Rational Solutions of Polynomial-Exponential Equations

Ayhan Günaydın

CMAF

Universidade de Lisboa

ayhan@ptmat.fc.ul.pt

May 16, 2012

The Equation

Today I will concentrate on the following equation:

$$\sum_{i=1}^{s} p_i(\mathbf{X})\boldsymbol{\beta}_i^{\mathbf{X}} = 0,$$

where $\mathbf{X} = (X_1, \ldots, X_t)$ is a tuple of indeterminates, $p_1, \ldots, p_s \in \mathbb{C}[\mathbf{X}]$, $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_s \in (\mathbb{C}^{\times})^t$, and $\boldsymbol{\beta}_i^{\mathbf{X}}$ is short for $\prod_{j=1}^{t} \beta_{ij}^{X_j}$.

Why?

On November 6, 2009, Amador (Martin-Pizarro) told me about the following:

Question 1. Assume *Schanuel's Conjecture*. Is it correct that given a variety $V \subset \mathbb{C}^{2n}$ defining a *minimal extension of predimension* 0, there is a generic point in V of the form $(z, \exp(z))$?

Why?

I will not explain the second italic phrase, because we wanted to attack the following easiest case which does not involve that phrase:

Question 2.0. Assume *Schanuel's Conjecture*. Let $p(X, Y) \in \mathbb{C}[X, Y]$ be an irreducible polynomial in which both X and Y appear, defining a curve $C \subseteq \mathbb{C}^n$. Is it the case that there are algebraically independent complex numbers $\alpha_1, \alpha_2, \dots$ such that each $(\alpha_j, e^{\alpha_j}) \in C$?

Why?

The following special case is proven by D. Marker:

Theorem

Assume Schanuel's Conjecture. Let $p(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ *be an irreducible polynomial in which both* X *and* Y *appear, defining a curve* $C \subseteq \mathbb{C}^n$*. Then there are algebraically independent complex numbers* $\alpha_1, \alpha_2, \ldots$ *such that each* $(\alpha_j, e^{\alpha_j}) \in C$*?*

Why?

How to attack Question 2.0? Let p and C be as in Question 2.0.

It follows from *Hadamard Factorization Theorem* that there are always infinitely many points on C of the form (α, e^{α}). How to choose them to be algebraically independent?

Say $K \subseteq \mathbb{C}$ is an arbitrary algebraically closed subfield of finite transcendence degree. We would have a positive answer to Question 2.0, if there were only finitely many $\alpha \in K$ such that $(\alpha, e^{\alpha}) \in C$. (Because in that case, we could keep finding new solutions outside of the algebraic closure of finitely many solutions.)

Why?

So we could reduce Question 2.0 to the following:

Question 2.1. Assume *Schanuel's Conjecture*. Let p and C be as in Question 2.0 and let $K \subseteq \mathbb{C}$ be an algebraically closed subfield of finite transcendence degree. Is it the case that there are only finitely many $\alpha \in K$ such that $(\alpha, e^{\alpha}) \in C$?

Schanuel's Conjecture

Here it is:

Conjecture. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be $\mathbb{Q}$-linearly independent. Then

$$\mathrm{trdeg}_{\mathbb{Q}}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}) \geq n.$$

A very popular consequence of this is that e and π are algebraically independent. Another -known- special case is :

Theorem (Lindemann-Weierstrass)

If algebraic numbers $\alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent.

Schanuel's Conjecture

The consequence that is important for our purpose is the following:

Lemma

Assume Schanuel's Conjecture and let p, C, K be as in Question 2.1. Then there is a finite dimensional $\mathbb{Q}$-subspace V of K such that for each $\alpha \in K$ if $(\alpha, e^{\alpha}) \in C$, then $\alpha \in V$.

Why? - Final

Let $\{\alpha_1, \ldots, \alpha_t\} \subseteq K$ be a basis of V and write

$$p(X, Y) = \sum_{i=0}^{s} \tilde{p}_i(X) Y^i.$$

With this notation in hand, we want to solve the following for $(X_1, \ldots, X_t) \in \mathbb{Q}^t$:

$$\sum_{i=0}^{s} \tilde{p}_i(X_1\alpha_1 + \cdots + X_t\alpha_t)\, \beta_1^{iX_1} \cdots \beta_t^{iX_t} = 0$$

Now defining $p_i(\mathbf{X}) = \tilde{p}_i(X_1\alpha_1 + \cdots + X_t\alpha_t)$ and $\beta_{ij} = \beta_j^i$, this is exactly *the equation*! (Well, after changing the index set a little.)

So this settles the *why*.

Integer Solutions of the Equation

The integer solutions of the equation are well known. Many people worked on that subject; I will mention only the first one.

Theorem (M. Laurent)

(i) If p_i is constant for each i, then the set of nondegenerate solutions of the equation is a finite union of translates of

$$H := \{\mathbf{n} \in \mathbb{Z}^t : \prod_{j=1}^{t} \beta_{ij}^{n_j} = \prod_{j=1}^{t} \beta_{i'j}^{n_j} \text{ for every } i, i' \in \{1, \ldots, s\}\}$$

.

(ii) There are constants $c, d \in \mathbb{R}$ depending on the p_i's and the β_{ij}'s such that if $\mathbf{n} = (n_1, \ldots, n_t)$ is a nondegenerate solution of the equation, then there is $\mathbf{n}' = (n'_1, \ldots, n'_t) \in H$ such that $|\mathbf{n} - \mathbf{n}'| < c \log(|\mathbf{n}|) + d$.

(*Nondegenerate* means "no subsum vanishes".)

Integer Solutions of the Equation

This theorem has the following consequence:

Corollary

If the numbers β_{ij} are multiplicatively independent. Then the equation has only finitely many nondegenerate integer solution.

Proof.

The multiplicative dependence assumption means that H is trivial. So if $\mathbf{n} = (n_1, \ldots, n_t)$ is a nondegenerate solution of the equation, then $|\mathbf{n}| < c\log(|\mathbf{n}|) + d$. But there are only finitely many such $\mathbf{n}$.

□

Rational Solutions of the Equation

In the remaining time, I will illustrate a sketch of the proof of this corollary with the word *integer* replaced by *rational*:

Theorem

Let $\{\alpha_{ij} \in \mathbb{C} : i = 1, \ldots, s, j = 1, \ldots, t\}$ *be a* $\mathbb{Q}$*-linearly independent set and* $p_1, \ldots, p_s \in \mathbb{C}[X_1, \ldots, X_t]$*. Then there only finitely many* $\mathbf{q} = (q_1, \ldots, q_t) \in \mathbb{Q}^t$ *such that* $\sum_{i=1}^{s} p_i(\mathbf{q}) \exp(q_1\alpha_{i1} + \cdots + q_t\alpha_{it}) = 0$ *and* $\sum_{i \in I} p_i(\mathbf{q}) \exp(q_1\alpha_{i1} + \cdots + q_t\alpha_{it}) \neq 0$ *for every proper nonempty* $I \subseteq \{1, \ldots, s\}$*.*

The main idea is to reduce the rational case to finitely many integer cases.

Some Notation

Definition

Let G be an abelian group, written multiplicatively. For $n > 0$ put $G^{[n]} = \{g^n : g \in G\}$. We say that H is *radical* in G if $H \cap G^{[n]} = H^{[n]}$ for all $n > 0$ and it contains all the torsion elements of G.Given $A \subseteq G$, we set $\langle A \rangle_G$ to be the smallest radical subgroup of G containing A.

That is,

$$\langle A \rangle_G = \{g \in G \mid g^n \in [A]_G \text{ for some } n \in \mathbb{N}\}$$

where $[A]_G$ is the subgroup generated by A.

When G is clear from the context, we will drop the subscripts and just write $\langle A \rangle$ and $[A]$.

Also $\mathbb{U}$ denotes the multiplicative group of roots of unity.

Linear Relations in Multiplicative Groups

For a field K and a subgroup $\Gamma$of $K^\times$ consider the solutions in Γ of

$$\lambda_1 x_1 + \cdots + \lambda_k x_k = 1, \tag{*}$$

where $\lambda_1, \ldots, \lambda_k \in K$.
We say that a solution $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_k)$ in Γ of (*) is *non-degenerate* if $\sum\limits_{i \in I} \lambda_i \gamma_i \neq 0$ for every nonempty proper subset I of $\{1, \ldots, k\}$.
The main result we need is the following:

Lemma (van den Dries - G.)

Let $E \subseteq F$ be fields such that $E \cap \mathbb{U} = F \cap \mathbb{U}$ and G be a radical subgroup of $E^\times$. Then given $\lambda_1, \ldots, \lambda_n \in E^\times$, the equation (*) has the same non-degenerate solutions in G as in $\langle G \rangle_{F^\times}$.

The Proof

We apply the lemma in the following setting: let A be a finite set containing the coefficients of the p_i's and the numbers β_{ij} and put $\Gamma = \langle A \rangle_{\mathbb{C}^\times}$.

If $\mathbf{q} \in \mathbb{Q}^t$ is a nondegenerate solution of the equation, then the tuple $(\exp(\mathbf{q} \cdot \boldsymbol{\alpha}_i) : i = 1, \ldots, s) \in \Gamma^s$ is a non-degenerate solution of the linear equation

$$p_1(\mathbf{q}) Y_1 + \cdots + p_s(\mathbf{q}) Y_s = 0. \tag{**}$$

Let $E := \mathbb{Q}(\mathbb{U} \cup A)$ and $G := \langle A \rangle_{E^\times}$. Now by taking $\mathbb{C}$ in the place of F in the lemma, we see that all the possible solutions of the linear equation (**) in Γ are in G.

The Proof

Let G' be the complement of $\mathbb{U}$ in G.

If G' were finitely generated, we would be halfway there. Is it? Yes; here is why:

Theorem (Zilber)

Let L be a finitely generated extension of $\mathbb{Q}(\mathbb{U})$. Then the quotient group $L^\times/\mathbb{U}$ is a free abelian group.

So G', being a subgroup of a free group, is free. But it is also of finite $\mathbb{Q}$-rank. So it is indeed finitely generated.

The Proof

Say $G' = \gamma_1^{\mathbb{Z}} \cdots \gamma_r^{\mathbb{Z}}$.

Then a rational solution of the equation is reduced to an integer solution up to a root of unity!

However, it is not a big problem; using the multiplicative independence assumption, one can deduce that only finitely many roots of unity could be involved. Hence considering the integer solutions of finitely many different equations, we get the desired finiteness result.