Publ. Math. Debrecen
68/3-4 (2006), 261–282

Finite sets of binary forms

By PAULO RIBENBOIM (Kingston)

Abstract. We prove the finiteness of certain sets of binary cubic forms with given non-zero discriminant or having discriminants with bounded radical. To obtain finite sets we impose appropriate conditions on the coefficients, or on the Hessian and the cubic covariant of the forms. Some of the results are extended to binary forms of degree higher than these. We also give theorems which are proved under the assumption that the (ABC) conjecture is true.

1. The results in this paper

Let $n \geq 2$. A homogeneous polynomial $f(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_{n-1}XY^{n-1} + a_nY^n$ is called a *binary form* of degree n. We shall always assume that the coefficients $a_0, a_1, \ldots, a_n$ are integers.

If $n = 3$ the binary cubic form $f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3$ is also denoted by $f = \langle a, b, c, d\rangle$. We shall write "form" instead of "binary form" and we exclude the zero form from our considerations.

If f is a form of degree $n \geq 2$ there exist algebraic numbers α_i, β_i such that

$$f = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y).$$

Mathematics Subject Classification: 11D41.
Key words and phrases: binary cubic form, (ABC) conjecture, binary forms with given discriminant.

By definition, the *discriminant* of f is

$$\Delta_f = \prod_{i<j}(\alpha_i\beta_j - \beta_i\alpha_j)^2.$$

Then Δ_f is an integer and $\Delta_f = 0$ if and only if f has two proportional linear factors in the above decomposition.

The discriminant may be computed in terms of the coefficients of the form. More precisely, for every $n \geq 2$ there exists a polynomial $\Phi_n \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$, such that Φ_n is homogeneous of degree $2(n-1)$, and if $f = a_0X^n + a_1X^{n-1} + \cdots + a_nY^n$ then $\Delta_f = \Phi_n(a_0, a_1, \ldots, a_n)$. We also note that Φ_n has degree $n-1$ in X_0 and also in X_n. It follows that if e is any non-zero integer then $\Delta_{ef} = e^{2(n-1)}\Delta_f$.

For cubic forms $f = \langle a, b, c, d\rangle$ we have:

$$\Delta_f = b^2c^2 + 18\,a\,b\,c\,d - 4\,ac^3 - 4b^3\,d - 27\,a^2d^2.$$

In this paper we shall describe sets of forms which are finite and effectively computable. We shall prove that a set of forms is finite and effectively computable by applying theorems, producing effective bounds for the elements of the set, which are based on Bakers's theorems on linear forms in logarithms [1].

We obtain our results comparing the set of forms under consideration with sets known to be finite and effectively computable.

In this section we state the theorems which will be proved in the paper, but we do not state explicity the results which may be obtained by interchanging X and Y. Thus, for cubic forms $f = \langle a, b, c, d\rangle$, the theorems are also true interchanging a and d, and b and c.

A) Sets of form with a given non-zero discriminant and additional conditions on the coefficients

In the first theorems we consider cubic forms $f = \langle a, b, c, d\rangle$ and we impose conditions on the coefficients a, b and c.

First, we consider forms with $a = 0$. If $N \equiv 0$ or $1 \pmod 4$, the set S of forms $f = \langle 0, b, c, d\rangle$ with $\Delta_f = N$ is infinite. Indeed, let $c > |N|$ and $c = N + 2k$, then $c^2 \equiv N^2 \pmod 4$ $c^2 - N \equiv N(N-1) \equiv 0 \pmod 4$. Let $d = \frac{c^2-N}{4}$, then $f = \langle 0, 1, c, d\rangle$ has discriminant $\Delta_f = c^2 - 4d = N$. On the

other hand, it is easily seen that if $N \equiv 2$ or $3 \pmod 4$ then the set of all $f = \langle 0, b, c, d\rangle$ with $\Delta_f = N$ is empty.

The Theorems 1.1, 1.2 and 1.3 are special cases of Corollary 1.3 of GYŐRY [8] (which is formulated for polynomials in $\mathbb{Z}[X]$). The interest of the proofs presented here lies in the fact that, except for an appel to the theorem of SCHINZEL and TIJDEMAN, the proofs are entirely elementary.

1.1. Theorem. *Let $N \neq 0$ be an integer, let S be the set of all cubic forms $f = \langle a, b, c, d\rangle$ such that $b = 0$ and $\Delta_f = N$. Then S is finite and effectively computable.*

1.2. Theorem. *Let N, a_0, b_0 be non-zero integers, let S be the set of all cubic forms $f = \langle a, b, c, d\rangle$ such that $\Delta_f = N$, $a = a_0$, $b = b_0$. Then S is finite and effectively computable.*

1.3. Theorem. *Let $N \neq 0$, $a_0 \neq 0$ and c_0 be integers and let S be the set of all cubic forms $f = \langle a, b, c, d\rangle$ such that $\Delta_f = N$, $a = a_0$ and $c = c_0$. Then S is finite and effectively computable.*

1.4. Theorem. *Let $N \neq 0$, b_0, c_0 be integers, let S be the set of all cubic forms $f = \langle a, b, c, d\rangle$ such that $\Delta_f = N$, $b = b_0$ and $c = c_0$. Then S is finite and effectively computable.*

In the results which follow we consider forms f of degree $n \geq 2$ and we impose, for example, conditions to be satisfied by $f(1, 0)$ and $f(0, 1)$.

If $k \geq 2$ the symbol $\Diamond^{(k)}$ denotes a non-zero integer which is a h^{th} power, for some $h \geq k$. In particular, $\Diamond^{(k)}$ may be equal to 1.

1.5. Theorem. *Let N, m and m' be non-zero integers. Let S be the set of all forms f of degree 2 such that:*

1) $\Delta_f = N$
2) $f(1, 0) = m$
3) $f(0, 1) = m'\Diamond^{(3)}$.

Then S is finite and effectively computable.

1.6. Corollary. *Let* $P = \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right)$ *with* $x, x', y, y' \in \mathbb{Z}$ *and* $\det P \neq 0$.

Then the statement of Theorem 1.5 still holds replacing $(1,0)$ *by* (x,y) *and* $(0,1)$ *by* (x',y').

If R is a positive square-free integer, let $R^\times$ denote the set of all integers all of whose prime factors divide R. If n is a non-zero integer, the *radical* of n is the product of the distinct prime factors of n. We denote the radical of n by $\operatorname{rad} n$. Clearly $\operatorname{rad} n$ divides R if and only if $n \in R^\times$.

The special case of Theorem 1.7(a) where $f(1,0) = 1$ and $f(0,1) \in R^\times$ was proved by GYŐRY [9] (see Corollary 1).

1.7. Theorem. *Let* $n \geq 3$, *let* R *be a positive square-free integer. Let* W *be the set of all forms* f *of degree* n, *such that* $\Delta_f \neq 0$ *and* $f(1,0) \in R^\times$.

a) *Let* N *and* m' *be non-zero integers, let* S *be the set of all* $f \in W$ *such that:*

a1) $\Delta_f = N$

a2) $f(0,1) \in R^\times$ *or* $f(0,1) = n'\Diamond^{(2)}$.

Then S is finite and effectively computable.

b) *Let* S *be the set of all* $f \in W$ *such that:*

b1) $\Delta_f \in R^\times$

b2) $f(0,1) \in R^\times$

Then there exists a finite effectively computable subset S_0 *of* S *such that if* $f \in S$ *there exists* $f_0 \in S_0$ *and* $e, k, \ell \in R^\times$ *such that* $ef(X,Y) = f_0(kX, \ell Y)$.

1.8. Corollary. *Let* R *be a positive square-free integer, let* $Q = \left(\begin{smallmatrix} z & z' \\ t & t' \end{smallmatrix}\right)$ *and* $d = \det Q \neq 0$.

a) (1.7) *holds, replacing* $(1,0)$ *by* (z,t) *and* $(0,1)$ *by* (z',t') .

b) *Let* $Q^* = \left(\begin{smallmatrix} t' & -z' \\ -t & z \end{smallmatrix}\right)$ *let* S *be the set of all binary forms* f *of degree* n *with* $\Delta_f \in R^\times$, $f(z,t) \in R^\times$, $f(z',t') \in R^\times$.

Then for every $f \in S$ *there exists* $e, k, \ell \in R^\times$, $h \in$ ..., $P \in \mathcal{P}_h$ *(with the notation of* (1.7)*) such that* $d^n e\, f = h_{P\left(\begin{smallmatrix} k & 0 \\ 0 & \ell \end{smallmatrix}\right)Q^*}$.

Let $n \geq 1$ and $0 \leq j \leq n-1$. If f is a form of degree n, we shall use the notation $D^j f = \frac{\partial^j f}{\partial X^j}$. So $D^j f$ is a form of degree $n - j$.

1.9. Theorem. *Let $n \geq 3$ and $0 \leq j \leq n-2$, let $N_0, N_1, \ldots, N_j$ be integers such that $N_j \neq 0$. Let W be the set of all forms f of degree n such that*

1) $\Delta_{D^i f} = N_i$ *for* $i = 0, 1, \ldots, j$

a) *Let $j \geq n-3$, let R be a positive square-free integer and $m' \neq 0$. Let S be the set of all forms $f \in W$ such that:*

2) $f(1,0) \in R^\times$

3) *either* $D^j f(0,1) \in R^\times$ or $D^j f(0,1) = m' \Diamond^{(2)}$.

b) *Let $j = n-2$, let m, m' be non-zero integers, let S be the set of all forms $f \in W$ such that:*

2) $f(1,0) = m$

3) $D^j f(0,1) = m' \Diamond^{(3)}$.

Then in both cases (a) *and* (b) *the set S is finite and effectively computable.*

B) Sets of cubic forms with Hessian and cubic covariant satisfying certain conditions

Let $f = \langle a, b, c, d \rangle$. By definition, the *Hessian* of f is

$$H_f(X,Y) = \frac{1}{4}\left[\frac{\partial^2 f}{\partial X^2} \cdot \frac{\partial^2 f}{\partial Y^2} - \left(\frac{\partial^2 f}{\partial X \partial Y}\right)^2\right]$$

and the *cubic covariant* of f is

$$Q_f(X,Y) = \frac{\partial f}{\partial X} \cdot \frac{\partial H}{\partial Y} - \frac{\partial f}{\partial Y} \cdot \frac{\partial H}{\partial X}.$$

We shall give in Section 3 the explicit expressions of the Hessian and the cubic covariant in terms of the coefficients of $f(X,Y)$. In Section 3 we shall also give the fundamental identity satisfied by the Hessian and the cubic covariant.

1.10. Theorem. *Let $P = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$ with $x, y, x', y' \in \mathbb{Z}$ and $\det P = 1$. Let N, B, B' be non-zero integers such that $2B^2$ and $2B'^2$ are not cubes. Let S be the set of all cubic forms f such that:*

1) $\Delta_f = N$

2) $Q_f(x,y) = B$ *and* $Q_f(x',y') = B'$.

Then S is finite and effectively computable.

1.11. Theorem. *Let* $P = \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right)$ *with* $\det P = 1$, *let* N, A, A' *be non-zero integers, such that* A *and* A' *are not squares. Let* S *be the set of all cubic forms* f *such that:*

1) $\Delta_f = N$
2) $H_f(x, y) = A$, $H_f(x', y') = A'$.
   a) *If* $N > 0$ *then* S *is finite and effectively computable.*
   b) *If* $N < 0$ *then either* $S = \emptyset$ *or* S *is infinite and there is an algorithm to determine when* S *is empty.*

1.12. Theorem. *Let* $P = \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right)$ *with* $\det P = 1$, *let* A, B *be integers such that* $4A^3 - B^2 \neq 0$. *Let* S *be the set of all cubic forms* f *such that:*

1) $H_f(x, y) = A$, $Q_f(x, y) = B$;
   either:
2) *there exists a positive square-free integer* R *such that*

$$f(x', y') \in R^\times;$$

or 2') *there exists* $m' \neq 0$ *such that* $f(x', y') = m'\Diamond^{(2)}$;

or 2") *there exist integers* A', B' *such that* $4A'^3 - B'^2 \neq 0$ *and* $H_f(x', y') = A'$, $Q_f(x', y') = B'$.

Then S *is finite and effectively computable.*

1.13. Theorem. *Let* $P = \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right)$ *with* $x, x', y, y' \in \mathbb{Z}$ *and* $\det P = 1$, *let* R *be a positive square-free integer and* $e \geq 1$, $m' \neq 0$. *Let* S *be the set of all cubic forms* f *such that:*

1) $\Delta_f \in R^\times$, $f(xy) \in R^\times$
2) $\gcd(H_f(x, y), Q_f(x, y)) = e$
3) *either* $f(x', y') \in R^\times$ *or* $f(x', y') \in m'\Diamond^{(2)}$.

Then S *is finite and effectively computable.*

1.14. Theorem. *Let* R *be a positive square-free integer, let* $e \geq 1$, $m' \neq 0$. *Let* S *be the set of all cubic forms* $f = \langle a, b, c, d \rangle$ *such that:*

1) $\Delta_f \in R^\times$, $a \in R^\times$

2) $\gcd(3ac - b^2, 3a(9ad - bc)) = e$

3) *either* $d \in R^\times$, *or* $d = m'\Diamond^{(2)}$.

Then S is finite and effectively computable.

C) Result proved under the assumption that the (ABC) Conjecture is true.

We state the (ABC) Conjecture (see Nitaj [16], Ribenboim [1]):

1.15. (ABC) **Conjecture.** *For every real number $\varepsilon > 0$, there exists a real number $K_\varepsilon > 0$ (depending on ε) such that if A, B, C are non-zero coprime integers such that $A + B + C = 0$, then $\max\{|A|, |B|, |C|\} \le K_\varepsilon[\mathrm{rad}(ABC)]^{1+\varepsilon}$.*

If n is a non-zero integer, the *radical index* of n, denoted by $\operatorname{rad}\operatorname{ind} n$, is the real number $\gamma \ge 1$ such that $(\operatorname{rad} n)^\gamma = |n|$ (see Ribenboim [18]). Let R be a positive square-free integer, let $\gamma \ge 1$. We denote by $I(R, \gamma)$ the set of all integers uv, where

$$u \in R^\times, \quad v \ge 1, \quad \gcd(v, R) = 1$$

and $\operatorname{rad}\operatorname{ind} v \ge \gamma$.

The next theorem is a modified and connected version of a result suggested by the referee of this paper.

1.16. Theorem. *Assume that the (ABC) Conjecture is true. Let $n \ge 3$, $0 \le j \le n-2$, let R be a positive square-free integer and $\delta > 0$. Let W be the set of all forms f of degree n such that:*

1) $\Delta_f \ne 0$, $\Delta_{D^j f} \ne 0$

2) $f(1,0) \in I\big(R, \frac{n}{n-2} + \delta\big)$

3) $D^j f(0,1) \in I\big(R, \frac{n-j}{n-j-1} + \delta\big)$

   a) *Let $N \ne 0$ and let S be the set of all $f \in W$ such that $\Delta_f = N$. Then S is finite.*

   b) *Let S be the set of all forms $f \in W$ such that $\Delta_f \in R^\times$. Then there exists a finite subset S_0 of S such that if $f \in S$ there exists $f_0 \in S_0$ and $e, k, \ell \in R^\times$ such that $ef(X, Y) = f_0(kX, \ell X)$.*

2. Proof of the results of Section 1(A)

Let f be a form of degree $n \geq 2$, let $P = \left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right)$. We define $f_P(X,Y) = f(x_1X+y_1Y, x_2X+y_2Y)$, so f_P is again a form of the same degree n and we have $\Delta_{f_P} = \Delta_f(\det P)^{n(n-1)}$. If P' is also a matrix, then $f_{PP'} = (f_P)_{P'}$.

Henceforth we shall only consider matrices with integer entries. If $g = f_P$ for some 2×2 matrix P with (integer entries and) $\det P = \pm 1$, we say that the forms f and g are *equivalent*; then

$$\Delta_f = \Delta_g.$$

Hermite showed in [10]:

2.1. Theorem. *For any non-zero integer N the set ε of equivalence classes of forms of degree 2 (respectively 3) with $\Delta_f = N$ is finite and effectively computable.*

See also Cassels [4].

We shall need the following theorem of Schinzel & Tijdeman ([19]):

2.2. Theorem. *Let be given $f \in \mathbb{Z}[X]$ and a non-zero integer a. Then there exists $C > 0$, effectively computable in terms of f and a, and such that if x, k, t are integers satisfying $f(x) = at$, with $k \geq 2$ if f has at least three simple roots, or with $k \geq 3$ if f has exactly two simple roots, then $\max\{|x|, |t^k|\} \leq C$.*

2.3. Proof of Theorem 1.1. Let S be the set of all $f = \langle a, b, c, d\rangle$ with $b = 0$ and $\Delta_f = N$. So $-a(4c^3 + 27\,ad^2) = N$, hence $a \neq 0$ and a belongs to the finite and effectively computable set of factors of N. Let a_0 be any factor of N. Then $4c^3 + 27\,a_0d^2 = -\frac{N}{a_0} \neq 0$, that is $4c^3 + \frac{N}{a_0} = -27a_0d^2$. If $d = 0$ then c has at most one possible value. Now let $d \neq 0$.

The polynomial $f(X) = 4X^3 + \frac{N}{a_0}$ has three simple roots. By 2.2 there exists an effectively computable integer $C(a_0) > 0$ such that $|c|$, $|d| < C(a_0)$. This is true for every factor a_0 of N, hence the set S is finite and effectively computable. □

2.4. Proof of Theorem 1.2. If $f = \langle a_0, b_0, c, d\rangle \in S$ then $N = b_0^2c^2 + 18\,a_0b_0cd - 4\,a_0c^3 - 4\,b_0^3d - 27\,a_0^2d^2$. If $d = 0$ then $N = b_0^2c^2 - 4a_0c^3$ so c belongs to a finite and effectively computable set and the subset of all $f = \langle a_0, b_0, c, 0\rangle$ of S is finite and effectively computable.

Now let $d \neq 0$. We have:

$$27\,a_0^2d^2 - (18\,a_0b_0c + 4\,b_0^3)d + (N - b_0^2c^2 + 4\,a_0c^3) = 0.$$

Case 1. $N - b_0^2c^2 + 4a_0c^3 = 0$ so c belongs to a finite and effectively computable set. But $d \neq 0$, then $27\,a_0^2d - (18\,a_0b_0c + 4\,b_0^3) = 0$ so d also belongs to a finite and effectively computable set.

Case 2. $N - b_0^2c^2 + 4a_0c^3 \neq 0$. From the quadratic relation satisfied by d, we must have

$$(18\,a_0b_0c + 4\,b_0^3)^2 - 4 \times 27\,a_0^2(N - b_0^2c^2 + 4\,a_0c^3) = \square,$$

where $\square$ denotes any square.

We shall show that the polynomial

$$(18\,a_0b_0X + 4\,b_0^3)^2 - 4 \times 27\,a_0^2(N - b_0^2X^2 + 4\,a_0X^3)$$

has simple roots, equivalently,

$$F(X) = 4 \times 27\,a_0^3X^3 - 108\,a_0^2b_0^2X^2 - 36a_0b_0^4X + (27\,a_0^2N - 4\,b_0^6)$$

has simple roots. The roots of $F'(X)$ are $\frac{b_0^2}{3a_0}(1 \pm \sqrt{2}\,)$. If these are also roots of $F(X)$ then by a simple calculation $(-24\,b_0^6 + 27\,a_0^2N) \mp 16\,b_0^6\sqrt{2} = 0$, which is impossible.

By the theorem of Schinzel & Tijdeman the set $\{c \mid d \neq 0$ and $f = \langle a_0, b_0, c, d\rangle \in S\}$ is finite and effectively computable and from the quadratic relation satisfied by d, the set $\{d \mid f = \langle a_0, b_0, c, d\rangle \in S\}$ is also finite and effectively computable. $\square$

2.5. Proof of Theorem 1.3. If $f = \langle a_0, b, c_0, d\rangle \in S$ then $N = b^2c_0^2 + 18\,a_0bc_0d - 4\,a_0c_0^3 - 4b^3d - 27\,a_0^2d^2$. If $d = 0$ then $N = b^2c_0^2 - 4a_0c_0^3$ so b belongs to a finite and effectively computable set, hence the set $\{f \in S \mid d = 0\}$ is finite and effectively computable. If $d \neq 0$ we have $27\,a_0^2d^2 - (18\,a_0bc_0 + 4\,b^3)d + (N - b^2c_0^2 + 4\,a_0c_0^3) = 0$.

Case 1. $N - b^2c_0^2 + 4\,a_0c_0^3 = 0$. Since $N \neq 0$ we have $c_0 \neq 0$ and b is defined by the above relation; finally, the quadratic relation satisfies by d, defines d and this case is settled.

Case 2. $N - b^2c_0^2 + 4\,a_0c_0^3 \neq 0$. Since d satisfies the quadratic relation indicated, we have $(18\,a_0bc_0 + 4\,b^3)^2 - 4 \times 27\,a_0^2(N - b^2c_0^2 + 4\,a_0c_0^3) = \square$.

Subcase (a): $N = -8a_0c_0^3$. Then $(18\,a_0bc_0 + 4\,b^3)^2 + 4 \times 27\,a_0^2(4\,a_0c_0^3 + b^2c_0^2) = \square$ and this gives $(b^2 + 3a_0c_0)^3 = \square$, hence there exists an integer t such that $b^2 + 3a_0c_0 = t^2$. Thus $t^2 - b^2 = 3a_0c_0$, so $t + b$ and $t - b$ belong to the finite and effectively computable set of divisors of $3a_0c_0$, the same holds for b. It follows from the quadratic relation satisfied by d that d also belongs to a finite and effectively computable set and this subcase is settled.

Subcase (b): $N \neq -8a_0c_0^3$. We shall show that the polynomial $G(X) = (18\,a_0c_0X + 4\,X^3)^2 - 4 \times 27\,a_0^2(N - c_0^2X^2 + 4a_0c_0^3) = 4X^6 + 36\,a_0c_0X^4 + 108\,a_0^2c_0^2X^2 - 27\,a_0^2N - 4 \times 27\,a_0^3c_0^3$ has at least three simple zeros.

Let $H(Y) = 4Y^3 + 36\,a_0c_0Y^2 + 108\,a_0^2c_0^2Y - (27\,a_0^2N + 108\,a_0^3c_0^3)$. Then $H'(Y) = 12(Y + 3a_0c_0)^2$. If $H(Y)$ has a double root α, then $\alpha = -3a_0c_0$. But $H(-3a_0c_0) = 4(-3a_0c_0)^3 + 36\,a_0c_0(-3a_0c_0)^2 + 108\,a_0^2c_0^2(-3a_0c_0) - (27\,a_0^2N + 108\,a_0^3c_0^3) = -27\,a_0^2(N + 8a_0c_0^3) \neq 0$.

This shows that $H(Y)$ has three simple roots, hence $G(X)$ has six simple roots.

It follows from the theorem of Schinzel & Tijdeman that b belongs to a finite and effectively computable set. Finally, from the quadratic relation satisfied by d, we conclude that d belongs to a finite and effectively computable set also in this subcase.

This concludes the proof. □

2.6. Proof of Theorem 1.4. For every $f \in S$ we have $N = b_0^2c_0^2 + 18\,b_0c_0ad - 4\,ac_0^3 - 4b_0^3d - 27\,a^2d^2$. If $b_0 = 0$ or $c_0 = 0$ then by 1.1 S is finite and effectively computable. Let $b_0c_0 \neq 0$. We rewrite $27\,a^2d^2 + (4b_0^3 - 18\,b_0c_0a)d + (N - b_0^2c_0^2 + 4ac_0^3) = 0$.

If $a = 0$ then $d = \frac{1}{4b_0^3}(b_0^2c_0^2 - N)$. Now let $a \neq 0$ hence $d = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$ where $A = 3^3a^2$, $B = 4b_0^3 - 18\,b_0c_0a$, $C = N - b_0^2c_0^2 + 4ac_0^3$.

We have

$$|d| \le \frac{|B|}{2\times 3^3a^2} + \frac{\sqrt{B^2-4AC}}{2\times 3^3a^2}\cdot$$
$$\frac{|B|}{2\times 3^3a^2} \le \frac{4|b_0|^3}{2\times 3^3a^2} + \frac{18|b_0c_0|\times|a|}{2\times 3^3a^2} \le \frac{2|b_0|^3}{3^3} + \frac{|b_0c_0|}{3}.$$

Next

$$\frac{|B^2-4\,AC|}{2^2\times 3^6a^4} \le \frac{B^2}{2^2\times 3^6a^4} + \frac{|AC|}{3^6a^4},$$
$$\frac{B^2}{2^2\times 3^6a^4} = \frac{|2^4b_0^6 + 2^2\times 3^4b_0^2a_0^2a^2 - 2^4\times 3^2b_0^4c_0a|}{2^2\times 3^6a^4}$$
$$\frac{2^2|b_0|^6}{3^6a^4} + \frac{|b_0c_0|^2}{3^2a^2} + \frac{2^2|b_0|^4|c_0|}{3^4|a|^3} \le \frac{2^2|b_0|^6}{3^6} + \frac{|b_0c_0|^2}{3^2} + \frac{2^2|b_0|^4|c_0|}{3^4},$$
$$\frac{|AC|}{3^3a^4} = \frac{|3^3a^2(N-b_0^2c_0^2+4ac_0^3)|}{3^3a^4} \le \frac{|N|}{a^2} + \frac{|b_0c_0|^2}{a^2} + \frac{4|c_0|^3}{|a|}$$
$$\le |N| + |b_0c_0|^2 + 4|c_0|^3.$$

Putting together, there exists an integer $K>0$ (depending on N, b_0, c_0) such that $|d|\le K$. Similarly, there exists $K'>0$ such that $|a|\le K'$. Hence S is finite and effectively computable. □

2.7. Proof of Theorem 1.5. Let $f = aX^2+bXY+cY^2 \in S$. So $\Delta_f = b^2-4ac = N$.

By assumption $a=m$, $c=m'\Diamond^{(3)}$ so $b^2-N = 4mm'\Diamond^{(3)}$. Since the polynomial X^2-N has simple roots, by the Theorem of Schinzel & Tijdeman 2.2 the set $\{b \mid f\in S\}$ is finite and effectively computable, so the same holds for the set $\{c \mid f\in S\}$, hence S is finite and effectively computable. □

2.8. Proof of Corollary 1.6. Let $d=\det P\neq 0$, let $P^* = \left(\begin{smallmatrix} y' & -x' \\ -y & x\end{smallmatrix}\right)$ so $\det P^* = d$, $PP^* = P^*P = dI$. Let $f\in S$ and $\tilde f = f_P$, then $\tilde f(1,0) = f_P(1,0) = f(x,y) = m$, $\tilde f(0,1) = f_P(0,1) = f(x',y') = m'\Diamond^{(3)}$. Moreover $\Delta_{\tilde f} = \Delta_{f_P} = d^2N$. By Theorem 1.5 the set $\{\tilde f = f_P \mid f\in S\}$ is finite and effectively computable. Now we observe that the mapping $f\mapsto f_P$

is injective. Indeed, if $f, g \in S$ and $f_P = g_P$ then $d^2 f = f_{dI} = f_{PP^*} = g_{PP^*} = d^2 g$, so $f = g$ and this concludes the proof. □

We shall need the Theorem of Birch & Merriman [2] which extends to forms of any degree the Theorem of Hermite [10].

Let L be a positive square-free integer.

The forms f, h of degree $n \geq 2$ are said to be *L-equivalent* if there exist $e \in L^\times$ and P, with $\det P \in L^\times$ such that $ef = h_P$. If $L = 1$ this means that f and h are equivalent.

If $P = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$, let $P^* = \begin{pmatrix} y' & -x' \\ -y & x \end{pmatrix}$, then $PP^* = P^*P = dI$ where $d = \det P = \det P^* \in L^\times$. It follows that $ef_{P^*} = h_{dI}$, hence $e^{n-1}d^n h = f_{P^*.eI}$.

Part (a) of the next theorem was proved by Birch & Merriman [2], while part (b) is due to Evertse & Győry [5].

2.9. Theorem. *Let $n \geq 2$ let L be a positive square-free integer and let $\mathcal{E}$ be the set of L-equivalence classes of forms f of degree n, with $\Delta_f \in L^\times$.*

a) *$\mathcal{E}$ is a finite set.*

b) *$\mathcal{E}$ is effectively computable.*

In the next proof we shall need the following theorem of Thue & Mahler (see [20]):

2.10. Theorem. *Let f be a form of degree $n \geq 3$, with non-zero discriminant, let R be a positive square-free integer. Then the set of pairs of coprime integers (x, y) such that $f(x, y) \in R^\times$ is finite and effectively computable.*

2.11. Lemma. *Let $Q = \begin{pmatrix} r & p \\ s & q \end{pmatrix}$ with $\det Q = 1$. For each pair (x', y') of coprime integers such that $P = \begin{pmatrix} r & x' \\ s & y' \end{pmatrix}$ has non zero determinant, let $Q^{-1}P = \begin{pmatrix} 1 & z \\ 0 & w \end{pmatrix}$. Then:*

a) *The mapping $(x', y') \mapsto (z, w)$ is a bijection and $w = \det P$.*

b) *If h is a form of any degree, if $g = h_Q$ then $g(z, w) = h_P(0, 1) = h(x', y')$.*

Proof. The first assertion is trivial. Next

$$g(z, w) = g_{Q^{-1}P}(0, 1) = h_P(0, 1) = h(x', y'). \qquad \square$$

2.12. Proof of Theorem 1.7. Let L be a positive square-free integer. By Theorem 2.9 there exits a finite and effectively computable set H of forms of degree n such that every $f \in W$ is L-equivalent to some $h \in H$.

Let $\mathcal{P}$ be the set of matrices $P = \left(\begin{smallmatrix} x_P & x'_P \\ y_P & y'_P \end{smallmatrix}\right)$ such that $\det P \in L^\times$

$$\gcd(x_P, y_P) = 1 \quad \text{and} \quad \gcd(x'_P, y'_P) = 1.$$

For each $h \in H$ let $\mathcal{P}_h = \{p \in \mathcal{P} \mid h_P \in W\}$. If $P \in \mathcal{P}_h$ then

$$h(x_P, y_P) = h_P(1,0) \in R^\times.$$

By the Theorem of Thue & Mahler the set $C_h = \{(x_P, y_P) \mid P \in \mathcal{P}_h\}$ is finite and effectively computable.

Proof of (a). We take $L = 1$, so every $f \in S$ is equivalent to some $h \in H$. Let $\mathcal{P}_h = \{P \in \mathcal{P}_h \mid h_P \in S\}$ so $\det P = 1$ for all $h_P \in \mathcal{P}'_h$. It suffices to show that each set $\mathcal{P}'_h$ is finite and effectively computable.

If $f(0,1) \in R^\times$ for all $f \in S$, we have $h(x'_P, y'_P) = h_P(0,1) = f(0,1) \in R^\times$. By the Theorem of Thue & Mahler the set $C'_h = \{(x'_P, y'_P) \mid P \in \mathcal{P}'_h\}$ is finite and effectively computable. This implies that $\mathcal{P}'_h$ is finite and effectively computable as it was required to prove.

Now assume that $f(0,1) = m'\Diamond^{(2)}$ for all $f \in S$. Let $(r,s) \in C_h$. Let $Q = \left(\begin{smallmatrix} r & p \\ s & q \end{smallmatrix}\right)$, with $\det Q = 1$. For every $P = \left(\begin{smallmatrix} r & x'_P \\ s & y'_P \end{smallmatrix}\right) \in \mathcal{P}'_h$ we have $\det P = 1$ and $Q^{-1}P = \left(\begin{smallmatrix} 1 & z_P \\ 0 & w_P \end{smallmatrix}\right)$. By Lemma 2.11 the mapping $(x'_P, y'_P) \mapsto (z_P, w_P)$ is a bijection and $w_P = 1$. Moreover if $g = h_Q$ then $g(z_P, 1) = g_{Q^{-1}P}(0,1) = h_P(0,1) = h(x'_P, y'_P) = m'\Diamond^{(2)}$. Since $\Delta_g \neq 0$, the roots of the polynomial $G(X) = g(X,1)$ are simple . By the Theorem of Schinzel & Tijdeman when $P = \left(\begin{smallmatrix} r & x'_P \\ s & y'_P \end{smallmatrix}\right) \in \mathcal{P}'_h$ the set of integers z_P is finite and effectively computable and so is the set of pairs (x'_P, y'_P). Since this holds for every $(r,s) \in C_h$ it follows that $\mathcal{P}'_h$ is finite and effectively computable.

Proof of (b). We take $L = R$. For each $h \in H$ let $\mathcal{P}'_h = \{P \in \mathcal{P}_h \mid h_P \in S\}$ and $S_0 = \{h_P \mid h \in H,\ P \in \mathcal{P}'_h\}$. Hence $S_0 \subseteq S$. If $P \in \mathcal{P}'_h$ then $h(x'_P, y'_P) = h_P(0,1) = f(0,1) \in R^\times$. By the Theorem of Thue & Mahler $C'_h = \{(x'_P, y'_P) \mid P \in \mathcal{P}'_h\}$ is finite and effectively computable, hence the same is true for $\mathcal{P}'_h$, for each $h \in H$. Therefore S_0 is finite and effectively computable.

Now let $f \in S$, so there exists $e \in R^\times$ and P with $\det P \in R^\times$, as well as $h \in H$ such that $ef = h_P$. Let $P = \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right)$ with $\gcd(x,y) = k$, $\gcd(x',y') = \ell$. Let $x = k\bar{x}$, $y = k\bar{y}$, $x' = \ell\bar{x}'$, $y' = \ell\bar{y}'$. Let $\bar{P} = \left(\begin{smallmatrix} \bar{x} & \bar{x}' \\ \bar{y} & \bar{y}' \end{smallmatrix}\right)$ so $P = \bar{P}\left(\begin{smallmatrix} k & 0 \\ 0 & \ell \end{smallmatrix}\right)$, hence $k\ell(\det \bar{P}) = \det P \in R^\times$, hence $\det \bar{P}$, $k, \ell \in R^\times$. We have

$$ef(X,Y) = h_P(kX, \ell Y).$$

It remains to show that $h_{\bar{P}} \in S$, therefore $h_{\bar{P}} \in S_0$. First,

$$e^{2(n-1)}\Delta_f = \Delta_{h_{\bar{P}}}(k\ell)^{n(n-1)}$$

hence $\Delta_{h_{\bar{P}}} \in R^\times$.

Also $k^n h_{\bar{P}}(1,0) = h_{\bar{P}}(k,0) = h_P(1,0)\ ef(1,0) \in R^\times$ because $f \in S$; so $h_{\bar{P}}(1,0) \in R^\times$.

Similarly $h_{\bar{P}}(0,1) \in R^\times$. This proves that $h_{\bar{P}} \in S$ and concludes the proof of the Theorem. □

2.13. Proof of Corollary 1.6. a) Let $\tilde{S} = \{f_Q \mid f \in S\}$. Then $\Delta_{f_Q} = \Delta_f(\det Q)^{n(n-1)} = N(\det Q)^{n(n-1)} \neq 0$. Also $f_Q(1,0) = f(z,t) \in R^\times$, $f_Q(0,1) = f(z',t') \in R^\times$. By 1.7 the set $\tilde{S}$ is finite and effectively computable. As it was shown in 1.6, the mapping $f \mapsto f_Q$ from S to $\tilde{S}$ is injective, hence S is also finite and effectively computable.

b) If $f \in S$, by 1.7 there exists $e, k, \ell \in R^\times$, $h \in H$, $P \in \mathcal{P}'_h$ such that $ef_Q = h_{P\left(\begin{smallmatrix} k & 0 \\ 0 & \ell \end{smallmatrix}\right)}$. We have $QQ^* = dI$ hence $d^n ef = ef_{dI} = ef_{QQ^*} = h_{P\left(\begin{smallmatrix} k & 0 \\ 0 & \ell \end{smallmatrix}\right)Q^*}$. □

We shall need the following lemma:

2.14. Lemma. *Let $n \geq 2$, let f be a form of degree n and let N be any integer. Then the set T of all forms g such that $Dg = Df$ and $\Delta_g = N$ is finite and effectively computable.*

Proof. Let $f(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n$. We have $Dg = Df$ of and only if there exists an integer b such that $g(X,Y) = f(X,Y) + bY^n$. As it was recalled earlier, there exists a homogeneous polynomial $\Phi_n(X_0, X_1, \ldots, X_n)$, with coefficients in $\mathbb{Z}$, total degree $2(n-1)$, with degree $n-1$ in X_n such that $\Delta_g = \Phi_n(a_0, a_1, \ldots, a_{n-1}, a_n + b)$. Thus the set $\{b \in \mathbb{Z} \mid \Delta_g = N\}$ is finite and effectively computable and so is $\{g \mid Dg = Df, \text{ and } \Delta_g = N\}$. □

2.15. Proof of Theorem 1.9. Let $N_0, N_1, \dots, N_j$ be integers such that $N_j \neq 0$.

We have $D^j f(1,0) = n(n-1)\dots(n-j+1)f(1,0)$.

a) Let $R_j = \mathrm{rad}(n(n-1)\dots(n-j+1)R)$. If $f \in S$ then $D^j f(1,0) \in R_j^\times$ and $D^j f(0,1) \in R^\times \subseteq R_j^\times$ or $D^j f(0,1) = m'\Diamond^{(2)}$. From $\Delta_{D^j f} = N_j \neq 0$, by Theorem 1.7 the set $T_j = \{D^j f \mid f \in S,\ \Delta_{D^j f} = N_j\}$ is finite and effectively computable.

By repeated application of Lemma 2.14 the set of all $f \in S$ such that $\Delta_f = N_0$, $\Delta_{Df} = N_1, \dots, \Delta_{D^j f} = N_j$ is finite and effectively computable.

b) Let $f \in S$ be such that $\Delta_{D^j f} = N_j \neq 0$. Since $D^j f(1,0) = n(n-1)\dots(n-j+1)m$ and $D^j f(0,1) = m'\Diamond^{(3)}$, by Theorem 1.5 the set $T_j = \{D^j f \mid \Delta_{D^j f} = N_j,\ f \in S\}$ is finite and effectively computable. The proof is concluded as in part (a). □

3. Proof of the results of Section 1, (B)

Let $f = \langle a, b, c, d\rangle$. We recall that, the Hessian $H_f(X,Y)$ and the cubic covariant $Q_f(X,X)$ were defined in Section 1, (B).

With a simple calculation, we obtain $H_f(X,Y) = (3ac - b^2)X^2 + (9ad - bc)XY + (3db - c^2)Y^2$. As is easily seen:

$$Q_f(X,Y) = AX^3 + BX^2Y + CXY^2 + DY^3$$

where

$$A = 27\,a^2d - 9\,abc + 2b^3$$

$$B = 27\,abd - 18\,ac^2 + 3\,b^2c$$

$$C = 27\,acd - 18\,b^2d + 3\,bc^2$$

$$D = 27\,ad^2 - 9\,bcd + 2\,c^3.$$

We have the following remarkable identity:

$$27\,\Delta_f[f(X,Y)]^2 = 4[H_f(X,Y)]^3 - [Q_f(X,Y)]^2.$$

Thus if $\Delta_f \neq 0$ and if $f(x,y) \neq 0$ then $(H_f(x,y), Q_f(x,y) \neq (0,0)$. For the above definitions and results see Fricke [6] or Mordell [13].

3.1. Proof of Theorem 1.10. If $f \in S$ then

$$27\,N[f(x,y)]^2 = 4[H_f(x,y)]^3 - B^2 \neq 0,$$

by assumption. Since the polynomial $4X^3 - B^2$ has three simple roots by the Theorem of Schinzel & Tijdeman the set $M = \{f(x,y) \mid f \in S\}$ is finite and effectively computable and $0 \notin M$. By a similar argument, the set $M' = \{f(x',y') \mid f \in S\}$ is also finite and effectively computable and $0 \notin M'$. For each pair $(m,m') \in M \times M'$, by Corollary 1.8 the set of $f \in S$ such that $f(x,y) = m$ and $f(x',y') = m'$ is finite and effectively computable. Hence S is finite and effectively computable. □

For the proof of the next theorem we shall need the following theorem of Nagell ([14], [15]):

3.2. Theorem. *Let $D > 0$, $C \neq 0$ be integers. Then there exists an effectively computable integer $B > 0$, depending on D and C, such that there exist integers x, y satisfying $x^2 - Dy^2 = C$ if and only if there exist integers a, b such that $0 \leq a \leq B$ and $0 \leq b \leq B$ and $a^2 - Db^2 = C$. In the affirmative, the set $\{(x,y) \mid x^2 - Dy^2 = C\}$ is infinite.*

3.3. Proof of Theorem 1.11. If $f \in S$ let $g_f = Q_f(x,y)$, $g'_f = Q_f(x',y')$, $m = 3f(x,y)$, $m' = 3f(x',y')$. So $g^2 + 3Nm^2 = 4A^3$ and $g'^2 + 3Nm'^2 = 4A'^3$.

a) If $N > 0$ and $A < 0$ or $A' < 0$ the above set of relations is impossible.

If $A > 0$ and $A' > 0$ then $M = \{m \mid f \in S\}$ and $M' = \{m' \mid f \in S\}$ are finite and effectively computable.

By assumption these sets do not contain 0. By Corollary 1.8, for each pair $(m,m') \in M \times M'$ the set $\{f \in S \mid 3f(x,y) = m \text{ and } 3f(x',y') = m'\}$ is finite and effectively computable, hence S is finite and effectively computable.

b) Let $D = -N > 0$. By Theorem 3.2 the sets $\{(x,y) \mid x^2 - Dy^2 = 4A^3\}$ and $\{(x',y') \mid x'^2 - Dy'^2 = 4A'^3\}$ are either empty or infinite and there is an algorithm to decide if the above sets are empty or in finite. □

3.4. Proof of Theorem 1.12. If $f \in S$ then $27\Delta_f[f(x,y)]^2 = 4A^3 - B^2 \neq 0$. Then $L = \{\Delta_f \mid f \in S\}$ is finite and effectively computable, $0 \notin L$ and the set $M = \{f(x,y) \mid f \in S\}$ is finite and effectively computable

and $0 \notin M$. For each pair $(N,m) \in L \times M$ let $S_{(N,m)} = \{f \in S \mid \Delta_f = N, f(x,y) = m\}$. It suffices to show that each set $S_{(N,m)}$ is finite and effectively computable. If condition (2) or (2′) is satisfied, by Corollary 1.8 $S_{(N,m)}$ is finite and effectively computable. If condition (2″) is satisfied, the above argument shows that $M' = \{f(x',y') \mid f \in S\}$ is finite and effectively computable and $0 \notin M'$. By Corollary 1.8 $S_{(N,m)}$ is finite and effectively computable, concluding the proof. □

We shall need the following Theorem of Bugeaud [3]:

3.5. Theorem. *Let A, B be non-zero integers, let $R > 0$ be a square-free integer, let $m \geq 2$, $n \geq 2$ with $mn \geq 6$. Then there exists an effectively computable integer $C > 0$ such that if x, y are non-zero coprime integers such that $Ax^m + By^m \in R^\times$ then $|x|, |y| < C$.*

3.6. Proof of Theorem 1.13. If $f \in S$ we write $h_f = H_f(x,y)$, $g_f = Q_f(x,y)$ and $h_f = eu_f$, $g_f = ev_f$, where $gcd(u_f, v_f) = 1$. We have $4e^3u_f^3 - e^2v_f^2 = 4h_f^3 - g_f^2 = 27\Delta_f[f(x,y)]^2 \in R^\times$, where $R_1 = \operatorname{rad} 3R$. By the Theorem of Bugeaud $\{(u_f, v_f) \mid f \in S\}$ is finite and effectively computable, and so is $W = \{(h_f, g_f) \mid f \in S\}$. We note that from $\Delta_f \neq 0$, and $f(x,y) \neq 0$ then $4w^3 - w'^2 \neq 0$ for all $(w,w') \in W$. By Theorem 1.12 S is finite and effectively computable. □

3.7. Proof of Corollary 1.14. If $f = \langle a,b,c,d\rangle$ then $H_f(1,0) = 3ac - b^2$ and $Q_f(1,0) = 27\,a^2d - 9\,abc + 2b^3 = -2b(3ac - b^2) + 3a(9ad - bc)$. From the assumption we have $\gcd(H_f(1,0), Q_f(1,0)) = e$, and the corollary is a special case of Theorem 1.13. □

3.8. Remark. We give an example of an infinite set S of cubic forms $f = \langle a,b,c,d\rangle$ satisfying the following conditions

1) $\Delta_f \neq 0$
2) $\gcd(H_f(1,1), Q_f(1,1) = 1$
3) the set $\{p$ prime $\mid$ there exists $f \in S$ such that p divides $\Delta_f\}$ is infinite.

Let d be a non-zero integer, let $f = f_d = \langle d,0,1,-d\rangle$ and let $S = \{f_d \mid d \equiv 1 \pmod{61}\}$, so S is an infinite set. A simple calculation gives $\Delta_f = -d(4 + 27d^3)$ $f(1,1) = 1$, $H(1,1) = -9d^2 + 3d - 1$, $Q_f(1,1) =$

$-27d^2-18d+2$. Then $H_f(1,1) \equiv 2 \pmod 3$ and $Q_f(1,1) \equiv 2 \pmod 3$, so $H_f(1,1) \neq 0$ and $Q_f(1,1) \neq 0$. We verify that $\gcd(H_f(1,1), Q_f(1,1)) = 1$.

If a prime power p^e divides $H_f(1,1)$ and $Q_f(1,1)$, it is easily seen that p^e divides 61. But $H_f(1,1) \equiv 2 \pmod 3$ so $p^e = 1$.

Finally, by the Theorem of Dirichlet there is an infinite sequence $d_1 < d_2 \cdots < d_n < \ldots$ of primes, each $d_n \equiv 1 \pmod{61}$, each d_n dividing $\Delta_{f_{d_n}}$. □

4. Proof of theorems under the assumption that the (*ABC*) Conjecture is true

The next theorem, due to Granville [7], was proved earlier by Langevin [11], [12], with the additional requirement that $f(1,0) \neq 0$ and $f(0,1) \neq 0$.

4.1. Theorem. *Assume that the* (ABC) *Conjecture is true and let* f *be a form of degree* n *such that* $\Delta_f \neq 0$. *Then for every real number* $\varepsilon > 0$ *there exits a real number* $K > 0$ *(depending on* ε *and* f*) such that if* x, y *are coprime integers and* $f(x,y) \neq 0$ *then* $\operatorname{rad} f(x,y) \geq \max\{|x|,|y|\}^{n-2-\varepsilon}$.

With an additional assumption we obtain a better lower bound for $\operatorname{rad} f(x,y)$:

4.2. Lemma. *Assume that the* (ABC) *Conjecture is true. Let* $n \geq 2$, *let* L *be a positive square-free integer and let* f *be a form of degree* n *with* $\Delta_f \neq 0$ *and* $f(1,0) \neq 0$.

Then for every real number $\varepsilon > 0$ *there exists* $K > 0$, *depending on* ε, f *and* L *such that if* x, y *are coprime integers, such that* $y \in L^\times$ *and* $f(x,y) \neq 0$ *then* $\operatorname{rad} f(x,y) \geq K \max\{|x|,|y|\}^{n-1-\varepsilon}$.

Proof. Let $g(X,Y) = Yf(X,Y)$ so g is a form of degree $n+1$. We have $\Delta_g = f(1,0)^2\Delta_f \neq 0$. We apply the preceding Theorem to the form g, noting that $g(x,y) \neq 0$; $L \operatorname{rad} f(x,y) \geq \operatorname{rad}(yf(x,y)) = \operatorname{rad} g(x,y) \geq K \max\{|x|,|y|\}^{(n+1)-2-\varepsilon}$. So $\operatorname{rad} f(x,y) \geq \frac{K}{L} \max\{|x|,|y|\}^{n-1-\varepsilon}$ where $\frac{K}{L}$ depends on ε, f and L. □

The following calculations will be used repeatedly:

4.3. Lemma. *Assume that the (ABC) Conjecture is true. Let R be a positive square-free integer, let $\delta > 0$.*

a) *Let g be a form of degree $n \geq 3$, with $\Delta_g \neq 0$, let T be the set of all pairs of coprime integers (x, y) such that $g(x, y) \in I\big(R, \frac{n}{n-2} + \delta\big)$. Then T is finite.*

b) *Let g be a form of degree $n \geq 2$ with $\Delta_g \neq 0$ and such that $g(1, 0) \neq 0$. Let L be a positive square-free integer and let T be the set of all pairs of coprime integers (x, y), such that $y \in L^\times$, $g(x, y) \in I\big(R, \frac{n}{n-1} + \delta\big)$. Then T is finite.*

Proof. a) If $(x, y) \in T$ then $g(x, y) = uv$ where $u \in R^\times$, $\gcd(v, R) = 1$ and $\operatorname{rad} \operatorname{ind} v = \gamma \geq \frac{n}{n-2} + \delta$. Then $\operatorname{rad} g(x, y) = \operatorname{rad} uv \leq R|v|^{\frac{1}{\gamma}} \leq R|uv|^{\frac{1}{\gamma}} = R|g(x, y)|^{\frac{1}{\gamma}} \leq R\big[(n+1)\|g\|\big]^{\frac{1}{\gamma}} \times m_{(x,y)}^{\frac{n}{\gamma}} \leq R\big[(n+1)\|g\|\big]^{\ell} m_{(x,y)}^{n\ell}$ where $\|g\|$ is the height of g, $m_{(x,y)} = \max\{|x|, |y|\}$ and $\ell = \frac{1}{\frac{n}{n-2}+\delta}$. We have $n - 2 > n\ell$. Let $n < \varepsilon < n - 2 - n\ell$. By 4.1 there exists $K > 0$, depending on ε, and g, such that $\operatorname{rad} g(x, y) \geq K m_{(x,y)}^{n-2-\varepsilon}$.

From $m_{(x,y)}^{n-2-\varepsilon-n\ell} \leq \frac{R}{K}\big[(n+1)\|g\|\big]^{\ell}$ it follows that $m_{(x,y)}$ is bounded, so T is finite.

b) The proof is similar and appeals to Lemma 4.2. □

4.4. Proof of Theorem 1.16. 1°) The proof is similar to that of Theorem 1.7 – see 2.12 – and we consider L, H, $\mathcal{P}$, $\mathcal{P}_h$ as defined there. Again, $S_0 = \{h_P \mid P \in \mathcal{P}_h,\ h \in H\}$, so $S_0 \subseteq S$.

2°) Proof that S_0 is finite and effectively computable. It suffices to show that for every $h \in H$ the set $\mathcal{P}_h$ is finite. For every $P \in \mathcal{P}_h$ let $f = h_P$, so $h(x_P, y_P) = h_P(1, 0) = f(1, 0) \in I\big(R, \frac{n}{n-2} + \delta\big)$. By Lemma 4.6 the set $C_h = \{(x_P, y_P) \mid P \in \mathcal{P}_h\}$ is finite.

We proceed as in Lemma 2.11. Let $(r, s) \in C_h$, let $Q = \left(\begin{smallmatrix} r & p \\ s & q \end{smallmatrix}\right)$ with $\det Q = 1$. If $P = \left(\begin{smallmatrix} r & x'_P \\ s & y'_P \end{smallmatrix}\right) \in \mathcal{P}_h$ then $Q^{-1}P = \left(\begin{smallmatrix} 1 & z_P \\ O & w_P \end{smallmatrix}\right)$ with $w_P \equiv \det P \in L^\times$ and the mapping $(x'_P, y'_P) \mapsto (z_P, w_P)$ is a bijection. Let $g = h_Q$ so $g_{Q^{-1}P} = h_P = f \in S_0$.

With a simple calculation we see that if $0 \leq j \leq n-2$ then $(D^j g)_{Q^{-1}P} = D^j(g_{Q^{-1}P})$. If $h_P = f \in S_0$ then

$$(D^j g)(1, 0) = (D^j g)_{Q^{-1}P}(1, 0) = D^j(g_{Q^{-1}P})(1, 0)$$

$$= D^j(h_P)(1,0) = D^j f(1,0)$$
$$= n(n-1)\dots(n-j+1)f(1,0) \neq 0.$$

Also $D^j_g(z_P, w_P) = (D^j g)_{Q^{-1}P}(0,1) = D^j f(0,1) \in I\big(R, \frac{n-j}{n-j-1} + \delta\big)$. Since $w_P \in L^\times$ by Lemma 4.3 the set $C^* = \left\{(z_P, w_P) \mid P = \left(\begin{smallmatrix} r & x'_P \\ s & y'_P \end{smallmatrix}\right) \in \mathcal{P}_h\right\}$ is finite.

By Lemma 2.11 the corresponding pairs (x'_P, y'_P) belong to a finite set. Since this is true for each $(r,s) \in C_h$, it follows that $\mathcal{P}_h$ is finite, which suffices to show that S_0 is finite.

3°) Proof of (a).

We take $L = 1$ then $S = S_0$ so S is finite.

4°) Proof of (b).

Now we take $L = R$. Let $f \in S$ so there exist $h \in H$, $e \in R^\times$ and P such that

$$\det P \in R^\times \quad \text{and} \quad ef = h_P.$$

Let $P = \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right)$, $k = \gcd(x,y)$, $\ell = \gcd(x', y')$, $x = k\bar{x}$, $y = k\bar{y}$, $x' = \ell\bar{x'}$, $y' = \ell\bar{y'}$ and let $\bar{P} = \left(\begin{smallmatrix} \bar{x} & \bar{x'} \\ \bar{y} & \bar{y'} \end{smallmatrix}\right)$, hence $P = \bar{P}\left(\begin{smallmatrix} k & o \\ o & \ell \end{smallmatrix}\right)$; thus $(\det \bar{P})k\ell = \det P \in R^\times$ hence $\det \bar{P} \in R^\times$, $k, \ell, \in R^\times$. So $ef(X,Y) = h_{\bar{P}}(kX, \ell Y)$.

It suffices to show that $h_{\bar{P}} \in S$, hence $h_{\bar{P}} \in S_0$. From $ef = h_P$ then $\Delta_h(\det P)^{n(n-1)} = e^{2(n-1)}\Delta_f \in R^\times$, so $\Delta_h \in R^\times$ and therefore $\Delta_{h_{\bar{P}}} \in R^\times$.

We have $h_P = h_{\bar{P}}(kX, \ell Y)$ hence $D^j(h_P) = k^j(D^j h_{\bar{P}})(kX, \ell Y) = k^j(D^j h_{\bar{P}})_{\left(\begin{smallmatrix} k & o \\ o & \ell \end{smallmatrix}\right)}$.

It follows that $e^{2(n-j-1)}\Delta_{D^j f} = k^{2j(n-j-1)} \cdot (k\ell)^{(n-j)(n-j-1)} \times \Delta_{D^j h_{\bar{P}}}$ hence $\Delta_{D^j h_{\bar{P}}} \neq 0$.

Next we have $k^n h_{\bar{P}}(1,0) = h_{\bar{P}}(k,0) = h_P(1,0) = ef(1,0) = euv$ where $u \in R^\times$ $\gcd(v,R) = 1$, $\operatorname{rad}\operatorname{ind} v \geq \frac{n}{n-2} + \delta$. From $k \in R^\times$ then k^n divides eu, hence $h_{\bar{P}}(1,0) \in I\big(R, \frac{n}{n-2} + \delta\big)$. In a similar way we show that $D^j h_{\bar{P}}(0,1) \in I\big(R, \frac{n-j}{n-j-1} + \delta\big)$.

We have $eD^j f = D^j(h_P) = D^j(h_{\bar{P}}(kX, \ell Y)) = k^j D^j(h_{\bar{P}})(kX, \ell X)$. So $\ell^{n-j}k^j D^j(h_{\bar{P}})(0,1) = k^j D^j(h_{\bar{P}})(0,1) = e(D^j f)(0,1) = euv$ where $u \in R^\times$, $\gcd(v,R) = 1$ and $\operatorname{rad}\operatorname{ind} v \geq \frac{n-j}{n-j-1} + \delta$. Then $\ell^{n-j}k^j$ divides cu and so $D^j(h_{\bar{P}})(0,1) \in I\big(R, \frac{n-j}{n-j-1} + \delta\big)$.

This shows that $h_{\bar{P}} \in S_0$ and concludes the proof of (b). □

4.5. Remark. The real number K, which appears in the statement of 4.1 is effectively computable in terms of the real number, which we had still denoted by K, in the statement of the (ABC) Conjecture.

As a result, the number of elements of sets appearing in 4.2, 4.3 and 4.4 are effectively computable in terms of K and the given data.

ACKNOWLEDGEMENTS. I am grateful to K. GYŐRY for expert advice and to the referee for constructive criticism of an earlier version of this paper, as well as for the suggested Theorem 1.13.

References

[1] A. BAKER, Transcendental Number Theory, *Cambridge Univ. Press*, *Cambridge*, 1975.

[2] B. J. BIRCH and J. R. MERRIMAN, Finitess for binary forms with given discriminant, *Proc. London Math. Soc.* (3) **24** (1972), 385–394.

[3] Y. BUGEAUD, On the greatest prime factor of $ax^m + by^n$, II, *Bull. London Math. Soc.* **32** (2000), 673–678.

[4] J. W. S. CASSELS, An Introduction to the Geometry of Numbers, *Springer-Verlag*, *New Nork*, 1971.

[5] J. H. EVERTSE and K. GYŐRY, Effective finiteness results for binary forms with given discriminant, *Compos. Math.* **79** (1991), 196–204.

[6] R. FRICKE, Lehrbuch der Algebra, vol. I, *Vieweg & Sohn*, *Braunschweig*, 1924.

[7] A. GRANVILLE, *ABC* allows us to count square-frees, *Intern. Math. Res. Notes* **10** (1998), 991–1009.

[8] K. GYŐRY, Sur les polynômes à coefficients entiers et de discriminant donné, III, *Publ. Math. Debrecen* **21** (1976), 141–165.

[9] K. GYŐRY, On polynomials with integer coeficients and given discriminant, V. p-adic generalizations, *Acta Math. Acad. Sci. Hung.* **32** (1978), 175–190.

[10] C. HERMITE, Sur l' introduction des variables continues dans la théorie des nombres, *J. reine angew. Math.* **47** (1851), 191–216.

[11] M. LANGEVIN, Partie sans facteur carré de $F(a, b)$ (modulo la conjecture (abc)), *Sém. Th. Nombres, Publ. Math. Univ. Caen* (1993-4), 8 pages.

[12] M. LANGEVIN, Imbrications entre le théorème de Mason, la descente de Belyi et les différentes formes de la conjecture (abc), *J. Th. Nombres Bordeaux* **11** (1999), 91–109.

[13] L. J. MORDELL, Diophantine Equations, *Academic Press*, *New York*, 1970.

[14] T. NAGELL, Über die Darstellung ganzer Zahlen durch eine indefinite binäre quadratische Form, *Archiv d. Math.* **2** (1949/50), 161–165.

[15] T. Nagell, Bemerkung über die Diophantische Gleichung $u^2 - Dv^2 = C$, *Archiv d. Math.* **3** (1952), 8–9.

[16] A. Nitaj, La conjecture *abc*, *L' Enseign. Math.* **1996**, 3–24.

[17] P. Ribenboim, *ABC* candies, *J. Number Theory* **81** (2000), 48–60.

[18] P. Ribenboim, The (*ABC*) conjecture and the radial index of integers, *Acta Arith.* **96** (2001), 389–404.

[19] A. Schinzel and R. Tijdeman, On the equation $y^m = P(x)$, *Acta Arith.* **31** (1976), 199–204.

[20] T. N. Shorey and R. Tijdeman, Exponential Diophantine Equations, *Cambridge Univ. Press*, *Cambridge*, 1986.

PAULO RIBENBOIM
DEPARTMENT OF MATHEMATICS AND STATISTICS
QUEEN'S UNIVERSITY
KINGSTON, ON, K7L3N6
CANADA

(Received February 14, 2002; revised March 1, 2005)