Unit equations in characteristic p

Peter Koymans
Universiteit Leiden

XXXth Journées Arithmétiques

Caen, France, July 2017

Introduction

Let K be a number field with unit group $\mathcal{O}_K^*$. For fixed $a, b, c \in K^*$ consider the unit equation

$$ax + by = c$$

to be solved in $x, y \in \mathcal{O}_K^*$. Unit equations frequently show up when solving Diophantine equations. One well known example of such a Diophantine equation is the Thue equation

$$F(x, y) = \delta \text{ in } x, y \in \mathbb{Z}$$

for a given square-free binary form $F(X, Y) \in \mathbb{Z}[X, Y]$ of degree $n \geq 3$ and $\delta \in \mathbb{Z} \setminus \{0\}$. By reducing the Thue equation to several unit equations, one can show that the Thue equation has only finitely many solutions.

History of unit equations

Finiteness results have been proved for the following types of unit equations:

Siegel (1921): $ax + by = c$ in $x, y \in \mathcal{O}_K^*$,

Mahler (1933): $ax + by = c$ in $x, y \in \mathbb{Z}_S^*$

$\mathbb{Z}_S := \mathbb{Z}[(p_1 \cdots p_t)^{-1}]$ ($S = \{p_1, \ldots, p_t\}$ finite set of primes)

$\mathbb{Z}_S^* = \{\pm p_1^{e_1} \cdots p_t^{e_t} : e_i \in \mathbb{Z}\}$,

Lang (1960): $ax + by = c$ in $x, y \in A^*$

A arbitrary finitely generated domain

over $\mathbb{Z}$ of characteristic 0.

The above results are all ineffective.

History II

Mahler and Evertse gave explicit upper bounds for the number of solutions of unit equations. The best and most general result is due to Beukers and Schlickewei (1996). They considered

$$x + y = 1 \tag{1}$$

to be solved in $(x, y) \in G$, where G is a multiplicative subgroup of $\mathbb{C}^* \times \mathbb{C}^*$ with $\dim_{\mathbb{Q}}(G \otimes_{\mathbb{Z}} \mathbb{Q}) = r$.

Theorem 1

Equation (1) has at most 2^{8r+8} solutions $(x, y) \in G$.

Characteristic p

A natural question is to prove an analogue in positive characteristic. Let K be a field of characteristic p and let G be a finitely generated multiplicative subgroup of $K^* \times K^*$ with $\dim_{\mathbb{Q}}(G \otimes_{\mathbb{Z}} \mathbb{Q}) = r$. Consider the equation

$$x + y = 1 \tag{2}$$

to be solved in $(x, y) \in G$. Can one still hope to show that there are finitely many solutions?

No, consider for example $K = \mathbb{F}_p(t)$ and $G = \langle (t, 1-t) \rangle$. Then we have

$$t^{p^k} + (1-t)^{p^k} = 1$$

for all integers $k \geq 0$, leading to infinitely many solutions of (2).

Our result

In view of the previous one can hope to show finiteness "up to Frobenius".

Theorem 2 (joint work with Carlo Pagano)

Let K be a field of characteristic $p > 0$ and let G be a finitely generated multiplicative subgroup of $K^* \times K^*$ with $\dim_{\mathbb{Q}}(G \otimes_{\mathbb{Z}} \mathbb{Q}) = r$. Then the equation

$$x + y = 1 \text{ in } (x, y) \in G \tag{3}$$

has at most $31 \cdot 19^r$ solutions (x, y) satisfying $(x, y) \notin G^p$. Equivalently, there is a set S of cardinality $|S| \leq 31 \cdot 19^r$ such that any solution of (3) with $x, y \notin \overline{\mathbb{F}_p}$ is of the shape s^{p^k}, where $s \in S$ and $k \in \mathbb{Z}_{\geq 0}$.

This answers a conjecture of Voloch (1998), who had previously shown a bound of the shape p^{Cr} with C an absolute constant.

Proof outline

Our proof is a modified version of the proof due to Beukers and Schlickewei. Their proof consists of roughly four parts:

1. Reduce to the case that G is a finitely generated subgroup of $\overline{\mathbb{Q}}^* \times \overline{\mathbb{Q}}^*$.
2. Prove several height inequalities for the solutions.
3. Map the solutions to a normed vector space V.
4. Transfer the height inequalities to V and deduce finiteness.

It turns out that the second step is by far the most tricky. We will first discuss the proof of Beukers and Schlickewei in characteristic 0 and then later on the necessary modifications in characteristic $p > 0$.

Diophantine approximation

In order to prove the desired height bounds, Beukers and Schlickewei need some binary forms from Diophantine approximation. Define for $N \in \mathbb{Z}_{>0}$ the binary form $W_N(X, Y) \in \mathbb{Z}[X, Y]$

$$W_N(X, Y) = \sum_{m=0}^{N} \binom{2N-m}{N-m} \binom{N+m}{m} X^{N-m}(-Y)^m.$$

Lemma 3

Put $Z := -X - Y$. Then we have the following identities in $\mathbb{Z}[X, Y]$.

(i) $W_N(Y, X) = (-1)^N W_N(X, Y)$;

(ii) $X^{2N+1} W_N(Y, Z) + Y^{2N+1} W_N(Z, X) + Z^{2N+1} W_N(X, Y) = 0$;

(iii) *there exists a non-zero integer c_N such that*

$$\det \begin{pmatrix} Z^{2N+1} W_N(X, Y) & Y^{2N+1} W_N(Z, X) \\ Z^{2N+3} W_{N+1}(X, Y) & Y^{2N+3} W_{N+1}(Z, X) \end{pmatrix} = c_N (XYZ)^{2N+1} (X^2 + XY + Y^2).$$

The normed vector space

Define a homomorphism $\varphi : G \to \mathbb{R}^{2s}$ by

$$\varphi : (x_1, x_2) \mapsto (\log |x_i|_v : v \in S, i = 1, 2)\,.$$

Write $\mathcal{S}$ for the image under φ of the set of $(x, y) \in G$ with $x + y = 1$. One can show that φ is at most two to one when restricted to this set.

Lemma 4

The set $\mathcal{S}$ has the following properties:

(i) *for any two distinct $u_1, u_2 \in \mathcal{S}$ we have*

$$||u_1|| \leq 2||u_2 - u_1|| + \log 4;$$

(ii) *for any two distinct $u_1, u_2 \in \mathcal{S}$ and any positive integer N, there is $M \in \{N, N+1\}$ such that*

$$||u_1|| \leq \frac{2}{M+1}||u_2 - (2M+1)u_1|| + \log 64;$$

(iii) *for any three distinct $u_0, u_1, u_2 \in \mathcal{S}$ we have*

$$||u_1 - u_0|| + ||u_2 - u_0|| > 0.09.$$

Positive characteristic

Most of the machinery from the Beukers and Schlickewei proof carries through to positive characteristic. There are two obvious issues:

(i) Recall that there exists a non-zero integer c_N such that

$$\det \begin{pmatrix} Z^{2N+1} W_N(X,Y) & Y^{2N+1} W_N(Z,X) \\ Z^{2N+3} W_{N+1}(X,Y) & Y^{2N+3} W_{N+1}(Z,X) \end{pmatrix} = c_N (XYZ)^{2N+1} (X^2 + XY + Y^2).$$

But now we would like $c_N \not\equiv 0 \bmod p$, which imposes some restrictions on N.

(ii) The Beukers and Schlickewei method shows finiteness and this is no longer true in positive characteristic.

A formula for c_N

So far no explicit formula was known for c_N in the literature. We were able to derive an explicit formula for c_N.

Lemma 5

We have

$$W_N(2,-1) = \sum_{i=0}^{N} \binom{2N-i}{N} \binom{N+i}{N} 2^{-i} = 4^N \binom{\frac{3}{2}N}{N}.$$

Proof.

This follows from some identities for hypergeometric functions. □

Corollary 6

Let p be an odd prime number and let N be a positive integer with $N < \frac{p}{3} - 2$. Then $c_N \not\equiv 0 \bmod p$.

Proof.

Use the previous lemma to give an explicit formula for c_N. □

Properties of $\mathcal{S}$

We get a similar homomorphism $\varphi : G \to \mathbb{R}^{2s}$ from G into a finite dimensional vector space as before. Denote by $\mathcal{S}$ the image under φ of all $(x, y) \in G$ satisfying $x + y = 1$ and $x, y \notin \overline{\mathbb{F}_p}$. In our new setting $\mathcal{S}$ has the following properties.

Lemma 7

(i) *for any two distinct $u, v \in \mathcal{S}$ we have*

$$||u|| \leq 2||v - u||;$$

(ii) *for any two distinct $u, v \in \mathcal{S}$ and any positive integer N such that $N < \frac{p}{3} - 2$, there is $M \in \{N, N+1\}$ such that*

$$||u|| \leq \frac{2}{M+1}||v - (2M+1)u||;$$

(iii) $p\mathcal{S} \subseteq \mathcal{S}$.

The end

Questions?