The method of Lawrence-Venkatesh in the case of the S-unit equation

Oberseminar *Diophantine problems and p-adic period mappings*

Milan Malčić

Universität Heidelberg
Arbeitsgruppe Arithmetische Geometrie

June 10, 2020

The following notation will be fixed throughout.

- K a number field with ring of integers $\mathcal{O}_K$.
- S a finite set of places of K containing all the archimedean places.
- $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ the prime ideals of $\mathcal{O}_K$ corresponding to the finite places in S.
- $\mathcal{O}_S$ the ring of S-integers.

Reminder on S-integers

An element $x \in K$ is called S-integer if $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ for all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ different from $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. The S-integers form a subring of K, which contains $\mathcal{O}_K$ as a subring. For $r = 0$ it is equal to $\mathcal{O}_K$. We have $\mathcal{O}_S \subseteq \mathcal{O}_{S'}$ for $S \subseteq S'$.

Example: If $K = \mathbb{Q}$ and $S = \{\infty, 7\}$, then $\mathcal{O}_S = \mathbb{Z}[1/7]$.

The S-unit equation (in two unknowns)

Many diophantine problems can be reduced to *S-unit equations* of the form

$$\alpha x + \beta y = 1 \quad \text{in } x, y \in \mathcal{O}_S^\times, \tag{1}$$

where α, β are fixed non-zero elements of K. Such equations are well-studied:

Theorem

The equation (1) has only finitely many solutions.

This theorem was implicitly proved by Siegel (1921) for $\mathcal{O}_S = \mathcal{O}_K$ and implicitly proved by Mahler (1933) for general $\mathcal{O}_S$. The first explicit proof is due to Lang (1960).

Lawrence and Venkatesh gave yet another proof in the case $\alpha = \beta = 1$:

Theorem 4.1 in [LV18]

The set

$$U := \{t \in \mathcal{O}_S^\times : 1 - t \in \mathcal{O}_S^\times\}$$

is finite.

Their proof serves as a proof-of-concept of their method.

Goal for today: Study their proof.

Notation: Henceforth we write $\mathcal{O} = \mathcal{O}_S$.

Suppose that $\sigma\colon E \longrightarrow E$ is a field automorphism of finite order m, with fixed field F. Then E/F is a finite Galois extension of degree $[E:F] = m$.
We will need the following lemma later on.

Lemma 2.1 in [LV18]

Let V be a finite-dimensional E-vector space, and $\psi\colon V \longrightarrow V$ a σ-semilinear automorphism. Define the centralizer of ψ in the ring of E-linear endomorphisms of V via

$$\mathfrak{Z}(\psi) := \{f\colon V \longrightarrow V \text{ an } E\text{-linear map}, f\psi = \psi f\};$$

it is an F-vector space. Then

$$\dim_F \mathfrak{Z}(\psi) = \dim_E \mathfrak{Z}(\psi^m),$$

where ψ^m is now E-linear.

A priori, from $\mathfrak{Z}(\psi)$ being an F-vector space we can only deduce $\dim_F \mathfrak{Z}(\psi) \leq (\dim_F V)^2$.

With Lemma 2.1, we get $\dim_F \mathfrak{Z}(\psi) \leq (\dim_E V)^2$.

So our naive bound improves by a factor of $[E : F]^2$.

In our application later:
$F = K_v$, a finite unramified extension of $\mathbb{Q}_p$;
$E = K_v(t_0^{1/m})$, an unramified extension of K_v of degree m;
$\sigma = \mathrm{Frob}_{E/K_v} \in \mathrm{Gal}(E/K_v)$; so indeed $F = E^\sigma$;
V a suitable H^i_{dR}, φ_v the Frobenius on V;
$\psi = \varphi_v^{[K_v:\mathbb{Q}_p]}$.

ψ is indeed σ-semilinear, as φ_v is τ-semilinear and $\sigma = \tau^{[K_v:\mathbb{Q}_p]}$, where $\tau = \mathrm{Frob}_{E/\mathbb{Q}_p}$. Note that $\tau|_{K_v} = \mathrm{Frob}_{K_v/\mathbb{Q}_p}$.

Recall the notation:

- $\pi\colon \mathcal{X} \longrightarrow \mathcal{Y}$ a smooth proper morphism of smooth $\mathcal{O}$-schemes,
  $\pi\colon X \longrightarrow Y$ its base change to K.
- Fix
  1. a place v of K such that
     - the prime number p below v satisfies $p > 2$,
     - $K_v/\mathbb{Q}_p$ is unramified,
     - no prime above p lies in S,
  2. an embedding $\iota\colon K \hookrightarrow \mathbb{C}$,
  3. a cohomology degree $i \geq 0$,
  4. a point $y_0 \in \mathcal{Y}(\mathcal{O})$.
- For $y \in \mathcal{Y}(\mathcal{O})$, we have
  $\rho_y\colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}\, H^i_{\text{ét}}(X_y \times_K \overline{K}, \mathbb{Q}_p)$.

More notation

- The residue disks at y_0:

$$U_v := \{y \in \mathcal{Y}(\mathcal{O}) \colon y \equiv y_0 \mod v\},$$
$$\Omega_v := \{y \in \mathcal{Y}(\mathcal{O}_v) \colon y \equiv y_0 \mod v\},$$
$$U_v^{\mathrm{ss}} := \{y \in \mathcal{Y}(\mathcal{O}) \colon y \equiv y_0 \mod v \text{ and } \rho_y \text{ is semisimple}\}.$$

Remark

In fact, Faltings shows that all the representations we consider are semisimple, so $U_v = U_v^{\mathrm{ss}}$. This requires the full weight of his argument. To give an independent proof, Lawrence and Venkatesh need to contemplate $U_v - U_v^{\mathrm{ss}}$. In the case of the S-unit equation, this is the subject of [LV18, Lemma 4.4 (Generic simplicity)].

Recalling Prop. 3.4

- Let $V := H^i_{dR}(X_{y_0}/K)$, with base changes along v resp. ι denoted by V_v resp. $V_{\mathbb{C}}$.
- $\mathcal{H}$ the K-variety of flags in V with the same dimensional data as the Hodge filtration on V, and $h_0 \in \mathcal{H}(K)$ the point corresponding to the Hodge filtration on V.
- Let $\varphi_v \colon V_v \longrightarrow V_v$ be the τ-semilinear Frobenius coming from crystalline cohomology.
- Let Γ be the Zariski closure of the monodromy $\mu \colon \pi_1(Y_{\mathbb{C}}(\mathbb{C}), y_0) \longrightarrow \mathrm{GL}(V_{\mathbb{C}})$. Note that Γ acts on $\mathcal{H}_{\mathbb{C}}(\mathbb{C})$.

Prop. 3.4 in [LV18]

Suppose that

$$\dim_{K_v} Z(\varphi_v^{[K_v:\mathbb{Q}_p]}) < \dim_{\mathbb{C}} \Gamma \cdot h_0^{\iota}$$

where $Z(\ldots)$ denotes the centralizer in $\mathrm{GL}_{K_v}(V_v)$.Then U_v^{ss} is contained in a proper K_v-analytic subvariety of Ω_v.

Proof of Thm 4.1: First attempt

We choose

$$\begin{aligned}\mathcal{Y} &= \mathbb{P}^1_{\mathcal{O}} - \{0,1,\infty\} \\ &= \mathbb{A}^1_{\mathcal{O}} - \{0,1\} \\ &= \operatorname{Spec}\mathcal{O}[T, T^{-1}, (T-1)^{-1}].\end{aligned}$$

Then $\mathcal{Y}(\mathcal{O}) = \{t \in \mathcal{O}_S^\times : 1 - t \in \mathcal{O}_S^\times\} =: U$.

Let $\pi\colon \mathcal{X} \longrightarrow \mathcal{Y}$ be the Legendre family of elliptic curves, so that its fiber over t is (the smooth proper model of) the elliptic curve $E_t\colon y^2 = x(x-1)(x-t)$.

We fix an arbitrary $y_0 \in \mathcal{Y}(\mathcal{O})$, and an arbitrary v that fulfils the desired conditions we recalled.
We choose $i = 1$, so that $V_v = H^1_{dR}(X_{y_0}/K_v)$. Then $\dim_{K_v}(V_v) = 2$.

We need $\dim_{K_v} Z(\varphi_v^{[K_v:\mathbb{Q}_p]}) < \dim_{\mathbb{C}} \Gamma \cdot h_0^{\iota}$ to hold.

Claim: The left-hand side could be as large as 4.

Proof.

Indeed, φ_v could be a scalar, in which case $Z(\varphi_v^{[K_v:\mathbb{Q}_p]}) = \mathrm{GL}_{K_v}(V_v)$. The claim now follows since $\dim_{K_v}(V_v) = 2$ and the algebraic group GL_2 has dimension 4. □

Claim: The right-hand side is 1.

Proof.

Indeed, $\Gamma \cdot h_0^{\iota} \subseteq \mathcal{H}_{\mathbb{C}}(\mathbb{C}) = \{1\text{-dimensional subspaces of } V_{\mathbb{C}}\}$.
Fix a basis of $V_{\mathbb{C}}$. So $\mathrm{im}(\mu)$ lies in $\mathrm{GL}_2(\mathbb{C})$, and $\mathcal{H}_{\mathbb{C}}(\mathbb{C}) = \mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$.
By [Lit], $\mathrm{im}(\mu)$ is a finite-index subgroup of a conjugate of $\mathrm{SL}_2(\mathbb{Z})$.
Such groups are Zariski-dense in $\mathrm{SL}_2(\mathbb{C})$.
So $\Gamma = \mathrm{SL}_2(\mathbb{C})$. Thus $\Gamma \cdot h_0^{\iota} = \mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$. □

The inequality $4 < 1$ does not hold, so we can't apply Prop. 3.4.

Let $m \in \mathbb{N}$. Suppose that we can modify the Legendre family so that each fiber is a disjoint union of m elliptic curves.

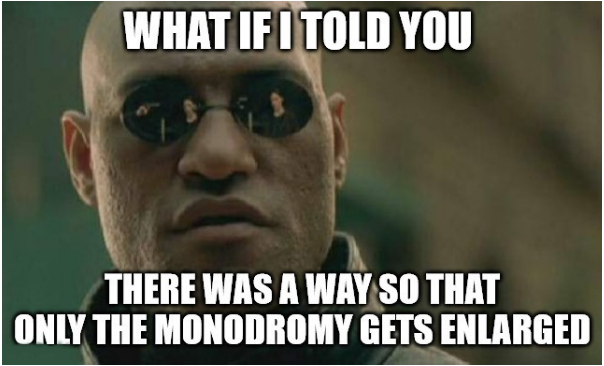
Then the splitting of $X_{y_0,\mathbb{C}}$ into geometric components induces a splitting $V_{\mathbb{C}} = \bigoplus_{j=1}^{m} V_j$, with $\dim_{\mathbb{C}}(V_j) = 2$ for all j.

One should then be able to deduce (from the monodromy of the unmodified Legendre family) that $\dim_{\mathbb{C}} \Gamma \cdot h_0^{\iota} = m$.

On the other hand, $\dim_{K_v}(V_v) = 2m$, so our naive bound for the centralizer amounts to $4m^2$.

So both the monodromy and the centralizer grow, whence the false inequality $4 < 1$ becomes the false inequality $4m^2 < m$, and we seemingly gain nothing...

But...


WHAT IF I TOLD YOU
THERE WAS A WAY SO THAT
ONLY THE MONODROMY GETS ENLARGED

Suppose that, because of the disconnectedness of the fibers, V_v obtains the structure of an E-vector space, where E/K_v is a certain finite unramified extension of degree m.

Lemma 2.1 then improves our naive bound by m^2, i.e. we get

$$\dim_{K_v} Z'(\varphi^{[K_v:\mathbb{Q}_p]}) \leq 4m^2/m^2 = 4$$

where $Z'(...)$ is now the centralizer in $\mathrm{GL}_E(V_v)$. The reason we may shift our interest from Z to Z' is that the Gauss-Manin identifications are in a certain way compatible with the E-linear structure.

Altogether, the false inequality $4m^2 < m$ becomes the potentially correct inequality $4 < m$. We won't be able to choose m freely in the rigorous proof, e.g. it will have to be a power of 2. So we will need to ensure that $m \geq 8$. This won't be a problem. (Indeed, as we shall see, we could force m to be arbitrarily large.)

Theorem 4.1 in [LV18]

The set

$$U := \{t \in \mathcal{O}_S^\times : 1 - t \in \mathcal{O}_S^\times\}$$

is finite.

Structure of the proof:

(I) Setup and reduction to Lemma 4.2,

(II) "Generic simplicity" (Lemma 4.4),

(III) Modified Legendre family and main argument (Lemma 4.2),

(IV) "Big monodromy" (Lemma 4.3).

We will focus on (III), and sketch or assume the rest.

(I) Setup and reduction to Lemma 4.2

Let m be the largest power of 2 dividing the order of the group of roots of unity in K.

We may freely enlarge K and S (this only makes U larger), so w.l.o.g. assume that $m \geq 8$ and S contains all the places above 2.

Define $U_1 := \{t \in U \colon t \notin (K^\times)^2\}$. A short elementary argument shows that $U \subseteq U_1 \cup U_1^2 \cup U_1^4 \cup \ldots \cup U_1^m$.

Hence it suffices to show that U_1 is finite.

The definitions of m and U_1 ensure that, for every $t \in U_1$, the degree of the cyclic Galois extension $K(t^{1/m})/K$ is m.

By Hermite-Minkowski, the set

$$\left\{K(t^{1/m})\colon\, t \in U_1\right\} \big/ K\text{-isomorphy}$$

is finite.
Fixing a cyclic Galois extension L/K of degree m, we see that it suffices to show that

$$U_{1,L} := \{t \in U_1\colon\, K(t^{1/m}) \cong L\}$$

is finite.

Choose a prime v of K such that

(i) the Frobenius at v generates $\mathrm{Gal}(L/K)$;

(ii) the prime p of $\mathbb{Q}$ below v is unramified in K;

(iii) no prime of S lies above p.

Side note: Property (i) implies that v is inert in L and that the degree of the unramified extension L_v/K_v is also m.
Property (ii) implies that $K_v/\mathbb{Q}_p$ is unramified.

In summary, it suffices to prove the following lemma.

Lemma 4.2 in [LV18]

In the situation as above, the set

$$U_{1,L,v} := \{t \in U_{1,L} \colon t \equiv t_0 \mod v\}$$

is finite for any fixed $t_0 \in \mathcal{O}$.

For the proof of Lemma 4.2, we will need:

Lemma 4.4 in [LV18] (Generic simplicity)

Let L' be a number field and p' an odd prime number that is unramified in L'. There are only finitely many $z \in L'$ such that

- z and $1 - z$ are both p'-units, and
- the Galois representation of $\mathrm{Gal}(\overline{L'}/L')$ on the Tate module $T_{p'}(E_z) = H^1_{\text{ét}}(E_{z,\overline{L'}}, \mathbb{Q}_{p'})$ of the elliptic curve $E_z\colon y^2 = x(x-1)(x-z)$ is not simple.

Let $\mathcal{Y} = \mathbb{P}^1_{\mathcal{O}} - \{0, 1, \infty\}$ and let $\mathcal{Y}' = \mathbb{P}^1_{\mathcal{O}} - \{0, \mu_m, \infty\}$.

Let $\mathcal{X} \longrightarrow \mathcal{Y}'$ be the Legendre family and let π be the composition

$$\mathcal{X} \longrightarrow \mathcal{Y}' \xrightarrow{u \mapsto u^m} \mathcal{Y},$$

which we call the Modified Legendre family. The geometric fiber X_t over $t \in Y(K)$ is

$$\coprod_{z^m = t} E_z$$

where E_z is the curve $y^2 = x(x-1)(x-z)$.

Crucial observation: X_t is a priori a K-scheme, but the factorization $X \longrightarrow Y' \longrightarrow Y$ induces on X_t the structure of a $K(t^{1/m})$-scheme via the morphism $X_t \longrightarrow Y'_t \cong \operatorname{Spec} K(t^{1/m})$.

In particular, V_v is naturally a vector space over $K_v(t^{1/m})$. Note that $K_v(t^{1/m})/K_v$ is unramified and $[K_v(t^{1/m}) : K_v] = m$, as we have previously observed in a side note.

Proof of Lemma 4.2: The proof won't be an application of Prop. 3.4, but rather an argument similar to the proof of Prop. 3.4, with added complication coming from the interaction of the fields K and L.

Fix a $t_0 \in U_{1,L}$. Need to show:

$$U_{1,L,v} := \{t \in U_{1,L} \colon t \equiv t_0 \mod v\}$$

is finite.
By Lemma 4.4, $U_{1,L,v} - (U_{1,L,v})^{\mathrm{ss}}$ is finite.
By Lemma 2.3, $(U_{1,L,v})^{\mathrm{ss}}$ produces finitely many isomorphy classes of representations.
Fix an isomorphy class of pairs $\left(K(t^{1/m}), \rho_t|_{G_{K(t^{1/m})}}\right)$. Via restriction we get an isomorphy class of pairs $\left(K_v(t^{1/m}), \rho_t|_{G_{K_v(t^{1/m})}}\right)$. By p-adic Hodge theory, it corresponds to an isomorphy class of the data

$$D_t := \left(H^1_{\mathrm{dR}}(X_t/K_v) \text{ as } K_v(t^{1/m})\text{-module}, \mathrm{Frob}, \mathrm{Fil}\right).$$

We see that it suffices to show that

$$\underline{\underline{U}}_{1,L,v} := \{t \in U_{1,L,v} \colon D_t \text{ is in the fixed class}\}$$

is finite.

One can show that the Gauss-Manin connection induces a K_v-isomorphism $K_v(t^{1/m}) \cong K_v(t_0^{1/m})$ such that the identifications

$$\mathrm{GM}\colon V_v = H^1_{\mathrm{dR}}(X_{t_0}/K_v) \xrightarrow{\sim} H^1_{\mathrm{dR}}(X_t/K_v)$$

are compatible with the structure of $K_v(t^{1/m}) \cong K_v(t_0^{1/m})$ -modules.

Hence the period map

$$\begin{tikzcd}
\Omega_v \arrow[dr, "\Phi"] & & \\
& \{K_v\text{-subspaces of dimension } m \text{ in } V_v\} \arrow[r, "\sim"] & \mathrm{Gr}(2m, m)_{K_v}
\end{tikzcd}$$

factors as

$$\begin{tikzcd}
\Omega_v \arrow[r] \arrow[dr, "\Phi"'] & \{K_v(t_0^{1/m})\text{-lines in } V_v\} \arrow[r, "\sim"] \arrow[d] & \mathbb{P}^1_{K_v(t_0^{1/m})} \arrow[d] \\
& \{K_v\text{-subspaces of dimension } m \text{ in } V_v\} \arrow[r, "\sim"] & \mathrm{Gr}(2m, m)_{K_v}
\end{tikzcd}$$

Altogether, it follows that

$$\Phi\left(\underline{\underline{U}}_{1,L,v}\right) \subseteq \bigcup_{i=1}^{m} \text{a } Z_{\alpha_i}\text{-orbit} \tag{2}$$

where $\{\alpha_1, \dots, \alpha_m\} = \mathrm{Gal}(K_v(t_0^{1/m})/K_v)$ and

$Z_{\alpha_i} := \{\alpha_i\text{-linear isomorphisms } V_v \longrightarrow V_v \text{ that commute with } \varphi_v\}$.

Let $\psi := \varphi_v^{[K_v:\mathbb{Q}_p]}$. We can replace Z_{α_i} by $Z_{\alpha_i}(\psi)$ in (2).

The Lie algebra of the latter is

$\mathfrak{Z}_{\alpha_i} := \{\alpha_i\text{-linear endomorphisms } V_v \longrightarrow V_v \text{ that commute with } \psi\}$.

It is isomorphic to $\mathfrak{Z}_{\mathrm{id}} =: \mathfrak{Z}$, and $\dim_{K_v} \mathfrak{Z} \leq 4$ by Lemma 2.1.

Hence the right-hand side of (2) is contained in a Zariski-closed subset of dimension ≤ 4.

To conclude the proof of Lemma 4.2 by applying Lemma 3.3, it remains to show that $\dim_{\mathbb{C}} \Gamma \cdot h_0^{\iota} > 4$. Indeed, knowing the monodromy of the (unmodified) Legendre family, one deduces that $\dim_{\mathbb{C}} \Gamma \cdot h_0^{\iota} = m$. This is the subject of Lemma 4.4 (Big monodromy). Since $m \geq 8 > 4$, this completes the proof.

[Lit] Daniel Litt.
Variation of hodge structures.
Notes for Number Theory Learning Seminar on Shimura Varieties. Available at http://virtualmath1.stanford.edu/~conrad/shimsem/2013Notes/Littvhs.pdf.

[LV18] Brian Lawrence and Akshay Venkatesh.
Diophantine problems and p-adic period mappings.
Preprint, 2018.
Available at https://arxiv.org/abs/1807.02721v3.