PAIRS OF BINARY FORMS WITH GIVEN RESULTANT

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

CNTA 9 VANCOUVER
July 13, 2006

Preprint:
http://www.math.leidenuniv.nl/~evertse/publications.shtml

RESULTANTS

The resultant of

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

is given by

$$R(F,G)=\underline{\prod_{i=1}^{m}\prod_{j=1}^{n}}(\alpha_i\delta_j-\beta_i\gamma_j)$$

For $A=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ define $F_A(X,Y)=F(aX+bY,cX+dY)$

Two pairs of binary forms (F_1,G_1), (F_2,G_2) in $\mathbb{Z}[X,Y]$ are called equivalent if $\exists\, U\in SL_2(\mathbb{Z})$ with $\underline{F_2}=(F_1)_U$, $G_2=(G_1)_U$

<u>Facts</u>: i) $F,G\in\mathbb{Z}[X,Y]\Rightarrow R(F,G)\in\mathbb{Z}$

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

iii) (F_1,G_1), (F_2,G_2) equivalent $\Rightarrow$

$$R(F_1,G_1)=R(F_2,G_2).$$

RESULTANT EQUATIONS

We consider the equation

$R(F,G)=c$ in binary forms $F, G \in \mathbb{Z}[X,Y]$
$(c \in \mathbb{Z}, c \neq 0)$

The solutions (F,G) can be divided into equivalence classes.

Under certain constraints imposed on F, G the number of equivalence classes is finite

We want to estimate from above the number of equivalence classes

Def. A binary form $F \in \mathbb{Z}[X,Y]$ is said to be associated to a sequence of number fields $K_1, \ldots, K_r$ if we can factor F as

$$F = \prod_{i=1}^{r} F_i,$$

where $F_i \in \mathbb{Z}[X,Y]$ is irreducible and $\exists\, \theta_i$ with $F_i(\theta_i, 1) = 0$, $K_i = \mathbb{Q}(\theta_i)$ for $i = 1, \ldots, r$.

Fact. $\deg F = \sum_{i=1}^{r} [K_i : \mathbb{Q}]$.

THEOREM A (GYŐRY, E., 1993)

Let $m \geq 3$, $n \geq 3$, $c \in \mathbb{Z}$, $c \neq 0$ and let $K_1, \dots, K_r$, $L_1, \dots, L_s$ be number fields with

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

Then there are only finitely many equivalence classes of pairs of binary forms $F, G \in \mathbb{Z}[X, Y]$ such that

(1) $$R(F, G) = c$$

(2) $\begin{cases} F, G \text{ have no multiple factors} \\ F \text{ associated to } K_1, \dots, K_r \\ G \text{ associated to } L_1, \dots, L_s \end{cases}$

Remarks
- (2) implies $\deg F = m$, $\deg G = n$
- There may be infinitely many equivalence classes if $m \leq 2$, $n \leq 2$ or if F, G do not have their roots in prescribed number fields

EXAMPLES :

1) $m \leq 2$ or $n \leq 2$

$F(X,Y) = X^2 - dY^2 \quad (d \in \mathbb{Z}_{>0},\ d \neq \square)$

$G(X,Y) = \prod_{i=1}^{n} (y_i X - x_i Y),$

with $x_i^2 - dy_i^2 = 1$ for $i = 1, \ldots, n$

$\Rightarrow R(F,G) = 1$

2) F, G not associated to given number fields

Let $m \leq n$. Pick any two binary forms $F_0, G_0 \in \mathbb{Z}[X,Y]$ of degrees m, n respectively

Then for any binary form $H \in \mathbb{Z}[X,Y]$ of degree $n-m$, $R(F_0, G_0 + HF_0) = R(F_0, G_0)$

CONES

It is too difficult to give an explicit upper bound for the number of equivalence classes in the Theorem. Instead, we estimate the number of cones.

<u>Def.</u> $NS_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad-bc \neq 0 \right\}$

A cone is a set of pairs of binary forms of the shape

$$\mathcal{C}(F_0, G_0) = \left\{ (F, G) : F, G \in \mathbb{Z}[X, Y],\ \exists A \in NS_2(\mathbb{Z}) \text{ such that } F = (F_0)_A,\ G = (G_0)_{(\det A)^{-1}A} \right\}$$

with given $F_0, G_0 \in \mathbb{Z}[X, Y]$

<u>Facts.</u> 1) $(F, G) \in \mathcal{C}(F_0, G_0) \Rightarrow R(F, G) = R(F_0, G_0)$

2) A cone is the union of finitely many equivalence classes.

THEOREM 1 (BÉRCZES, GYŐRY, E., 2006)

Let $m, n, c, K_1, \ldots, K_r, L_1, \ldots, L_s$ be as in Theorem A.

Then the collection of pairs of binary forms $F, G \in \mathbb{Z}[X,Y]$ with (1), (2) is contained in the union of at most

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

cones.

Def. For $c = \pm p_1^{k_1} \cdots p_t^{k_t}$ (p_i distinct primes) we put

$$\psi(c) := 2^t \prod_{i=1}^{t} \binom{mn + k_i + 2}{mn + 2}$$

THE MAIN TOOL:
(Schlickewei, Schmidt, E., 2002)

Let $a_1, \dots, a_n \in \overline{\mathbb{Q}}^*$ ($\overline{\mathbb{Q}}$ = alg. closure of $\mathbb{Q}$).
Let Γ be a finitely generated subgroup of $\overline{\mathbb{Q}}^*$ of rank r.

Then the equation

$$a_1 x_1 + \dots + a_n x_n = 1 \quad \text{in } x_1, \dots, x_n \in \Gamma$$

has at most

$$e^{(6n)^{4n}(r+1)}$$

solutions with

$$\sum_{i \in I} a_i x_i \neq 0 \quad \text{for each non-empty } I \subseteq \{1, \dots, n\}$$

IDEA OF THE PROOF:

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

be two binary forms satisfying the conditions of Theorem 1.

Then $R(F,G) = \prod_{i=1}^{m}\prod_{j=1}^{n} \Delta_{ij} = c$

with $\Delta_{ij} = \alpha_i\delta_j - \beta_i\gamma_j$.

For any $i,j,k \in \{1,\dots,m\}$, $f,g,h \in \{1,\dots,n\}$,

$$\begin{vmatrix} \Delta_{if} & \Delta_{ig} & \Delta_{ih} \\ \Delta_{jf} & \Delta_{jg} & \Delta_{jh} \\ \Delta_{kf} & \Delta_{kg} & \Delta_{kh} \end{vmatrix} = 0,$$

hence

$$u_1 + u_2 + u_3 + u_4 + u_5 = 1,$$

with

$$u_1 = \frac{\Delta_{if}\,\Delta_{jg}\,\Delta_{kh}}{\Delta_{kf}\,\Delta_{jg}\,\Delta_{ih}} \quad \text{etc.}$$

$u_1,\dots,u_5$ belong to a finitely generated group independent of F,G.

Applying the upper bound of SSE to $u_1+u_2+u_3+u_4+u_5=1$ gives an explicit bound N such that the set of pairs (F,G) satisfying the conditions of Theorem 1 lies in the union of at most N $\overline{\mathbb{Q}}$-cones

$$C_{\overline{\mathbb{Q}}}(F_1,G_1)=\left\{ (F,G) : F,G\in\mathbb{Z}[X,Y], \; \exists A\in GL_2(\overline{\mathbb{Q}}) \text{ with } F=(F_1)_A,\; G=(G_1)_{(\det A)^{-1}A} \right\}$$

with F_1,G_1 given <u>binary</u> forms in $\overline{\mathbb{Q}}[X,Y]$

An elementary argument gives the number of cones going into a $\overline{\mathbb{Q}}$-cone.

EQUIVALENCE CLASSES INSTEAD OF CONES

THEOREM 2 (BGE, 2006)

Let $m, n, c, K_1, \dots, K_r, L_1, \dots, L_s$ be as in Theorem A.

Then the number of equivalence classes of pairs of linear forms $F, G \in \mathbb{Z}[X, Y]$ with (1), (2) is at most

$$O\left(|c|^{\frac{1}{mn}+\varepsilon}\right) \quad \text{as } |c| \to \infty$$

for every $\varepsilon > 0$.

The implied constant depends on $\varepsilon, m, n, K_1, \dots, K_r$, $L_1 \dots L_s$, and is ineffective.

<u>Remark.</u> The exponent on $|C|$ is up to ε best possible.

Pick binary forms $F, G \in \mathbb{Z}[X,Y]$ of degrees $m \geq 3$, $n \geq 3$ with $R(F,G) \neq 0$

Let p be a prime. For $b = 0, 1, \ldots, p-1$ define

$$F_b(X,Y) := F(X+bY, pY), \quad G_b(X,Y) := G(X+bY, pY)$$

Then $R(F_b, G_b) = p^{mn} R(F,G) =: C$,

and the pairs (F_b, G_b) $(b = 0, 1, \ldots, p-1)$

lie in $p \gg |C|^{1/mn}$ distinct equivalence classes

THEOREM 1 $\Rightarrow$ THEOREM 2

Let $\mathcal{C}(F_0, G_0)$ be one of the cones from Theorem 1.

The number of equivalence classes in $\mathcal{C}(F_0, G_0)$ depends on the discriminant $D(G_0)$ of G_0.

THEOREM (Győry, E., 1993)

If $\deg F_0 = m$, $\deg G_0 = n$, F_0, G_0 have no multiple factors, F_0 is associated to $K_1 \dots K_r$ and G_0 to $L_1 \dots L_s$, then

$$|D(G_0)| \ll^{\mathrm{eff}}_{\substack{m,n \\ K_1 \dots K_r \\ L_1 \dots L_s}} |R(F_0, G_0)|^{10(n-1)/m}.$$

<u>Proof</u>: Subspace Theorem.

APPLICATION TO THUE EQUATIONS

Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a binary form of degree ≥ 3 and $c \in \mathbb{Z}$, $c \neq 0$. Consider

(T) $$F(x,y) = c \quad \text{in } x, y \in \mathbb{Z}$$

(solutions (x,y), $(-x,-y)$ are considered equal)

THEOREM B (Győry, E., 1989)

Let $m \geq 3$, $c \in \mathbb{Z}$, $c \neq 0$ and let $K_1, \ldots, K_r$ be number fields with $\sum_{i=1}^{r} [K_i : \mathbb{Q}] = m$.

Then there are only finitely many $SL_2(\mathbb{Z})$-equivalence classes of binary forms $F \in \mathbb{Z}[X,Y]$ such that

(1) (T) has at least 3 solutions

(2) $\begin{cases} F \text{ has no multiple factors} \\ F \text{ is associated to } K_1, \ldots, K_r \end{cases}$

THEOREM 3 (BGE, 2006)

Let $m, C, K_1, \ldots, K_r$ be as in Theorem B

Then the number of $SL_2(\mathbb{Z})$-equivalence classes of binary forms $F \in \mathbb{Z}[X, Y]$ with (1), (2) is at most

$$O(|C|^{\frac{1}{m}+\varepsilon}) \text{ as } |C| \to \infty$$

for every $\varepsilon > 0$.

The implied constant depends on $\varepsilon, m, K_1, \ldots, K_r$ and is <u>ineffective</u>

Theorem 2 $\Rightarrow$ Theorem 3

Suppose (T) has 3 solutions $(x_1, y_1), (x_2, y_2), (x_3, y_3)$.

Put $G(X, Y) := \prod_{i=1}^{3} (y_i X - x_i Y)$.

Then $R(F, G) = \prod_{i=1}^{3} F(x_i, y_i) = C^3$.

FINAL REMARK:

All results have been proved in a more general form for equations

$$R(F,G) = c \cdot u$$

in binary forms $F,G \in \mathbb{Z}_S[X,Y]$, $u \in \mathbb{Z}_S^*$ where

$S = \{p_1 \dots p_t\}$ finite set of primes,

$\mathbb{Z}_S = \mathbb{Z}[\frac{1}{p_1 \dots p_t}]$ ring of S-integers,

$\mathbb{Z}_S^* = \{\pm p_1^{w_1} \cdots p_t^{w_t} : w_i \in \mathbb{Z}\}$ group of S-units