UNIVERSITÄT BAYREUTH

Simultaneous Torsion in the Legendre Family of Elliptic Curves

Michael Stoll
Universität Bayreuth

Torsion groups and Galois representations of elliptic curves

Zagreb

June 29, 2018

News Alert

On Wednesday, Peter Bruin, Maarten Derickx and I, motivated by Daeyeol Jeon's talk, proved the following.

Theorem.
Up to the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, there is exactly one elliptic curve E defined over a cyclic cubic extension K of $\mathbb{Q}$ such that E is not defined over $\mathbb{Q}$ and $E(K)$ contains a point of order 13.

The curve E is

$$y^2 + (1-r)xy - sy = x^3 - sx^2,$$

where

$$r = \frac{6\alpha^2 + 50\alpha - 208}{3^2 \cdot 13^2} \qquad \text{and} \qquad s = \frac{10\alpha^2 + 90\alpha - 1936}{3^2 \cdot 13^3}$$

and $\alpha^3 - \alpha^2 - 82\alpha + 64 = 0$ (disc$(K) = (13 \cdot 19)^2$; $K = 3.3.61009.1$).

And now for something completely different . . .

Introduction

Consider, for $\lambda \in \mathbb{C} \setminus \{0, 1\}$, the Legendre elliptic curve

$$E_\lambda \colon y^2 = x(x-1)(x-\lambda)\,.$$

For $\alpha \in \mathbb{C} \setminus \{0, 1\}$, let $P_\lambda(\alpha) \in E_\lambda$ be a point with x-coordinate α and define

$$T(\alpha) = \{\lambda \in \mathbb{C} \setminus \{0, 1\} : P_\lambda(\alpha) \in E_\lambda(\mathbb{C}) \text{ is torsion}\}.$$

Then $T(\alpha)$ is a countably infinite set
consisting of elements algebraic over $\mathbb{Q}(\alpha)$.

Now consider $\alpha, \beta \in \mathbb{C} \setminus \{0, 1\}$ with $\alpha \neq \beta$ and set $T(\alpha, \beta) = T(\alpha) \cap T(\beta)$.

Question.
What can we say about $T(\alpha, \beta)$?

Known Results

There are three cases:

- α and β are algebraic.
- $\mathrm{trdeg}_{\mathbb{Q}}\big(\mathbb{Q}(\alpha, \beta)\big) = 1$.
- α and β are algebraically independent. Then $T(\alpha, \beta) = \emptyset$.

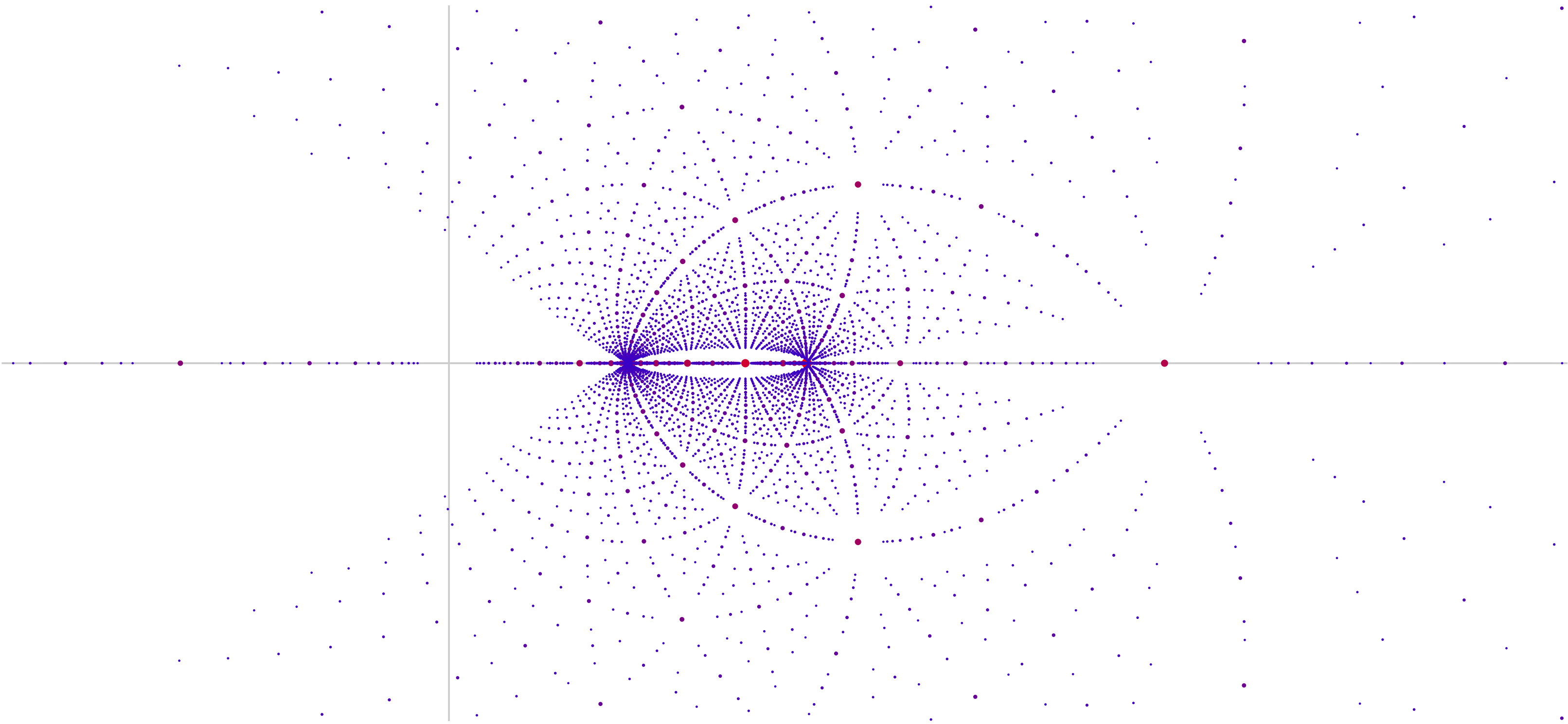
Masser and Zannier showed that $T(2, 3)$ is finite
and then proved the following more general result.

Theorem (Masser and Zannier).
$T(\alpha, \beta)$ is always finite; when $\mathrm{trdeg}_{\mathbb{Q}}\big(\mathbb{Q}(\alpha, \beta)\big) = 1$, this is effective.

Goals of this talk:
(1) Get effectivity for some algebraic α, β.
(2) Get optimal result for transcendence degree 1.
(3) Use this to get more information on the algebraic case.

Structure of $T(\alpha)$

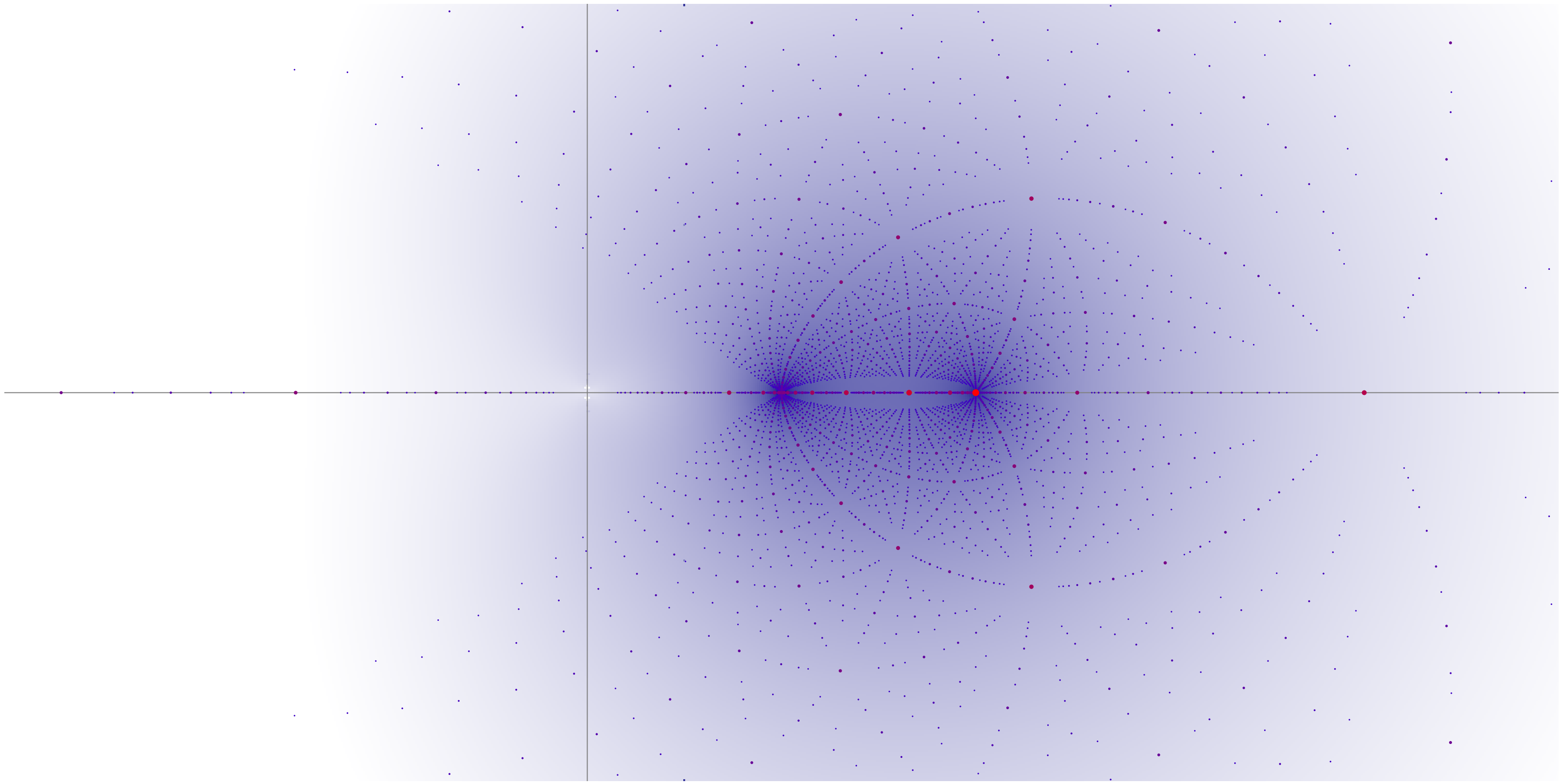
In $\mathbb{C}$, $T(\alpha)$ is all over the place,
reflecting the fact that E_{tors} is dense in $E(\mathbb{C})$:



This shows $T_{40}(2)$, where $T_n(\alpha) = \{\lambda \in T(\alpha) : P_\lambda(\alpha) \in E_\lambda \text{ has order } \leq n\}$.

Aside

DeMarco, Wang and Ye show
that there is actually a limiting distribution μ_α
and that $\mu_\alpha \neq \mu_\beta$ when $\alpha \neq \beta$.



Aside

DeMarco, Wang and Ye show
that there is actually a limiting distribution μ_α
and that $\mu_\alpha \neq \mu_\beta$ when $\alpha \neq \beta$.

So when $T(\alpha, \beta)$ is infinite,
we can approximate both μ_α and μ_β with the same sequence of points,
implying $\mu_\alpha = \mu_\beta$ and therefore $\alpha = \beta$.

This gives an alternative proof of the Masser-Zannier result.

Structure of $T(\alpha)$, p-adically

Fix a prime p.
In contrast to the situation over $\mathbb{C}$, E_{tors} is discrete in $E(\mathbb{C}_p)$.
This translates into $T(\alpha)$ being discrete in $\mathbb{C}_p \setminus \{0, 1\}$.

Since $T(\alpha)$ moves continuously with α,
we can show that $T(\alpha, \beta)$ is empty if α and β are p-adically close:

Proposition.
Let $\alpha, \beta \in \mathbb{C}_p$ with $0 < |\alpha(\alpha - 1)|_p \leq 1$ and $0 < |\beta - \alpha|_p < |\alpha(\alpha - 1)|_p \, |p|_p^{2/(p-1)}$.
Then $T(\alpha, \beta) = \emptyset$.

We also get that $T(\alpha, \beta) = \emptyset$ when $|\alpha|_p < |p|_p^{2/(p-1)}$ and $|\beta - 1|_p < |p|_p^{2/(p-1)}$.

There are slightly better results when $p = 2$.

Application

If $\alpha \in \mathbb{Z}$, then there are only finitely many $\beta \in \mathbb{Z} \setminus \{0,1\}$ with $T(\alpha,\beta) \neq \emptyset$.

Example.
Consider $\alpha = 2$ and $\beta \in \mathbb{Z} \setminus \{0,1\}$.
We will see in a moment that $T(2,\beta) = \emptyset$ when β is odd.
From the above, we get that $T(2,\beta) = \emptyset$ when
$\beta - 2$ is divisible by 8, 9 or a prime $p \geq 5$.
This leaves only $\beta = -10, -4, -2, 4, 6, 8, 14$.

It turns out that the sets $T(2,\beta)$ for these β can all be determined explicitly with the methods discussed later in this talk.

We obtain that $T(2,\beta) = \emptyset$ except for $\beta \in \{-2, 4\}$
and that $T(2,-2) = T(2,4) = \{4\}$.

Idea for Effectivity

If we can show that $T(\alpha) \subset \mathbb{C}_p$ is sufficiently localized,
then we get a handle on $T(\alpha, \beta)$ when α and β are not p-adically close.

Easy Lemma.

For $\alpha, \lambda \in \mathbb{C}_p \setminus \{0, 1\}$ the following are equivalent:

- $\lambda \in T(\alpha)$.
- $\lambda = \alpha$, or $\psi_n(\lambda, \alpha) = 0$ for some $n \geq 3$,
  where $\psi_n(\lambda, x)$ is the nth division polynomial of E_λ.
- α is preperiodic for the Lattès map $f_\lambda \colon x \longmapsto \dfrac{(x^2 - \lambda)^2}{4x(x-1)(x-\lambda)}$ on $\mathbb{P}^1$.
  (This point of view was used by Mavraki.)

2-adic Localization

We look specifically at $p = 2$. $|\cdot|$ denotes the 2-adic absolute value.

It is easy to see that $T(1/\alpha) = \{1/\lambda : \lambda \in T(\alpha)\}$, so we can assume that $|\alpha| \le 1$.
Then for all $\lambda \in T(\alpha)$, we have $|\lambda| \le 1$ as well
(as can be seen from the division polynomials or from the Lattès map).

If $|\lambda| \le 1$ and $x \in \mathbb{C}_2$ has $|x| > 1$, then $|f_\lambda(x)| = 4|x|$,
and x cannot be preperiodic.

So if $\lambda \in T(\alpha)$, we must have that $\lambda = \alpha$ ($\iff f_\lambda(\alpha) = \infty$) or $|f_\lambda(\alpha)| \le 1$.
The latter means $|\lambda - \alpha^2|^2 \le |4\alpha(\alpha - 1)(\alpha - \lambda)| \le |4|$, which says that

$$\lambda \equiv \alpha^2 \bmod 2\,.$$

Corollary. $T(2,3) = \emptyset$.

A Slightly More Precise Result

Note that we have

$$\lambda \in T(\alpha) \iff f_\lambda(\alpha) \in \{0, 1, \lambda, \infty\} \quad \text{or} \quad \lambda \in T(f_\lambda(\alpha)) .$$

The first condition is

$$\lambda \in S(\alpha) := \left\{\alpha, \alpha^2, \alpha(2-\alpha), \tfrac{\alpha^2}{2\alpha-1}\right\} .$$

We can easily show that for $|\alpha| \leq 1$ (similarly for $|\alpha| > 1$),

$$T(f_\lambda(\alpha)) \subset R(\alpha) := \{\alpha^2 + 2u\alpha(1-\alpha) : u \in \mathbb{C}_2, |u^2 - \alpha| < 1\} .$$

So if $R(\alpha) \cap R(\beta) = \emptyset$, then we can determine $T(\alpha, \beta)$:

$$T(\alpha, \beta) \subset S(\alpha) \cup S(\beta) .$$

This will be the case when α and β are 2-adically sufficiently distinct.

Examples

The result applies to show the following.

- $T(2,3) = \emptyset$.
- $T(2,4) = \{4\}$.
- $T(3,-3) = \{-3, 9\}$.
- $T(\omega, \omega^2) = \{\omega, \omega^2\}$, where ω is a primitive cube root of unity.

Let $\boldsymbol{\mu}$ be the set of all roots of unity.
Then $\#(T(\alpha) \cap \boldsymbol{\mu}) \leq 3$ for all α, and

$$\#(T(\alpha) \cap \boldsymbol{\mu}) = 3 \iff \alpha \in \boldsymbol{\mu} \quad \text{and} \quad \mathrm{ord}(\alpha) \in \{3, 6, 12\}.$$

Further Refinement

We can extend this line of argument.
Assume that $|\alpha|, |\beta| \leq 1$ and that $\lambda \in T(\alpha, \beta)$.
Then the x-coordinate of any point $mP_\lambda(\alpha) + nP_\lambda(\beta)$ with $m, n \in \mathbb{Z}$ must be either infinite or of absolute value ≤ 1.

This translates into conditions of the form

$$p(\lambda) = 0 \qquad \text{or} \qquad |p_1(\lambda)| \leq |p_2(\lambda)|$$

for certain polynomials p, p_1, p_2.

If, for some choice of pairs (m, n),
the conditions of the second type are contradictory,
then we have effectively bounded $T(\alpha, \beta)$ by a finite set.

More Examples

- $T(-3,9) = \{9, -\frac{27}{5}\}$ (with $(m,n) = (6,0),\ (0,4)$).
- $T\left(\frac{-3}{5}, \frac{9}{5}\right) = \{\frac{9}{25}, -\frac{27}{5}\}$ (with $(m,n) = (4,0),\ (0,6)$).
- $T\left(\frac{9}{25}, \frac{9}{5}\right) = \{\frac{9}{25}, \frac{189}{125}\}$ (with $(m,n) = (2,0),\ (0,3)$).

Not successful so far for:

- $T\left(-\frac{27}{5}, -\frac{3}{5}\right)$ (another representative in $\mathbb{Q} \times \mathbb{Q}$ with $\#T_{50} = 2$).
- $T\left(-\frac{3}{5}, \frac{9}{25}\right)$ (the essentially only rational pair with $\#T_{50} = 3$).

Question.

Can we always determine $T(\alpha, \beta)$ in this way?

Transcendence Degree 1

Assume that $\mathrm{trdeg}_{\mathbb{Q}}\big(\mathbb{Q}(\alpha,\beta)\big) = 1$
and let $F \in \mathbb{Z}[a,b]$ be irreducible such that $F(\alpha,\beta) = 0$.
Assume that $\lambda \in T(\alpha,\beta)$. Then

$$\big(\lambda = \alpha \text{ or } \exists n \geq 3\colon \psi_n(\lambda,\alpha) = 0\big) \quad \text{and} \quad \big(\lambda = \beta \text{ or } \exists n \geq 3\colon \psi_n(\lambda,\beta) = 0\big).$$

Eliminating λ, we see that F divides
$\psi_n(a,b)$ or $\psi_n(b,a)$ or $R_n(a,b) := \mathrm{Res}_t(\psi_n(t,a),\psi_n(t,b))/(a-b)^{\deg_t \psi_n(t,x)}$,
for some $n \geq 3$.

Proposition 1.
For all $n \geq 3$, the polynomial $\psi_n(a,b)\psi_n(b,a)R_n(a,b)$ is squarefree in $\mathbb{Q}[a,b]$.

Sketch of proof. Write the possible b near $a = 0$ as Puiseux series in a (using Tate parameterization) and check that they are distinct.

Result

Let, for $n \geq 3$, C_n be the curve in $\mathbb{P}^1_a \times \mathbb{P}^1_b$ given by

$$\psi_n(a,b)\psi_n(b,a)R_n(a,b) = 0$$

and let $C = \bigcup_n C_n$ be the filtered union (by divisibility) of the C_n.

By Proposition 1, C is reduced.
This implies that each component of C corresponds
to a family of triples (α, β, λ) with $\lambda \in T(\alpha, \beta)$, where λ is unique.
This gives

Proposition 2.
Let $\alpha, \beta \in \mathbb{C} \setminus \{0, 1\}$ with $\alpha \neq \beta$. Then
$\#T(\alpha, \beta) \leq$ the number of branches of C passing through (α, β).

Consequences

- If $(\alpha, \beta) \notin C$, then $T(\alpha, \beta) = \emptyset$.
  This applies when α and β are algebraically independent.
- If (α, β) is a smooth point on C, then $\#T(\alpha, \beta) \leq 1$.
  This applies when $\operatorname{trdeg}_{\mathbb{Q}}\big(\mathbb{Q}(\alpha, \beta)\big) = 1$ and $T(\alpha, \beta) \neq \emptyset$.
- If $\#T(\alpha, \beta) \geq 2$, then (α, β) is a singular point on a component of C or an intersection point of two or more components of C.

If $F = 0$ describes a component of C, we can bound n in terms of $\deg F$.
This gives effectivity in the $\operatorname{trdeg} = 1$ case.
Note that we have to know F: we can't say whether $T(e, \pi)$ is empty or not!

(Masser and Zannier show $\#T(\alpha, \beta) \leq 6(12 \deg F)^{32}$ when $\operatorname{trdeg} = 1$.)

Computations

We have computed all $F \in \mathbb{Q}[a, b]$ giving irreducible components of C satisfying $\deg_{ab} F := \deg_a F + \deg_b F \leq 192$.

Based on this,
we computed all singularities on components with $(\deg_{ab} F)^2 \leq 384$
and all intersections of components with $(\deg_{ab} F_1)(\deg_{ab} F_2) \leq 384$.
We then computed $T_{50}(\alpha, \beta) = T_{50}(\alpha) \cap T_{50}(\beta)$ for these points (α, β),
leading to $> 2 \cdot 10^6$ pairs with $\#T_{50}(\alpha, \beta) \geq 2$.

558 of these have $\#T_{50}(\alpha, \beta) \geq 3$ (with all torsion orders ≤ 18),
15 of these have $\#T_{50}(\alpha, \beta) \geq 4$,
and 3 of these have $\#T_{50}(\alpha, \beta) = 5$; a representative is $(i, -i)$ with

$$T_{100}(i, -i) = \{-1, 3 \pm 2\sqrt{2}, \tfrac{1}{3} \pm \tfrac{2}{3}\sqrt{-2}\}.$$

Conjectures

Conjecture 1.

$T(i,-i) = \{-1, 3 \pm 2\sqrt{2}, \frac{1}{3} \pm \frac{2}{3}\sqrt{-2}\}$.

Conjecture 2 (Uniform boundedness).

$\#T(\alpha,\beta)$ is uniformly bounded (perhaps by 5).

Conjecture 3 (Finiteness).

There are only finitely many (α,β) with $\#T(\alpha,\beta) \geq 3$.

Conjecture 4 (Bounded height).

The height of (α,β) such that $\#T(\alpha,\beta) \geq 2$ is uniformly bounded.

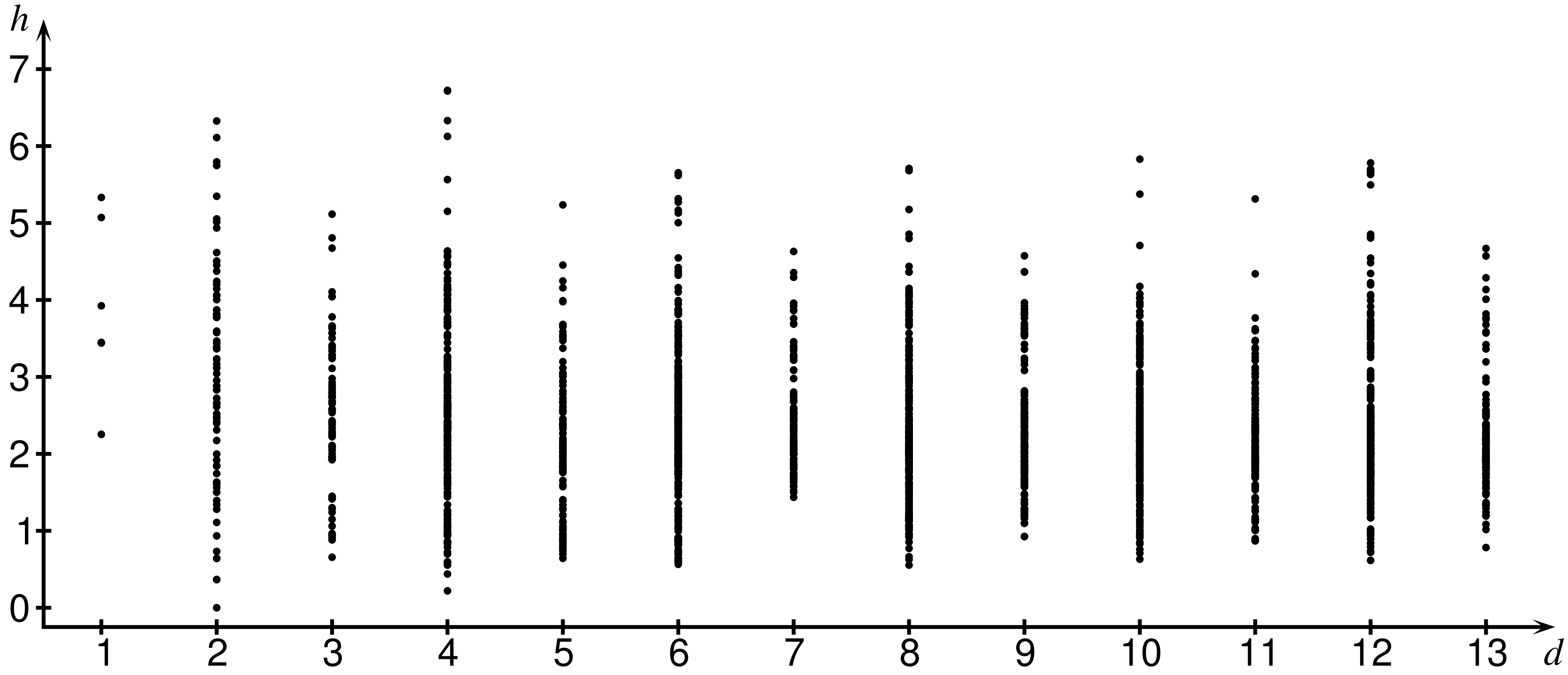
Conjecture 5 (Bounded degree).

There is a uniform bound for $\left[\mathbb{Q}(\alpha,\beta,\lambda) : \mathbb{Q}(\alpha,\beta)\right]$ when $\lambda \in T(\alpha,\beta)$.
The bound might even be 2.

Conjecture 5 would imply effectivity of $T(\alpha,\beta)$.

Heights

This shows the (symmetrized) heights h of pairs (α, β) with $\#T(\alpha, \beta) \geq 2$, ordered according to the degree d of $\mathbb{Q}(\alpha, \beta)$.



Thank You!