ACTA ARITHMETICA
128.1 (2007)

On the number of pairs of binary forms with given degree and given resultant

by

Attila Bérczes (Debrecen), Jan-Hendrik Evertse (Leiden)
and Kálmán Győry (Debrecen)

1. Introduction. Let us denote by $R(F,G)$ the resultant of two binary forms F, G. Let $S = \{p_1, \dots, p_t\}$ be a finite, possibly empty set of primes. The ring of S-integers and group of S-units are defined by

$$\mathbb{Z}_S = \mathbb{Z}[(p_1 \cdots p_t)^{-1}], \quad \mathbb{Z}_S^* = \{\pm p_1^{w_1} \cdots p_t^{w_t} : w_1, \dots, w_t \in \mathbb{Z}\},$$

respectively, where $\mathbb{Z}_S = \mathbb{Z}$, $\mathbb{Z}_S^* = \{\pm 1\}$ if $S = \emptyset$. We deal with the so-called *resultant equation*

$$R(F,G) \in c\mathbb{Z}_S^* \tag{1.1}$$

to be solved in binary forms $F, G \in \mathbb{Z}_S[X,Y]$, where c is a positive integer. It turns out that the set of pairs (F,G) satisfying this equation can be divided into equivalence classes, where two pairs of binary forms (F_1,G_1), (F_2,G_2) are said to be equivalent if there are $\varepsilon, \eta \in \mathbb{Z}_S^*$ and a matrix $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_S)$ such that $F_2(X,Y) = \varepsilon F_1(aX+bY, cX+dY)$, $G_2(X,Y) = \eta G_1(aX+bY, cX+dY)$.

First Győry [10], [11] for monic binary forms F, G (i.e., with $F(1,0) = G(1,0) = 1$), and later Evertse and Győry [7] for arbitrary binary forms F, G, proved results which imply that there are only finitely many equivalence classes of pairs of binary forms $F, G \in \mathbb{Z}_S[X,Y]$ that satisfy (1.1) and certain additional conditions. In [11], Győry established his results on monic binary forms in a quantitative form, giving explicit upper bounds for the number of equivalence classes, while the results for arbitrary binary forms from [7] were established only in a qualitative form. In the present paper, we improve

2000 *Mathematics Subject Classification*: 11D57, 11D72.
Key words and phrases: resultant, binary forms, polynomials.
The research was supported in part by the Hungarian Academy of Sciences (A.B., K.G.), and by grants T42985 (A.B., K.G.), and T48791 (A.B.) of the Hungarian National Foundation for Scientific Research.

the quantitative results from [11], and prove quantitative versions of the finiteness results from [7].

In a simplified form, one of our results (Theorem 2.3 below) can be stated as follows. Let $m \geq 3$, $n \geq 3$ be integers and L a number field. Then the set of pairs of binary forms (F, G) in $\mathbb{Z}_S[X, Y]$ satisfying (1.1) such that F has degree m, G has degree n, F, G do not have multiple factors and F, G split into linear factors in $L[X, Y]$ is contained in the union of $O(c^{(1/mn)+\delta})$ equivalence classes as $c \to \infty$ for every $\delta > 0$. Here, the implied constant depends on L, m, n, S, δ and cannot be computed effectively from our method of proof. It is shown that the exponent on c cannot be improved to something smaller than $1/mn$.

On the other hand, if we restrict ourselves to monic binary forms F, G, we can derive an upper bound for the number of equivalence classes which is completely explicit in terms of m, n, t and c (see Theorem 2.1 below). We derive a similar such explicit bound for binary forms F, G that are not necessarily monic, but there we have to impose a suitable minimality condition on one of F, G. We explain that without this condition it probably becomes very difficult to obtain a fully explicit upper bound for the number of equivalence classes. As a corollary of our Theorem 2.2, we give a quantitative version of a result by Evertse and Győry [6] on Thue–Mahler equations (Corollary 2.4 below).

In Section 2 we state Theorems 2.1–2.3 and Corollary 2.4. Theorem 2.1 will be proved in Sections 3, 4 and Theorem 2.2 in Sections 5–8. The main tools are explicit upper bounds from [4] and [9] for the number of solutions of linear equations with unknowns from a multiplicative group. The latter is a consequence of the quantitative subspace theorem. In our arguments we use ideas from [8], [7] and [2]. Theorem 2.3 is proved in Section 9. Here the hard core is an inequality from [7] relating the resultant of two binary forms to the discriminants of these forms. This inequality is a consequence of the qualitative subspace theorem.

2. Results. We introduce some terminology. The resultant of two binary forms

$$F = a_0X^m + a_1X^{m-1}Y + \cdots + a_mY^m = \prod_{k=1}^{m}(\alpha_kX - \beta_kY),$$

$$G = b_0X^n + b_1X^{n-1}Y + \cdots + b_nY^n = \prod_{l=1}^{n}(\gamma_lX - \delta_lY)$$

is given by

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

From the well-known expression for $R(F,G)$ as a determinant (see [13, §34]) we infer 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 $n=\deg G$ in $a_0,\dots,a_m$ and homogeneous of degree $m=\deg F$ in $b_0,\dots,b_n$. Further, for any scalars λ, μ and any matrix $A=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ we have

$$R(\lambda F_A,\mu G_A)=\lambda^n\mu^m(\det A)^{mn}R(F,G), \tag{2.1}$$

where for a binary form F we define F_A by

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

For a domain Ω, we denote by $\mathrm{NS}_2(\Omega)$ the set of 2×2-matrices with entries in Ω and non-zero determinant, and by $\mathrm{GL}_2(\Omega)$ the group of 2×2-matrices with entries in Ω and determinant in the unit group Ω^*. Two binary forms $F_1,F_2\in\Omega[X,Y]$ are called *Ω-equivalent* if there are $\varepsilon\in\Omega^*$, $U\in\mathrm{GL}_2(\Omega)$ such that $F_2=\varepsilon(F_1)_U$. Two pairs of binary forms (F_1,G_1), (F_2,G_2) are called *Ω-equivalent* if there are $\varepsilon,\eta\in\Omega^*$, $U\in\mathrm{GL}_2(\Omega)$ such that $F_2=\varepsilon(F_1)_U$, $G_2=\eta(G_1)_U$. A binary form F with $F(1,0)=1$ is called *monic*. Two pairs of monic binary forms (F_1,G_1), (F_2,G_2) in $\Omega[X,Y]$ are called *strongly Ω-equivalent* if $F_2(X,Y)=F_1(X+bY,\varepsilon Y)$, $G_2(X,Y)=G_1(X+bY,\varepsilon Y)$ for some $b\in\Omega$, $\varepsilon\in\Omega^*$.

We return to the resultant equation (1.1). Let $S=\{p_1,\dots,p_t\}$ be a finite, possibly empty set of primes. Without loss of generality we may assume that the number c in (1.1) is a positive integer which is coprime to $p_1\cdots p_t$ if $S\neq\emptyset$. Clearly, if (F,G) is a pair of binary forms with (1.1), then by (2.1) every pair $\mathbb{Z}_S$-equivalent to (F,G) also satisfies (1.1). Therefore, the set of solutions of (1.1) decomposes into Z_S-equivalence classes. Likewise, the set of pairs of monic binary forms $F,G\in\mathbb{Z}_S[X,Y]$ with (1.1) decomposes into strong $\mathbb{Z}_S$-equivalence classes.

There were some earlier finiteness results on (1.1) in which one of the binary forms F,G was kept fixed, but Győry was the first to obtain results on (1.1) in which both F,G are allowed to vary. He proved [10, Theorem 7] the following result for monic binary forms. Let L be a given number field, and m,n integers with $m\geq 2$, $n\geq 2$, $m+n\geq 5$. 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 (1.1) such that $\deg F=m$, $\deg G=n$, F,G have no multiple factors and $F\cdot G$ has splitting field L (i.e., L is the smallest number field over which $F\cdot G$ splits into linear factors). Further, in [11], Győry obtained explicit upper bounds for both $\deg F+\deg G$ and the number of strong equivalence classes. In fact, by combining Győry's arguments from [11] with the explicit upper bound for the number of non-degenerate solutions of S-unit equations from [5, Theorem 3], one can show that the pairs of monic binary forms (F,G) with the properties given above lie in at most

$$\{2(m+n+1)^4 2^{1050[L:\mathbb{Q}](t+\omega(c)+1)}\}^{m+n-2} \tag{2.2}$$

strong $\mathbb{Z}_S$-equivalence classes, where $\omega(c)$ is the number of distinct primes dividing c. Note that $1 \le [L:\mathbb{Q}] \le m!n!$ ([1]).

Evertse and Győry [7, Corollary 1] extended Győry's qualitative result to binary forms which are not necessarily monic. Under the slightly stronger hypothesis $m \ge 3$, $n \ge 3$, they proved that there are only finitely many $\mathbb{Z}_S$-equivalence classes of pairs of binary forms F, G satisfying (1.1) such that $\deg F = m$, $\deg G = n$, F, G have no multiple factors and $F \cdot G$ has splitting field L. Further, they showed that $\deg F + \deg G$ is bounded above in terms of S, L and c. We mention that both Győry for monic binary forms and Evertse and Győry for not necessarily monic binary forms proved more general results for binary forms with coefficients in the ring of S-integers of a number field ([2]). For a generalization to binary forms with given semi-resultant, see Győry [12].

Győry [11] and Evertse and Győry [7] also showed that their finiteness results do not remain valid if the conditions on m, n are relaxed, or if neither F nor G is required to split into linear factors over a prescribed number field. It is not known whether the finiteness results can be extended to the case that only one of F, G is required to split over a given number field; see [3] for a discussion on this. Probably the condition that F, G have no multiple factors can be removed if we assume that F, G have sufficiently many distinct factors in $\mathbb{C}[X,Y]$ (see [11] in the monic case).

Below we give precise quantitative versions of our results mentioned above. In contrast to the above discussion, we do not deal with binary forms F, G such that $F \cdot G$ has a given splitting field but instead with binary forms associated with certain given number fields. We say that a binary form $F \in \mathbb{Q}[X,Y]$ is *associated* with a number field K if F is irreducible in $\mathbb{Q}[X,Y]$ and if there is θ such that $F(\theta,1) = 0$ and $K = \mathbb{Q}(\theta)$. We agree that the binary forms aY ($a \in \mathbb{Q}^*$) are associated with $\mathbb{Q}$. A binary form $F \in \mathbb{Q}[X,Y]$ is said to be *associated* with the sequence of number fields $K_1, \dots, K_u$ if it can be factored as $\prod_{i=1}^{u} F_i$ where $F_i \in \mathbb{Q}[X,Y]$ is an irreducible binary form associated with K_i, for $i = 1, \dots, u$. It is easy to check that a binary form F associated with $K_1, \dots, K_u$ has degree $\sum_{i=1}^{u} [K_i : \mathbb{Q}]$.

For a non-zero integer d, we denote by $\omega(d)$ the number of distinct primes dividing d, and by $\mathrm{ord}_p(d)$ the exponent of the prime number p in the prime factorization of d.

([1]) The results in [10], [11] were formulated in terms of monic polynomials instead of monic binary forms. The formulation in terms of monic binary forms fits more conveniently into the present paper.

([2]) In the monic case, the results of [10], [11] were established in the even more general situation when the ground ring is an integrally closed and finitely generated domain over $\mathbb{Z}$.

Our first theorem gives a quantitative result on (1.1) for monic binary forms which is better than (2.2) if the degrees of the number fields with which F, G are associated are not too small.

THEOREM 2.1. *Let m, n be integers with $m \geq 2$, $n \geq 2$, $m + n \geq 5$ and $K_1, \ldots, K_u$, $L_1, \ldots, L_v$ number fields with*

$$\sum_{i=1}^{u} [K_i : \mathbb{Q}] = m, \qquad \sum_{i=1}^{v} [L_i : \mathbb{Q}] = n.$$

Further, let $S = \{p_1, \ldots, p_t\}$ be a finite, possibly empty set of primes and c a positive integer, coprime to $p_1 \cdots p_t$ if $S \neq \emptyset$. Then the set of pairs of monic binary forms $F, G \in \mathbb{Z}_S[X, Y]$ with

$$R(F, G) \in c\mathbb{Z}_S^* \tag{1.1}$$

for which

- *F is associated with $K_1, \ldots, K_u$, G is associated with $L_1, \ldots, L_v$,*
- *F, G do not have multiple factors*

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.

Clearly, our bound can be replaced by $e^{18(m+n)mn(t+\omega(c)+1)}$ if $m + n$ is sufficiently large. We note that from Theorem 2.2 below one can derive a result similar to Theorem 2.1 but with a larger bound.

In Theorem 2.2, we give an explicit upper bound for the number of equivalence classes for not necessarily monic binary forms, but instead we have to assume that one of the binary forms satisfies a certain minimality condition. More precisely, a binary form $F \in \mathbb{Z}_S[X, Y]$ is called *$\mathbb{Z}_S$-minimal* if there are no binary form $G \in \mathbb{Z}_S[X, Y]$ and matrix $A \in \mathrm{NS}_2(\mathbb{Z}_S) \backslash \mathrm{GL}_2(\mathbb{Z}_S)$ such that $F = G_A$.

THEOREM 2.2. *Let m, n be integers with $m \geq 3$, $n \geq 3$. Further, let $K_1, \ldots, K_u$, $L_1, \ldots, L_v$, S and c be as in Theorem* 2.1. *Then the set of pairs of binary forms $F, G \in \mathbb{Z}_S[X, Y]$ satisfying* (1.1) *for which*

- *F is associated with $K_1, \ldots, K_u$, G is associated with $L_1, \ldots, L_v$,*
- *F, G do not have multiple factors,*
- *F is $\mathbb{Z}_S$-minimal*

is contained in the union of at most

$$e^{10^{24}(m+n)mn(t+1)}\psi(c)$$

$\mathbb{Z}_S$-equivalence classes, where

$$\psi(c) := 2^{\omega(c)} \prod_{p|c} \binom{\mathrm{ord}_p(c) + mn + 2}{mn + 2}.$$

Using the arguments of the proof of Theorem 2.2 we could have given also an explicit upper bound for $\deg F + \deg G$. We will not work this out in the present paper.

If in Theorem 2.2 we drop the condition that F be $\mathbb{Z}_S$-minimal, the number of $\mathbb{Z}_S$-equivalence classes remains finite, but we are no longer able to give an explicit upper bound for it. In fact, we believe that to give an explicit upper bound for the number of equivalence classes without the minimality constraint is a difficult problem, and at the end of this section we give an example to illustrate this. We only managed to prove the following asymptotic result.

THEOREM 2.3. *Let again m, n be integers with $m \geq 3$, $n \geq 3$, and let $K_1, \ldots, K_u$, $L_1, \ldots, L_v$, S and c be as in Theorem* 2.1. *Then the number of $\mathbb{Z}_S$-equivalence classes of pairs of binary forms $F, G \in \mathbb{Z}_S[X, Y]$ which satisfy* (1.1) *and for which*

- *F is associated with $K_1, \ldots, K_u$, G is associated with $L_1, \ldots, L_v$,*
- *F, G do not have multiple factors*

is, for every $\delta > 0$, at most $O(c^{(1/mn)+\delta})$ as $c \to \infty$, where the implied constant depends on $K_1, \ldots, K_u$, $L_1, \ldots, L_v$, m, n, S and δ. This constant cannot be computed effectively from our method of proof.

The following example shows that the exponent of c cannot be replaced by something smaller than $1/mn$. Fix two binary forms $F, G \in \mathbb{Z}[X, Y]$ of degrees $m \geq 3$, $n \geq 3$, respectively, without multiple factors, and having resultant $R(F, G) =: r \neq 0$. Suppose that F is associated with the number fields $K_1, \ldots, K_u$ and G with the number fields $L_1, \ldots, L_v$. Let p be any prime number. Then the pairs of binary forms (F_b, G_b) given by $F_b(X, Y) = F(pX, bX + Y)$, $G_b(X, Y) = G(pX, bX + Y)$ $(b = 0, \ldots, p - 1)$ are pairwise $\mathbb{Z}$-inequivalent. Further, F_b is associated with $K_1, \ldots, K_u$ and G_b with $L_1, \ldots, L_v$ and F_b, G_b do not have multiple factors. By (2.1) we have $R(F_b, G_b) = rp^{mn}$. So if we take $c := |r|p^{mn}$ and let $p \to \infty$, we obtain infinitely many integers c such that the pairs of binary forms (F, G) satisfying the conditions of Theorem 2.3 with $S = \emptyset$ lie in $\gg c^{1/mn}$ $\mathbb{Z}$-equivalence classes.

We give a consequence for Thue–Mahler equations of the shape

$$F(x, y) \in c\mathbb{Z}_S^* \quad \text{in } (x, y) \in \mathbb{Z}_S \times \mathbb{Z}_S, \quad \text{with } \gcd(x, y) = 1, \tag{2.3}$$

where F is a binary form in $\mathbb{Z}_S[X, Y]$ and c is a positive integer coprime to the primes in S. Two solutions (x_1, y_1), (x_2, y_2) of (2.3) are called *propor-*

tional if $(x_2, y_2) = \lambda(x_1, y_1)$ for some $\lambda \in \mathbb{Q}^*$. Evertse and Győry [6] proved the following. Let $m \geq 3$ and let L be a given number field. Then the binary forms $F \in \mathbb{Z}_S[X, Y]$ of degree m such that F has no multiple factors, F splits into linear factors over L and such that (2.3) has at least three pairwise non-proportional solutions, lie in finitely many $\mathbb{Z}_S$-equivalence classes.

We prove the following quantitative result:

COROLLARY 2.4. *Let m be an integer with $m \geq 3$, $K_1, \ldots, K_u$ number fields with $\sum_{i=1}^{u}[K_i : \mathbb{Q}] = m$, $S = \{p_1, \ldots, p_t\}$ a finite, possibly empty set of primes, and c a positive integer coprime to $p_1 \cdots p_t$ if $S \neq \emptyset$. Then the set of binary forms $F \in \mathbb{Z}_S[X, Y]$ such that*

- (2.3) *has three pairwise non-proportional solutions,*
- *F is associated with $(K_1, \ldots, K_u)$, F has no multiple factors,*
- *F is Z_S-minimal*

is contained in the union of at most

$$e^{3\cdot 10^{24} m(m+3)(t+1)} \cdot 2^{\omega(c)} \prod_{p \mid c} \binom{3\,\mathrm{ord}_p(c) + 3m + 2}{3m+2}$$

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

Proof. We derive Corollary 2.4 from Theorem 2.2. Let $F \in \mathbb{Z}_S[X, Y]$ be a binary form satisfying the conditions of Corollary 2.4. Let (x_1, y_1), (x_2, y_2), (x_3, y_3) be pairwise non-proportional solutions of (2.3). Define the binary form $G(X, Y) = \prod_{i=1}^{3}(y_i X - x_i Y)$. Then

$$R(F, G) = \prod_{i=1}^{3} F(x_i, y_i) \in c^3 \mathbb{Z}_S^*.$$

Hence the pair (F, G) satisfies the conditions of Theorem 2.2 with $n = 3$, $(L_1, \ldots, L_v) = (\mathbb{Q}, \mathbb{Q}, \mathbb{Q})$, and with c^3 instead of c. By applying Theorem 2.2 with these data, we see that the pairs (F, G) lie in at most N $\mathbb{Z}_S$-equivalence classes, where N is the quantity obtained by substituting $n = 3$ and c^3 for c in the upper bound in Theorem 2.2. Hence the binary forms F lie in at most N $\mathbb{Z}_S$-equivalence classes. ∎

We return to the problem, addressed above, to give a fully explicit upper bound for the number of equivalence classes of pairs (F, G) satisfying the conditions of Theorem 2.3 without the constraint that F be $\mathbb{Z}_S$-minimal. In Lemma 9.3 in Section 9 we prove that for every pair of binary forms (F, G) in $\mathbb{Z}_S[X, Y]$ with (1.1) there are a pair of binary forms (F_0, G_0) in $\mathbb{Z}_S[X, Y]$ with (1.1) such that F_0 is $\mathbb{Z}_S$-minimal, and a matrix $A \in \mathrm{NS}_2(\mathbb{Z}_S)$, such that

$$F = (F_0)_A, \quad G = (G_0)_{(\det A)^{-1}A}. \tag{2.4}$$

Now Theorem 2.2 gives an explicit upper bound for the number of $\mathbb{Z}_S$-equivalence classes of pairs (F_0, G_0), so what we would like is to give an explicit upper bound for the number of $\mathbb{Z}_S$-equivalence classes of pairs (F, G) corresponding to a given pair (F_0, G_0) as in (2.4). But for this we would need some "effective information" about the pair (F_0, G_0) that is not provided by our method of proof.

To illustrate more concretely the problems that arise, we consider a special case. Let $S = \{p_1, \dots, p_t\}$ be a finite set of primes. Consider binary forms

$$F = X(X - a_1Y)(X - a_2Y), \quad G = Y(b_1X - Y)(b_2X - Y), \tag{2.5}$$

where $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $a_1 > 0$, $a_2, b_1, b_2 \neq 0$, $a_1 \neq a_2$, $b_1 \neq b_2$. These constraints on a_1, a_2, b_1, b_2 imply that any two distinct pairs of binary forms of the type (2.5) are $\mathbb{Z}_S$-inequivalent. We have

$$R(F, G) = -\prod_{i=1}^{2}\prod_{j=1}^{2}(1 - a_ib_j). \tag{2.6}$$

We consider

$$R(F, G) \in \mathbb{Z}_S^* \text{ in binary forms of the type (2.5).} \tag{2.7}$$

From (2.6), (2.7) it follows that

$$\varepsilon_{ij} := 1 - a_ib_j \in \mathbb{Z}_S^* \quad \text{for } i, j = 1, 2. \tag{2.8}$$

Further,

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & \varepsilon_{11} & \varepsilon_{12} \\ 1 & \varepsilon_{21} & \varepsilon_{22} \end{vmatrix} = 0. \tag{2.9}$$

Lemma 3.3 in Section 3 of the present paper gives an explicit upper bound for the number of solutions $\varepsilon_{11}, \varepsilon_{12}, \varepsilon_{21}, \varepsilon_{22} \in \mathbb{Z}_S^*$ of (2.9) such that

$$\text{each } 2 \times 2\text{-subdeterminant of the left-hand side is} \neq 0. \tag{2.10}$$

Notice that this is satisfied by the numbers of the type (2.8).

Let $\varepsilon_{11}, \varepsilon_{12}, \varepsilon_{21}, \varepsilon_{22} \in \mathbb{Z} \cap \mathbb{Z}_S^*$ be any solution of (2.9), (2.10). Define the quantities

$$b_1' := \pm\gcd(1-\varepsilon_{11}, 1-\varepsilon_{21}), \quad a_1' := \frac{1-\varepsilon_{11}}{b_1'}, \quad a_2' := \frac{1-\varepsilon_{21}}{b_1'}, \quad b_2' := \frac{1-\varepsilon_{12}}{a_1'},$$

where we choose the sign of b_1' such that $a_1' > 0$. Then $a_1', a_2', b_1' \in \mathbb{Z}$ and moreover $b_2' \in \mathbb{Z}$ since $a_1'/a_2' = (1-\varepsilon_{11})/(1-\varepsilon_{21}) = (1-\varepsilon_{12})/(1-\varepsilon_{22})$ and $\gcd(a_1', a_2') = 1$. Further, $\varepsilon_{11} = 1 - a_1'b_1'$, $\varepsilon_{21} = 1 - a_2'b_1'$, $\varepsilon_{12} = 1 - a_1'b_2'$, $\varepsilon_{22} = 1 - a_2'b_2'$.

If we require that F be $\mathbb{Z}_S$-minimal then $\gcd(a_1, a_2) = 1$. In that case we have $a_1 = a_1'$, $a_2 = a_2'$, $b_1 = b_1'$, $b_2 = b_2'$ and so a_1, a_2, b_1, b_2 are uniquely determined by $\varepsilon_{11}, \varepsilon_{12}, \varepsilon_{21}, \varepsilon_{22}$. Thus, we obtain an explicit upper bound for the number of solutions (F, G) of (2.7) for which F is $\mathbb{Z}_S$-minimal.

If we do not require that F be $\mathbb{Z}_S$-minimal, we obtain for every solution $\varepsilon_{11}, \varepsilon_{21}, \varepsilon_{12}, \varepsilon_{22} \in \mathbb{Z} \cap \mathbb{Z}_S^*$ of (2.9), (2.10) and every positive divisor d of

$$\gcd(b_1', b_2') = \gcd(1 - \varepsilon_{11}, 1 - \varepsilon_{21}, 1 - \varepsilon_{12}, 1 - \varepsilon_{22})$$

a solution (F, G) of (2.7), given by

$$a_1 = da_1', \quad a_2 = da_2', \quad b_1 = b_1'/d, \quad b_2 = b_2'/d.$$

Thus, to obtain an explicit upper bound for the total number of solutions (F, G) of (2.7), we need for every solution $\varepsilon_{11}, \varepsilon_{12}, \varepsilon_{21}, \varepsilon_{22} \in \mathbb{Z}_S^* \cap \mathbb{Z}$ of (2.9) an explicit upper bound for the number of divisors of the quantity $\gcd(1 - \varepsilon_{11}, 1 - \varepsilon_{21}, 1 - \varepsilon_{12}, 1 - \varepsilon_{22})$. We have no clue how to determine such a bound.

3. Auxiliary results. Let $(\mathbb{C}^*)^N$ be the N-fold direct product of $\mathbb{C}^*$ with coordinatewise multiplication $(x_1, \dots, x_N)(y_1, \dots, y_N) = (x_1y_1, \dots, x_Ny_N)$. We say that a subgroup Γ of $(\mathbb{C}^*)^N$ has *rank* r if Γ has a free subgroup Γ_0 of rank r such that for every $\mathbf{u} \in \Gamma$ there is $s \in \mathbb{Z}_{>0}$ with $\mathbf{u}^s \in \Gamma_0$.

LEMMA 3.1. *Let Γ be a subgroup of $(\mathbb{C}^*)^N$ of rank r and $a_1, \dots, a_N \in \mathbb{C}^*$. Then the equation*

$$a_1x_1 + \cdots + a_Nx_N = 1 \quad \text{in } \mathbf{x} = (x_1, \dots, x_N) \in \Gamma \tag{3.1}$$

has at most $e^{(6N)^{3N}(r+1)}$ solutions with

$$\sum_{i \in I} a_ix_i \neq 0 \quad \text{for each non-empty subset } I \text{ of } \{1, \dots, N\}. \tag{3.2}$$

Proof. See Evertse, Schlickewei, and Schmidt [9, Theorem 1.1]. ∎

For $N = 2$, the following lemma gives a sharper result.

LEMMA 3.2. *Let $N = 2$ and let Γ, a_1, a_2 be as in Lemma* 3.1. *Then equation* (3.1) *has at most $2^{8(r+2)}$ solutions.*

Proof. This is an immediate consequence of Theorem 1.1 of Beukers and Schlickewei [4]. ∎

LEMMA 3.3. *For $i, j = 1, 2$, let Γ_{ij} be a subgroup of $\mathbb{C}^*$ of rank r. Then equation*

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & x_{11} & x_{12} \\ 1 & x_{21} & x_{22} \end{vmatrix} = 0 \quad \text{in } x_{ij} \in \Gamma_{ij} \text{ for } i, j = 1, 2 \tag{3.3}$$

has at most $e^{30^{15}(4r+2)}$ *solutions such that*

(3.4) *each* 2×2*-subdeterminant of the left-hand side of* (3.3) *is* $\neq 0$.

Proof. This can be proved by going through the proof of Evertse, Győry, Stewart and Tijdeman [8, Theorem 1], see also Bérczes [1]. By expanding (3.3) we obtain

$$x_{11}x_{22} - x_{12}x_{21} + x_{21} - x_{22} + x_{12} - x_{11} = 0. \tag{3.5}$$

Notice that the summands of (3.5) lie in the group generated by $-1, \Gamma_{11}, \Gamma_{12}, \Gamma_{21}, \Gamma_{22}$, which has rank at most $4r$. We have to consider all partitions of the left-hand side of (3.5) into minimal vanishing subsums and apply Lemma 3.1 to each subsum. We consider only two cases; the other cases can be dealt with in a similar way following [8].

First, we consider the solutions of (3.3), (3.4) such that no proper subsum of the left-hand side of (3.5) vanishes. On dividing (3.5) by x_{11} we obtain

$$x_{22} - \frac{x_{12}x_{21}}{x_{11}} + \frac{x_{21}}{x_{11}} - \frac{x_{22}}{x_{11}} + \frac{x_{12}}{x_{11}} = 1.$$

By Lemma 3.1 with $N = 5$, we have at most $e^{30^{15}(4r+1)}$ possibilities for the tuple $\left(x_{22}, \frac{x_{12}x_{21}}{x_{11}}, \frac{x_{21}}{x_{11}}, \frac{x_{22}}{x_{11}}, \frac{x_{12}}{x_{11}}\right)$. Each such tuple determines uniquely the tuple $(x_{11}, x_{12}, x_{21}, x_{22})$. Hence (3.3), (3.4) have at most $e^{30^{15}(4r+1)}$ solutions such that no proper subsum of the left-hand side of (3.5) vanishes.

Next, we consider those solutions of (3.3), (3.4) for which

$$x_{11}x_{22} - x_{12}x_{21} + x_{21} = 0, \qquad -x_{22} + x_{12} - x_{11} = 0 \tag{3.6}$$

and no proper subsum of any of these sums vanishes. By dividing the first sum by x_{21} and the second sum by x_{11} we obtain

$$x_{12} - \frac{x_{11}x_{22}}{x_{21}} = 1, \qquad \frac{x_{12}}{x_{11}} - \frac{x_{22}}{x_{11}} = 1.$$

By Lemma 3.1 we have at most

$$(e^{12^6(4r+1)})^2 < \frac{1}{200}\, e^{30^{15}(4r+1)}$$

possibilities for the tuple $\left(x_{12}, \frac{x_{11}x_{22}}{x_{21}}, \frac{x_{12}}{x_{11}}, \frac{x_{22}}{x_{11}}\right)$. This tuple determines uniquely the tuple $(x_{11}, x_{12}, x_{21}, x_{22})$. Hence (3.3), (3.4) have at most $\frac{1}{200}e^{30^{15}(4r+1)}$ solutions such that (3.6) holds, and no proper subsum of the sums in (3.6) vanishes.

Following [8] one can show that each other partition of (3.5) into minimal vanishing subsums also gives rise to at most $\frac{1}{200}e^{30^{15}(4r+1)}$ solutions of (3.3), (3.4). The total number of partitions of (3.5) into minimal vanishing subsums is at most $\binom{6}{2} + \binom{6}{3} + \binom{6}{2}\binom{4}{2} = 125$ (we are very generous here). Hence the

total number of solutions of (3.3), (3.4) is at most

$$\left(1+\frac{125}{200}\right)e^{30^{15}(4r+1)} < e^{30^{15}(4r+2)}. \ \blacksquare$$

4. Proof of Theorem 2.1. We shall deduce Theorem 2.1 from the following.

LEMMA 4.1. *Let m, n be integers with $m \geq 2$, $n \geq 2$ and $m+n \geq 5$. For $i = 1, \dots, m$, $j = 1, \dots, n$, let Γ_{ij} be subgroups of $\mathbb{C}^*$ of rank at most r. If $(x_1, \dots, x_m, y_1, \dots, y_n)$ runs through the tuples in $\mathbb{C}^{m+n}$ for which*

$$\begin{cases} x_i - y_j \in \Gamma_{ij} & \text{for } 1 \leq i \leq m,\ 1 \leq j \leq n, \\ x_1, \dots, x_m, y_1, \dots, y_n \text{ are pairwise distinct}, \end{cases} \tag{4.1}$$

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

$$3 \cdot 2^{24(r+1)(m+n-4)} e^{18^9(4r+1)}. \tag{4.2}$$

Proof. We proceed by induction on $m+n$. First suppose that $m = 2$, $n = 3$. Let $(x_1, x_2, y_1, y_2, y_3) \in \mathbb{C}^5$ be a tuple with (4.1). For $1 \leq j < k \leq 3$, consider the identity

$$(x_1 - y_j) + (y_j - x_2) + (x_2 - y_k) + (y_k - x_1) = 0. \tag{4.3}$$

It is easily seen that the 4-term sum on the left-hand side of (4.3) can have a vanishing subsum for at most one pair (j, k). We may assume that for $(j, k) = (1, 2)$ and $(1, 3)$ there is no vanishing subsum on the left-hand side. For $(j, k) = (1, 2)$, identity (4.3) gives

$$\frac{x_2 - y_1}{x_1 - y_1} - \frac{x_2 - y_2}{x_1 - y_1} + \frac{x_1 - y_2}{x_1 - y_1} = 1. \tag{4.4}$$

Notice that the summands of (4.4) belong to the group generated by $-1, \Gamma_{11}, \Gamma_{12}, \Gamma_{21}, \Gamma_{22}$, which has rank at most $4r$. Hence, by Lemma 3.1, there are at most $C_1 = e^{18^9(4r+1)}$ possibilities for the tuple $\left(\frac{x_2-y_1}{x_1-y_1}, \frac{x_2-y_2}{x_1-y_1}, \frac{x_1-y_2}{x_1-y_1}\right)$. If we fix $\frac{x_2-y_1}{x_1-y_1}$ and set $a_1 = \frac{x_1-y_1}{x_1-x_2}$, $a_2 = -a_1$, then we infer from (4.3) with $(j, k) = (1, 3)$ that

$$a_1 \frac{x_1 - y_3}{x_1 - y_1} + a_2 \frac{x_2 - y_3}{x_1 - y_1} = 1. \tag{4.5}$$

By Lemma 3.2 there are at most $C_2 = 2^{8(3r+3)}$ possibilities for the tuple $\left(\frac{x_1-y_3}{x_1-y_1}, \frac{x_2-y_3}{x_1-y_1}\right)$. This proves the assertion for $m + n = 5$ with the bound $3C_1C_2$.

Consider now the case $m + n > 5$. We may assume without loss of generality that $n \geq 3$. Suppose that Lemma 4.1 has already been proved for $m + n - 1$. This means that if $(x_1, \dots, x_m, y_1, \dots, y_{n-1})$ runs through the tuples in $\mathbb{C}^{m+n-1}$ with (4.1), then the tuple $\left(\frac{x_i-y_j}{x_1-y_1}\right)_{i=1,\dots,m,\ j=1,\dots,n}$ runs

through a set of cardinality at most $3C_1C_2^{m+n-5}$. Fix such a tuple $\left(\frac{x_i-y_j}{x_1-y_1}\right)$ with $1 \le i \le m$, $1 \le j \le n-1$. Then $\frac{x_1-x_2}{x_1-y_1}$ is uniquely determined. So we get equation (4.5) again, but with y_n instead of y_3, and we infer as above that there are at most C_2 possibilities for the tuple $\left(\frac{x_1-y_n}{x_1-y_1}, \frac{x_2-y_n}{x_1-y_1}\right)$. If such a tuple is fixed, then $\frac{x_i-y_n}{x_1-y_1}$ is uniquely determined for each $i > 2$. Hence the set of tuples under consideration $\left(\frac{x_i-y_j}{x_1-y_1}\right)$ with $1 \le i \le m$, $1 \le j \le n$ has cardinality at most $3C_1C_2^{m+n-4}$, which proves our assertion. ∎

Proof of Theorem 2.1. We view $K_1, \dots, K_u, L_1, \dots, L_v$ as subfields of $\mathbb{C}$. For $i = 1, \dots, u$, let σ_{ij} $(j = 1, \dots, [K_i : \mathbb{Q}])$ be the embeddings of K_i in $\mathbb{C}$, and let $K_1, \dots, K_m$ be the sequence of fields consisting of $\sigma_{ij}(K_i)$ $(i = 1, \dots, u, j = 1, \dots, [K_i : \mathbb{Q}])$. Likewise, we augment $L_1, \dots, L_v$ to a sequence of fields $L_1, \dots, L_n$. Denote by T the set of primes consisting of $p_1, \dots, p_t$ and the distinct prime factors of c. For $i = 1, \dots, m$, $j = 1, \dots, n$, let Γ_{ij} be the unit group of the integral closure of $\mathbb{Z}_T$ in the compositum K_iL_j of K_i and L_j. Then Γ_{ij} is a subgroup of $\mathbb{C}^*$ of rank at most $mn(t+\omega(c)+1)-1$.

Let F, G be any pair of binary forms with coefficients in $\mathbb{Z}_S$ satisfying (1.1) and the other conditions of Theorem 2.1. Then

$$F(X,Y) = \prod_{i=1}^{m}(X - \alpha_i Y), \qquad G(X,Y) = \prod_{j=1}^{n}(X - \beta_j Y)$$

where $\alpha_i \in K_i$ for $i = 1, \dots, m$, $\beta_j \in L_j$ for $j = 1, \dots, n$, the numbers $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n$ are pairwise distinct, and

$$R(F,G) = \prod_{i=1}^{m}\prod_{j=1}^{n}(\beta_j - \alpha_i) \in \mathbb{Z}_T^*.$$

This implies that $\alpha_i - \beta_j \in \Gamma_{ij}$ for $i = 1, \dots, m$, $j = 1, \dots, n$. So by Lemma 4.1 and the fact that each group Γ_{ij} has rank at most $mn(t+\omega(c)+1)-1$, the mn-tuple $\left(\frac{\alpha_i-\beta_j}{\alpha_1-\beta_1} : 1 \le i \le m, 1 \le j \le n\right)$ belongs to a set independent of F, G of cardinality at most C, where C denotes the quantity obtained by substituting $mn(t+\omega(c)+1)-1$ for r in the bound in (4.2).

It follows from (1.1) that

$$R(F,G) = \varrho_1^{mn}\varrho_0 c \tag{4.6}$$

where $\varrho_1, \varrho_0 \in \mathbb{Z}_S^*$ and where ϱ_0 may assume at most $2(mn)^t$ distinct values. Any choice of ϱ_0 and a tuple $\left(\frac{\alpha_i-\beta_j}{\alpha_1-\beta_1} : 1 \le i \le m, 1 \le j \le n\right)$ determines uniquely the tuple $\left(\frac{\alpha_i/\varrho_1-\beta_j/\varrho_1}{\alpha_1/\varrho_1-\beta_1/\varrho_1}\right)$ with $1 \le i \le m$, $1 \le j \le n$ and, by (4.6), also the number $(\alpha_1/\varrho_1 - \beta_1/\varrho_1)^{mn}$. This leaves at most mn possibilities for $\alpha_1/\varrho_1 - \beta_1/\varrho_1$. Then any choice of $\alpha_1/\varrho_1 - \beta_1/\varrho_1$ determines uniquely the numbers $\alpha_i/\varrho_1 - \beta_j/\varrho_1$ and $\beta_j/\varrho_1 - \beta_1/\varrho_1$ $(i = 1, \dots, m, j = 1, \dots, n)$.

By combining the above we deduce that there is a set V of cardinality at most $2(mn)^{t+1}C$ with the following property: if (F,G) is any pair of binary forms satisfying (1.1) and the conditions of Theorem 2.1, then there are $\varrho_1 \in \mathbb{Z}_S^*$ and an ordering of the zeros $\alpha_1,\dots,\alpha_m$, $\beta_1,\dots,\beta_n$ of F,G, such that $(\alpha_i/\varrho_1 - \beta_1/\varrho_1, \beta_j/\varrho_1 - \beta_1/\varrho_1 : 1 \le i \le m,\ 1 \le j \le n) \in V$.

If now F',G' is another pair of binary forms in $\mathbb{Z}_S[X,Y]$ with (1.1) whose zeros, say, $\alpha_1',\dots,\alpha_m'$, $\beta_1',\dots,\beta_n'$ yield for some $\varrho_1' \in \mathbb{Z}_S^*$ the same tuple $(\alpha_i'/\varrho_1' - \beta_1'/\varrho_1', \beta_j'/\varrho_1' - \beta_1'/\varrho_1' : 1 \le i \le m,\ 1 \le j \le n)$, then

$$\alpha_i' = \varrho\alpha_i + b \quad \text{and} \quad \beta_j' = \varrho\beta_j + b$$

for $i = 1,\dots,m$ and $j = 1,\dots,n$, where $\varrho \in \mathbb{Z}_S^*$ and where b is integral over $\mathbb{Z}_S$. Using $\alpha_1 + \cdots + \alpha_m \in \mathbb{Q}$, $\beta_1 + \cdots + \beta_n \in \mathbb{Q}$ we infer that $b \in \mathbb{Q}$. Consequently, $b \in \mathbb{Z}_S$. This means that the pairs (F',G') and (F,G) are strongly $\mathbb{Z}_S$-equivalent.

It follows that the pairs of binary forms (F,G) satisfying (1.1) and the conditions of Theorem 2.1 lie in the union of at most

$$\begin{aligned} 2(mn)^{t+1}C &= 2(mn)^{t+1} \cdot 3 \cdot 2^{24mn(t+\omega(c)+1)(m+n-4)} e^{18^9(4mn(t+\omega(c)+1)-3)} \\ &\le e^{17(m+n+10^{11})mn(t+\omega(c)+1)} \end{aligned}$$

strong $\mathbb{Z}_S$-equivalence classes. This completes the proof of Theorem 2.1. ∎

5. Augmented forms. In the proof of Theorem 2.2 it will be more convenient to work with so-called augmented forms F^*, which are tuples consisting of a binary form F and the zeros of F on the projective line.

Let K be a field and $\mathbb{P}^1(K) := \{(\xi:\eta) : \xi,\eta \in K,\ (\xi,\eta) \ne (0,0)\}$ the projective line over K where $(\xi:\eta) = (\xi':\eta')$ if and only if $(\xi',\eta') = \lambda(\xi,\eta)$ for some $\lambda \in K^*$. The projective transformation of $\mathbb{P}^1(K)$ defined by a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ is given by $\langle A\rangle : (\xi:\eta) \mapsto (a\xi + b\eta : c\xi + d\eta)$. Clearly, two matrices define the same projective transformation if and only if they are proportional.

Let Ω be a domain with quotient field K of characteristic 0. Choose an algebraic closure $\overline{K}$ of K. By an *augmented binary form of degree m over Ω* we mean a tuple

$$F^* = (F, (\beta_1:\alpha_1), \dots, (\beta_m:\alpha_m)),$$

where F is a binary form in $\Omega[X,Y]$, and $(\beta_1:\alpha_1),\dots,(\beta_m:\alpha_m)$ are *distinct* points in $\mathbb{P}^1(\overline{K})$ such that $F = \lambda\prod_{i=1}^m(\alpha_i X - \beta_i Y)$ for some $\lambda \in \overline{K}^*$. So it is part of the definition that F does not have multiple factors. We define $\deg F^* := \deg F = m$. We denote by $\mathcal{A}(\Omega,m)$ the collection of augmented forms of degree m over Ω. We write $F^* = (F,\dots)$ if F is the binary form corresponding to F^*.

Given $F^* = (F, (\beta_1 : \alpha_1), \dots, (\beta_m : \alpha_m)) \in \mathcal{A}(\Omega, m)$, $\varepsilon \in \Omega^*$, $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\Omega)$, we define

$$\varepsilon F_U^* = (\varepsilon F_U, \langle U^{-1}\rangle(\beta_1 : \alpha_1), \dots, \langle U^{-1}\rangle(\beta_m : \alpha_m)).$$

Then again, $\varepsilon F_U^* \in \mathcal{A}(\Omega, m)$. Two augmented forms $F_1^*, F_2^* \in \mathcal{A}(\Omega, m)$ are called *Ω-equivalent* if $F_2^* = \varepsilon(F_1^*)_U$ for some $\varepsilon \in \Omega^*$ and $U \in \mathrm{GL}_2(\Omega)$. Two pairs $(F_1^*, G_1^*), (F_2^*, G_2^*) \in \mathcal{A}(\Omega, m) \times \mathcal{A}(\Omega, n)$ are called *Ω-equivalent* if $F_2^* = \varepsilon(F_1^*)_U$, $G_2^* = \eta(G_1^*)_U$ for some $\varepsilon, \eta \in \Omega^*$ and $U \in \mathrm{GL}_2(\Omega)$.

Denote by G_K the Galois group of $\overline{K}$ over K and for $\sigma \in G_K$ and $(\xi : \eta) \in \mathbb{P}^1(\overline{K})$ let $\sigma((\xi : \eta)) := (\sigma(\xi) : \sigma(\eta))$. If $F^* = (F, (\beta_1 : \alpha_1), \dots, (\beta_m : \alpha_m)) \in \mathcal{A}(\Omega, m)$, then every $\sigma \in G_K$ permutes $(\beta_1 : \alpha_1), \dots, (\beta_m : \alpha_m)$. By a *$G_K$-action* on $\{1, \dots, m\}$ we mean a group homomorphism from G_K to the permutation group of $\{1, \dots, m\}$. Given a G_K-action φ of $\{1, \dots, m\}$, we denote by $\mathcal{A}(\Omega, \varphi)$ the collection of augmented forms of degree m over Ω,

$$F^* = (F, (\beta_1 : \alpha_1), \dots, (\beta_m : \alpha_m)),$$

such that

$$\sigma(\beta_i : \alpha_i) = (\beta_{\varphi(\sigma)(i)} : \alpha_{\varphi(\sigma)(i)}) \quad \text{for } \sigma \in G_K,\ i = 1, \dots, m.$$

It is easy to check that $\mathcal{A}(\Omega, \varphi)$ is closed under Ω-equivalence, and that for any two actions φ on $\{1, \dots, m\}$, ψ on $\{1, \dots, n\}$, $\mathcal{A}(\Omega, \varphi) \times \mathcal{A}(\Omega, \psi)$ is closed under Ω-equivalence.

A binary form $F \in \Omega[X, Y]$ is called *Ω-primitive* if the ideal generated by its coefficients is equal to Ω. We call F *Ω-minimal* if there are no binary form $G \in \Omega[X, Y]$ and matrix $A \in \mathrm{NS}_2(\Omega) \setminus \mathrm{GL}_2(\Omega)$ such that $F = G_A$. (These notions are meaningless if Ω is a field.)

We start with a useful lemma.

LEMMA 5.1. *Let K be a field of characteristic 0, $\overline{K}$ an algebraic closure of K, and L an extension of $\overline{K}$. Further, let $m \geq 3$ and let φ be a G_K-action on $\{1, \dots, m\}$. Lastly, let $F_1^*, F_2^* \in \mathcal{A}(K, \varphi)$, and suppose that there are $A \in \mathrm{GL}_2(L)$ and $\lambda \in L^*$ such that*

$$F_2^* = \lambda(F_1^*)_A.$$

(i) *Let $A' \in \mathrm{GL}_2(L)$, $\lambda' \in L^*$ be any other pair with $F_2^* = \lambda'(F_1^*)_{A'}$. Then $A' = \mu A$ for some $\mu \in L^*$.*

(ii) *There are $B \in \mathrm{GL}_2(K)$ and $\nu \in L^*$ such that $A = \nu B$.*

Proof. (i) Write $F_i^* = (F_i, (\beta_{i1} : \alpha_{i1}), \dots, (\beta_{im} : \alpha_{im}))$ for $i = 1, 2$. By assumption, $m \geq 3$ and $\langle A^{-1}\rangle(\beta_{1j} : \alpha_{1j}) = (\beta_{2j} : \alpha_{2j})$, $\langle A'^{-1}\rangle(\beta_{1j} : \alpha_{1j}) = (\beta_{2j} : \alpha_{2j})$ for $j = 1, \dots, m$. Since a projective transformation of the projective line is uniquely determined by its action on three points, this implies $\langle A^{-1}\rangle = \langle A'^{-1}\rangle$, hence $A' = \mu A$ for some $\mu \in L^*$.

(ii) Since $(\beta_{ij} : \alpha_{ij}) \in \mathbb{P}^1(\overline{K})$ for $i = 1, 2$, $j = 1, \dots, m$, the projective transformation $\langle A^{-1} \rangle$ is defined over $\overline{K}$. This implies that there are $\nu \in L^*$ and $B \in \mathrm{GL}_2(\overline{K})$ such that $A = \nu B$. Without loss of generality we assume that one of the entries of B is equal to 1. For $\sigma \in G_K$, denote by $\sigma(B)$ the matrix obtained by applying σ to the entries of B. Then for $\sigma \in G_K$ we have $\langle \sigma(B)^{-1} \rangle \sigma(\beta_{i1} : \alpha_{i1}) = \sigma(\beta_{i2} : \alpha_{i2})$ for $i = 1, \dots, m$ and this implies $\langle \sigma(B)^{-1} \rangle (\beta_{i1} : \alpha_{i1}) = (\beta_{i2} : \alpha_{i2})$ for $i = 1, \dots, m$ since $\sigma(\beta_{ij} : \alpha_{ij}) = (\beta_{i,\varphi(\sigma)(j)} : \alpha_{i,\varphi(\sigma)(j)})$ for $i = 1, 2$, $j = 1, \dots, m$, $\sigma \in G_K$. Hence for each $\sigma \in G_K$ there is $\kappa_\sigma \in \overline{K}^*$ such that $\sigma(B) = \kappa_\sigma B$. But one of the entries of B is equal to 1, so $\sigma(B) = B$ for $\sigma \in G_K$. Therefore, $B \in \mathrm{GL}_2(K)$. ∎

We now formulate a proposition for augmented forms over $\mathbb{Z}_S$ and then deduce Theorem 2.2 from this. As before, $S = \{p_1, \dots, p_t\}$ is a finite, possibly empty set of primes, and c a positive integer coprime to the primes in S. Condition (5.2) below has been inserted for technical convenience.

PROPOSITION 5.2. *Let $m \geq 3$, $n \geq 3$. Let φ be a $G_{\overline{\mathbb{Q}}}$-action on $\{1, \dots, m\}$ and ψ a $G_{\overline{\mathbb{Q}}}$-action on $\{1, \dots, n\}$. Then the set of pairs of augmented forms $F^* = (F, \dots)$, $G^* = (G, \dots)$ such that*

(5.1) $F^* \in \mathcal{A}(\mathbb{Z}_S, \varphi)$, $G^* \in \mathcal{A}(\mathbb{Z}_S, \psi)$,

(5.2) *F, G are $\mathbb{Z}_S$-primitive,*

(5.3) *F is $\mathbb{Z}_S$-minimal,*

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

is contained in the union of at most

$$N(c) = e^{10^{24}(m+n)mn(t+1)} 2^{\omega(c)} \cdot \prod_{p|c} \binom{\mathrm{ord}_p(c) + mn}{mn}$$

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

Proposition 5.2 will be proved in Sections 6 to 8.

Proof of Theorem 2.2. Let $K_1, \dots, K_u$ be one of the sequences of fields from Theorem 2.2. By assumption, $\sum_{i=1}^{u} [K_i : \mathbb{Q}] = m$. For $i = 1, \dots, u$ denote by σ_{ij} $(j = 1, \dots, m_i := [K_i : \mathbb{Q}])$ the isomorphisms of K_i into $\overline{\mathbb{Q}}$. Pick ξ_i with $\mathbb{Q}(\xi_i) = K_i$ for $i = 1, \dots, u$, such that the elements of the sequence

$$(\eta_1, \dots, \eta_m)$$
$$:= (\sigma_{11}(\xi_1), \dots, \sigma_{1,m_1}(\xi_1), \sigma_{21}(\xi_2), \dots, \sigma_{2,m_2}(\xi_2), \dots, \sigma_{u1}(\xi_u), \dots, \sigma_{u,m_u}(\xi_u))$$

are distinct. Then every $\sigma \in G_{\mathbb{Q}}$ permutes $(\eta_1, \dots, \eta_m)$. We define an action φ on $\{1, \dots, m\}$ by requiring that

$$\sigma(\eta_k) = \eta_{\varphi(\sigma)(k)} \quad \text{for } \sigma \in G_{\mathbb{Q}},\ k = 1, \dots, m.$$

Now let $F \in \mathbb{Z}_S[X,Y]$ be a binary form without multiple factors associated with $K_1, \ldots, K_u$. Then F can be expressed as

$$F(X,Y) = \lambda \prod_{i=1}^{u} \prod_{j=1}^{m_i} (\sigma_{ij}(\theta_i)X - \sigma_{ij}(\zeta_i)Y)$$

where $\theta_i, \zeta_i \in K_i$ for $i = 1, \ldots, u$ and $\lambda \in \mathbb{Q}^*$. Define the augmented form

$$F^* := (F, (\beta_1 : \alpha_1), \ldots, (\beta_m : \alpha_m)),$$

where $(\beta_1 : \alpha_1), \ldots, (\beta_m : \alpha_m)$ is the following sequence of points in $\mathbb{P}^1(\overline{\mathbb{Q}})$:

$$(\sigma_{11}(\zeta_1) : \sigma_{11}(\theta_1)), \ldots, (\sigma_{1,m_1}(\zeta_1) : \sigma_{1,m_1}(\theta_1)), \ldots, \\ (\sigma_{u1}(\zeta_u) : \sigma_{u1}(\theta_u)), \ldots, (\sigma_{u,m_u}(\zeta_u) : \sigma_{u,m_u}(\theta_u)).$$

Clearly, $\sigma(\beta_i : \alpha_i) = (\beta_{\varphi(\sigma)(i)} : \alpha_{\varphi(\sigma)(i)})$ for $\sigma \in G_{\mathbb{Q}}$, $i = 1, \ldots, m$. Thus, we have defined an action φ on $\{1, \ldots, m\}$ depending only on $K_1, \ldots, K_u$, and every binary form $F \in \mathbb{Z}_S[X,Y]$ without multiple factors associated with $K_1, \ldots, K_u$ can be extended to an augmented form $F^* \in \mathcal{A}(\mathbb{Z}_S, \varphi)$. Completely similarly, we can construct an action ψ on $\{1, \ldots, n\}$ from the sequence of fields $L_1, \ldots, L_v$, and extend every binary form $G \in \mathbb{Z}_S[X,Y]$ without multiple factors associated with $L_1, \ldots, L_v$ to an augmented form $G^* \in \mathcal{A}(\mathbb{Z}_S, \psi)$.

For the moment we consider pairs of binary forms (F,G) in $\mathbb{Z}_S[X,Y]$ which satisfy the conditions of Theorem 2.2 and in addition are $\mathbb{Z}_S$-primitive. From the definitions it is clear that the corresponding pairs (F^*, G^*) constructed above satisfy (5.1)–(5.4). Further, if two pairs of augmented forms are $\mathbb{Z}_S$-equivalent, then so are the corresponding pairs of binary forms. With these observations, it follows at once that the pairs of binary forms (F,G) which satisfy the conditions of Theorem 2.2 and which are $\mathbb{Z}_S$-primitive lie in the union of at most $N(c)$ $\mathbb{Z}_S$-equivalence classes, where $N(c)$ is the upper bound from Proposition 5.2.

Now let (F,G) be a pair of binary forms in $\mathbb{Z}_S[X,Y]$ satisfying the conditions of Theorem 2.2 which are not both $\mathbb{Z}_S$-primitive. Write $F = d_1 F'$, $G = d_2 G'$ where d_1, d_2 are positive integers coprime to the primes in S and where both F', G' are $\mathbb{Z}_S$-primitive. Then by (2.1), $d_1^n d_2^m$ divides c and the pair (F', G') satisfies all conditions of Theorem 2.2 but with $c/d_1^n d_2^m$ instead of c. It follows that the set of pairs of binary forms (F,G) in $\mathbb{Z}_S[X,Y]$ satisfying the conditions of Theorem 2.2 is contained in the union of at most

$$\sum_{d_1, d_2 : d_1^n d_2^m \mid c} N(c/d_1^n d_2^m) \\ \leq e^{10^{24}(m+n)mn(t+1)} 2^{\omega(c)} \prod_{p \mid c} \sum_{u,v} \binom{\mathrm{ord}_p(c) - nu - mv + mn}{mn}$$

$$\leq e^{10^{24}(m+n)mn(t+1)}2^{\omega(c)}\prod_{p|c}\binom{\operatorname{ord}_p(c)+mn+2}{mn+2}$$

$\mathbb{Z}_S$-equivalence classes, where the summation is over all pairs of non-negative integers u, v such that $nu + mv \leq \operatorname{ord}_p(c)$. This completes the proof of Theorem 2.2. ∎

6. Local-to-global arguments. For a prime number p, let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ at p, $\overline{\mathbb{Q}}_p$ an algebraic closure of $\mathbb{Q}_p$, $\mathbb{Z}_p \subset \mathbb{Q}_p$ the ring of p-adic integers, and $\overline{\mathbb{Z}}_p$ the integral closure of $\mathbb{Z}_p$ in $\overline{\mathbb{Q}}_p$. By $|\cdot|_p$ we denote the standard p-adic absolute value with $|p|_p = 1/p$, extended to $\overline{\mathbb{Q}}_p$. As before, $S = \{p_1, \dots, p_t\}$ is a finite, possibly empty set of primes.

LEMMA 6.1. *Let $m \geq 3$, $n \geq 3$, φ a G_K-action on $\{1, \dots, m\}$, ψ a G_K-action on $\{1, \dots, n\}$, $F_1^*, F_2^* \in \mathcal{A}(\mathbb{Z}_S, \varphi)$, $G_1^*, G_2^* \in \mathcal{A}(\mathbb{Z}_S, \psi)$. Then (F_1^*, G_1^*) is $\mathbb{Z}_S$-equivalent to (F_2^*, G_2^*) if and only if (F_1^*, G_1^*) is $\mathbb{Z}_p$-equivalent to (F_2^*, G_2^*) for every prime $p \notin S$.*

Proof. The "only if" part is obvious. To prove the "if part", assume that (F_1^*, G_1^*) is $\mathbb{Z}_p$-equivalent to (F_2^*, G_2^*) for every prime $p \notin S$. This means that for every prime $p \notin S$, there are $U_p \in \mathrm{GL}_2(\mathbb{Z}_p)$ and $\varepsilon_p, \eta_p \in \mathbb{Z}_p^*$ such that

$$F_2^* = \varepsilon_p (F_1^*)_{U_p}, \quad G_2^* = \eta_p (G_1^*)_{U_p}. \tag{6.1}$$

We may assume that we have inclusions $\mathbb{Q} \subset \mathbb{Q}_p \subset \overline{\mathbb{Q}}_p$ and $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$. Apply Lemma 5.1(ii) with $K = \mathbb{Q}$, $L = \overline{\mathbb{Q}}_p$. Thus, there are $\lambda_p \in \overline{\mathbb{Q}}_p^*$ and $\widetilde{U}_p \in \mathrm{GL}_2(\mathbb{Q})$ such that $U_p = \lambda_p \widetilde{U}_p$. Without loss of generality, we may assume that the entries of $\widetilde{U}_p$ are integers in $\mathbb{Z}$ with gcd 1. Since $U_p \in \mathrm{GL}_2(\mathbb{Z}_p)$, this implies that $\lambda_p \in \mathbb{Z}_p^*$. Together with (6.1) this gives

$$F_2^* = \widetilde{\varepsilon}_p (F_1^*)_{\widetilde{U}_p}, \quad G_2^* = \widetilde{\eta}_p (G_1^*)_{\widetilde{U}_p} \tag{6.2}$$
$$\text{with } \widetilde{\varepsilon}_p, \widetilde{\eta}_p \in \mathbb{Q} \cap \mathbb{Z}_p^* \text{ and } \widetilde{U}_p \in \mathrm{GL}_2(\mathbb{Q}) \cap \mathrm{GL}_2(\mathbb{Z}_p).$$

By Lemma 5.1(i), the matrices $\widetilde{U}_p$ ($p \notin S$) are proportional. Since we assumed that the entries of $\widetilde{U}_p$ have gcd 1, the matrices $\widetilde{U}_p$ ($p \notin S$) are equal up to sign. Hence there are $\widetilde{U} \in \mathrm{NS}_2(\mathbb{Z})$ and $\widetilde{\varepsilon}, \widetilde{\eta} \in \mathbb{Q}^*$ such that

$$F_2^* = \widetilde{\varepsilon} (F_1^*)_{\widetilde{U}}, \quad G_2^* = \widetilde{\eta} (G_1^*)_{\widetilde{U}},$$

and $\widetilde{U} = \pm \widetilde{U}_p$, $\widetilde{\varepsilon} = \pm \widetilde{\varepsilon}_p$, $\widetilde{\eta} = \pm \widetilde{\eta}_p$ for every prime $p \notin S$. But then $\det \widetilde{U} = \det \widetilde{U}_p \in \mathbb{Z}_p^*$ for every prime $p \notin S$, and therefore $\det \widetilde{U} \in \mathbb{Z}_S^*$ and $\widetilde{U} \in \mathrm{GL}_2(\mathbb{Z}_S)$. Likewise, $\widetilde{\varepsilon}, \widetilde{\eta} \in \mathbb{Z}_p^*$ for every prime $p \notin S$, which implies $\widetilde{\varepsilon}, \widetilde{\eta} \in \mathbb{Z}_S^*$. This proves Lemma 6.1. ∎

LEMMA 6.2. *Let $F \in \mathbb{Z}_S[X, Y]$ be a binary form. Then F is $\mathbb{Z}_S$-minimal if and only if F is $\mathbb{Z}_p$-minimal for every prime $p \notin S$.*

Proof. If F is not $\mathbb{Z}_S$-minimal, then there is a matrix $A \in \mathrm{NS}_2(\mathbb{Z}_S)$ with $A \notin \mathrm{GL}_2(\mathbb{Z}_S)$ such that $F_{A^{-1}} \in \mathbb{Z}_S[X,Y]$. There is a prime $p \notin S$ such that $A \notin \mathrm{GL}_2(\mathbb{Z}_p)$, while $F_{A^{-1}} \in \mathbb{Z}_p[X,Y]$. Hence F is not $\mathbb{Z}_p$-minimal.

Now assume that F is not $\mathbb{Z}_p$-minimal for some prime $p \notin S$. We have to prove that F is not $\mathbb{Z}_S$-minimal. By assumption, there are a binary form $G \in \mathbb{Z}_p[X,Y]$ and a matrix $A \in \mathrm{NS}_2(\mathbb{Z}_p) \setminus \mathrm{GL}_2(\mathbb{Z}_p)$ such that $F = G_A$. We have $A = UB$, where $U \in \mathrm{GL}_2(\mathbb{Z}_p)$ and

$$B = \begin{pmatrix} p^{\theta_1} & b \\ 0 & p^{\theta_2} \end{pmatrix}$$

with $\theta_1, \theta_2 \in \mathbb{Z}_{\geq 0}$ and $b \in \mathbb{Z}$. Let $H := G_U$. Then $F = H_B$. The binary form H belongs to $\mathbb{Q}[X,Y]$ since $B \in \mathrm{GL}_2(\mathbb{Q})$. Further, $H \in \mathbb{Z}_p[X,Y]$ since H is $\mathbb{Z}_p$-equivalent to G, and for every prime $q \notin S \cup \{p\}$ we have $H \in \mathbb{Z}_q[X,Y]$ since $B \in \mathrm{GL}_2(\mathbb{Z}_q)$. Hence $H \in \mathbb{Z}_S[X,Y]$. This shows that indeed F is not $\mathbb{Z}_S$-minimal. ∎

7. Equivalence over the algebraic closure. Let $S = \{p_1, \dots, p_t\}$ be a finite set of primes, $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$ and $\overline{\mathbb{Z}}_S$ the integral closure of $\mathbb{Z}_S$ in $\overline{\mathbb{Q}}$. By a *finitely generated $\overline{\mathbb{Z}}_S$-fractional ideal* we mean a finitely generated $\overline{\mathbb{Z}}_S$-submodule of $\overline{\mathbb{Q}}$. The non-zero finitely generated $\overline{\mathbb{Z}}_S$-fractional ideals form a group under multiplication. Those $\overline{\mathbb{Z}}_S$-fractional ideals generated by finitely many elements from a number field K form a subgroup. Every finitely generated $\overline{\mathbb{Z}}_S$-fractional ideal is principal. We denote by $[a_1, \dots, a_r]$ the fractional $\overline{\mathbb{Z}}_S$-ideal generated by $a_1, \dots, a_r$. For a polynomial P with coefficients in $\overline{\mathbb{Q}}$ we denote by $[P]$ the $\overline{\mathbb{Z}}_S$-fractional ideal generated by the coefficients of P.

In this section we estimate the number of $\overline{\mathbb{Q}}$-equivalence classes containing the pairs of augmented forms with (5.1)–(5.4). In fact, we prove slightly more and we use this in Section 8 to complete the proof of Proposition 5.2.

We introduce some notation. Let $m \geq 3$, $n \geq 3$, let φ be a $G_{\mathbb{Q}}$-action on $\{1, \dots, m\}$ and ψ a $G_{\mathbb{Q}}$-action on $\{1, \dots, n\}$. Let

$$F^* = (F, (\beta_1 : \alpha_1), \dots, (\beta_m : \alpha_m)), \quad G^* = (G, (\delta_1 : \gamma_1), \dots, (\delta_n : \gamma_n)) \tag{7.1}$$

be a pair of augmented forms with (5.1)–(5.4). Thus,

$$F = \lambda \prod_{i=1}^{m} (\alpha_i X - \beta_i Y), \qquad G = \mu \prod_{j=1}^{n} (\gamma_j X - \delta_j Y) \tag{7.2}$$

where $\lambda, \mu, \alpha_i, \beta_i, \gamma_j, \delta_j \in \overline{\mathbb{Q}}^*$.

We define the $\overline{\mathbb{Z}}_S$-fractional ideals

$$\mathfrak{d}_{ij}(F^*, G^*) := \frac{[\alpha_i \delta_j - \beta_i \gamma_j]}{[\alpha_i, \beta_i] \cdot [\gamma_j, \delta_j]} \quad (i = 1, \dots, m,\ j = 1, \dots, n) \tag{7.3}$$

and the numbers

$$\theta_{i_1,i_2;j_1,j_2}(F^*,G^*) := \frac{(\alpha_{i_1}\delta_{j_1}-\beta_{i_1}\gamma_{j_1})(\alpha_{i_2}\delta_{j_2}-\beta_{i_2}\gamma_{j_2})}{(\alpha_{i_1}\delta_{j_2}-\beta_{i_1}\gamma_{j_2})(\alpha_{i_2}\delta_{j_1}-\beta_{i_2}\gamma_{j_1})} \quad (i_1,i_2\in\{1,\dots,m\},\ j_1,j_2\in\{1,\dots,n\}). \tag{7.4}$$

Both these fractional ideals and these numbers are independent of the choice of λ,μ and the $\alpha_i,\beta_i,\gamma_j,\delta_j$.

Since $[\alpha_i\delta_j-\beta_i\gamma_j]\subseteq[\alpha_i,\beta_i]\cdot[\gamma_j,\delta_j]$ we have $\mathfrak{d}_{ij}(F^*,G^*)\subseteq\overline{\mathbb{Z}}_S$, i.e., $\mathfrak{d}_{ij}(F^*,G^*)$ is a finitely generated ideal of $\overline{\mathbb{Z}}_S$.

By applying Gauss' lemma to (7.2) and using our assumption (5.2) we obtain

$$[\lambda]\prod_{i=1}^{m}[\alpha_i,\beta_i]=[F]=[1],\qquad [\mu]\prod_{j=1}^{n}[\gamma_j,\delta_j]=[G]=[1], \tag{7.5}$$

while by (2.1), (5.4) we have

$$[R(F,G)]=[\lambda]^n[\mu]^m\prod_{i=1}^{m}\prod_{j=1}^{n}[\alpha_i\delta_j-\beta_i\gamma_j]=[c].$$

Hence

$$\prod_{i=1}^{m}\prod_{j=1}^{n}\mathfrak{d}_{ij}(F^*,G^*)=[c]. \tag{7.6}$$

We have some freedom to choose λ,μ and the $\alpha_i,\beta_i,\ \gamma_j,\delta_j$ in (7.2). By our assumption (5.1) we can choose these numbers such that

$$\begin{cases}\lambda,\mu\in\mathbb{Q}^*,\\ \sigma(\alpha_i)=\alpha_{\varphi(\sigma)(i)},\quad \sigma(\beta_i)=\beta_{\varphi(\sigma)(i)} & \text{for } \sigma\in G_{\mathbb{Q}},\ i=1,\dots,m,\\ \sigma(\gamma_j)=\gamma_{\psi(\sigma)(j)},\quad \sigma(\delta_j)=\delta_{\psi(\sigma)(j)} & \text{for } \sigma\in G_{\mathbb{Q}},\ j=1,\dots,n.\end{cases} \tag{7.7}$$

For the moment we keep this choice; later we will make another.

We prove the following lemma:

LEMMA 7.1. *If (F^*,G^*) runs through the pairs of augmented forms with* (5.1)–(5.4), *then the tuple $(\mathfrak{d}_{ij}(F^*,G^*) : i=1,\dots,m,\ j=1,\dots,n)$ runs through a collection of cardinality at most*

$$\prod_{p\mid c}\binom{\operatorname{ord}_p(c)+mn}{mn}.$$

Proof. $G_{\mathbb{Q}}$ acts on $\{1,\dots,m\}\times\{1,\dots,n\}$ by means of $\varphi\times\psi$ which is given by $(\varphi\times\psi)(\sigma)(i,j)=(\varphi(\sigma)(i),\psi(\sigma)(j))$ for $\sigma\in G_{\mathbb{Q}}$, $i=1,\dots,m$, $j=1,\dots,n$. Let $\mathcal{C}_1,\dots,\mathcal{C}_u$ be the orbits of $\{1,\dots,m\}\times\{1,\dots,n\}$ under this action and choose a representative $(i_w,j_w)\in\mathcal{C}_w$ for $w=1,\dots,u$. Further,

define the field M_w by

$$\mathrm{Gal}(\overline{\mathbb{Q}}/M_w) = \{\sigma \in G_{\mathbb{Q}} : \varphi(\sigma)(i_w) = i_w,\ \psi(\sigma)(j_w) = j_w\}. \tag{7.8}$$

Let (F^*, G^*) be a pair with (5.1)–(5.4). Then, by (7.7),

$$\sigma(\mathfrak{d}_{ij}(F^*, G^*)) = \mathfrak{d}_{\varphi(\sigma)(i),\psi(\sigma)(j)}(F^*, G^*)$$

for $\sigma \in G_{\mathbb{Q}}$, $i = 1, \dots, m$, $j = 1, \dots, n$. Hence the tuple $(\mathfrak{d}_{ij}(F^*, G^*) : i = 1, \dots, m,\ j = 1, \dots, n)$ is determined by the tuple $(\mathfrak{d}_{i_w j_w}(F^*, G^*) : w = 1, \dots, u)$. Furthermore, by (7.7), $\mathfrak{d}_{i_w j_w}(F^*, G^*)$ is generated by elements from M_w, and the conjugates of $\mathfrak{d}_{i_w j_w}(F^*, G^*)$ over $\mathbb{Q}$ are precisely the ideals $\mathfrak{d}_{ij}(F^*, G^*)$ with $(i, j) \in \mathcal{C}_w$. Thus, we can rewrite (7.6) as

$$\prod_{w=1}^{u} N_{M_w/\mathbb{Q}}(\mathfrak{d}_w) = [c], \tag{7.9}$$

where $\mathfrak{d}_w$ is the ideal in the integral closure of $\mathbb{Z}_S$ in M_w determined by $\mathfrak{d}_{i_w j_w}(F^*, G^*) = \mathfrak{d}_w \overline{\mathbb{Z}}_S$ for $w = 1, \dots, u$.

Let p be a prime with $p \mid c$. Let $\mathfrak{p}_{w1}, \dots, \mathfrak{p}_{w,g(w)}$ be the prime ideals of M_w above p and $f_{w1}, \dots, f_{w,g(w)}$ their respective residue class degrees. Let x_{wj} $(j = 1, \dots, g(w))$ be the exponent of $\mathfrak{p}_{wj}$ in the prime ideal factorization of $\mathfrak{d}_w$. Then the exponent of p in the prime number factorization of $N_{M_w/\mathbb{Q}}(\mathfrak{d}_w)$ is $\sum_{j=1}^{g(w)} f_{wj} x_{wj}$. So, by (7.9),

$$\sum_{w=1}^{u} \sum_{j=1}^{g(w)} f_{wj} x_{wj} = \mathrm{ord}_p(c).$$

Let $\mathbf{x}(p) := (x_{wj} : w = 1, \dots, u,\ j = 1, \dots, g(w))$. Then $\mathbf{x}(p)$ consists of $\sum_{w=1}^{u} g(w) \le \sum_{w=1}^{u} [M_w : \mathbb{Q}] = \sum_{w=1}^{u} \#\mathcal{C}_w = mn$ non-negative integers, and moreover,

$$\sum_{w=1}^{u} \sum_{j=1}^{g(w)} x_{wj} \le \mathrm{ord}_p(c).$$

Hence for $\mathbf{x}(p)$ there are at most

$$\binom{\mathrm{ord}_p(c) + \sum_{w=1}^{u} g(w)}{\sum_{w=1}^{u} g(w)} \le \binom{\mathrm{ord}_p(c) + mn}{mn} =: N_p$$

possibilities.

The tuples $\mathbf{x}(p)$ $(p \mid c)$ determine the ideals $\mathfrak{d}_w$, hence also $\mathfrak{d}_{i_w j_w}(F^*, G^*)$ $(w = 1, \dots, u)$. So by what was explained above, they determine the ideals $\mathfrak{d}_{ij}(F^*, G^*)$ $(i = 1, \dots, m, j = 1, \dots, n)$ as well. This implies that if (F^*, G^*) runs through all pairs with (5.1)–(5.4), then the tuple $(\mathfrak{d}_{ij}(F^*, G^*) : i = 1, \dots, m,\ j = 1, \dots, n)$ runs through a collection of cardinality at most $\prod_{p \mid c} N_p$. ∎

We fix a tuple $(\mathfrak{d}_{ij} : i = 1, \dots, m,\ j = 1, \dots, n)$ of ideals of $\overline{\mathbb{Z}}_S$, and consider the set

$$\mathcal{I}(\{\mathfrak{d}_{ij}\})$$

consisting of the pairs (F^*, G^*) that satisfy (5.1)–(5.4) and for which

$$\mathfrak{d}_{ij}(F^*, G^*) = \mathfrak{d}_{ij} \quad \text{for } i = 1, \dots, m,\ j = 1, \dots, n. \tag{7.10}$$

LEMMA 7.2. *For each $i_1, i_2 \in \{1, \dots, m\}$ with $i_1 \neq i_2$ and $j_1, j_2 \in \{1, \dots, n\}$ with $j_1 \neq j_2$, there is a subgroup $\Gamma_{i_1,i_2;j_1,j_2}$ of rank at most*

$$4mn(t+1) - 3 \tag{7.11}$$

such that for every pair $(F^*, G^*) \in \mathcal{I}(\{\mathfrak{d}_{ij}\})$ we have

$$\theta_{i_1,i_2;j_1,j_2}(F^*, G^*) \in \Gamma_{i_1,i_2;j_1,j_2}. \tag{7.12}$$

Proof. For $i = 1, \dots, m,\ j = 1, \dots, n$ define the number fields K_i, L_j, M_{ij} by

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{Q}}/K_i) &= \{\sigma \in G_{\mathbb{Q}} : \varphi(\sigma)(i) = i\}, \\ \mathrm{Gal}(\overline{\mathbb{Q}}/L_j) &= \{\sigma \in G_{\mathbb{Q}} : \psi(\sigma)(j) = j\}, \\ \mathrm{Gal}(\overline{\mathbb{Q}}/M_{ij}) &= \{\sigma \in G_{\mathbb{Q}} : \varphi(\sigma)(i) = i,\ \psi(\sigma)(j) = j\}. \end{aligned}$$

Let H be a positive common multiple of the class numbers of these fields.

Assume that the set $\mathcal{I}(\{\mathfrak{d}_{ij}\})$ is non-empty and pick a pair (F^*, G^*) from this set. Let $\alpha_i, \beta_i, \gamma_j, \delta_j$ be as in (7.1), (7.2), (7.7). Then there are $\lambda_i \in K_i$, $\mu_j \in L_j$ such that

$$[\alpha_i, \beta_i]^H = [\lambda_i], \quad [\gamma_j, \delta_j]^H = [\mu_j] \quad \text{for } i = 1, \dots, m,\ j = 1, \dots, n. \tag{7.13}$$

By (7.7), the ideal $\mathfrak{d}_{ij}$ is generated by elements from M_{ij}. Hence there are $\nu_{ij} \in M_{ij}$ such that

$$\mathfrak{d}_{ij}^H = [\nu_{ij}] \quad \text{for } i = 1, \dots, m,\ j = 1, \dots, n. \tag{7.14}$$

Let Γ_{ij} be the unit group of the integral closure of $\mathbb{Z}_S$ in M_{ij}. Then

$$\operatorname{rank} \Gamma_{ij} \le [M_{ij} : \mathbb{Q}](t+1) - 1 \le mn(t+1) - 1. \tag{7.15}$$

By (7.13), (7.14), (7.10) we have $[(\alpha_i\delta_j - \beta_i\gamma_j)^H/\lambda_i\mu_j] = \mathfrak{d}_{ij}^H = [\nu_{ij}]$, hence

$$\frac{(\alpha_i\delta_j - \beta_i\gamma_j)^H}{\lambda_i\mu_j} = \nu_{ij}\varepsilon_{ij} \quad \text{with } \varepsilon_{ij} \in \Gamma_{ij} \quad \text{for } i = 1, \dots, m,\ j = 1, \dots, n. \tag{7.16}$$

Then for $i_1, i_2 \in \{1, \dots, m\}$, $j_1, j_2 \in \{1, \dots, n\}$ with $i_1 \neq i_2$, $j_1 \neq j_2$ we have

$$\theta_{i_1,i_2;j_1,j_2}(F^*, G^*)^H = \left(\frac{\nu_{i_1,j_1}\nu_{i_2,j_2}}{\nu_{i_1,j_2}\nu_{i_2,j_1}}\right)\left(\frac{\varepsilon_{i_1,j_1}\varepsilon_{i_2,j_2}}{\varepsilon_{i_1,j_2}\varepsilon_{i_2,j_1}}\right) \tag{7.17}$$

(note that the terms λ_i, μ_j cancel). Hence $\theta_{i_1,i_2;j_1,j_2}(F^*, G^*)^H$ belongs to the group generated by $\nu_{i_1,j_1}\nu_{i_2,j_2}/\nu_{i_1,j_2}\nu_{i_2,j_1}$ and by Γ_{i_p,j_q} $(p, q = 1, 2)$, which has rank at most $4\{mn(t+1)-1\}+1 \le 4mn(t+1)-3$. But then $\theta_{i_1,i_2;j_1,j_2}(F^*, G^*)$

belongs to the set of Hth roots of the elements of this group, which is also a group of rank at most $4mn(t+1)-3$. This proves Lemma 7.2. ∎

LEMMA 7.3. *Let $i_1, i_2 \in \{1,\dots,m\}$, $j_1, j_2 \in \{1,\dots,n\}$ with $i_1 \neq i_2$, $j_1 \neq j_2$. Then if (F^*, G^*) runs through $\mathcal{I}(\{\mathfrak{d}_{ij}\})$, the quantity $\theta_{i_1,i_2;j_1,j_2}(F^*, G^*)$ runs through a set of cardinality at most*

$$e^{30^{15}\{16mn(t+1)-11\}}.$$

Proof. Pick $(F^*, G^*) \in \mathcal{I}(\{\mathfrak{d}_{ij}\})$, let $\alpha_i, \beta_i, \gamma_j, \delta_j$ be as in (7.1), (7.2), (7.7), write $\theta_{i_1,i_2;j_1,j_2}$ for $\theta_{i_1,i_2;j_1,j_2}(F^*, G^*)$ and define $\Delta_{ij} := \alpha_i\delta_j - \beta_i\gamma_j$. Then

$$\theta_{i_1,i_2;j_1,j_2} = \frac{\Delta_{i_1,j_1}\Delta_{i_2,j_2}}{\Delta_{i_1,j_2}\Delta_{i_2,j_1}}.$$

Choose $i_3 \in \{1,\dots,m\} \setminus \{i_1, i_2\}$, $j_3 \in \{1,\dots,n\} \setminus \{j_1, j_2\}$. Then

$$\begin{vmatrix} \Delta_{i_1j_1} & \Delta_{i_1j_2} & \Delta_{i_1j_3} \\ \Delta_{i_2j_1} & \Delta_{i_2j_2} & \Delta_{i_2j_3} \\ \Delta_{i_3j_1} & \Delta_{i_3j_2} & \Delta_{i_3j_3} \end{vmatrix} = 0$$

hence

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & \theta_{i_1,i_2;j_1,j_2} & \theta_{i_1,i_2;j_1,j_3} \\ 1 & \theta_{i_1,i_3;j_1,j_2} & \theta_{i_1,i_3;j_1,j_3} \end{vmatrix} = 0. \tag{7.18}$$

From the fact that $(\beta_i : \alpha_i)$ $(i = i_1, i_2, i_3)$, $(\delta_j : \gamma_j)$ $(j = j_1, j_2, j_3)$ are distinct, it follows that each 2×2-subdeterminant is non-zero. Now by applying Lemma 3.3 to (7.18), invoking Lemma 7.2, it follows immediately that if (F^*, G^*) runs through $\mathcal{I}(\{\mathfrak{d}_{ij}\})$, then $\theta_{i_1,i_2;j_1,j_2}(F^*, G^*)$ runs through a set of cardinality at most

$$e^{30^{15}(4\{4mn(t+1)-3\}+1)} = e^{30^{15}\{16mn(t+1)-11\}}. \ ∎$$

We now come to the main result of this section.

LEMMA 7.4. *There is a collection $\mathcal{I} \subset \mathcal{A}(\overline{\mathbb{Z}}_S, m) \times \mathcal{A}(\overline{\mathbb{Z}}_S, n)$ of cardinality at most*

$$e^{10^{24}(m+n)mn(t+1)} \prod_{p|c} \binom{\mathrm{ord}_p(c) + mn}{mn} \tag{7.19}$$

with the following property: for every pair (F^*, G^*) with (5.1)–(5.4), there are $(F_0^*, G_0^*) \in \mathcal{I}$, $A \in \mathrm{NS}_2(\overline{\mathbb{Z}}_S)$ and $\varepsilon, \eta \in \overline{\mathbb{Z}}_S^*$ such that

$$F^* = \varepsilon(F_0^*)_A, \qquad G^* = \eta(G_0^*)_{(\det A)^{-1}A}. \tag{7.20}$$

Proof. Our pair (F_0^*, G_0^*) will depend only on the data

$$\begin{cases} \mathfrak{d}_{ij}(F^*, G^*), & i = 1, \dots, m,\ j = 1, \dots, n, \\ \theta_{i,1;2,1}(F^*, G^*), & i = 2, \dots, m, \\ \theta_{1,2;1,j}(F^*, G^*), & j = 2, \dots, n, \end{cases} \tag{7.21}$$

where $\mathfrak{d}_{ij}(F^*, G^*)$ are the ideals given by (7.3) and $\theta_{i_1,j_1;i_2,j_2}(F^*, G^*)$ are the numbers given by (7.4). By Lemmata 7.1, 7.3, if (F^*, G^*) runs through all pairs with (5.1)–(5.4), the tuple given by (7.21) runs through a set of cardinality at most

$$\left\{\prod_{p|c} \binom{\mathrm{ord}_p(c) + mn}{mn}\right\} e^{30^{15}\{16mn(t+1)-11\}(m-1+n-1)} < e^{10^{24}(m+n)mn(t+1)} \prod_{p|c} \binom{\mathrm{ord}_p(c) + mn}{mn}.$$

Hence the number of possibilities for (F_0^*, G_0^*) is bounded above by (7.19).

Let (F^*, G^*) be a pair with (5.1)–(5.4). Put

$$\theta_{i_1,i_2;j_1,j_2} := \theta_{i_1,i_2;j_1,j_2}(F^*, G^*), \quad \mathfrak{d}_{ij} := \mathfrak{d}_{ij}(F^*, G^*).$$

Further, choose $\delta_{ij} \in \overline{\mathbb{Z}}_S$ such that $\mathfrak{d}_{ij} = [\delta_{ij}]$. Therefore, δ_{ij} depends only on (7.21).

By assumption (5.2), Gauss' lemma and the fact that every finitely generated ideal of $\overline{\mathbb{Z}}_S$ is principal, we can express F^* and G^* as

$$F^* = (F, (\beta_1 : \alpha_1), \dots, (\beta_m : \alpha_m)), \quad G^* = (G, (\delta_1 : \gamma_1), \dots, (\delta_n : \gamma_n)),$$

where

$$\begin{cases} F = \displaystyle\prod_{i=1}^{m} (\alpha_i X - \beta_i Y), & [\alpha_i, \beta_i] = [1] \quad \text{for } i = 1, \dots, m, \\ G = \displaystyle\prod_{j=1}^{n} (\gamma_j X - \delta_j Y), & [\gamma_j, \delta_j] = [1] \quad \text{for } j = 1, \dots, n. \end{cases} \tag{7.22}$$

Put

$$\Delta_{ij} := \alpha_i \delta_j - \beta_i \gamma_j \quad (i = 1, \dots, m,\ j = 1, \dots, n).$$

Then with the decomposition of F^*, G^* in (7.22), definition (7.3) becomes

$$\mathfrak{d}_{ij} = [\Delta_{ij}].$$

Hence

$$\Delta_{ij} = \delta_{ij} \varepsilon_{ij} \quad \text{with } \varepsilon_{ij} \in \overline{\mathbb{Z}}_S^* \quad \text{for } i = 1, \dots, m,\ j = 1, \dots, n. \tag{7.23}$$

Further, (7.4) can be rewritten as

$$\theta_{i_1,i_2;j_1,j_2} = \frac{\Delta_{i_1,j_1} \Delta_{i_2,j_2}}{\Delta_{i_1,j_2} \Delta_{i_2,j_1}} \quad \text{for } i_1, i_2 \in \{1, \dots, m\},\ j_1, j_2 \in \{1, \dots, n\}. \tag{7.24}$$

Define the following $\overline{\mathbb{Q}}$-linear subspace of $\overline{\mathbb{Q}}^m$:

$$V = \left\{ \left(\frac{\alpha_1 x - \beta_1 y}{\Delta_{11}}, \dots, \frac{\alpha_m x - \beta_m y}{\Delta_{m1}} \right) : x, y \in \overline{\mathbb{Q}} \right\}. \tag{7.25}$$

By substituting $(x, y) = (\delta_1, \gamma_1)$, $(x, y) = \frac{\Delta_{11}}{\Delta_{12}}(\delta_2, \gamma_2)$ respectively, we obtain a basis of V, that is,

$$(1, \dots, 1),$$
$$\left(1, \frac{\Delta_{11}\Delta_{22}}{\Delta_{21}\Delta_{12}}, \frac{\Delta_{11}\Delta_{32}}{\Delta_{31}\Delta_{12}}, \dots, \frac{\Delta_{11}\Delta_{m2}}{\Delta_{m1}\Delta_{12}}\right) = (1, \theta_{1,2;1,2}, \theta_{1,3;1,2}, \dots, \theta_{1,m;1,2})$$

where the last identity follows from (7.24). This basis of V, hence V itself, depends only on (7.21).

Consider the $\overline{\mathbb{Z}}_S$-module

$$\mathcal{M} = \{(\xi_1, \dots, \xi_m) \in V : \delta_{11}\xi_1 \in \overline{\mathbb{Z}}_S, \dots, \delta_{m1}\xi_m \in \overline{\mathbb{Z}}_S\}. \tag{7.26}$$

Since every finitely generated ideal of $\overline{\mathbb{Z}}_S$ is principal, $\mathcal{M}$ is a free $\overline{\mathbb{Z}}_S$-module of rank 2. Choose a basis $\{(a_1, \dots, a_m), (b_1, \dots, b_m)\}$ of $\mathcal{M}$. The module $\mathcal{M}$, hence this basis, depends only on (7.21). Now define

$$F_0 := \prod_{i=1}^{m} \delta_{i1} \cdot \prod_{i=1}^{m} (a_i X - b_i Y), \qquad F_0^* := (F_0, (b_1 : a_1), \dots, (b_m : a_m)).$$

Then F_0^* depends only on (7.21). Further, $F_0 \in \overline{\mathbb{Z}}_S[X, Y]$, which implies $F_0^* \in \mathcal{A}(\overline{\mathbb{Z}}_S, m)$.

By (7.23), $\left(\frac{\alpha_1}{\Delta_{11}}, \dots, \frac{\alpha_m}{\Delta_{m1}}\right) \in \mathcal{M}$. Hence there are $u_{11}, u_{12}, u_{21}, u_{22} \in \overline{\mathbb{Z}}_S$ such that

$$\begin{cases} \left(\dfrac{\alpha_1}{\Delta_{11}}, \dots, \dfrac{\alpha_m}{\Delta_{m1}} \right) = u_{11}(a_1, \dots, a_m) - u_{21}(b_1, \dots, b_m), \\ \left(\dfrac{\beta_1}{\Delta_{11}}, \dots, \dfrac{\beta_m}{\Delta_{m1}} \right) = -u_{12}(a_1, \dots, a_m) + u_{22}(b_1, \dots, b_m). \end{cases} \tag{7.27}$$

Set $A := \left(\begin{smallmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{smallmatrix}\right)$. Thus, by (7.23),

$$\begin{aligned} (F_0)_A &= \left(\prod_{i=1}^{m} \delta_{i1} \right) \cdot \prod_{i=1}^{m} (a_i(u_{11}X + u_{12}Y) - b_i(u_{21}X + u_{22}Y)) \\ &= \prod_{i=1}^{m} \frac{\delta_{i1}}{\Delta_{i1}} \cdot \prod_{i=1}^{m} (\alpha_i X - \beta_i Y) = \left(\prod_{i=1}^{m} \varepsilon_{i1}^{-1} \right) \cdot F. \end{aligned}$$

Further, $(b_i : a_i) = \langle A^{-1} \rangle (\beta_i : \alpha_i)$ for $i = 1, \dots, m$. So

$$F^* = \varepsilon (F_0^*)_A \quad \text{with } \varepsilon := \prod_{i=1}^{m} \varepsilon_{i1} \in \overline{\mathbb{Z}}_S^*. \tag{7.28}$$

We now construct G_0^*. Solve c_j, d_j $(j = 1, \dots, n)$ from

$$a_1 d_j - b_1 c_j = 1, \quad a_2 d_j - b_2 c_j = \theta_{2,1;j,1} \quad (j = 1, \dots, n) \tag{7.29}$$

and define

$$G_0 := \prod_{j=1}^{n} \frac{\delta_{1j}}{\delta_{11}} \cdot \prod_{j=1}^{n} (c_j X - d_j Y), \quad G_0^* := (G_0, (d_1 : c_1), \dots, (d_n : c_n)).$$

Then G_0^* is determined by (7.21). We have

$$\begin{pmatrix} a_1 & -b_1 \\ a_2 & -b_2 \end{pmatrix} \begin{pmatrix} d_j \\ c_j \end{pmatrix} = \begin{pmatrix} 1 \\ \theta_{2,1;j,1} \end{pmatrix} \quad \text{for } j = 1, \dots, n$$

by (7.29), and

$$\begin{pmatrix} a_1 & -b_1 \\ a_2 & -b_2 \end{pmatrix} A = \begin{pmatrix} \frac{\alpha_1}{\Delta_{11}} & -\frac{\beta_1}{\Delta_{11}} \\ \frac{\alpha_2}{\Delta_{21}} & -\frac{\beta_2}{\Delta_{21}} \end{pmatrix}$$

by (7.27). Hence

$$\begin{pmatrix} \frac{\alpha_1}{\Delta_{11}} & -\frac{\beta_1}{\Delta_{11}} \\ \frac{\alpha_2}{\Delta_{21}} & -\frac{\beta_2}{\Delta_{21}} \end{pmatrix} A^{-1} \begin{pmatrix} d_j \\ c_j \end{pmatrix} = \begin{pmatrix} 1 \\ \frac{\Delta_{2j}\Delta_{11}}{\Delta_{21}\Delta_{1j}} \end{pmatrix} \quad \text{for } j = 1, \dots, n.$$

On the other hand,

$$\begin{pmatrix} \frac{\alpha_1}{\Delta_{11}} & -\frac{\beta_1}{\Delta_{11}} \\ \frac{\alpha_2}{\Delta_{21}} & -\frac{\beta_2}{\Delta_{21}} \end{pmatrix} \cdot \begin{pmatrix} \delta_j \\ \gamma_j \end{pmatrix} = \begin{pmatrix} \frac{\Delta_{1j}}{\Delta_{11}} \\ \frac{\Delta_{2j}}{\Delta_{11}} \end{pmatrix} \quad \text{for } j = 1, \dots, n.$$

Hence $A^{-1}\binom{d_j}{c_j} = \frac{\Delta_{11}}{\Delta_{1j}}\binom{\delta_j}{\gamma_j}$ for $j = 1, \dots, n$. Now, by (7.23),

$$\begin{aligned}
(G_0)_A &= \prod_{j=1}^{n} \frac{\delta_{1j}}{\delta_{11}} \cdot \prod_{j=1}^{n} (c_j(u_{11}X + u_{12}Y) - d_j(u_{21}X + u_{22}Y)) \\
&= \prod_{j=1}^{n} \frac{\delta_{1j}}{\delta_{11}} \cdot \prod_{j=1}^{n} \{(u_{11}c_j - u_{21}d_j)X - (-u_{12}c_j + u_{22}d_j)Y\} \\
&= (\det A)^n \prod_{j=1}^{n} \frac{\delta_{1j}}{\delta_{11}} \cdot \prod_{j=1}^{n} \left(\frac{\Delta_{11}}{\Delta_{1j}} (\gamma_j X - \delta_j Y) \right) = (\det A)^n \left(\prod_{j=1}^{n} \frac{\varepsilon_{11}}{\varepsilon_{1j}} \right) G.
\end{aligned}$$

Thus, $G = \eta(G_0)_{(\det A)^{-1}A}$ with $\eta := \prod_{j=1}^{n}(\varepsilon_{11}/\varepsilon_{1j}) \in \overline{\mathbb{Z}}_S^*$. Now $G_0 = \eta^{-1} G_{(\det A)A^{-1}} \in \overline{\mathbb{Z}}_S[X, Y]$, hence $G_0^* \in \mathcal{A}(\overline{\mathbb{Z}}_S, n)$. Further, $(\delta_j : \gamma_j) = \langle A^{-1} \rangle (d_j : c_j)$ for $j = 1, \dots, n$. Hence

$$G^* = \eta(G_0^*)_{(\det A)^{-1}A} \quad \text{with } \eta \in \overline{\mathbb{Z}}_S^*.$$

Together with (7.28) this gives (7.20). Lemma 7.4 is proved. ∎

8. Proof of Proposition 5.2. Proposition 5.2 is deduced from Lemma 7.4 above and the following local lemma.

LEMMA 8.1. *Let p be a prime, $c \in \mathbb{Z}_p$ with $c \neq 0$, and φ_p, ψ_p be $G_{\mathbb{Q}_p}$-actions of $\{1,\dots,m\}$, $\{1,\dots,n\}$, respectively. Further, let $F_0^* \in \mathcal{A}(\overline{\mathbb{Z}}_p, m)$, $G_0^* \in \mathcal{A}(\overline{\mathbb{Z}}_p, n)$. Then the collection of pairs of augmented forms $F^* = (F, \dots)$, $G^* = (G, \dots)$ such that*

(8.1) $F^* = \varepsilon(F_0^*)_A, G^* = \eta(G_0^*)_{(\det A)^{-1}A}$ *for some* $A \in \mathrm{NS}_2(\overline{\mathbb{Z}}_p)$, $\varepsilon, \eta \in \overline{\mathbb{Z}}_p^*$,

(8.2) $F^* \in \mathcal{A}(\mathbb{Z}_p, \varphi_p)$, $G^* \in \mathcal{A}(\mathbb{Z}_p, \psi_p)$,

(8.3) F, G *are* $\mathbb{Z}_p$*-primitive*,

(8.4) F *is* $\mathbb{Z}_p$*-minimal*,

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

is contained in at most one $\mathbb{Z}_p$-equivalence class if $p \nmid c$, and in the union of at most two $\mathbb{Z}_p$-equivalence classes if $p \mid c$.

We first deduce Proposition 5.2.

Proof of Proposition 5.2. Let $S = \{p_1, \dots, p_t\}$ and c, m, n, φ, ψ be as in the statement of Proposition 5.2.

Let (F_0^*, G_0^*) be a pair of augmented forms from the set $\mathcal{I}$ from Lemma 7.4. Denote by $\mathcal{V}(F_0^*, G_0^*)$ the set of pairs of augmented forms (F^*, G^*) that satisfy (5.1)–(5.4) and for which there are $\varepsilon, \eta \in \overline{\mathbb{Z}}_S^*$, $A \in \mathrm{NS}_2(\overline{\mathbb{Z}}_S^*)$ such that (7.20) holds. Pick $(F^*, G^*) \in \mathcal{V}(F_0^*, G_0^*)$. Let p be a prime outside S. We view $\overline{\mathbb{Q}}$ as a subfield of $\overline{\mathbb{Q}}_p$. Clearly, (F^*, G^*) satisfies (8.1), (8.3), (8.5). Further, this pair satisfies (8.2) where φ_p, ψ_p are the $G_{\mathbb{Q}_p}$-actions of $\{1,\dots,m\}$, $\{1,\dots,n\}$ induced by φ, ψ. Lastly, by Lemma 6.2 it also satisfies (8.4). So the pairs $(F^*, G^*) \in \mathcal{V}(F_0^*, G_0^*)$ satisfy (8.1)–(8.5) for every prime $p \notin S$.

Now Lemmata 8.1 and 6.1 imply that $\mathcal{V}(F_0^*, G_0^*)$ is contained in the union of at most $2^{\omega(c)}$ $\mathbb{Z}_S$-equivalence classes. So the total number of $\mathbb{Z}_S$-equivalence classes of pairs (F^*, G^*) with (5.1)–(5.4) is bounded above by $2^{\omega(c)}$ multiplied with the bound from Lemma 7.4. The resulting bound is precisely that of Proposition 5.2. ∎

Proof of Lemma 8.1. Let p be a prime. Given $a_1, \dots, a_r \in \overline{\mathbb{Q}}_p$, we denote by $[a_1, \dots, a_r]$ the $\overline{\mathbb{Z}}_p$-fractional ideal generated by $a_1, \dots, a_r$. Every finitely generated $\overline{\mathbb{Z}}_p$-fractional ideal is principal. For a polynomial P with coefficients in $\overline{\mathbb{Z}}_p$, denote by $[P]$ the $\overline{\mathbb{Z}}_p$-fractional ideal generated by the coefficients of P. By Gauss' lemma, we may express F_0^*, G_0^* as

$$F_0^* = (F_0, (\beta_{10} : \alpha_{10}), \dots, (\beta_{m0} : \alpha_{m0})),$$
$$G_0^* = (G_0, (\delta_{10} : \gamma_{10}), \dots, (\delta_{n0} : \gamma_{n0}))$$

where

$$\text{(8.6)}\qquad \begin{cases} F_0 = \prod_{i=1}^{m}(\alpha_{i0}X - \beta_{i0}Y), & [\alpha_{i0}, \beta_{i0}] \subseteq [1], \\ G_0 = \prod_{j=1}^{n}(\gamma_{j0}X - \delta_{j0}Y), & [\gamma_{j0}, \delta_{j0}] \subseteq [1] \end{cases}$$

for $i = 1, \dots, m$, $j = 1, \dots, n$.

The remainder of the proof of Lemma 8.1 is divided into a few lemmata. For the moment, we work with two pairs of augmented forms (F_1^*, G_1^*), (F_2^*, G_2^*) satisfying (8.1)–(8.5) which are not $\mathbb{Z}_p$-equivalent. Just as for F_0^*, G_0^*, we may express $F_1^*, F_2^*, G_1^*, G_2^*$ as

$$\text{(8.7)}\qquad \begin{cases} F_k^* = (F_k, (\beta_{1k} : \alpha_{1k}), \dots, (\beta_{mk} : \alpha_{mk})), \\ G_k^* = (G_k, (\delta_{1k} : \gamma_{1k}), \dots, (\delta_{nk} : \gamma_{nk})) \end{cases}$$

for $k = 1, 2$, with

$$\text{(8.8)}\qquad \begin{cases} F_k = \prod_{i=1}^{m}(\alpha_{ik}X - \beta_{ik}Y), & [\alpha_{ik}, \beta_{ik}] = [1], \\ G_k = \prod_{j=1}^{n}(\gamma_{jk}X - \delta_{jk}Y), & [\gamma_{jk}, \delta_{jk}] = [1] \end{cases}$$

for $i = 1, \dots, m$, $j = 1, \dots, n$, $k = 1, 2$, where the stronger assertions $[\alpha_{ik}, \beta_{ik}] = [1]$, $[\gamma_{jk}, \delta_{jk}] = [1]$ follow from Gauss' lemma and our assumption (8.3) that F_k^*, G_k^* $(k = 1, 2)$ are $\mathbb{Z}_p$-primitive.

LEMMA 8.2. *Let (F_1^*, G_1^*), (F_2^*, G_2^*) be two pairs of augmented forms satisfying* (8.1)–(8.5) *which are not $\mathbb{Z}_p$-equivalent and suppose that they are represented as in* (8.7), (8.8). *Then there are a matrix $B \in \mathrm{NS}_2(\mathbb{Z}_p)$ with $|\det B|_p = p^{-1}$, a number $\zeta \in \mathbb{Q}$ with $0 < \zeta < 1$, and numbers $\lambda, \mu \in \mathbb{Q}_p^*$, $\lambda_i \in \overline{\mathbb{Q}}_p^*$ $(i = 1, \dots, m)$ such that*

$$\text{(8.9)}\quad F_2^* = \lambda (F_1^*)_B, \quad G_2^* = \mu (G_1^*)_{(\det B)^{-1}B} \quad \text{with } |\lambda|_p = p^{m\zeta},\ |\mu|_p = p^{-n\zeta},$$

$$\text{(8.10)}\qquad (\det B) B^{-1} \begin{pmatrix} \beta_{i1} \\ \alpha_{i1} \end{pmatrix} = \lambda_i \begin{pmatrix} \beta_{i2} \\ \alpha_{i2} \end{pmatrix} \quad \text{with } |\lambda_i|_p = p^{-\zeta} \text{ for } i = 1, \dots, m.$$

If moreover $p \nmid c$ then there are $\mu_j \in \overline{\mathbb{Q}}_p^*$ $(j = 1, \dots, n)$ such that

$$\text{(8.11)}\qquad (\det B) B^{-1} \begin{pmatrix} \delta_{j1} \\ \gamma_{j1} \end{pmatrix} = \mu_j \begin{pmatrix} \delta_{j2} \\ \gamma_{j2} \end{pmatrix} \quad \text{with } |\mu_j|_p = p^{\zeta - 1} \text{ for } j = 1, \dots, n.$$

Proof. By (8.1), there are matrices $A_1, A_2 \in \mathrm{NS}_2(\overline{\mathbb{Z}}_p)$ and numbers $\varepsilon_1, \varepsilon_2, \eta_1, \eta_2 \in \overline{\mathbb{Z}}_p^*$ such that

$$\text{(8.12)}\qquad F_k^* = \varepsilon_k (F_0^*)_{A_k}, \quad G_k^* = \eta_k (G_0^*)_{(\det A_k)^{-1}A_k} \quad \text{for } k = 1, 2.$$

This implies $F_2^* = \varepsilon_2\varepsilon_1^{-1}(F_1^*)_{A_1^{-1}A_2}$, $G_2^* = \eta_2\eta_1^{-1}(G_1^*)_{\det(A_1^{-1}A_2)^{-1}A_1^{-1}A_2}$. Then by (8.2) and Lemma 5.1, there are $B \in \mathrm{GL}_2(\mathbb{Q}_p)$, $\kappa \in \overline{\mathbb{Q}}_p^*$ such that $A_1^{-1}A_2 = \kappa B$. Without loss of generality we may assume that $B \in \mathrm{NS}_2(\mathbb{Z}_p)$ and that the entries of B have gcd 1 in $\mathbb{Z}_p$. Define ζ, θ by

$$|\kappa|_p = p^{\zeta}, \quad |\det B|_p = p^{-\theta}. \tag{8.13}$$

Then, on putting $\lambda := \varepsilon_2\varepsilon_1^{-1}\kappa^m$, $\mu := \eta_2\eta_1^{-1}\kappa^{-n}$, we get

$$F_2^* = \lambda(F_1^*)_B, \quad G_2^* = \mu(G_1^*)_{(\det B)^{-1}B} \quad \text{with } |\lambda|_p = p^{m\zeta},\ |\mu|_p = p^{-n\zeta}. \tag{8.14}$$

It is clear that $\lambda, \mu \in \mathbb{Q}_p^*$. If $\theta = 0$ then $B \in \mathrm{GL}_2(\mathbb{Z}_p)$, and also $\lambda, \mu \in \mathbb{Z}_p^*$ since by (8.3) the binary forms F_k, G_k $(k = 1, 2)$ are $\mathbb{Z}_p$-primitive. So if $\theta = 0$ then (F_1^*, G_1^*), (F_2^*, G_2^*) are $\mathbb{Z}_p$-equivalent, contrary to our assumption. The number θ is clearly a non-negative integer. Hence

$$\theta \geq 1. \tag{8.15}$$

By (8.12), (8.6), (8.8) we have

$$(\det A_k)A_k^{-1}\begin{pmatrix}\beta_{i0}\\ \alpha_{i0}\end{pmatrix} = \nu_{ik}\begin{pmatrix}\beta_{ik}\\ \alpha_{ik}\end{pmatrix} \quad \text{for } k = 1, 2,\ i = 1, \dots, m,$$

where $\nu_{ik} \in \overline{\mathbb{Q}}_p^*$. Since $(\det A_k)A_k^{-1} \in \mathrm{NS}_2(\overline{\mathbb{Z}}_p)$ and $[\alpha_{ik}, \beta_{ik}] = [1]$ for $i = 1, \dots, m$, $k = 1, 2$, we have $\nu_{ik} \in \overline{\mathbb{Z}}_p$ for $i = 1, \dots, m$, $k = 1, 2$. Further,

$$(F_0)_{A_k}(X, Y) = \prod_{i=1}^{m}(\nu_{ik}(\alpha_{ik}X - \beta_{ik}Y)) \quad \text{for } k = 1, 2,$$

hence $\prod_{i=1}^m \nu_{ik} = \varepsilon_k^{-1} \in \overline{\mathbb{Z}}_p^*$. Therefore

$$(\det A_k)A_k^{-1}\begin{pmatrix}\beta_{i0}\\ \alpha_{i0}\end{pmatrix} = \nu_{ik}\begin{pmatrix}\beta_{ik}\\ \alpha_{ik}\end{pmatrix} \quad \text{with } \nu_{ik} \in \overline{\mathbb{Z}}_p^* \text{ for } k = 1, 2,\ i = 1, \dots, m. \tag{8.16}$$

On putting $\lambda_i = \nu_{i2}\nu_{i1}^{-1}\kappa^{-1}$ and inserting $A_1^{-1}A_2 = \kappa B$ and (8.13) we obtain

$$(\det B)B^{-1}\begin{pmatrix}\beta_{i1}\\ \alpha_{i1}\end{pmatrix} = \lambda_i\begin{pmatrix}\beta_{i2}\\ \alpha_{i2}\end{pmatrix} \quad \text{with } |\lambda_i|_p = p^{-\zeta} \text{ for } i = 1, \dots, m. \tag{8.17}$$

Since $(\det B)B^{-1} \in \mathrm{NS}_2(\mathbb{Z}_p)$ and since $[\alpha_{i2}, \beta_{i2}] = [1]$ for $i = 1, \dots, m$ in view of (8.8), we have $\zeta \geq 0$. We now show that $\theta = 1$ and $0 < \zeta < 1$. Here we use the fact that F_1, F_2 satisfy (8.4), i.e., that F_1, F_2 are $\mathbb{Z}_p$-minimal.

Since $\mathbb{Z}_p$ is a principal ideal domain and the entries of B have gcd 1, there are $U_1, U_2 \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that

$$B = U_1\begin{pmatrix}1 & 0\\ 0 & p^{\theta}\end{pmatrix}U_2.$$

By inserting this into (8.17) we obtain

$$\begin{pmatrix} 1 & 0 \\ 0 & p^\theta \end{pmatrix} \begin{pmatrix} \beta'_{i1} \\ \alpha'_{i1} \end{pmatrix} = \lambda_i \begin{pmatrix} \beta'_{i2} \\ \alpha'_{i2} \end{pmatrix} \quad \text{with } |\lambda_i|_p = p^{-\zeta} \text{ for } i = 1, \dots, m, \tag{8.18}$$

where

$$\begin{pmatrix} \beta'_{i1} \\ \alpha'_{i1} \end{pmatrix} = (\det U_1) U_1^{-1} \begin{pmatrix} \beta_{i1} \\ \alpha_{i1} \end{pmatrix}, \quad \begin{pmatrix} \beta'_{i2} \\ \alpha'_{i2} \end{pmatrix} = (\det U_2)^{-1} U_2 \begin{pmatrix} \beta_{i2} \\ \alpha_{i2} \end{pmatrix} \tag{8.19}$$

for $i = 1, \dots, m$.

By (8.18) we have $|\beta'_{i1}|_p = |\lambda_i \beta'_{i2}|_p \le p^{-\zeta}$ for $i = 1, \dots, m$. Suppose $\zeta \ge 1$. Then $\beta'_{i1}/p \in \overline{\mathbb{Z}}_p$ for $i = 1, \dots, m$. Hence, with $C := \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) U_1^{-1}$,

$$(\det C)^{-1} C \begin{pmatrix} \beta_{i1} \\ \alpha_{i1} \end{pmatrix} = \begin{pmatrix} \beta'_{i1}/p \\ \alpha'_{i1} \end{pmatrix} \in \overline{\mathbb{Z}}_p^2.$$

Consequently, $(F_1)_{C^{-1}} \in \overline{\mathbb{Z}}_p[X, Y]$. But then $(F_1)_{C^{-1}} \in \mathbb{Z}_p[X, Y]$, since $(F_1)_{C^{-1}} \in \mathbb{Q}_p[X, Y]$. Hence F_1 is not $\mathbb{Z}_p$-minimal, contrary to our assumption. Thus we conclude that $\zeta < 1$. From (8.18) we also infer that

$$|\alpha'_{i2}|_p = |p^\theta \lambda_i^{-1} \alpha'_{i1}|_p \le p^{\zeta - \theta} \quad \text{for } i = 1, \dots, m.$$

By the same argument as above, using the $\mathbb{Z}_p$-minimality of F_2, we infer that $0 \le \theta - \zeta < 1$. Combining this with (8.15) and $\theta \in \mathbb{Z}$, it follows that $\theta = 1$ and $0 < \zeta < 1$.

We have proved that (8.9), (8.10) hold for a suitable ζ with $0 < \zeta < 1$. Next, in view of (8.13) we have $|\det B|_p = p^{-1}$. It remains to prove (8.11). Assume that $p \nmid c$. By (8.14) we have

$$(\det B) B^{-1} \begin{pmatrix} \delta_{j1} \\ \gamma_{j1} \end{pmatrix} = \mu_j \begin{pmatrix} \delta_{j2} \\ \gamma_{j2} \end{pmatrix} \quad \text{with } \mu_j \in \overline{\mathbb{Q}}_p^* \text{ for } j = 1, \dots, n. \tag{8.20}$$

By (8.8), (8.5),

$$\prod_{i=1}^{m} \prod_{j=1}^{n} |\alpha_{ik} \delta_{jk} - \beta_{ik} \gamma_{jk}|_p = |R(F_k, G_k)|_p = |c|_p = 1 \quad \text{for } k = 1, 2.$$

Further, $\alpha_{ik} \delta_{jk} - \beta_{ik} \gamma_{jk} \in \overline{\mathbb{Z}}_p$. Hence

$$|\alpha_{ik} \delta_{jk} - \beta_{ik} \gamma_{jk}|_p = 1 \quad \text{for } i = 1, \dots, m,\ j = 1, \dots, n,\ k = 1, 2.$$

Now by (8.10), (8.20),

$$|\det B|_p^{-1} |\alpha_{i1} \delta_{j1} - \beta_{i1} \gamma_{j1}|_p = |\lambda_i \mu_j (\alpha_{i2} \delta_{j2} - \beta_{i2} \gamma_{j2})|_p,$$

so

$$|\lambda_i \mu_j|_p = |\det B|_p,$$

which together with the already established identities $|\det B|_p = p^{-1}$ and $|\lambda_i|_p = p^{-\zeta}$ implies $|\mu_j|_p = p^{\zeta-1}$ for $j = 1, \dots, n$. This proves (8.11), and completes the proof of Lemma 8.2. ∎

LEMMA 8.3. *Assume that $p \nmid c$. Then the pairs of augmented forms (F^*, G^*) with (8.1)–(8.5) lie in at most one $\mathbb{Z}_p$-equivalence class.*

Proof. Assume there are two $\mathbb{Z}_p$-inequivalent pairs (F_1^*, G_1^*), (F_2^*, G_2^*) with (8.1)–(8.5). Let B be the matrix and $\zeta \in \mathbb{Q}$ the number from Lemma 8.2. There are $U_1, U_2 \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that $B = U_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) U_2$. Together with (8.10), (8.11) this implies

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} \beta'_{i1} \\ \alpha'_{i1} \end{pmatrix} = \lambda_i \begin{pmatrix} \beta'_{i2} \\ \alpha'_{i2} \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} \delta'_{j1} \\ \gamma'_{j1} \end{pmatrix} = \mu_j \begin{pmatrix} \delta'_{j2} \\ \gamma'_{j2} \end{pmatrix}$$

with

$$\begin{pmatrix} \beta'_{i1} \\ \alpha'_{i1} \end{pmatrix} = (\det U_1) U_1^{-1} \begin{pmatrix} \beta_{i1} \\ \alpha_{i1} \end{pmatrix}, \quad \begin{pmatrix} \beta'_{i2} \\ \alpha'_{i2} \end{pmatrix} = (\det U_2) U_2^{-1} \begin{pmatrix} \beta_{i2} \\ \alpha_{i2} \end{pmatrix},$$
$$\begin{pmatrix} \delta'_{j1} \\ \gamma'_{j1} \end{pmatrix} = (\det U_1) U_1^{-1} \begin{pmatrix} \delta_{j1} \\ \gamma_{j1} \end{pmatrix}, \quad \begin{pmatrix} \delta'_{j2} \\ \gamma'_{j2} \end{pmatrix} = (\det U_2) U_2^{-1} \begin{pmatrix} \delta_{j2} \\ \gamma_{j2} \end{pmatrix}$$

for $i = 1, \dots, m$, $j = 1, \dots, n$. Thus $|\beta'_{i1}|_p = |\lambda_i \beta'_{i2}|_p \le p^{-\zeta}$ for $i = 1, \dots, m$, $|\delta'_{j1}|_p = |\mu_j \delta'_{j2}|_p \le p^{\zeta-1}$ for $j = 1, \dots, n$. Hence

$$\begin{aligned} |\alpha_{i1}\delta_{j1} - \beta_{i1}\gamma_{j1}|_p &= |\det U_1|_p^{-1} |\alpha'_{i1}\delta'_{j1} - \beta'_{i1}\gamma'_{j1}|_p = |\alpha'_{i1}\delta'_{j1} - \beta'_{i1}\gamma'_{j1}|_p \\ &\le \max(p^{-\zeta}, p^{\zeta-1}) < 1 \end{aligned}$$

for $i = 1, \dots, m$, $j = 1, \dots, n$. But then

$$|R(F_1, G_1)|_p = \prod_{i=1}^{m} \prod_{j=1}^{n} |\alpha_{i1}\delta_{j1} - \beta_{i1}\gamma_{j1}|_p < 1$$

contradicting our assumptions that $p \nmid c$ and that (F_1^*, G_1^*) satisfies (8.5). ∎

LEMMA 8.4. *Assume that $p \mid c$. Then the pairs (F^*, G^*) with (8.1)–(8.5) lie in at most two $\mathbb{Z}_p$-equivalence classes.*

Proof. Assume there are three $\mathbb{Z}_p$-inequivalent pairs (F_k^*, G_k^*) $(k = 1, 2, 3)$ with (8.1)–(8.5). Then by Lemma 8.2, there are matrices $B_{12}, B_{13}, B_{23} \in \mathrm{NS}_2(\mathbb{Z}_p)$ with $|\det B_{12}|_p = |\det B_{13}|_p = |\det B_{23}|_p = p^{-1}$, as well as numbers $\lambda_{12}, \lambda_{13}, \lambda_{23} \in \mathbb{Q}_p^*$ such that

$$F_2^* = \lambda_{12}(F_1^*)_{B_{12}}, \quad F_3^* = \lambda_{13}(F_1^*)_{B_{13}}, \quad F_3^* = \lambda_{23}(F_2^*)_{B_{23}}.$$

Thus $F_3^* = \lambda_{12}\lambda_{23}(F_1^*)_{B_{12}B_{23}}$. Hence by Lemma 5.1, $B_{12}B_{23} = \lambda B_{13}$ with $\lambda \in \mathbb{Q}_p^*$. But this implies

$$|\lambda|_p^2 = \frac{|\det B_{12}|_p |\det B_{23}|_p}{|\det B_{13}|_p} = p^{-1},$$

which is impossible. So three pairwise $\mathbb{Z}_p$-inequivalent pairs with (8.1)–(8.5) cannot exist. Lemma 8.4 follows. ∎

Now Lemma 8.1 is an immediate consequence of Lemmata 8.3 and 8.4. ∎

9. Proof of Theorem 2.3. The discriminant of a binary form $F = \sum_{k=0}^{m} a_k X^{m-k} Y^k = \prod_{i=1}^{m} (\alpha_i X - \beta_i Y)$ is given by

$$D(F) = \prod_{1 \le i < j \le m} (\alpha_i \beta_j - \alpha_j \beta_i)^2.$$

Recall that $D(F)$ is a homogeneous polynomial in $\mathbb{Z}[a_0, \dots, a_m]$ of degree $2m-2$. Further, for any scalar λ and any 2×2-matrix A we have

$$D(\lambda F_A) = \lambda^{2m-2} (\det A)^{m(m-1)} D(F). \tag{9.1}$$

Let again $S = \{p_1, \dots, p_t\}$ be a finite, possibly empty set of primes. Every non-zero $a \in \mathbb{Z}_S$ can be expressed uniquely as $a = \varepsilon |a|_S$, where $\varepsilon \in \mathbb{Z}_S^*$ and $|a|_S$ is a positive integer coprime to the primes in S. For a binary form $F = \sum_{i=0}^{m} a_i X^{m-i} Y^i \in \mathbb{Z}_S[X, Y]$, we define $[F]_S := \gcd(|a_0|_S, \dots, |a_m|_S)$. Then for any two $\mathbb{Z}_S$-equivalent binary forms F_1, F_2 we have

$$[F_1]_S = [F_2]_S, \quad |D(F_1)|_S = |D(F_2)|_S.$$

The first equality is obvious, while the second follows from (9.1).

Let $F \in \mathbb{Z}_S[X, Y]$ be a binary form and consider the matrices $A \in \mathrm{NS}_2(\mathbb{Z}_S)$ such that $F_{A^{-1}} \in \mathbb{Z}_S[X, Y]$. If a matrix A satisfies this condition, then so does every matrix in the left $\mathrm{GL}_2(\mathbb{Z}_S)$-coset $\mathrm{GL}_2(\mathbb{Z}_S)A = \{UA : U \in \mathrm{GL}_2(\mathbb{Z}_S)\}$.

LEMMA 9.1. *Let $F \in \mathbb{Z}_S[X, Y]$ be a binary form of degree m without multiple factors. Suppose that F is associated with the number fields $K_1, \dots, K_u$. Then the set of matrices*

$$\{A \in \mathrm{NS}_2(\mathbb{Z}_S) : F_{A^{-1}} \in \mathbb{Z}_S[X, Y]\}$$

is a union of

$$\ll [F]_S^{1/m} [D(F)]_S^{\delta} \tag{9.2}$$

left $\mathrm{GL}_2(\mathbb{Z}_S)$-cosets for every $\delta > 0$, where the implied constant depends only on $K_1, \dots, K_u$, δ, S, m.

Proof. In all Vinogradov symbols $\ll$ used below, the implied constant depends only on $K_1, \dots, K_u$, δ, S, m.

Every matrix $A \in \mathrm{NS}_2(\mathbb{Z}_S)$ can be expressed as UB, where $U \in \mathrm{GL}_2(\mathbb{Z}_S)$ and $B = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $a, b, d \in \mathbb{Z}$, $a > 0$, $d > 0$, $0 \le b < d$ and $\gcd(ad, p_1 \cdots p_t) = 1$ (if $S \neq \emptyset$). Therefore, it suffices to show that the number of such matrices B with $F_{B^{-1}} \in \mathbb{Z}_S[X, Y]$ is bounded above by (9.2).

By (9.1) we have $|D(F)|_S = (ad)^{m(m-1)}|D(F_{B^{-1}})|_S$, hence $(ad)^{m(m-1)}$ is a divisor of $|D(F)|_S$. The number of pairs (a,d) with this property is $\ll |D(F)|_S^{\delta}$ for every $\delta > 0$. We show that for given a, d the number of $b \in \mathbb{Z}$ such that $0 \le b < d$ and $F_{B^{-1}} \in \mathbb{Z}_S[X,Y]$ is $\ll [F]_S^{(1/m)+\delta}$ for every $\delta > 0$. This implies the bound (9.2), since by (9.1), $[F]_S^{m(m-1)}$ divides $[D(F)]_S$.

If in the matrix B we replace b by another integer in the same residue class mod d, we obtain a matrix in the same left $\mathrm{GL}_2(\mathbb{Z}_S)$-coset. Therefore, it suffices to show that the number of residue classes b mod d in $\mathbb{Z}_S$ such that $F_{B^{-1}} \in \mathbb{Z}_S[X,Y]$ is $\ll [F]_S^{(1/m)+\delta}$ for every $\delta > 0$. In view of the Chinese Remainder Theorem, it suffices to estimate from above the number of residue classes b mod d in $\mathbb{Z}_p$ for every prime $p \,|\, d$ and then take the product. More precisely, for each prime $p \,|\, d$ let R_p denote the number of residue classes b mod d in $\mathbb{Z}_p$ such that

$$F_{B^{-1}}(X,Y) = F(a^{-1}X - b(ad)^{-1}Y, d^{-1}Y) \in \mathbb{Z}_p[X,Y]. \tag{9.3}$$

Then we have to show that

$$\prod_{p|d} R_p \ll [F]_S^{(1/m)+\delta} \quad \text{for every } \delta > 0. \tag{9.4}$$

Let p be a prime dividing d. Denote by $\mathrm{ord}_p(F)$ the exponent of p in the prime factorization of $[F]_S$. Let L_p denote the splitting field of F over $\mathbb{Q}_p$, and O_p the integral closure of $\mathbb{Z}_p$ in L_p. For $\alpha_1, \dots, \alpha_r \in L_p$ we denote by $[\alpha_1, \dots, \alpha_r]$ the O_p-fractional ideal generated by $\alpha_1, \dots, \alpha_r$. For a polynomial with coefficients in L_p, we denote by $[P]$ the O_p-fractional ideal generated by the coefficients of P. There is $\pi \in O_p$ such that every O_p-fractional ideal is equal to $[\pi]^r$ for some $r \in \mathbb{Z}$. In particular we have

$$[p] = [\pi]^e \quad \text{with } 1 \le e \le [L_p : \mathbb{Q}_p] \le m!. \tag{9.5}$$

Let $b \in \mathbb{Z}_p$ satisfy (9.3). By Gauss' lemma, we can factor F in $O_p[X,Y]$ as

$$F(X,Y) = \gamma \prod_{i=1}^{m} (\alpha_i X - \beta_i Y) \tag{9.6}$$
$$\text{with } [\gamma] = [F] \text{ and } [\alpha_i, \beta_i] = [1] \text{ for } i = 1, \dots, m.$$

Then

$$F_{B^{-1}}(X,Y) = \gamma \prod_{i=1}^{m} \left(\frac{\alpha_i}{a} X - \frac{b(\alpha_i/a) + \beta_i}{d} Y \right). \tag{9.7}$$

Define integers r_i $(i = 1, \dots, m)$ by

$$[\pi]^{-r_i} = \left[\frac{\alpha_i}{a}, \frac{b(\alpha_i/a) + \beta_i}{d} \right]. \tag{9.8}$$

Then since

$$\left[\frac{\alpha_i}{a}, \frac{b(\alpha_i/a) + \beta_i}{d} \right] \supseteq \left[\frac{\alpha_i}{a}, \frac{b\alpha_i}{a} + \beta_i \right] \supseteq \left[\frac{\alpha_i}{a}, \beta_i \right] \supseteq [\alpha_i, \beta_i] = [1],$$

we have

$$r_i \geq 0 \quad \text{for } i = 1, \ldots, m. \tag{9.9}$$

Further, by Gauss' lemma, the product over $i = 1, \ldots, m$ of the ideals on the right-hand side of (9.8) is $[F_{B^{-1}}][F]^{-1}$. Together with (9.3), (9.5) this implies

$$[\pi]^{r_1+\cdots+r_m} = [F][F_{B^{-1}}]^{-1} \supseteq [F] = [\pi]^{e \operatorname{ord}_p(F)}.$$

Hence

$$r_1 + \cdots + r_m \leq e \operatorname{ord}_p(F). \tag{9.10}$$

Inequalities (9.9), (9.10) imply that for the tuple $(r_1, \ldots, r_m)$ we have at most

$$\binom{m + e \operatorname{ord}_p(F)}{m} \tag{9.11}$$

possibilities.

We now fix a tuple $(r_1, \ldots, r_m)$ and estimate the number of residue classes $b \bmod d$ in $\mathbb{Z}_p$ with (9.3), (9.8). For $i = 1, \ldots, m$ define $\kappa_i, \lambda_i \in L_p$ by

$$\frac{\alpha_i}{a} = \kappa_i \pi^{-r_i}, \qquad \frac{b(\alpha_i/a) + \beta_i}{d} = \lambda_i \pi^{-r_i}. \tag{9.12}$$

This implies that for $i = 1, \ldots, m$ we have

$$b\kappa_i + \pi^{r_i}\beta_i = \lambda_i d, \tag{9.13}$$

$$b + a\,\frac{\beta_i}{\alpha_i} = \frac{\lambda_i d}{\kappa_i}. \tag{9.14}$$

Define integers s_i $(i = 1, \ldots, m)$ by

$$[\kappa_i, d] = [\pi]^{s_i}. \tag{9.15}$$

These integers are uniquely determined by a, d, F, $r_1, \ldots, r_m$, so they are independent of b. We claim that

$$0 \leq s_i \leq r_i \quad \text{for } i = 1, \ldots, m. \tag{9.16}$$

Indeed, by (9.8) we have $[\kappa_i, \lambda_i] = [1]$ for $i = 1, \ldots, m$. Hence $\kappa_i, d \in O_p$ and so $s_i \geq 0$ for $i = 1, \ldots, m$. On the other hand, by (9.13),

$$[\kappa_i, d] = [\kappa_i, \lambda_i d] = [\kappa_i, b\kappa_i + \pi^{r_i}\beta_i] = [\kappa_i, \pi^{r_i}\beta_i] = \pi^{r_i}[\alpha_i/a, \beta_i] \supseteq [\pi]^{r_i},$$

and therefore, $s_i \leq r_i$ for $i = 1, \ldots, m$.

From (9.14) it follows that

$$b + \frac{a\beta_i}{\alpha_i} \equiv 0 \pmod{d\pi^{-s_i}} \quad \text{for } i = 1, \ldots, m. \tag{9.17}$$

Thus, every $b \in \mathbb{Z}_p$ with (9.3), (9.8) satisfies (9.17).

Let b_1, b_2 be two numbers in $\mathbb{Z}_p$ with (9.3), (9.8). Then

$$b_1 \equiv b_2 \pmod{d\pi^{-s_i}}$$

and so, by (9.5),

$$b_1 \equiv b_2 \pmod{dp^{-[s_i/e]}}.$$

By (9.9), (9.10), there is $i \in \{1, \dots, m\}$ with $r_i \le e \operatorname{ord}_p(F)/m$. By (9.16), for this i we have $[s_i/e] \le [\operatorname{ord}_p(F)/m]$. Hence for any two numbers $b_1, b_2 \in \mathbb{Z}_p$ with (9.3), (9.8), we have

$$b_1 \equiv b_2 \pmod{dp^{-[\operatorname{ord}_p(F)/m]}}.$$

Consequently, the numbers $b \in \mathbb{Z}_p$ with (9.3), (9.8) lie in at most $p^{[\operatorname{ord}_p(F)/m]}$ residue classes mod d in $\mathbb{Z}_p$.

This gives an upper bound for the number of residue classes b mod d for fixed $r_1, \dots, r_m$. Invoking the upper bound (9.11) for the number of possibilities for $(r_1, \dots, r_m)$, we infer that for the number R_p of residue classes b mod d in $\mathbb{Z}_p$ with (9.3) we have

$$R_p \le \binom{m + e \operatorname{ord}_p(F)}{m} p^{[\operatorname{ord}_p(F)/m]}.$$

Since $\prod_{p|d} p^{[\operatorname{ord}_p(F)/m]} \le [F]_S^{1/m}$, it follows easily that $\prod_{p|d} R_p \ll [F]_S^{(1/m)+\delta}$ for every $\delta > 0$. This proves (9.4), and completes the proof of Lemma 9.1. ∎

LEMMA 9.2. *Let $F, G \in \mathbb{Z}_S[X, Y]$ be binary forms of degrees $m \ge 3$, $n \ge 3$, respectively, such that FG has no multiple factors, and suppose that F is associated with the number fields $K_1, \dots, K_u$ and G with the number fields $L_1, \dots, L_v$. Then*

$$|R(F, G)|_S \gg (|D(F)|_S^{n/(m-1)} |D(G)|_S^{m/(n-1)})^{(1/17)-\delta}$$

for every $\delta > 0$, where the implied constant depends only on $K_1, \dots, K_u$, $L_1, \dots, L_v$, m, n, S, δ, and is not effectively computable from the method of proof.

Proof. See Evertse and Győry [7, Theorem 1]. ∎

LEMMA 9.3. *Let $F, G \in \mathbb{Z}_S[X, Y]$ be binary forms without multiple factors. Then there are binary forms $F_0, G_0 \in \mathbb{Z}_S[X, Y]$ and a matrix $A \in \mathrm{NS}_2(\mathbb{Z}_S)$ such that*

- $F = (F_0)_A$, $G = (G_0)_{(\det A)^{-1}A}$,
- *F_0 is $\mathbb{Z}_S$-minimal, $R(F_0, G_0) = R(F, G)$.*

Proof. Assume that F is not $\mathbb{Z}_S$-minimal. Then there are a binary form $F_1 \in \mathbb{Z}_S[X, Y]$ and a matrix $A_1 \in \mathrm{NS}_2(\mathbb{Z}_S) \setminus \mathrm{GL}_2(\mathbb{Z}_S)$ such that $F = (F_1)_{A_1}$. By (9.1), $|D(F)|_S = |\det A_1|_S^{m(m-1)} |D(F_1)|_S > |D(F_1)|_S$. If F_1 is not $\mathbb{Z}_S$-minimal, there are a binary form $F_2 \in \mathbb{Z}_S[X, Y]$ and a matrix $A_2 \in \mathrm{NS}_2(\mathbb{Z}_S)$

such that $F_1 = (F_2)_{A_2}$ and $|D(F_2)|_S < |D(F_1)|_S$. Further, $F = (F_2)_{A_2A_1}$. It is clear that this argument can be repeated at most finitely many times. So eventually, we obtain a $\mathbb{Z}_S$-minimal binary form $F_0 \in \mathbb{Z}_S[X,Y]$ and a matrix $A \in \mathrm{NS}_2(\mathbb{Z}_S)$ such that $F = (F_0)_A$. Now put $G_0 := G_{(\det A)A^{-1}}$. Then $G_0 \in \mathbb{Z}_S[X,Y]$ and by (2.1) we have $R(F_0,G_0) = R(F,G)$. ∎

Proof of Theorem 2.3. The constants implied by the Vinogradov symbols $\ll$ used below depend only on $K_1,\dots,K_u$, $L_1,\dots,L_v$, m,n,S,δ.

Let (F,G) be a pair of binary forms in $\mathbb{Z}_S[X,Y]$ satisfying the conditions of Theorem 2.3, so in particular satisfying (1.1). Let F_0,G_0 be a pair of binary forms in $\mathbb{Z}_S[X,Y]$, and $A \in \mathrm{NS}_2(\mathbb{Z}_S)$ as in Lemma 9.3. Then (F_0,G_0) satisfies (1.1). By Theorem 2.2, the pairs of binary forms (F_0,G_0) constructed in this manner lie in $\ll c^\delta$ $\mathbb{Z}_S$-equivalence classes for every $\delta > 0$.

Let $\mathcal{F}$ be a full system of representatives for these classes. So

$$\#\mathcal{F} \ll c^\delta \quad \text{for every } \delta > 0. \tag{9.18}$$

Starting with a pair of binary forms (F,G) satisfying the conditions of Theorem 2.3, we first obtain a pair of binary forms (F_0,G_0) and a matrix $A \in \mathrm{NS}_2(\mathbb{Z}_S)$ as in Lemma 9.3, and then a pair $(F_1,G_1) \in \mathcal{F}$ and a matrix $U \in \mathrm{GL}_2(\mathbb{Z}_S)$ such that $F_0 = (F_1)_U$, $G_0 = (G_1)_U$. On putting $A_1 := (\det A)A^{-1}U^{-1}$, we obtain

$$F = \varepsilon(F_1)_{(\det A_1)A_1^{-1}}, \quad G = (G_1)_{A_1^{-1}} \quad \text{with } \varepsilon \in \mathbb{Z}_S^*,\ A_1 \in \mathrm{NS}_2(\mathbb{Z}_S). \tag{9.19}$$

For the matrix A_1 we have $(G_1)_{A_1^{-1}} \in \mathbb{Z}_S[X,Y]$. So by Lemma 9.1, there is a set of matrices $\mathcal{M}(G_1)$ in $\mathrm{NS}_2(\mathbb{Z}_S)$ depending only on G_1 of cardinality

$$\#\mathcal{M}(G_1) \ll [G_1]_S^{1/n}|D(G_1)|_S^\delta \quad \text{for every } \delta > 0 \tag{9.20}$$

such that $A_1 = UB$ for some $B \in \mathcal{M}(G_1)$, $U \in \mathrm{GL}_2(\mathbb{Z}_S)$. By inserting this into (9.19), we infer that every pair of binary forms (F,G) satisfying the conditions of Theorem 2.3 is $\mathbb{Z}_S$-equivalent to a pair

$$((F_1)_{(\det B)B^{-1}}, (G_1)_{B^{-1}}) \quad \text{with } (F_1,G_1) \in \mathcal{F},\ B \in \mathcal{M}(G_1). \tag{9.21}$$

We estimate the number of pairs in (9.21). Every pair $(F_1,G_1) \in \mathcal{F}$ satisfies (1.1). From (2.1) it follows that $[G_1]_S^m$ divides $R(F_1,G_1)$, hence c as well. Therefore, $[G_1]_S \ll c^{1/m}$. Further, by Lemma 9.2 (taking δ sufficiently small), we have

$$c = |R(F_1,G_1)|_S \gg |D(G_1)|_S^{m/17n},$$

therefore, $|D(G_1)|_S \ll c^{17n/m}$. By inserting this into (9.20) we deduce that $\mathcal{M}(G_1)$ has cardinality $\ll c^{(1/mn)+\delta}$ for every $\delta > 0$. Together with (9.18) this implies that the set of pairs in (9.21) has cardinality $\ll c^{(1/mn)+\delta}$ for every $\delta > 0$. The proof of Theorem 2.3 is complete. ∎

References

[1] A. Bérczes, *On the number of solutions of index form equations*, Publ. Math. Debrecen 56 (2000), 251–262.

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

[3] —, —, —, *Diophantine problems related to discriminants and resultants of binary forms*, in: Diophantine Geometry Proceedings, Scuola Norm. Sup. Pisa, 2005, to appear.

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

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

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

[7] —, —, *Lower bounds for resultants I*, Compositio Math. 88 (1993), 1–23.

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

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

[10] K. Győry, *On arithmetic graphs associated with integral domains*, in: A tribute to Paul Erdős, A. Baker, B. Bollobás and A. Hajnal (eds.), Cambridge Univ. Press, Cambridge, 1990, 207–222.

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

[12] —, *On pairs of binary forms with given resultant or given semi-resultant*, Math. Pannon. 4 (1993), 169–180.

[13] B. L. van der Waerden, *Algebra I*, 8th ed., Springer, Berlin, 1971 (in German).

Institute of Mathematics
University of Debrecen
and
Number Theory Research Group
(Hungarian Academy of Sciences
and University of Debrecen)
P.O. Box 12
H-4010 Debrecen, Hungary
E-mail: berczesa@math.klte.hu
gyory@math.klte.hu

Mathematical Institute
Universiteit Leiden
P.O. Box 9512
NL-2300 RA Leiden, The Netherlands
E-mail: evertse@math.leidenuniv.nl

Received on 20.3.2006
and in revised form on 16.2.2007 (5165)