DIOPHANTINE PROBLEMS RELATED TO DISCRIMINANTS AND RESULTANTS OF BINARY FORMS

ATTILA BÉRCZES, JAN-HENDRIK EVERTSE, AND KÁLMÁN GYŐRY

1. Introduction.

In this paper we give a survey of recent results obtained by the authors on discriminant and resultant equations.

The discriminant of a binary form $F = \sum_{i=0}^{m} a_i X^{m-i} Y^i = \prod_{k=1}^{m} (\alpha_k X - \beta_k Y)$ is defined by

$$D(F) = \prod_{1 \leqslant k < l \leqslant m} (\alpha_k \beta_l - \alpha_l \beta_k)^2.$$

As is well known, $D(F)$ is a homogeneous polynomial in $\mathbb{Z}[a_0, \ldots, a_m]$ of degree $2m - 2$. Further, for any scalar λ and any 2×2-matrix $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we have

$$D(\lambda F_U) = \lambda^{2m-2} (\det U)^{m(m-1)} D(F), \tag{1.1}$$

where $F_U(X, Y) := F(aX + bY, cX + dY)$.

The resultant of two binary forms

$$F = \sum_{i=0}^{m} a_i X^{m-i} Y^i = \prod_{k=1}^{m} (\alpha_k X - \beta_k Y),$$
$$G = \sum_{j=0}^{n} b_j X^{n-j} Y^j = \prod_{l=1}^{n} (\gamma_l X - \delta_l Y)$$

2000 Mathematics Subject Classification: 11D57, 11D72.

Keywords and Phrases: Discriminant, resultant, polynomials, binary forms.

The research was supported in part by the Hungarian Academy of Sciences (A.B.,K.G.), and by grants T42985 (A.B., K.G.), T38225 (A.B.,K.G.) and T48791 (A.B.) of the Hungarian National Foundation for Scientific Research.

is given by

$$R(F,G)=\prod_{k=1}^{m}\prod_{l=1}^{n}(\alpha_k\delta_l-\beta_k\gamma_l).$$

Using the well-known determinantal expression for the resultant (see [29, §34]), one shows that $R(F,G)$ is a polynomial in $\mathbb{Z}[a_0,\dots,a_m;b_0,\dots,b_n]$ which is homogeneous of degree n in $a_0,\dots,a_m$ and homogeneous of degree m in $b_0,\dots,b_n$. Further, for any scalars λ,μ and any 2×2-matrix U one has

$$R(\lambda F_U,\mu G_U)=\lambda^n\mu^m(\det U)^{mn}R(F,G). \tag{1.2}$$

We note that the discriminant and resultant of monic binary forms F,G, i.e. with $F(1,0)=1$, $G(1,0)=1$ coincide with those of the polynomials $F(X,1)$, $G(X,1)$.

Let $S=\{p_1,\dots,p_t\}$ be a finite, possibly empty set of primes. The ring of S-integers is defined by $\mathbb{Z}_S=\mathbb{Z}[(p_1\cdots p_t)^{-1}]$ if $S\neq\emptyset$ and $\mathbb{Z}_S=\mathbb{Z}$ if $S=\emptyset$. The unit group of $\mathbb{Z}_S$ is ${\mathbb{Z}_S}^*=\{\pm\prod_{i=1}^t p_i^{w_i}: w_i\in\mathbb{Z}\}$ if $S\neq\emptyset$ and $\{\pm1\}$ if $S=\emptyset$. We consider the discriminant equation

$$D(F)\in c{\mathbb{Z}_S}^*$$

to be solved in binary forms $F\in\mathbb{Z}_S[X,Y]$, and the resultant equation

$$R(F,G)\in c{\mathbb{Z}_S}^*$$

to be solved in pairs of binary forms $F,G\in\mathbb{Z}_S[X,Y]$, where c is a positive integer. The solutions of these equations can be divided in a natural way into equivalence classes. In the monic case the earlier results concerning these equations were stated and proved in terms of polynomials. In this paper, we give a survey on recent results obtained by us concerning the number of equivalence classes. In Section 2 we present some results from [2] on the discriminant equation, while Section 3 is devoted to some new results on the resultant equation which will appear in [3].

The focus of this paper will be on estimates for the number of equivalence classes, and so we will not discuss algorithmic results. In the literature there are finiteness results for much more general equations and inequalities, such as 'inhomogeneous versions', inequalities involving discriminants or resultants, or discriminant and resultant equations for binary forms with coefficients in an arbitrary finitely generated domain of characteristic 0, etc. Again, we refrain from a discussion of those. For simplicity we restrict ourselves to results on binary forms with coefficients in $\mathbb{Z}_S$, but we note that some of our results in [2] have been established for binary forms with coefficients in the ring of S-integers of an arbitrary algebraic number field.

2. Discriminant equations.

For a domain Ω we denote by Ω^* the unit group of Ω, by $\mathrm{NS}_2(\Omega)$ the set of non-singular 2×2-matrices with entries in Ω, and by $\mathrm{GL}_2(\Omega)$ the group of matrices in $\mathrm{NS}_2(\Omega)$ with determinant in Ω^*. Two binary forms $F, G \in \Omega[X,Y]$ are called Ω-equivalent if there are $\varepsilon \in \Omega^*$ and $U \in \mathrm{GL}_2(\Omega)$ such that $G = \varepsilon F_U$. [1] For monic binary forms F, we define a stronger notion of equivalence as follows: two monic binary forms $F, G \in \Omega[X,Y]$ are called strongly Ω-equivalent if there are $\varepsilon \in \Omega^*$ and $a \in \Omega$ such that $G(X,Y) = F(X+aY, \varepsilon Y)$. It is immediate from (1.1) that if $F, G \in \Omega[X,Y]$ are Ω-equivalent, then $D(G) = \varepsilon D(F)$ for some $\varepsilon \in \Omega^*$.

From classical results of Lagrange and Gauss it follows that for any non-zero integer c, the binary quadratic forms $F \in \mathbb{Z}[X,Y]$ with discriminant $D(F) = c$ lie in only finitely many $\mathbb{Z}$-equivalence classes. Hermite proved the analogous result for binary cubic forms in $\mathbb{Z}[X,Y]$. The proofs of Lagrange, Gauss and Hermite are effective in that they give an effective procedure to determine a full system of representatives for the equivalence classes.

In 1972, Birch and Merriman [6] extended the finiteness results of Lagrange, Gauss and Hermite as follows. Let O_S be the ring of S-integers in some number field K, where S is a finite set of places of K. Let $c \in O_S$, $c \neq 0$. Then for any integer $m \geqslant 2$, the binary forms $F \in O_S[X,Y]$ of degree m with

$$D(F) \in cO_S^* \tag{2.1}$$

[1] In [2], two binary forms $F, G \in \Omega[X,Y]$ such that $G = \varepsilon F_U$ for some $\varepsilon \in \Omega^*$, $U \in \mathrm{GL}_2(\Omega)$ are called weakly Ω-equivalent, while the notion of Ω-equivalence is used for binary forms F, G such that $G = F_U$ for some $U \in \mathrm{GL}_2(\Omega)$. This latter notion of Ω-equivalence is not used in the present paper.

lie in only finitely many O_S-equivalence classes. The proof of Birch and Merriman is ineffective.

In the 1970's, GYŐRY [19] proved in a quantitative form that every monic binary form $F \in O_S[X,Y]$ of degree m satisfying (2.1) is strongly O_S-equivalent to a monic binary form with height bounded above by an effectively computable number depending only on K, S and c. For monic binary forms, this is a more precise and effective version of the result of Birch and Merriman. Győry's results made it possible to find in principle all power integral bases of a given number field, and also to find in principle all solutions of an index form equation. Győry's proof depends on lower bounds for linear forms in logarithms of algebraic numbers, both in the archimedean and the p-adic case.

In 1991, EVERTSE and GYŐRY [12] proved an effective analogue of the result of Birch and Merriman in full generality, i.e., they proved that every binary form $F \in O_S[X,Y]$ with (2.1) is O_S-equivalent to a binary form with height effectively bounded above in terms of K, S and c. Again, the proof depends on lower bounds for linear forms in logarithms.

Below we discuss some recent results by the authors [2], giving explicit upper bounds for the number of equivalence classes of binary forms with (2.1). In [2] we proved results valid for binary forms having their coefficients in the ring of S-integers of an arbitrary number field. For simplicity we state here our results only over the ring of S-integers $\mathbb{Z}_S = \mathbb{Z}[(p_1 \cdots p_t)^{-1}]$ in $\mathbb{Q}$, where $S = \{p_1, \ldots, p_t\}$ is a finite, possibly empty set of primes.

We first deal with irreducible binary forms. Let $F(X,Y) = \sum_{i=0}^{m} a_i X^{m-i} Y^i$ $= a_0 \prod_{k=1}^{m} (X - \theta^{(i)} Y)$ be a binary form in $\mathbb{Z}_S[X,Y]$ which is irreducible over $\mathbb{Q}$, where $\theta^{(1)}, \ldots, \theta^{(m)}$ are the conjugates of some algebraic number θ and let $K = \mathbb{Q}(\theta)$. We define the *invariant order* O_F associated with F to be the $\mathbb{Z}_S$-module generated by

$$(2.2)\quad \omega_1 = 1,\ \omega_2 = a_0\theta,\ \omega_3 = a_0\theta^2 + a_1\theta, \ldots, \omega_m = a_0\theta^{m-1} + \cdots + a_{m-2}\theta\,.$$

As it turns out (see [25] or [28]), O_F is a $\mathbb{Z}_S$-order in K, i.e., an overring of $\mathbb{Z}_S$ which is finitely generated as a $\mathbb{Z}_S$-module and has quotient field K. Further, the discriminant of the basis given by (2.2), i.e., $D_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_m) =$

$\det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j))$, is precisely the discriminant of F. NAKAGAWA [25] and SIMON [28] showed that if $F, G \in \mathbb{Z}_S[X, Y]$ are two $\mathbb{Z}_S$-equivalent binary forms, then their associated orders O_F, O_G are isomorphic as $\mathbb{Z}_S$-algebras. Using an argument of DELONE and FADDEEV [7, II, §15], one can show that there is a one-to-one correspondence between $\mathbb{Z}_S$-equivalence classes of irreducible binary cubic forms in $\mathbb{Z}_S[X, Y]$ and isomorphism classes of $\mathbb{Z}_S$-orders in cubic number fields. On the other hand, SIMON [28] gave examples of number fields of degree 4 and higher, having orders not coming from a binary form. From the result of Birch and Merriman mentioned above it follows that there are only finitely many $\mathbb{Z}_S$-equivalence classes of binary forms whose associated order is isomorphic to a given order. The quantitative version below is the special case $k = \mathbb{Q}$ of BÉRCZES, EVERTSE and GYŐRY [2, Theorem 2.1].

Theorem 2.1. [2] *Let K be a number field of degree $m \geqslant 4$. Let $S = \{p_1, \dots, p_t\}$ be a finite, possibly empty set of primes. Let O be a $\mathbb{Z}_S$-order in K. Then the irreducible binary forms $F \in \mathbb{Z}_S[X, Y]$ with*

$$O_F \cong O \quad \text{as } \mathbb{Z}_S\text{-algebras} \tag{2.3}$$

lie in the union of at most $2^{24m^3(t+1)}$ $\mathbb{Z}_S$-equivalence classes.

An irreducible binary form $F \in \mathbb{Q}[X, Y]$ is said to be associated with a number field K if there is θ with $K = \mathbb{Q}(\theta)$ such that $F(\theta, 1) = 0$. We agree that the binary forms cY ($c \in \mathbb{Q}^*$) are associated with $\mathbb{Q}$. A binary form $F \in \mathbb{Q}[X, Y]$ is said to be associated with the number fields $K_0, \dots, K_r$ if it can be factored as $\prod_{i=0}^r F_i$, where F_i is an irreducible binary form in $\mathbb{Q}[X, Y]$ associated with K_i for $i = 0, \dots, r$. It is easy to check that $\deg F = \sum_{i=0}^r [K_i : \mathbb{Q}]$. The discriminant of a number field K is denoted by $D_{K/\mathbb{Q}}$. If $F \in \mathbb{Z}_S[X, Y]$ is an irreducible binary form associated with K, then with $\omega_1, \dots, \omega_m$ given by (2.2), we have

$$D(F) = D_{K/\mathbb{Q}}(\omega_1, \dots, \omega_m) \in (c^2 D_{K/\mathbb{Q}}) \cdot \mathbb{Z}_S^*, \tag{2.4}$$

where c is the index of O_F in the integral closure of $\mathbb{Z}_S$ in K.

More generally, let $F \in \mathbb{Z}_S[X, Y]$ be a binary form associated with the number fields $K_0, \dots, K_r$. Then F can be factored as $\prod_{i=0}^r F_i$ where F_i is an irreducible binary form in $\mathbb{Z}_S[X,Y]$ associated with K_i for $i=0,\dots,r$. From (1.1), (1.2) it follows easily that

$$D(F)=\prod_{i=0}^{r}D(F_i)\cdot\prod_{0\leqslant i<j\leqslant r}R(F_i,F_j)^2, \tag{2.5}$$

and in combination with (2.4) this gives that there is $c\in\mathbb{Z}_S\setminus\{0\}$ with

$$D(F)\in(c^2\prod_{i=0}^{r}D_{K_i/\mathbb{Q}})\cdot\mathbb{Z}_S^*. \tag{2.6}$$

The following result is the special case $k=\mathbb{Q}$ of [2, Theorem 2.3]. For a positive integer d we denote by $\omega(d)$ the number of distinct primes dividing d. Further, for $\alpha\in\mathbb{N}$, we put

$$\tau_\alpha(d):=\prod_{p\mid d}\binom{\mathrm{ord}_p(d)+\alpha}{\alpha}, \tag{2.7}$$

where the product is taken over all primes dividing d, and where $\mathrm{ord}_p(d)$ is the exponent of p in the prime factorization of d.

Theorem 2.2. [2] *Let $K_0,\dots,K_r$ be number fields with $[K_0:\mathbb{Q}]\geqslant 3$. Put $m:=\sum_{i=1}^{r}[K_i:\mathbb{Q}]$. Let $S=\{p_1,\dots,p_t\}$ be a possibly empty set of primes, and c a positive integer coprime with $p_1\cdots p_t$ if $t>0$. Then the set of binary forms $F\in\mathbb{Z}_S[X,Y]$ which are associated with $K_0,\dots,K_r$ and which satisfy (2.6) lie in the union of at most*

$$2^{24m^3(t+\omega(c)+1)}\cdot\tau_{m(m-1)/2}(c^2)\Big(\sum_{d^{m(m-1)/2}\mid c}d\Big)$$

$\mathbb{Z}_S$-equivalence classes, where the sum is taken over all positive integers d such that $d^{m(m-1)/2}$ divides c.

This may be compared with [10, Theorem 1], which deals with the special case that the binary forms F under consideration are monic. In this result, the splitting field of F is fixed and not the fields $K_0,\dots,K_r$. Further, in [19, Part II] and [10] explicit upper bounds are given for the degree of F.

The upper bound in Theorem 2.2 is of the shape $O(c^{\frac{2}{m(m-1)}+\delta})$ as $c\to\infty$ for every $\delta>0$. One can show as follows that this cannot be improved to

$O(c^{\kappa})$ as $c \to \infty$ for any $\kappa < 2/m(m-1)$. Pick a binary form $F_0 \in \mathbb{Z}_S[X,Y]$ of non-zero discriminant associated with $K_0, \ldots, K_t$. Then

$$D(F_0) \in (c_0^2 \prod_{i=0}^{r} D_{K_i/\mathbb{Q}}) \cdot \mathbb{Z}_S^*$$

for some non-zero $c_0 \in \mathbb{Z}$ coprime with $p_1 \cdots p_t$. Consider the binary forms $F = (F_0)_A$ for all matrices $A \in \mathrm{NS}_2(\mathbb{Z})$ with determinant equal to Δ, say, where Δ is coprime with $p_1 \cdots p_t$. By (1.1), each such binary form F satisfies (2.6) with $c = c_0 \Delta^{m(m-1)/2}$. Further, by an argument in [2, §9] these binary forms lie in at least $O(\Delta) = O(c^{2/m(m-1)})$ $\mathbb{Z}_S$-equivalence classes.

To obstruct the above construction we impose an additional condition on our binary forms. A binary form $F \in \mathbb{Z}_S[X,Y]$ is called $\mathbb{Z}_S$-*minimal* if it can not be expressed as $F = G_A$ with $G \in \mathbb{Z}_S[X,Y]$ and $A \in \mathrm{NS}_2(\mathbb{Z}_S) \backslash \mathrm{GL}_2(\mathbb{Z}_S)$. The following result is not contained in [2].

Theorem 2.3. *Let $K_0, \ldots, K_r$, m, S, c be as in Theorem 2.2. Then the set of $\mathbb{Z}_S$-minimal binary forms $F \in \mathbb{Z}_S[X,Y]$ which are associated with $K_0, \ldots, K_r$ and which satisfy (2.6), lie in the union of at most*

$$2^{24m^3(t+\omega(c)+1)} \cdot \tau_{m(m-1)/2}(c^2)$$

$\mathbb{Z}_S$-equivalence classes.

It should be noted that the bound in Theorem 2.3 is $O(c^{\delta})$ as $c \to \infty$ for every $\delta > 0$.

We mention that Theorems 2.1 and 2.2 have been established in [2] in a more general form, for binary forms having their coefficients in the ring of S-integers in an arbitrary number field instead of $\mathbb{Q}$. However, we have not been able to carry over Theorem 2.3 to number fields.

We sketch the proofs of the results mentioned above. For a field $\mathbb{K}$, we endow $(\mathbb{K}^*)^n$ with coordinatewise multiplication $(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n)$. Our main tool is the following result:

Theorem (Beukers, Schlickewei [5]). *Let $\mathbb{K}$ be a field of characteristic 0 and Γ a subgroup of $(\mathbb{K}^*)^2$ of finite rank ρ. Further, let $a, b \in \mathbb{K}^*$. Then* *the equation*

$$ax + by = 1 \text{ in } (x, y) \in \Gamma \tag{2.8}$$

has at most $2^{8\rho+16}$ *solutions.*

We first sketch the proof of Theorem 2.1. The first step of the proof is to estimate the number of $\mathbb{Q}$-equivalence classes of binary forms with (2.3), and the second step to estimate how many $\mathbb{Z}_S$-equivalence classes are contained in a $\mathbb{Q}$-equivalence class. Recall that according to the definition from the beginning of this section, two binary forms F, G are called $\mathbb{Q}$-equivalent if $G = \lambda F_U$ for some $\lambda \in \mathbb{Q}^*$ and $U \in \mathrm{GL}_2(\mathbb{Q})$.

Let $F \in \mathbb{Z}_S[X, Y]$ be a binary form with (2.3). Then F can be factored as

$$F(X, Y) = a_0 \prod_{k=1}^{m} (X - \theta_F^{(k)} Y),$$

with $\mathbb{Q}(\theta_F) = K$. The cross ratios associated with F are defined by

$$\Delta_{ijkl}(F) = \frac{(\theta_F^{(i)} - \theta_F^{(j)})(\theta_F^{(k)} - \theta_F^{(l)})}{(\theta_F^{(i)} - \theta_F^{(k)})(\theta_F^{(j)} - \theta_F^{(l)})}$$

($1 \leqslant i, j, k, l \leqslant m$). We denote by $\Delta(F)$ the tuple consisting of all these cross ratios. Let $K_{ijkl} := \mathbb{Q}(\theta_F^{(i)}, \theta_F^{(j)}, \theta_F^{(k)}, \theta_F^{(l)})$.

By an elementary argument (see [2, Lemma 5.1 and p. 390]) one shows that $\Delta_{ijkl}(F) = a_{ijkl} x_{ijkl}$, where a_{ijkl} depends only on the given order O, and where x_{ijkl} belongs to the unit group U_{ijkl} of the integral closure of $\mathbb{Z}_S$ in K_{ijkl}. By inserting this into the well-known relation $\Delta_{ijkl}(F) + \Delta_{ilkj}(F) = 1$, one obtains

$$a_{ijkl} x_{ijkl} + a_{ilkj} x_{ilkj} = 1.$$

Using the Dirichlet-Chevalley-Weil S-unit theorem, one can estimate from above the ranks of the groups U_{ijkl} in terms of m and t. Then an application of the result of Beukers and Schlickewei gives an explicit upper bound for the number of possibilities for the tuple of cross ratios $\Delta(F)$, as F runs through all binary forms with (2.3).

Now if F, G are two binary forms in $\mathbb{Z}_S[X, Y]$ with (2.3) and with $\Delta(F) = \Delta(G)$, then by elementary projective geometry there exists a unique projective transformation mapping the roots $\theta_F^{(1)}, \ldots, \theta_F^{(m)}$ of F to the roots $\theta_G^{(1)}, \ldots, \theta_G^{(m)}$ of G. This transformation is defined over $\mathbb{Q}$ since it is invariant under the action of the Galois group of the normal closure of K over $\mathbb{Q}$. Then by an elementary manipulation one shows that F, G are $\mathbb{Q}$-equivalent. Thus, one obtains an explicit upper bound for the number of $\mathbb{Q}$-equivalence classes of binary forms $F \in \mathbb{Z}_S[X, Y]$ satisfying (2.3).

By making the above argument more precise, one derives an upper bound $2^{24(m^3-m^2)(t+1)}$. Using an elementary argument (see [2, Lemma 3.3 and §5]) one shows that each $\mathbb{Q}$-equivalence class is contained in at most m^{t+1} $\mathbb{Z}_S$-equivalence classes. By multiplying the two bounds one obtains Theorem 2.1. $\square$

We now sketch the proofs of Theorems 2.2 and 2.3. We first assume that $c = 1$, and restrict ourselves to irreducible binary forms F associated with a number field K. For such forms, the order O_F is equal to the integral closure of $\mathbb{Z}_S$ in K. So by Theorem 2.1, the binary forms F under consideration lie in at most $2^{24m^3(t+1)}$ $\mathbb{Z}_S$-equivalence classes.

We keep our assumption $c = 1$, but now consider reducible binary forms in $\mathbb{Z}_S[X, Y]$ associated with a sequence of number fields $K_0, \ldots, K_r$. Such forms can be factored as $F = \prod_{i=0}^{r} F_i$, where $F_i \in \mathbb{Z}_S[X, Y]$ is irreducible and associated with K_i. Then by (2.4), (2.5), (2.6) we have $D(F_i) \in D_{K_i/\mathbb{Q}}\mathbb{Z}_S^*$ for $i = 0, \ldots, r$ and $R(F_i, F_j) \in \mathbb{Z}_S^*$ for $0 \leqslant i < j \leqslant r$. Using the already established result for irreducible binary forms one may estimate the number of $\mathbb{Z}_S$-equivalence classes for F_0, and given F_0 one may estimate the number of possibilities for $F_1, \ldots, F_r$, using a result for a special case of the resultant equation discussed in the next chapter. Thus, one proves Theorems 2.2 and 2.3 in the special case $c = 1$.

We now consider binary forms F satisfying (2.6) for arbitrary c. Let $T := S \cup \{p : p|c\}$. Then by what already has been established, the binary forms under consideration lie in at most $2^{24m^3(t+\omega(c)+1)}$ $\mathbb{Z}_T$-equivalence classes. One obtains Theorem 2.2 by using the elementary [2, Proposition 4.7], which implies that a $\mathbb{Z}_T$-equivalence class is contained in the union of at most $\tau_{m(m-1)/2}(c^2)\big(\sum_{d^{m(m-1)/2}|c} d\big)$ $\mathbb{Z}_S$-equivalence classes.

To prove Theorem 2.3 we have to make some modifications in the proof of [2, Proposition 4.7], which we discuss below.

For a prime number p, let $\mathbb{Z}_p$ denote the localization of $\mathbb{Z}$ at p; thus $\mathbb{Z}_S = \cap_{p\notin S}\mathbb{Z}_p$. A binary form $F \in \mathbb{Z}_p[X,Y]$ is called $\mathbb{Z}_p$-minimal, if there are no binary form $G \in \mathbb{Z}_p[X,Y]$ and $A \in \mathrm{NS}_2(\mathbb{Z}_p)\backslash\mathrm{GL}_2(\mathbb{Z}_p)$ such that $F = G_A$. Assume that F is not $\mathbb{Z}_p$-minimal for some $p \notin S$, i.e., that $F = G_A$ for some binary form $G \in \mathbb{Z}_p[X,Y]$ and some $A \in \mathrm{NS}_2(\mathbb{Z}_p) \setminus \mathrm{GL}_2(\mathbb{Z}_p)$. We may express A as $A = UB$, where $U \in \mathrm{GL}_2(\mathbb{Z}_p)$ and $B \in \mathrm{NS}_2(\mathbb{Z}_S)$ with $\det B = p^\beta$ for some positive integer β. Thus, $F = H_B$, where $H = G_U$. We have $H \in \mathbb{Z}_p[X,Y]$. Further, for every prime $q \notin S \cup \{p\}$ we have $B \in \mathrm{GL}_2(\mathbb{Z}_q)$, hence $H \in \mathbb{Z}_q[X,Y]$. This implies $H \in \mathbb{Z}_S[X,Y]$. So F is not $\mathbb{Z}_S$-minimal. That is, if we assume that the binary form F is $\mathbb{Z}_S$-minimal, then it is also $\mathbb{Z}_p$-minimal for every prime $p \notin S$.

Let $\mathcal{C}$ be a set of binary forms $F \in \mathbb{Z}_S[X,Y]$ which are $\mathbb{Z}_S$-minimal, are associated with $K_0,\dots,K_r$, satisfy (2.6), and are $\mathbb{Z}_T$-equivalent to one another. Let p be a prime outside S. By combining Lemmata 4.3 and 4.5 of [2], we infer the following: there is a collection $\mathcal{D}$ of binary forms $F_0 \in \mathbb{Z}_p[X,Y]$ of cardinality at most

$$\tau_p := \binom{2\,\mathrm{ord}_p(c) + \frac{1}{2}m(m-1)}{\frac{1}{2}m(m-1)}$$

such that for every $F \in \mathcal{C}$ there are $F_0 \in \mathcal{D}$ and $A \in \mathrm{NS}_2(\mathbb{Z}_p)$ with $F = (F_0)_A$. By the remarks above, the binary forms in $\mathcal{C}$ are $\mathbb{Z}_p$-minimal. Therefore, the binary forms in $\mathcal{C}$ lie in at most τ_p $\mathbb{Z}_p$-equivalence classes. Now basically this means that $\mathcal{C}$ is contained in the union of at most $\prod_{p\notin S}\tau_p = \tau_{m(m-1)/2}(c^2)$ S-equivalence classes. (In fact one has to work with 'augmented forms' as introduced in [2, §2] and use [2, Lemma 3.2]). Multiplying the latter bound with our estimate for the number of T-equivalence classes, we obtain Theorem 2.6. □

3. Resultant equations.

We introduce some terminology in addition to what has been introduced in the previous section. Let Ω be a domain. Two pairs of binary forms (F_1, G_1), (F_2, G_2) in $\Omega[X, Y]$ are called Ω-equivalent if $F_2 = \varepsilon(F_1)_U$, $G_2 = \eta(G_1)_U$ for some $\varepsilon, \eta \in \Omega^*$ and $U \in \mathrm{GL}_2(\Omega)$. Two pairs of *monic* binary forms (F_1, G_1), (F_2, G_2) in $\Omega[X, Y]$ are called strongly Ω-equivalent if $F_2(X, Y) = F_1(X + aY, \varepsilon Y)$, $G_2(X, Y) = G_1(X + aY, \varepsilon Y)$ for some $a \in \Omega$, $\varepsilon \in \Omega^*$.

Let again $S = \{p_1, \dots, p_t\}$ be a finite, possibly empty set of primes, and c a positive integer coprime with $p_1 \cdots p_t$ if $t > 0$. We deal with the resultant equation

$$R(F, G) \in c\mathbb{Z}_S^* \tag{3.1}$$

to be solved in binary forms $F, G \in \mathbb{Z}_S[X, Y]$.

At present, there are two types of finiteness results for (3.1). The first deals with the case that one of the binary forms, G, say, is fixed, and F is allowed to vary. Then from results of Schmidt [27], Fujiwara [18], Ru and Wong [26], and Győry [21] it follows that if $G \in \mathbb{Z}_S[X, Y]$ is a binary form of degree $n \geqslant 3$ with non-zero discriminant then up to multiplication by a factor from $\mathbb{Z}_S^*$, there are only finitely many binary forms $F \in \mathbb{Z}_S[X, Y]$ of degree $m < n/2$ that satisfy (3.1). Further, in [23] (see also [4]) the upper bound

$$\left(2^{34} n^2\right)^{m^3(t+\omega(c)+1)}$$

was given for the number of these binary forms F. By restricting to linear binary forms $F = yX - xY$, Eq. (3.1) reduces to the Thue-Mahler equation $G(x, y) \in c\mathbb{Z}_S^*$ and we deduce the well-known finiteness result for the latter. More generally, if one views the coefficients of F as variables $x_0, \dots, x_m$, one can express (3.1) as a *decomposable form equation* $H(x_0, \dots, x_m) \in c\mathbb{Z}_S^*$ in $x_0, \dots, x_m \in \mathbb{Z}_S$, where H is a decomposable form, i.e., a product of linear forms with algebraic coefficients. Győry [21], [23] obtained the finiteness results for (3.1) by applying general theory for decomposable form equations, see [8], [15].

In the second type of finiteness result, both F, G are allowed to vary, but one has to fix a number field L such that both F, G factor into linear forms in $L[X, Y]$. By (1.2), if (F, G) is a solution of (3.1) then so is any pair $\mathbb{Z}_S$-equivalent to (F, G). So if we allow both F, G to vary, we can prove only finiteness results up to $\mathbb{Z}_S$-equivalence. The first result of this type was proved by GYŐRY [20]. He showed that if m, n are integers with $m \geqslant 2$, $n \geqslant 2$ and $m + n \geqslant 5$, and L is a given number field, then there are only finitely many strong $\mathbb{Z}_S$-equivalence classes of pairs of monic binary forms $F, G \in \mathbb{Z}_S[X, Y]$ satisfying (3.1) such that $\deg F = m$, $\deg G = n$, F, G have non-zero discriminant and F, G factor into linear forms in $L[X, Y]$. Further, in [20] explicit upper bounds are given for the number of such $\mathbb{Z}_S$-equivalence classes and for $\deg F + \deg G$. Then EVERTSE and GYŐRY [14] proved an analogue for not necessarily monic binary forms, stating that if $m \geqslant 3$, $n \geqslant 3$, then up to (not necessarily strong) $\mathbb{Z}_S$-equivalence, there are only finitely many pairs of binary forms $F, G \in \mathbb{Z}_S[X, Y]$ satisfying (3.1) such that $\deg F = m$, $\deg G = n$, F, G have non-zero discriminant and F, G factor into linear factors in $L[X, Y]$. One can show in both the monic and non-monic case that the conditions on m, n cannot be relaxed. We mention that both types of finiteness results depend on the Subspace Theorem and are therefore ineffective.

Below, we give a survey of some new quantitative results concerning the second type of finiteness result for (3.1), which will appear in [3]. In what follows, $S = \{p_1, \ldots, p_t\}$ is a finite, possibly empty set of primes and c a positive integer, assumed to be coprime with $p_1 \cdots p_t$ if $S \neq \emptyset$. Further, $K_1, \ldots, K_r$, $L_1, \ldots, L_s$ are number fields. Put

$$m := \sum_{i=1}^{r} [K_i : \mathbb{Q}], \quad n := \sum_{i=1}^{s} [L_i : \mathbb{Q}].$$

We will deal with pairs of binary forms (F, G) such that F is associated with $K_1, \ldots, K_r$ and G with $L_1, \ldots, L_s$. Our first result concerns monic binary forms.

Theorem 3.1. [3] *Assume that* $m \geqslant 2$, $n \geqslant 2$, $m + n \geqslant 5$. *Then the set of pairs of monic binary forms* $F, G \in \mathbb{Z}_S[X, Y]$ *with* $\deg F = m$, $\deg G = n$ *and*

$$R(F,G) \in c\mathbb{Z}_S^* \tag{3.1}$$

for which

F is associated with $K_1,\ldots,K_r$, G is associated with $L_1,\ldots,L_s$,
F, G have non-zero discriminants,

is contained in the union of at most

$$e^{17(m+n+10^{11})mn(t+\omega(c)+1)}$$

strong $\mathbb{Z}_S$-equivalence classes.

This may be compared with the upper bound of [20, Theorem 2a], where the fields K_i and L_j are not fixed, but F and G split into linear factors over a given number field.

We now deal with binary forms which are not necessarily monic. Unfortunately, in this case we are able to give an explicit estimate only for the number of $\mathbb{Z}_S$-equivalence classes of those pairs of binary forms F, G such that at least one of F, G is $\mathbb{Z}_S$-minimal. Without this requirement, the number of $\mathbb{Z}_S$-equivalence classes remains finite, but we are no longer able to give an explicit upper bound for their number.

We mention that every pair of binary forms $F, G \in \mathbb{Z}_S[X,Y]$ satisfying (3.1) can be derived from a pair (F_0, G_0) of binary forms in $\mathbb{Z}_S[X,Y]$ satisfying (3.1) of which F_0 is $\mathbb{Z}_S$-minimal. Indeed, suppose that F, G are binary forms in $\mathbb{Z}_S[X,Y]$ satisfying (3.1) and that F is not $\mathbb{Z}_S$-minimal. Then $F = (F_1)_{A_1}$, where F_1 is a binary form in $\mathbb{Z}_S[X,Y]$ and $A_1 \in \mathrm{NS}_2(\mathbb{Z}_S) \setminus \mathrm{GL}_2(\mathbb{Z}_S)$. If F_1 is not $\mathbb{Z}_S$-minimal we have $F_1 = (F_2)_{A_2}$, where $F_2 \in \mathbb{Z}_S[X,Y]$ and $A_2 \in \mathrm{NS}_2(\mathbb{Z}_S) \setminus \mathrm{GL}_2(\mathbb{Z}_S)$, etc. In each step of this process, we obtain a binary form whose discriminant is a proper divisor of the discriminant of its predecessor. So after finitely many steps we find a $\mathbb{Z}_S$-minimal form, $F_0 \in \mathbb{Z}_S[X,Y]$, say, such that $F = (F_0)_A$ for some $A \in \mathrm{NS}_2(\mathbb{Z}_S) \setminus \mathrm{GL}_2(\mathbb{Z}_S)$. Now take $G_0 := G_{(\det A)A^{-1}}$. Then $F_0, G_0 \in \mathbb{Z}_S[X,Y]$, F_0 is $\mathbb{Z}_S$-minimal, and by (1.2), $R(F_0, G_0) = R(F,G) \in c\mathbb{Z}_S^*$.

Theorem 3.2 below gives an explicit upper bound for the number of $\mathbb{Z}_S$-equivalence classes of pairs (F_0, G_0). In order to estimate explicitly the number of $\mathbb{Z}_S$-equivalence classes of pairs (F, G), we would need more precise information about the matrix A, but this is not provided by our method of proof.

The arithmetic function $\tau_\alpha(d)$ is defined by (2.7). Now our quantitative result, with the requirement that F be $\mathbb{Z}_S$-minimal, reads as follows:

Theorem 3.2. [3] *Assume that $m \geqslant 3$, $n \geqslant 3$. Then the set of pairs of binary forms $F, G \in \mathbb{Z}_S[X,Y]$ such that*

$$R(F,G) \in c\mathbb{Z}_S^* \tag{3.1}$$

for which

F is associated with $K_1, \ldots, K_r$, G is associated with $L_1, \ldots, L_s$,
F, G have non-zero discriminants,
F is $\mathbb{Z}_S$-minimal,

is contained in the union of at most

$$e^{10^{24}mn(m+n)(t+1)} \cdot 2^{\omega(c)}\tau_{mn+2}(c)$$

$\mathbb{Z}_S$-equivalence classes.

If we drop the requirement that F be $\mathbb{Z}_S$-minimal, we can only prove a 'semi-effective' upper bound for the number of $\mathbb{Z}_S$-equivalence classes.

Theorem 3.3. [3] *Let $m \geqslant 3$, $n \geqslant 3$. Then the number of $\mathbb{Z}_S$-equivalence classes of pairs of binary forms $(F,G) \in \mathbb{Z}_S[X,Y]$ satisfying all conditions of Theorem 3.2 except for the $\mathbb{Z}_S$-minimality of F, is at most*

$$O\big(c^{\frac{1}{mn}+\delta}\big) \quad \text{as } c \to \infty$$

for every $\delta > 0$, where the implied constant depends on S, $K_1, \ldots, K_r$, $L_1, \ldots, L_s$ and δ and cannot be computed effectively from our method of proof.

The following example shows that the upper bound in Theorem 3.3 cannot be improved to $O(c^\kappa)$ as $c \to \infty$ for any $\kappa < \frac{1}{mn}$. Fix two binary forms $F, G \in \mathbb{Z}[X,Y]$ of degrees m, n, respectively, such that F, G have non-zero discriminant and $R(F,G) =: r \neq 0$. Let p be a large prime number. Then the pairs of binary forms (F_b, G_b) given by $F_b(X,Y) = F(pX - bY, Y)$,

$G_b(X,Y) = G(pX - bY, Y)$ $(b = 0, \dots, p-1)$ are pairwise $\mathbb{Z}$-inequivalent. By (1.2), the resultant of F_b, G_b is rp^{mn}. Hence, letting $p \to \infty$ and putting $c = |r|p^{mn}$, we have an infinite sequence of integers c, such that pairs of binary forms (F, G) satisfying the conditions of Theorem 3.3 lie in $\gg c^{\frac{1}{mn}}$ $\mathbb{Z}$-equivalence classes.

We deduce a consequence for Thue-Mahler equations

$$F(x,y) \in c\mathbb{Z}_S^* \quad \text{in } x, y \in \mathbb{Z}_S \text{ with } \gcd(x,y) = 1. \tag{3.2}$$

Two solutions $(x_1, y_1), (x_2, y_2)$ of (3.2) are called proportional if $(x_2, y_2) = \varepsilon(x_1, y_1)$ for some $\varepsilon \in \mathbb{Z}_S^*$. Evertse and Győry [11] proved that for every number field L there are only finitely many $\mathbb{Z}_S$-equivalence classes of binary forms $F \in \mathbb{Z}_S[X,Y]$ such that F splits into linear factors over L and (3.2) has at least three pairwise non-proportional solutions. We have the following quantitative result:

Corollary 3.4. [3] *Let $K_1, \dots, K_r$ be a sequence of number fields with $\sum_{i=1}^{r}[K_i : \mathbb{Q}] =: m \geqslant 3$ and c a positive integer coprime with the primes in S. Then the set of binary forms $F \in \mathbb{Z}_S[X,Y]$ such that*

F is associated with $K_1, \dots, K_u$, F has non-zero discriminant,
F is $\mathbb{Z}_S$-minimal,

and such that (3.2) has at least three pairwise non-proportional solutions,

is contained in the union of at most

$$e^{3\times 10^{24} m(m+3)(t+1)} \cdot 2^{\omega(c)} \tau_{3m+2}(c^3)$$

$\mathbb{Z}_S$-equivalence classes.

This can be deduced from Theorem 3.2 as follows. Let $F \in \mathbb{Z}_S[X,Y]$ be a binary form satisfying the conditions of Corollary 3.4. Then (3.2) has three pairwise non-proportional solutions, (x_j, y_j) $(j = 1, 2, 3)$, say. Define the binary form

$$G(X,Y) := \prod_{j=1}^{3}(y_j X - x_j Y).$$

Then

$$R(F,G)=\prod_{j=1}^{3}F(x_j,y_j)\in c^3\mathbb{Z}_S^*\,.$$

Now Corollary 3.4 follows at once by applying Theorem 3.2 with $n=3$, $(L_1,\dots,L_s)=(\mathbb{Q},\mathbb{Q},\mathbb{Q})$ and with c^3 instead of c. $\square$

At present, we have finiteness results for (3.1) only in the case that one of the binary forms F,G is fixed, or in the case that F,G are both allowed to vary, but both F,G split into linear factors over a prescribed number field. An intermediate case is, when both F,G are allowed to vary but only one of them is assumed to split over a given number field. Consider binary forms $F,G\in\mathbb{Z}_S[X,Y]$ satisfying (3.1) of degrees m,n, respectively, where $n\geqslant m$. The identity $R(F,G+HF)=R(F,G)$ for any binary form $H\in\mathbb{Z}_S[X,Y]$ of degree $n-m$ shows that we cannot prove finiteness for the number of $\mathbb{Z}_S$-equivalence classes if we do not fix a splitting field for the binary form with the larger degree. On the other hand, it is an open problem whether or not the number of $\mathbb{Z}_S$-equivalence classes is finite if we fix a splitting field for the binary form with the larger degree, but not for the form with the smaller degree.

More precisely, we suggest the following.

Problem. *Does there exist a function $c(m)$ depending only on m for which the following holds? Let L be a number field and m,n integers with $m\geqslant 3$ and $n\geqslant c(m)$. Then there are only finitely many $\mathbb{Z}_S$-equivalence classes of pairs of binary forms $F,G\in\mathbb{Z}_S[X,Y]$ satisfying (3.1) such that* $\deg F=m$, $\deg G=n$, *F,G have non-zero discriminants, G factors into linear forms in $L[X,Y]$ and no further condition is imposed on F.*

If the answer to this problem is affirmative, then by a similar argument as in the proof of Corollary 3.4 it will follow that up to $\mathbb{Z}_S$-equivalence there are only finitely many binary forms $F\in\mathbb{Z}_S[X,Y]$ of degree $m\geqslant 3$ and non-zero discriminant such that Eq. (3.2) has more than $c(m)$ pairwise non-proportional solutions. The latter has been proved in the special case $S=\emptyset$ with $c(m)=29m$ for $m<400$ [24] and $c(m)=6m$ for $m\geqslant 400$ [13], but for $S\neq\emptyset$ it is still open; it can be compared with Conjecture 1 in [11].

We briefly sketch the proofs of Theorems 3.1, 3.2 and 3.3.

We start with Theorem 3.1. The basic tool in the proof is the following result.

Theorem 3.5. [3] *Let* $\mathbb{K}$ *be a field of characteristic* 0 *and let* m, n *be integers with* $m \geqslant 2$, $n \geqslant 2$, $m+n \geqslant 5$. *For* $i = 1, \dots, m$, $j = 1, \dots, n$, *let* Γ_{ij} *be a subgroup of* $\mathbb{K}^*$ *of rank at most* ρ. *If* $(x_1, \dots, x_m, y_1, \dots, y_n)$ *runs through the tuples in* $\mathbb{K}^{m+n}$ *for which*

$$x_i - y_j \in \Gamma_{ij} \quad \textit{for } 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n,$$

$$x_1, \dots, x_m,\ y_1, \dots, y_n \textit{ are pairwise distinct,}$$

then the set of mn*-tuples* $\left(\frac{x_i - y_j}{x_1 - y_1} : i = 1, \dots, m,\ j = 1, \dots, n\right)$ *runs through a set of cardinality at most*

$$3 \times 2^{24(\rho+1)(m+n-4)} e^{18^9(4\rho+1)}.$$

The proof of Theorem 3.6 uses the following result of Evertse, Schlickewei and Schmidt [17]: if $N \geqslant 3$ and if Γ is a subgroup of $(\mathbb{K}^*)^N$ of finite rank ρ, then the equation

$$x_1 + \cdots + x_N = 1 \quad \text{in } (x_1, \dots, x_N) \in \Gamma \tag{3.3}$$

has at most $e^{(6N)^{3N}(N\rho+1)}$ non-degenerate solutions, i.e, with $\sum_{i \in I} x_i \neq 0$ for each non-empty subset I of $\{1, \dots, N\}$. We prove Theorem 3.5 by applying this result to the identities

$$\frac{x_i - y_1}{x_1 - y_1} - \frac{x_i - y_j}{x_1 - y_1} + \frac{x_1 - y_j}{x_1 - y_1} = 1.$$

□

Denote by $\sigma_{i1}, \dots, \sigma_{i,m_i}$ the isomorphic embeddings of K_i into $\mathbb{C}$ for $i = 1, \dots, r$ and by $\tau_{j1}, \dots, \tau_{j,n_j}$ the isomorphic embeddings of L_j into $\mathbb{C}$ for $j = 1, \dots, s$. Let $K_1, \dots, K_m$ be the fields $\sigma_{ik}(K_i)$ $(i = 1, \dots, r,\ k = 1, \dots, m_i)$ in some order, and $L_1, \dots, L_n$ the fields $\tau_{jl}(L_j)$ $(j = 1, \dots, s,\ l = 1, \dots, n_j)$ in some order.

Let $F, G \in \mathbb{Z}_S[X,Y]$ be two monic binary forms satisfying the conditions of Theorem 3.1. Then we can express F, G as

$$F(X,Y) = \prod_{i=1}^{m}(X - \beta_i Y), \quad G(X,Y) = \prod_{j=1}^{n}(X - \delta_j Y),$$

with $\beta_i \in K_i$ integral over $\mathbb{Z}_S$ for $i = 1, \dots, m$, and $\delta_j \in L_j$ integral over $\mathbb{Z}_S$ for $j = 1, \dots, n$. With these expressions, (3.1) becomes

$$\prod_{i=1}^{m}\prod_{j=1}^{n}(\delta_j - \beta_i) \in c\mathbb{Z}_S^*. \tag{3.4}$$

Let T be the set consisting of the primes in S and of the primes dividing c. Then $\delta_j - \beta_i \in \Gamma_{ij}$, where Γ_{ij} is the unit group of the integral closure of $\mathbb{Z}_T$ in the compositum $K_i L_j$. This group Γ_{ij} has rank at most $mn(t+\omega(c)+1)-1$. Now applying Theorem 3.5 to the tuples $(\beta_1, \dots, \beta_m, \delta_1, \dots, \delta_n)$, Theorem 3.1 follows. $\square$

The proof of Theorem 3.2 is rather different. Our main tool is the following result.

Theorem 3.6. [3] *Let $\mathbb{K}$ be a field of characteristic 0. For $i, j = 1, 2$, let Γ_{ij} be a subgroup of $\mathbb{K}^*$ of rank ρ. Then the equation*

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & x_{11} & x_{12} \\ 1 & x_{21} & x_{22} \end{vmatrix} = 0 \quad \textit{in } x_{ij} \in \Gamma_{ij} \textit{ for } i, j = 1, 2 \tag{3.5}$$

has at most $e^{30^{15}(4\rho+2)}$ solutions such that each 2×2-subdeterminant of the left-hand side of (3.5) is $\neq 0$.

The proof of Theorem 3.6 uses the result of Evertse, Schlickewei and Schmidt concerning equation (3.3). Following Evertse, Győry, Stewart and Tijdeman [16], one expands the determinant, considers all partitions of this expansion into minimal vanishing subsums, and applies the result on (3.3) to each of the subsums, see also [1] for a similar computation.

The proof of Theorem 3.2 has a similar structure as that of the results on discriminants in Section 2. Let $F, G \in \mathbb{Z}_S[X,Y]$ be two binary forms satisfying the conditions of Theorem 3.2. We may assume without loss of generality that $F(1,0)$ and $G(1,0)$ are distinct from 0. We can express F, G as

$$F(X,Y) = a_0 \prod_{k=1}^{m} (X - \alpha_k Y), \quad G(X,Y) = b_0 \prod_{l=1}^{n} (X - \beta_l Y).$$

Define the quantities

$$\Theta_{ijkl}(F,G) := \frac{(\alpha_i - \beta_k)(\alpha_j - \beta_l)}{(\alpha_i - \beta_l)(\alpha_j - \beta_k)} \quad (1 \leqslant i,j \leqslant m,\ 1 \leqslant k,l \leqslant n)$$

and let $\Theta(F,G)$ be the tuple consisting of all Θ_{ijkl} $(i,j = 1,\ldots,m,\ k,l = 1,\ldots,n)$. Now for any triples (i,j,g) from $\{1,\ldots,m\}$ and (k,l,h) from $\{1,\ldots,n\}$ one has

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & \Theta_{ijkl}(F,G) & \Theta_{ijhl}(F,G) \\ 1 & \Theta_{gjkl}(F,G) & \Theta_{gjhl}(F,G) \end{vmatrix} = 0$$

and moreover, each 2×2-subdeterminant of the left-hand side is non-zero. Using (3.1) one shows that each $\Theta_{ijkl}(F,G)$ belongs to a finitely generated multiplicative group independent of F, G with rank bounded above in terms of $m, n, t, \omega(c)$. So by applying Theorem 3.6 one obtains that if F, G runs through all pairs of binary forms in $\mathbb{Z}_S[X,Y]$ satisfying the conditions of Theorem 3.2, then $\Theta(F,G)$ runs through a finite set of cardinality bounded above in terms of m, n, t and $\omega(c)$.

Now one can show that any two pairs (F_1, G_1), (F_2, G_2) in $\mathbb{Z}_S[X,Y]$ satisfying the conditions of Theorem 3.2 and for which $\Theta(F_1,G_1) = \Theta(F_2,G_2)$, are $\mathbb{Q}$-equivalent, i.e., $F_2 = \lambda(F_1)_U$, $G_2 = \mu(G_1)_U$ for some $\lambda, \mu \in \mathbb{Q}^*$ and $U \in \mathrm{GL}_2(\mathbb{Q})$. Thus, one obtains an upper bound for the number of $\mathbb{Q}$-equivalence classes. By means of an elementary argument one estimates the number of $\mathbb{Z}_S$-equivalence classes contained in a $\mathbb{Q}$-equivalence class. In this way the proof of Theorem 3.2 is completed. $\square$

We now sketch the proof of Theorem 3.3. We use that every non-zero $a \in \mathbb{Z}_S$ can be expressed uniquely as $a = \varepsilon \cdot |a|_S$, where ε is a rational number composed of primes in S, and $|a|_S$ a positive integer composed of primes outside S. Given a binary form $F(X,Y)=\sum_{i=0}^{m} a_i X^{m-i}Y^i \in \mathbb{Z}_S[X,Y]$ we define $[F]_S :=\gcd(|a_0|_S,\dots,|a_m|_S)$.

Recall that for every pair of binary forms (F,G) in $\mathbb{Z}_S[X,Y]$ satisfying (3.1) there is a pair of binary forms (F_0,G_0) in $\mathbb{Z}_S[X,Y]$ such that $R(F_0,G_0)\in c\mathbb{Z}_S^*$, F_0 is $\mathbb{Z}_S$-minimal and $F=(F_0)_A$, $G_0=G_{(\det A)A^{-1}}$ for some matrix $A\in \mathrm{NS}_2(\mathbb{Z}_S)$. By Theorem 3.2, the pairs (F_0,G_0) lie in at most $O(c^{\delta})$ $\mathbb{Z}_S$-equivalence classes for any $\delta>0$. By an elementary argument one can show that for any given binary form $G_0\in\mathbb{Z}_S[X,Y]$, the set of binary forms $G\in\mathbb{Z}_S[X,Y]$ for which there exists $A\in\mathrm{NS}_2(\mathbb{Z}_S)$ such that $G_0=G_{(\det A)A^{-1}}$ is contained in the union of at most $O([G_0]_S^{1/n}|D(G_0)|_S^{\delta})$ $\mathbb{Z}_S$-equivalence classes for any $\delta>0$. By (1.2), $[G_0]_S^m$ is a divisor of c. Further, $|D(G_0)|_S$ can be estimated from above using the following inequality by Evertse and Győry [14]:

$$|R(F_0,G_0)|_S \gg \left(|D(F_0)|_S^{\frac{n}{m-1}}|D(G_0)|_S^{\frac{m}{n-1}}\right)^{\frac{1}{17}-\delta}$$

for every $\delta>0$, where the constant implied by $\gg$ depends on S, $K_1,\dots,K_r$, $L_1,\dots,L_s$, δ, and is not effectively computable from the method of proof. This implies that $|D(G_0)|_S\ll c^{17n/m}$ if we take δ sufficiently small. By combining this with the other facts mentioned above, Theorem 3.3 easily follows. □

Remark. As a common generalization of the discriminant equation (2.1) and the resultant equation (3.1), Győry [20], [22] studied the so-called semi-resultant equation. He obtained some finiteness results for this equation, partly in quantitative form. We note that with the arguments sketched in the present paper it is possible to obtain quantitative finiteness results for semi-resultant equations extending those of Győry.

References

[1] A. Bérczes, On the number of solutions of index form equations, *Publ. Math. Debrecen*, **2000**, 251–262.

[2] A. Bérczes, J.-H. Evertse, K. Győry, On the number of equivalence classes of binary forms of given degree and given discriminant, *Acta Arith.* **113** (2004), 363–399.

[3] A. Bérczes, J.-H. Evertse, K. Győry, On the number of pairs of binary forms with given degree and given resultant, *submitted for publication.*

[4] A. Bérczes, K. Győry, On the number of solutions of decomposable polynomial equations, *Acta Arith.* **101** (2002), 171–187.

[5] F. Beukers, H.P. Schlickewei, The equation $x + y = 1$ in finitely generated groups, *Acta Arith.*, **78** (1996), 189–199.

[6] B.J. Birch, J.R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc. (3)*, **24** (1972), 385–394.

[7] B.N. Delone, D.K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10, American Mathematical Society, Providence, R.I., 1964.

[8] J.-H. Evertse, The number of solutions of decomposable form equations, *Invent. Math.* **122** (1995), 559–601.

[9] J.-H. Evertse, K. Győry, On unit equations and decomposable form equations, *J. reine angew. Math.*, **358** (1985), 6–19.

[10] J.-H. Evertse, K. Győry, On the number of polynomials and integral elements of given discriminant, *Acta Math. Hungar.* **51** (1988), 341–362.

[11] J.-H. Evertse, K. Győry, Thue-Mahler equations with a small number of solutions, *J. reine angew. Math.* **399** (1989), 60–80.

[12] J.-H. Evertse, K. Győry, Effective finiteness results for binary forms with given discriminant, *Compositio Math.*, **79** (1991), 169–204.

[13] J.-H. Evertse, K. Győry, Thue inequalities with a small number of solutions, *The mathematical heritage of C.F. Gauss, G.M. Rassias, ed.*, World Scientific Publ. Co., Singapore, 1991, 204–224.

[14] J.-H. Evertse, K. Győry, Lower bounds for resultants I, *Compositio Math.*, **88** (1993), 1–23.

[15] J.-H. Evertse, K. Győry, The number of families of solutions of decomposable form equations, *Acta Arith.* **80** (1997), 367–394.

[16] J.-H. Evertse, K. Győry, C.L. Stewart, R. Tijdeman, On S-unit equations in two unknowns, *Invent. Math.* **92** (1988), 461–477.

[17] J.-H. Evertse, H.P. Schlickewei, W.M. Schmidt, Linear equations in variables which lie in a multiplicative group, *Annals of Math.* **155** (2002), 807-836.

[18] M. Fujiwara, On some applications of W.M. Schmidt's theorem, *Michigan Math. J.* **19** (1972), 315–319.

[19] K. Győry, Sur les polynômes à coefficients entiers et de dicriminant donné I,II,III,IV,V, *Acta Arith.* **23** (1973), 419–426; *Publ. Math. Debrecen* **21** (1974), 125–144; ibid. **23** (1976), 141–165; ibid. **25** (1978), 155–167; *Acta Math. Acad. Sci. Hung.*, **32** (1978), 175–190.

[20] K. Győry, On the number of pairs of polynomials with given resultant or given semi-resultant, *Acta Sci. Math.,* **57** (1993), 519–529.

[21] K. Győry, Some applications of decomposable form equations to resultant equations, *Colloq. Math.* **65** (1993), 267–275.

[22] K. Győry, On pairs of binary forms with given resultant or given semi-resultant, *Math. Pannonica* **4** (1993), 169–180.

[23] K. Győry, On the irreducibility of neighbouring polynomials, *Acta Arith.* **67** (1994), 283–294.

[24] K. Győry, Thue inequalities with a small number of primitive solutions, *Period. Math. Hung.* **42** (2001), 199–209.

[25] J. Nakagawa, Binary forms and orders of algebraic number fields, *Invent. Math.*, **97** (1989), 219–235.

[26] M. Ru, P.M. Wong, Integral points of $\mathbb{P}^n \setminus \{2n+1$ hyperplanes in general position$\}$, *Invent. Math.* **106** (1991), 195–216.

[27] W.M. Schmidt, Inequalities for resultants and for decomposable forms, *Diophantine Approximation and its Applications, Proc. Conf. Washington DC., 1972, C.F. Osgood, ed., Academic Press, 1972*, 235–253.

[28] D. Simon, The index of nonmonic polynomials, *Indag. Math. (N.S.)*, **12** (2001), 505–517.

[29] B.L. van der Waerden, Algebra I, 8. Auflage. *Springer Verlag*, Berlin, 1971.

A. Bérczes
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: berczesa@math.klte.hu

J.-H. Evertse
Universiteit Leiden, Mathematisch Instituut,
Postbus 9512, 2300 RA Leiden, The Netherlands

E-mail address: evertse@math.leidenuniv.nl

K. Győry
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: gyory@math.klte.hu