LINEAR EQUATIONS WITH UNKNOWNS FROM A MULTIPLICATIVE GROUP OF FINITE RANK

Jan-Hendrik Evertse (Leiden)

Lecture given at the
Colloquium on Number Theory
in honour of professors
Kálmán Győry and András Sárközy
on the occasion of their 60th birthday
July 3–July 7, 2000, Debrecen

We start with:

Theorem. (E., 1984)
Let $a, b \in \mathbf{Q}^*$, *let* $p_1, \ldots, p_r$ *be distinct prime numbers, and let* $\Gamma = \{\pm p_1^{z_1} \cdots p_r^{z_r} : z_i \in \mathbf{Z}\}$ *be the multiplicative group generated by* $p_1, \ldots, p_r$. *Then the equation*

$$ax + by = 1 \quad \text{in } x, y \in \Gamma$$

has at most $3 \times 7^{2r+3}$ *solutions.*

This can be generalized to equations with unknowns x, y in the group of S-units of a number field.

We consider a more general situation.

Notation.
K is any field of characteristic 0.
K^* is the multiplicative group of K.
Γ is a subgroup of K^* of rank r, i.e.
there are multiplicatively independent elements
$u_1, \ldots, u_r \in \Gamma$ such that
$\forall x \in \Gamma \; \exists m \in \mathbf{N}, z_i \in \mathbf{Z}$ with $x^m = u_1^{z_1} \cdots u_r^{z_r}$.

Theorem (Beukers, Schlickewei, 1996)
Let $a, b \in K^*$. Suppose Γ has rank r. Then the equation

$$ax + by = 1 \quad \textit{in } x, y \in \Gamma$$

has at most $2^{16(r+1)}$ solutions.

Remark: Earlier Schlickewei proved a similar result with the upper bound c^{r^2}.

Now let $a_1, \ldots, a_N \in K^*$ and consider the equation in N variables:

(1) $a_1 x_1 + \cdots + a_N x_N = 1$

in $x_1, \ldots, x_N \in \Gamma$.

To prevent easy constructions of infinite sets of solutions we consider only *non-degenerate* solutions, i.e., with

$\sum_{i \in I} a_i x_i \neq 0$ for each subset I of $\{1, \ldots, N\}$.

History:
1980's van der Poorten&Schlickewei, E., Laurent: (1) has finitely many non-degenerate solutions.

1990's Schlickewei: explicit upper bounds in special cases depending on N, $r =$rank Γ and other parameters.
Later improvements by E. and Schlickewei&Schmidt.

Theorem (Schlickewei, Schmidt, E.)
Suppose Γ *has rank* r. *Then the equation*

$$a_1x_1 + \cdots + a_Nx_N = 1 \quad \textit{in } x_1, \ldots, x_N \in \Gamma$$

has at most $2^{2^{6N}(r+1)}$ *non-degenerate solutions.*

Ingredients in proof of Theorem:
1. A specialization argument, to reduce equations over arbitrary fields of characteristic 0 to equations over number fields.
2. Estimates for the number of solutions of small height (Schmidt 1994, David&Philippon 2000).
3. A quantitative version of the Subspace Theorem (Schmidt 1989 $--\rightarrow$ Schlickewei& E. 2000), to treat solutions with large height.

Polynomial equations.

K is again an arbitrary field of char. 0.
f is an inhomogeneous polynomial in $K[X_1, \dots, X_N]$.
Γ is a subgroup of K^* of finite rank r.
We consider the equation

(2) $f(x_1, \dots, x_N) = 0 \quad$ in $x_1, \dots, x_N \in \Gamma$.

We must again exclude degenerate solutions to prevent easy constructions of infinite sets of solutions.

Definition: $\mathbf{x} = (x_1, \dots, x_N)$ is called a *degenerate* solution of $f(\mathbf{x}) = 0$ if there are integers $t_1, \dots, t_N$, not all zero, such that

$$f(x_1\lambda^{t_1}, \dots, x_N\lambda^{t_N}) = 0 \quad \text{identically in } \lambda.$$

Otherwise $\mathbf{x}$ is called *non-degenerate*.

Another formulation of degeneracy.

Write $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} \cdots x_N^{a_N}$ and let

$$f = \sum_{\mathbf{a} \in A} c(\mathbf{a}) \mathbf{x}^{\mathbf{a}}$$

where

$$c(\mathbf{a}) \neq 0 \text{ for } \mathbf{a} \in A, \quad A \subset (\mathbf{Z}_{\geq 0})^N \text{ finite.}$$

For a partition $\mathcal{P} = \{P_1, \ldots, P_k\}$ of A into pairwise disjoint sets, let $H_{\mathcal{P}}$ denote the abelian group generated by all vectors

$$\mathbf{a} - \mathbf{b} \quad (\mathbf{a}, \mathbf{b} \in P_i,\ i = 1, \ldots, k).$$

Lemma. $\mathbf{x}$ *is a degenerate solution of* $f(\mathbf{x}) = 0$ *if and only if there is a partition* $\mathcal{P} = \{P_1, \ldots, P_k\}$ *of* A *such that*

$$\textstyle\sum_{\mathbf{a} \in P_i} c(\mathbf{a}) \mathbf{x}^{\mathbf{a}} = 0 \quad \text{for } i = 1, \ldots, k,$$

$$H_{\mathcal{P}} \neq (\mathbf{0}).$$

Theorem. (Laurent, 1984)
Let $f \in K[X_1, \ldots, X_N]$ be an inhomogeneous polynomial and let Γ be a subgroup of K^* of finite rank. Then the equation

$$f(x_1, \ldots, x_N) = 0 \quad \textit{in } x_1, \ldots, x_N \in \Gamma$$

has only finitely many non-degenerate solutions.

Quantitative results:
1993, Győry: K number field, Γ group of S-units in K
1994, Schmidt: K arbitrary, Γ group of roots of unity in K

Theorem. (Schlickewei, E.)
Let $\operatorname{rank}\Gamma = r$. *Suppose that f has total degree D. Then the number of non-degenerate solutions of*

$$f(x_1, \ldots, x_N) = 0 \quad \textit{in } x_1, \ldots, x_N \in \Gamma$$

is at most

$$c(N, D)^{r+1} \text{ with } c(N, D) = 2^{2^{6\binom{N+D}{D}}}.$$

Back to linear equations.

Let again K be a field of characteristic 0, $a_1, \dots, a_N \in K^*$, Γ a subgroup of K^* of rank r and consider again

$$a_1x_1 + \cdots + a_Nx_N = 1 \quad \text{in } x_1, \dots, x_N \in \Gamma.$$

Two tuples of coefficients $\mathbf{a} = (a_1, \dots, a_N)$, $\mathbf{b} = (b_1, \dots, b_N)$ are called Γ-equivalent if $b_i = a_iu_i$ with $u_i \in \Gamma$ for $i = 1, \dots, N$.

Equations with Γ-equivalent tuples of coefficients have the same number of non-degenerate solutions.

Theorem. (Győry, Stewart, Tijdeman, E., 1986)
There are finitely many Γ*-equivalence classes of pairs in* $K^* \times K^*$ *such that for every pair* (a, b) *outside the union of these classes, the equation*

$$ax + by = 1 \quad \textit{in } x, y \in \Gamma$$

has at most two *solutions.*

Remark 1. The upper bound 2 is best possible.

Remark 2. The exceptional equivalence classes can not be determined effectively from the method of proof.

Remark 3. The situation for equations in $N \geq 3$ variables is much more complicated.

Denote by $H(\alpha)$ the height (the maximum of the absolute values of the coefficients of the minimal polynomial in $\mathbf{Z}[X]$) of an algebraic number α.

Theorem. (Győry, Stewart, Tijdeman, E., 1986)
Let $a, b \in \mathbf{Q}^*$, let $p_1, \ldots, p_r$ be distinct prime numbers, and let $\Gamma = \{\pm p_1^{z_1} \cdots p_r^{z_r} : z_i \in \mathbf{Z}\}$.
If the equation

$$ax + by = 1 \quad \textit{in } x, y \in \Gamma$$

has more than $r + 2$ solutions, then (a, b) is Γ-equivalent to a pair (a', b') with

$$\max(H(a'), H(b')) \leq C^{\text{eff}}(p_1, \ldots, p_r).$$

The proof uses estimates for linear forms in (ordinary and p-adic) logarithms.

This can be extended as follows:

Theorem. (E.) *Let* $a, b \in \overline{\mathbf{Q}}^*$ *and let* Γ *be a subgroup of* $\overline{\mathbf{Q}}^*$ *of rank* r*. Let* $u_1, \ldots, u_r$ *be multiplicatively independent elements of* Γ*. If*

$$ax + by = 1 \quad \textit{in } x, y \in \Gamma$$

has more than $2r + 2$ *solutions, then* (a, b) *is* Γ*-equivalent to a pair* (a', b') *with*

$$\max(H(a'), H(b')) \leq C^{\text{eff}}(u_1, \ldots, u_r),$$

$$\max(\deg a', \deg b') \leq C^{\text{eff}}(u_1, \ldots, u_r).$$

Fact: *Let* $N \geq 3$. *Then for every* $h > 0$ *there are* Γ *and infinitely many* Γ*- equivalence classes of tuples* $(a_1, \ldots, a_N)$ *such that the equation*

$$a_1x_1 + \cdots + a_Nx_N = 1 \quad \textit{in } x_1, \ldots, x_N \in \Gamma$$

has more than h *non-degenerate solutions.*

Example. Consider the equation

$$x_1 + \cdots + x_{N-1} = 1.$$

Choose Γ sufficiently large such that this equation has more than h non-degenerate solutions $x_1, \ldots, x_{N-1} \in \Gamma$.
Then for all but finitely many $\lambda \in K^*$, the equation

$$\lambda x_1 + \cdots + \lambda x_{N-1} + (1 - \lambda)x_N = 1$$

has more than h non-degenerate solutions $x_1, \ldots, x_N \in \Gamma$, with $x_N = 1$.

Let $A(\mathbf{a},\Gamma)$ denote the smallest integer t such that the set of $\mathbf{x} = (x_1, \ldots, x_N)$ with

$$a_1x_1 + \cdots + a_Nx_N = 1, \quad x_1, \ldots, x_N \in \Gamma$$

is contained in the union of not more than t proper linear subspaces of K^N.

Theorem. (Győry, E., 1989)
There are finitely many Γ-equivalence classes of tuples in $(K^*)^N$, such that for every tuple $\mathbf{a} = (a_1, \ldots, a_N)$ outside the union of these classes we have $A(\mathbf{a},\Gamma) \le 2^{(N+1)!}$.

In 1993 I improved this to $(N!)^{2N+2} \approx e^{2N^2 \log N}$. By a simple argument this can be improved somewhat further:

Theorem. (E.) *There are finitely many Γ-equivalence classes of tuples in $(K^*)^N$, such that for every tuple $\mathbf{a} = (a_1, \ldots, a_N)$ outside the union of these classes we have*

$$A(\mathbf{a},\Gamma) \le 2^{N^2}.$$

Sketch of proof.

Take $\mathbf{a} = (a_1, \dots, a_N) \in (K^*)^N$ and consider

$$a_1x_1 + \cdots + a_Nx_N = 1 \quad \text{in } x_1, \dots, x_N \in \Gamma.$$

By replacing $\mathbf{a}$ by a Γ-equivalent tuple we may assume that $(1, 1, \dots, 1)$ is a solution.
Take N other solutions
$\mathbf{x}_1 = (x_{11}, \dots, x_{1N}), \dots, \mathbf{x}_N = (x_{N1}, \dots, x_{NN})$.
Then

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & x_{11} & \cdots & x_{1N} \\ \vdots & \vdots & & \vdots \\ 1 & x_{N1} & \cdots & x_{NN} \end{vmatrix} = 0.$$

We apply the general result on polynomial equations.

We distinguish two cases:

a) $(x_{11}, \ldots, x_{NN})$ is non-degenerate.

Then $(x_{11}, \ldots, x_{NN})$ belongs to a finite set which is independent of the coefficients $a_1, \ldots, a_N$. Now we can solve $a_1, \ldots, a_N$ from

$$\begin{aligned} a_1 x_{11} + \cdots + a_N x_{1N} &= 1 \\ &\vdots \\ a_1 x_{N1} + \cdots + a_N x_{NN} &= 1 \end{aligned}$$

and we get finitely many possibilities for $a_1, \ldots, a_N$.

b) $(x_{11}, \dots, x_{NN})$ is degenerate.

This means that there are integers $t_{11}, \dots, t_{NN}$, not all zero, such that

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & \lambda^{t_{11}} x_{11} & \cdots & \lambda^{t_{1N}} x_{1N} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda^{t_{N1}} x_{N1} & \cdots & \lambda^{t_{NN}} x_{NN} \end{vmatrix} = 0 \quad \text{for every } \lambda.$$

Choosing $\lambda = -1$ we get

$$(3) \qquad \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & \pm x_{11} & \cdots & \pm x_{1N} \\ \vdots & \vdots & & \vdots \\ 1 & \pm x_{N1} & \cdots & \pm x_{NN} \end{vmatrix} = 0.$$

Now fix $\mathbf{x}_1 = (x_{11}, \dots, x_{1N}), \dots, \mathbf{x}_{N-1}$ and let $\mathbf{x}_N = (x_{N1}, \dots, x_{NN})$ run through the solutions of $a_1 x_1 + \cdots + a_N x_N = 1$ in Γ.

Then $\mathbf{x}_N$ satisfies one of at most 2^{N^2} linear equations determined by the signs in (3) and each equation determines a linear subspace of $(K^*)^N$. **QED.**

A lower bound for $A(\mathbf{a},\Gamma)$.

Take arbitrary $u_1,\dots,u_N\in\Gamma$ such that $b:=u_1+\cdots+u_N\neq 0$. Let $\mathcal{S}_N$ be the set of of permutations of $\{1,\dots,N\}$.
For $\sigma\in\mathcal{S}_N$ define $\mathbf{u}_\sigma=(u_{\sigma(1)},\dots,u_{\sigma(N)})$. Then $\mathbf{u}_\sigma$ is a solution of

$$\frac{1}{b}x_1+\cdots+\frac{1}{b}x_N=1.$$

The vectors $\mathbf{u}_\sigma$ with $\sigma(N)=i$ lie in the proper subspace given by the equation

$$u_i(x_1+\cdots+x_{N-1})-(b-u_i)x_N=0.$$

Hence the set $\{\mathbf{u}_\sigma:\sigma\in\mathcal{S}_N\}$ can be covered by N proper linear subspaces of K^N.

Fact: If $u_1,\dots,u_N$ are “sufficiently general” then the set $\{\mathbf{u}_\sigma:\sigma\in\mathcal{S}_N\}$ can not be covered by fewer than N proper linear subspaces of K^N.

So for $\mathbf{a}=(\frac{1}{b},\dots,\frac{1}{b})$ we have $A(\mathbf{a},\Gamma)\geq N$.