# Integral points on affine curves

Marius Leonhardt [1], joint work in progress with Martin Lüdtke [2]

[1]Universität Heidelberg [2]Max Planck Institute for Mathematics, Bonn

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

GAUS

## Motivation

What are the integer solutions to the equation

$$\mathcal{Y}\colon\quad v^3 = u(u^2+u+1)\,? \tag{1}$$

How many are there? How do we find them? What about rational solutions whose denominators are only divisible by primes in $S$?

## Background

Let $Y/\mathbb{Q}$ be a smooth affine hyperbolic curve with regular model $\mathcal{Y}/\mathbb{Z}$.

**Theorem 1** (Siegel, Faltings): *The set $\mathcal{Y}(\mathbb{Z}_S)$ is finite.*

However, this result does not give a method for finding the $S$-integral points nor does it give a bound on the size of the set $\mathcal{Y}(\mathbb{Z}_S)$. By using a variant of the Chabauty–Kim method, we proved

**Theorem 2** (L.-Lüdtke-Müller, [2]): *Let $p \notin S$ be a prime.*

1. *If $r + \#S < g + n - 1$, then $\mathcal{Y}(\mathbb{Z}_S)$ lies in a finite subset of $\mathcal{Y}(\mathbb{Z}_p)$.*
2. *If $\frac{1}{2}r(r+3) + \#S < \frac{1}{2}g(g+3) + n - 1$, then*

$$\#\mathcal{Y}(\mathbb{Z}_S) \le \kappa_p \cdot \prod_{\ell \in S}(n_\ell + n) \cdot \prod_{\ell \notin S} n_\ell \cdot \#\mathcal{Y}(\mathbb{F}_p) \cdot (4g+2n-2)^2(g+1)\,.$$

## Goals

1. Turn Theorem 2 into an algorithm that computes $\mathcal{Y}(\mathbb{Z}_S)$.
2. Improve the bound while only assuming $r + \#S < g + n - 1$.

## Notation

- $X$ a smooth projective curve over $\mathbb{Q}$ of genus $g$,
- $J$ its Jacobian, $r = \mathrm{rk}_{\mathbb{Z}}\, J(\mathbb{Q})$ its Mordell–Weil rank,
- $D \subset X$ a divisor consisting (for simplicity) of $n$ geometric points that are all $\mathbb{Q}$-rational, and $Y = X \setminus D$ the affine curve,
- $\mathcal{X}$ a proper regular model of $X$ over $\mathbb{Z}$ and $\mathcal{Y} = \mathcal{X} \setminus \mathcal{D}$, where $\mathcal{D}$ is the closure of $D$ in $\mathcal{X}$, with $n_\ell = \#(\text{components of } \mathcal{X}_{\mathbb{F}_\ell})$,
- $S$ a finite set of primes, $p \notin S$ a prime of good reduction for $(\mathcal{X}, \mathcal{D})$ and $\kappa_p = 1 + \frac{p-1}{(p-2)\log(p)}$,
- $P_0 \in \mathcal{Y}(\mathbb{Z}_S)$ a base point.

## The generalised Jacobian...

...is the semi-abelian variety $J_Y$ that sits in the short exact sequence

$$0 \longrightarrow (\mathbb{G}_m)^n/\mathbb{G}_m \longrightarrow J_Y \longrightarrow J \longrightarrow 0$$

whose $\mathbb{Q}$-points can be described as

$$J_Y(\mathbb{Q}) = \frac{\{\text{divisors on } Y \text{ of degree } 0\}}{\{(f) \mid f \in k(X)^\times \text{ with } f(Q) = 1 \text{ for all } Q \in D\}}.$$

We use $P_0$ for an Abel-Jacobi map $\mathrm{AJ}_{P_0}\colon Y \to J_Y,\ P \mapsto [P - P_0]$.

## Intersection numbers on $\mathcal{X}$

On the arithmetic surface $\mathcal{X}$ we can calculate intersection numbers $i_\lambda$ of two divisors [1, Ch. III]. There are two types of prime divisors:

1. horizontal: closures $\mathcal{P}$ in $\mathcal{X}$ of closed points $P \in X$,
2. vertical: components of the special fibres $\mathcal{X}_{\mathbb{F}_\ell}$.

From now on, assume for simplicity that $\mathcal{Q} \cap \mathcal{Q}' = \emptyset$ for any $Q, Q' \in D$, so that $\mathcal{D} \cong \coprod_Q \operatorname{Spec} \mathbb{Z}$. For a rational prime $\ell$ define the $\mathbb{Q}$-vector space $V_\ell = (\bigoplus_Q \mathbb{Q})/\mathbb{Q}$. Define

$$\sigma = (\sigma_\ell)_\ell\colon J_Y(\mathbb{Q}_\ell) \longrightarrow \bigoplus_\ell V_\ell$$

as follows. For a degree-0 divisor $F$ on $Y$, let $\Psi_\ell(F) = \mathcal{F} + \Phi_\ell(F)$ be an extension to a $\mathbb{Q}$-divisor on $\mathcal{X}_{\mathbb{Z}_\ell}$ having $\ell$-intersection number $0$ with every component of the special fibre $\mathcal{X}_{\mathbb{F}_\ell}$. Then

$$\sigma_\ell(F) := (i_{Q \bmod \ell}(\Psi_\ell(F), \mathcal{Q}))_Q.$$

**Lemma 3** : *$\sigma_\ell\colon J_Y(\mathbb{Q}_\ell) \to V_\ell$ and $\sigma$ are well-defined homomorphisms. Moreover, $\sigma$ is surjective.*

## Selmer subspace of $J_Y(\mathbb{Q})$

For every prime $\ell$, choose a component $\Sigma_\ell$ of $\mathcal{X}_{\mathbb{F}_\ell}$, and let $\Sigma = (\Sigma_\ell)_\ell$. Let $\mathcal{Y}(\mathbb{Z})_\Sigma$ denote those points whose mod-$\ell$ reduction lies on $\Sigma_\ell$ for every $\ell$.

**Lemma 4** : *The image of $\mathcal{Y}(\mathbb{Z})_\Sigma$ under $\sigma \circ \mathrm{AJ}_{P_0}$ is contained in an a-priori explicitly computable affine subspace $\mathfrak{S}_\Sigma$ of $\bigoplus_\ell V_\ell$ of dimension $\le \#S$.*

**Definition 5** : The $\Sigma$-Selmer space is the affine subspace

$$\mathrm{Sel}_\Sigma := \sigma^{-1}(\mathfrak{S}_\Sigma)$$

of $J_Y(\mathbb{Q})_\mathbb{Q} := \mathbb{Q} \otimes J_Y(\mathbb{Q})$. It has dimension $r + \#S$.

By Lemma 4, we know that $\mathrm{AJ}_{P_0}(\mathcal{Y}(\mathbb{Z})_\Sigma)$ is contained in $\mathrm{Sel}_\Sigma$.

## Chabauty–Kim diagram

The following diagram sums up the situation:

$$\begin{array}{ccccccc}
\mathcal{Y}(\mathbb{Z}_S)_\Sigma & \hookrightarrow & \mathcal{Y}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{Y}(\mathbb{Z}_p) & & \\
\downarrow & & \downarrow & & \downarrow & & \\
 & & Y(\mathbb{Q}) & \hookrightarrow & Y(\mathbb{Q}_p) & & \\
\downarrow & & \downarrow{\scriptstyle \mathrm{AJ}_{P_0}} & & \downarrow{\scriptstyle \mathrm{AJ}_{P_0}} & & \\
\mathrm{Sel}_\Sigma & \hookrightarrow & J_Y(\mathbb{Q})_\mathbb{Q} & \hookrightarrow & J_Y(\mathbb{Q}_p)_\mathbb{Q} & \xrightarrow{\log_{J_Y}} & \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1(D))^\vee \\
\downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} & & & & \\
\mathfrak{S}_\Sigma & \hookrightarrow & \bigoplus_\ell V_\ell & & & &
\end{array}$$

Here the map $\log_{J_Y}$ is given by $p$-adic integration of logarithmic differential forms that only have simple poles at $D$.

## Results

As $\dim_{\mathbb{Q}_p} \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1(D)) = g + n - 1$, we proved

**Theorem 6** (L.-Lüdtke): *If $r + \#S < g + n - 1$, then there exists a non-zero $\eta \in \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1(D))$ and a constant $a \in \mathbb{Q}_p$ such that*

$$\rho\colon \mathcal{Y}(\mathbb{Z}_p) \to \mathbb{Q}_p, \quad \rho(z) = \int_{P_0}^z \eta - a$$

*vanishes on $\mathcal{Y}(\mathbb{Z}_S)_\Sigma$. Moreover, $\eta$ and $a$ can be explicitly computed.*

By estimating the number of zeros of such integrals, we proved

**Theorem 7** (L.-Lüdtke): *If $r + \#S < g + n - 1$ and $p > 2g + n$ then*

$$\#\mathcal{Y}(\mathbb{Z}_S) \le \prod_{\ell \in S}(n_\ell + n) \cdot \prod_{\ell \notin S} n_\ell \cdot (\#\mathcal{Y}(\mathbb{F}_p) + 2g - 2 + n).$$

## Back to the start

For equation (1) we have $g = 1$, $X = J$ is the elliptic curve 243.a1 [3] with $r = 1$, $n_\ell = 1$ for all $\ell$, and $n = 3$. Take $p = 7$. Theorem 2 gives $\#\mathcal{Y}(\mathbb{Z}) \le 1862$, but Theorem 7 improves this to $\#\mathcal{Y}(\mathbb{Z}) \le 12$.

## References

[1] Serge Lang, *Introduction to Arakelov theory*, Springer-Verlag, New York, 1988. MR 969124

[2] Marius Leonhardt, Martin Lüdtke, and Jan Steffen Müller, *Linear and quadratic Chabauty for affine hyperbolic curves*, Int. Math. Res. Not. IMRN **21** (2023), 18752–18780.

[3] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2025, [Online; accessed 26 March 2025].

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) TRR 326 *Geometry and Arithmetic of Uniformized Structures*, project number 444845124.