}{6 \log \alpha} - c_{16} \geqslant \prod_{j=2}^{k-1} p_j = n\,.$$

Hence by Theorem 5 of Robin [8]

$$k(\log k + \log \log k) > \log_2 x + O(1)\,,$$

which gives after a computation

$$\text{(46)}\qquad k > \frac{\log_2 x}{\log_3 x} + (1 + o(1)) \frac{\log_2 x \cdot \log_4 x}{(\log_3 x)^2}\,.$$

Since the same value of y_3 can correspond by means of formulae (42) to at most two values of t we obtain

$$\text{(47)}\qquad N_0(x) \geqslant \tau\left(\frac{1}{2} u_{2n}\right) - 4 \geqslant 2^{\omega(u_{2n}) - 1} - 4\,,$$

where $\tau(u)$ is the number of divisors of u.

By the result of Carmichael [2] on primitive divisors of Lucas numbers and by (45)

$$\omega(u_{2n}) \geqslant \tau(2n) + O(1) = 2^{k-1} + O(1)$$

hence by (46) and (47)

$$N_0(x) \geqslant \exp(\log 2 \cdot (2^{k-1} + O(1))) \geqslant \exp_2((k-1)\log 2 + O(1)) \geqslant$$

$$\geqslant \exp_2\left(\frac{\log 2 \cdot \log_2 x}{\log_3 x}\right) \quad \text{for } x > x_0 .$$

REMARK 8. If each of the polynomials f_i has two integer zeros the estimate for $N(x)$ given in Theorem 2 is valid also for the number of positive integers $x_3 \leqslant x$ such that (1) has nontrivial solutions in positive integers.

EXAMPLE. For $f_1 = f_3 = x^2 - 1$, $f_2 = x^2$ we have

$$N(x) = \sqrt{2x} + O(x^{1/3} \log x) .$$

PROOF. All solutions in nonnegative integers of the equation

$$x_3^2 - (x_1^2 - 1)x_2^2 = 1$$

are given by the formula

$$x_3 + \sqrt{x_1^2 - 1}\,x_2 = (x_1 + \sqrt{x_1^2 - 1})^n \qquad (n = 0, 1, \ldots) .$$

For $n = 0$ or $x_1 \leqslant 1$ we obtain $x_3 \leqslant 1$. For $n = 1$ we obtain trivial solutions.

For $n = 2$ the formula gives $x_3 = 2x_1^2 - 1$ and the inequality $x_3 \leqslant x$ is satisfied for $\sqrt{x/2} + O(1)$ values of x_3. For each $n \geqslant 3$ the formula gives $x_3 \geqslant x_1^n$ hence the number of distinct $x_3 \leqslant x$, $x_3 > 1$ obtainable from the formula is less than $\sqrt[n]{x}$, and for $n > \log x / \log 2$ it is zero. Since $N(x)$ counts both positive and negative x_3 the asymptotic formula follows.

REFERENCES

[1] E. BOMBIERI - J. PILA, *The number of integral points on arcs and ovals*, Duke Math. J., **52** (1989), pp. 337-357.

[2] R. D. CARMICHAEL, *On the numerical factors of the arithmetic form* $\alpha^n \pm \beta^n$, Ann. Math. (2), **15** (1913-1914), pp. 30-70.

[3] P. G. L. DIRICHLET, *Vorlesungen über Zahlentheorie*, 4 Auflage, reprint Chelsea, New York (1968).

[4] F. DODD - L. MATTICS, *Solution of the problem* E 3138, Amer. Math. Monthly.
[5] M. N. HUXLEY, *A note on polynomial congruences, Recent Progress in Analytic Number Theory*, Vol. 1 (Durham 1979), pp. 193-196, Academic Press (1981).
[6] B. W. JONES, *The Arithmetic Theory of Quadratic Forms*, J. Wiley, New York (1950).
[7] O. PERRON, *Die Lehre von den Kettenbrüchen*, 2 Auflage, reprint Chelsea.
[8] G. ROBIN, *Estimation de la fonction de Tchebychef* Θ *sur le k-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de* n, Acta Arith., 42 (1983), pp. 367-389.
[9] G. SÁNDOR, *Über die Anzahl der Lösungen einer Kongruenz*, Acta Math., 87 (1952), pp. 13-16.
[10] A. SCHINZEL, *On some problems of the arithmetical theory of continued fractions*, Acta Arith., 7 (1961), pp. 393-413.
[11] A. SCHINZEL, *Selected Topics of Polynomials*, The University of Michigan Press, Ann Arbor (1982).
[12] D. WOLKE, *Multiplikative Funktionen auf schnell wachsenden Folgen*, J. Reine Angew. Math., 251 (1971), pp. 55-67.

Manoscritto pervenuto in redazione il 17 settembre 1990.