# Effective methods for the multiplicative Manin-Mumford problem

Kiran S. Kedlaya

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

RTG colloquium in algebraic geometry/algebra/number theory
University of California, San Diego
May 6, 2020

Supported by NSF (grant DMS-1802161) and UC San Diego (Warschawski Professorship). Thanks also to the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation.

# A general theorem

Let $A$ be a semiabelian variety over $\mathbb{C}$ (i.e., an extension of an abelian variety by a torus). Let $\Gamma$ be a finitely generated subgroup of $A(\mathbb{C})$. Let $\overline{\Gamma}$ be the divisible closure of $\Gamma$.

For $X$ a closed subscheme of $A$, define the $\Gamma$-*torsion closure* of $A$ to be the Zariski closure of $X \cap \overline{\Gamma}$. This is a closure operation (i.e., it is idempotent).

For example, define a $\Gamma$-*torsion coset* of $X$ to be a translate of a semiabelian subvariety of $A$ by an element of $\overline{\Gamma}$. Any such subscheme is its own $\Gamma$-torsion closure.

Theorem (McQuillan, 1995)

*The $\Gamma$-torsion closure of any closed subscheme $X$ of $A$ is a finite union of $\Gamma$-torsion cosets.*

In particular, there is a "finite" description of $X \cap \overline{\Gamma}$. But can one find this description explicitly in explicit instances?

# Special cases of the general theorem: rational points

Let $X_0$ be a curve of genus $g \geq 2$ over a number field $K$. Let $A_0$ be the Jacobian of $X$ and put $X := X_0 \times_K \mathbb{C}, A := A_0 \times_K \mathbb{C}$. Assuming $X_0(K) \neq \emptyset$, we can choose a point $P \in X_0(K)$ and use it to define an embedding $X_0 \hookrightarrow A_0$ whose image is not contained in any strict abelian subvariety of $A_0$ (and is not $A_0$ because $g \geq 2$).

Let $\Gamma$ be the group $A_0(K) \subseteq A(\mathbb{C})$. By the Mordell-Weil theorem, $\Gamma$ is finitely generated; we may thus deduce from the theorem that $X \cap \overline{\Gamma}$ is a finite set. In particular $X \cap \Gamma = X_0(K)$ is a finite set, so the Mordell conjecture holds. That is, McQuillan generalizes Faltings; its proof is based on a theorem of Vojta which itself generalizes Faltings.

However, there is *no fully general method** for determining $X_0(K)$, although there are good practical methods (e.g., Chabauty-Coleman).

*Disclaimer: Mochizuki's claimed proof of the ABC conjecture would provide such a method, albeit probably not a practical one.

# Special case of the general theorem: torsion points

In this talk, we will mostly be interested in the case $\Gamma = 0$. In this case, we refer to $\Gamma$-torsion cosets and closures also as *torsion* cosets and closures.

In this case, the general theorem specializes to a theorem of Hindry, answering a conjecture of Lang. If we further specialize to the setting on the previous slide, we get a theorem of Raynaud answering a conjecture of Manin-Mumford: a pointed curve contains only finitely many points which define torsion classes in the Jacobian.

For Raynaud's theorem, many algorithms can compute torsion points on a curve (e.g., Coleman's method of $p$-adic integration); see Poonen's survey. Many examples are known (e.g., Fermat curves, modular curves).

For Hindry's theorem, we do not know of a general algorithm to compute torsion closures within an arbitrary semiabelian variety. However, if we specialize to tori, then there are very good algorithms; the rest of the talk will be about this special case.

# Special case of the general theorem: torsion points on tori

From now on, we assume[†] that $A$ is a torus and $\Gamma = 0$. In this case, the general theorem again restricts to a previously known result.

**Theorem (Laurent, 1984)**

*The torsion closure of any closed subscheme of $A$ is a finite union of torsion cosets.*

To make this more concrete, write $A = \operatorname{Spec} \mathbb{C}[x_1^{\pm}, \ldots, x_n^{\pm}]$. Since $A$ is affine and noetherian, any closed subscheme $X$ can be defined by some finite collection $f_1, \ldots, f_m$ of Laurent polynomials, and we are trying to classify solutions of the equation

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0$$

where $x_1, \ldots, x_n$ are roots of unity.

[†] That said, it would be interesting to see whether the techniques for tori can be adapted to other semiabelian varieties.

# Torsion points on tori

Again, we are trying to classify solutions of the equation

$$f_1(x_1, \dots, x_n) = \cdots = f_m(x_1, \dots, x_n) = 0$$

where $x_1, \dots, x_n$ are roots of unity. The theorem predicts that the solutions can be described as a finite number of parametric solutions

$$x_i = c_i \prod_{j=1}^{l} y_j^{e_{ij}}$$

where $e_{ij}$ are some fixed integers, $c_i$ are some fixed roots of unity, and $y_1, \dots, y_l$ are parameters (which can specialize to any roots of unity). There is a unique minimal list of such solutions, up to permutation and reparametrization.

The problem is, given an explicit list $f_1, \dots, f_m$, to compute (perhaps on a computer) the minimal list of parametric solutions. To simplify, let's assume that the $f_i$ have coefficients in a cyclotomic field (including $\mathbb{Q}$).

# A theorem of Conway-Jones

### Theorem (Conway-Jones, 1979)

*Let $S$ be a set of at most 9 roots of unity with zero sum. Suppose that $S$ does not contain $\{\alpha, -\alpha\}$ or $\{\alpha, \zeta_3\alpha, \zeta_3^2\alpha\}$ for any $\alpha$. Then up to rotation, $S$ is one of*

$$\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\} \qquad \{-\zeta_3, -\zeta_3^2, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\},$$

$$\{1, \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6\}, \qquad \{1, \zeta_5, \zeta_5^4, -\zeta_3\zeta_5^2, -\zeta_3^2\zeta_5^2, -\zeta_3\zeta_5^3, -\zeta_3^2\zeta_5^3\},$$

$$\{-\zeta_3, -\zeta_3^2, \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6\},$$

$$\{\zeta_5, \zeta_5^4, -\zeta_3, -\zeta_3^2, -\zeta_3\zeta_5^2, -\zeta_3^2\zeta_5^2, -\zeta_3\zeta_5^3, -\zeta_3^2\zeta_5^3\},$$

$$\{1, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, -\zeta_3\zeta_7, -\zeta_3^2\zeta_7, -\zeta_3\zeta_7^6, -\zeta_3^2\zeta_7^6\},$$

$$\{1, -\zeta_3\zeta_5, -\zeta_3^2\zeta_5, -\zeta_3\zeta_5^2, -\zeta_3\zeta_5^2, -\zeta_3\zeta_5^3, -\zeta_3^2\zeta_5^3, -\zeta_3\zeta_5^4, -\zeta_3^2\zeta_5^4\}.$$

This improves a similar result of Włodarski, by providing a technique for resolving similar problems for *any* fixed number of roots of unity.

# Ingredients of the theorem

The key lemma of Conway-Jones is the following.

Lemma (Conway-Jones)

*Let $S$ be a (multi)set of roots of unity with zero sum, which is minimal: no nonempty proper (multi)subset of $S$ sums to zero.*

(a) *There exists a rotation of $S$ consisting of roots of unity of squarefree order.*

(b) *Let $N$ be the minimal integer for which $S$ admits a rotation consisting of $N$-th roots of unity. Then*

$$\#S \geq 2 + \sum_{p|N} (p-2).$$

Both statements follow from basic facts about cyclotomic fields.

# Applications of Conway-Jones

A literature search turns up applications of Conway-Jones in areas such as:

- Euclidean and non-Euclidean geometry;
- operator algebras;
- representation theory of finite groups;
- Kähler geometry;
- knot theory;
- dynamical systems;
- graph theory;

and more.

# An example of Grubb and Woll

Let $N \geq 4$ be an integer. Let $s$ be the ratio of the lengths of two diagonals (or sides) of a regular $N$-gon, which cannot occur for any smaller value of $N$. What is the degree of the number field $\mathbb{Q}(s)$?

This question can be answered[‡] by applying Conway-Jones to classify solutions of the equation

$$\frac{x_1 + x_1^{-1}}{x_2 + x_2^{-1}} = \frac{y_1 + y_1^{-1}}{y_2 + y_2^{-1}}$$

in roots of unity, then using this to identify cases where a nontrivial automorphism of $\mathbb{Q}(\zeta_N)$ fixes $s$.

[‡] Last I checked, this was only done for $N$ odd; but similar methods should work in the general case.

# An example of Poonen-Rubinstein

Theorem (Poonen-Rubinstein, 1998)

*The number of interior intersection points of the diagonals of a regular n-gon equals*

$$\binom{n}{4}+\frac{-5n^3+45n^2-70n+24}{24}\delta_2(n)-\frac{3n}{2}\delta_4(n)+\frac{-45n^2+232n}{6}\delta_6(n)+\cdots$$

*where* $\delta_m(n)=1$ *if* $n\equiv 0 \pmod{m}$ *and* $0$ *otherwise. (The missing terms involve* $\delta_{12},\delta_{18},\delta_{24},\delta_{30},\delta_{42},\delta_{60},\delta_{84},\delta_{90},\delta_{120},\delta_{210}$*.)*

The proof involves identifying all ways that three or more diagonals can intersect in a point. This requires extending the Conway-Jones classification to sums of 12 roots of unity, the current record.

# Making this an algorithm

The fact that the Conway-Jones method gives an algorithm for finding torsion closures in tori was formalized by Leroux.

- It is enough to deal with one Laurent polynomial $f \in K[x_1^{\pm}, \dots, x_n^{\pm}]$ at a time.
- Write $f$ as a sum of monomials whose coefficients are roots of unity. View this as a cyclotomic relation.
- Classify all minimal cyclotomic relations up to this length. Each one involves a single free parameter (choice of a rotation).
- Enumerate over all ways to combine the monomials we wrote down into minimal relations. For each of these, solve for the free parameters (this is essentially linear algebra over $\mathbb{Z}$).

This works in principle, but scales *very poorly* in the number of monomials.

# Cyclotomic factors of univariate polynomials

For a nonzero univariate polynomial $f(x)$ over $\mathbb{Q}$, define the *cyclotomic part* of $f$, denoted $C(f)$, as the product (without repetition) of those cyclotomic polynomials $\Phi_n(x)$ which divide $f(x)$.

There is a very efficient algorithm[§] of Bradford-Davenport to compute $C(f)$. We give here a slight variant due to Beukers-Smyth. (This is implemented in Sage as the `cyclotomic_part` method of a polynomial.)

- Compute $f_1(x) := \gcd(f, f(x^2)f(-x^2))$.
- If $\deg f_1 = \deg(f)$, put $h := f$. Otherwise, compute $f_2(x) := \gcd(f(x), f(-x))$, $g(x) := f_2(x^{1/2})$, then recursively compute $h := C(f_1)(x)C(g)(x^2)$.
- Then $C(f)$ is equal to the squarefree part of $h$ (that is, $h/\gcd(h, h')$).

[§] For a polynomial $f(x)$ over a number field $K$, one can extract the cyclotomic part by taking the field norm from $K(x)$ to $\mathbb{Q}(x)$, taking the cyclotomic part of the result, then computing the gcd with $f$.

# Cyclotomic factors of univariate polynomials

- Compute $f_1(x) := \gcd(f, f(x^2)f(-x^2))$.
- If $\deg f_1 = \deg(f)$, put $h := f$. Otherwise, compute $f_2(x) := \gcd(f(x), f(-x))$, $g(x) := f_2(x^{1/2})$, then recursively compute $h := C(f_1)(x)C(g)(x^2)$.
- Then $C(f)$ is equal to the squarefree part of $h$ (that is, $h/\gcd(h, h')$).

The fact that this algorithm works can be derived from the following.

### Lemma (Beukers-Smyth)

(a) *Suppose $f(x) \in \mathbb{C}[x]$ has this property: for every zero $\alpha$ of $f$, at least one of $\pm\alpha^2$ is also a zero of $f$. Then all zeroes of $f$ are roots of unity.*

(b) *If $\zeta \in \mathbb{C}$ is a root of unity, then it is Galois-conjugate over $\mathbb{Q}$ to at least one of $-\zeta, \zeta^2, -\zeta^2$.*

(c) *Conversely, if $\zeta \in \mathbb{C}^\times$ is Galois-conjugate over $\mathbb{Q}$ to either $\zeta^2$ or $-\zeta^2$, then $\zeta$ is a root of unity. (This is a special case of (a).)*

# The Beukers-Smyth method

Let $f \in \mathbb{Q}(\zeta_N)[x^{\pm}, y^{\pm}]$ be irreducible and not a binomial. We know that the torsion closure of $Z(f)$ is a finite set $Y$ of points.

- If $N$ is odd, then each point of $Y$ is a zero of one of

  $$f(x,-y), f(-x,y), f(-x,-y),$$
  $$f^\tau(x^2,y^2), f^\tau(x^2,-y^2), f^\tau(-x^2,y^2), f^\tau(-x^2,-y^2)$$

  where $f^\tau$ means apply the automorphism $\zeta_N \mapsto \zeta_N^2$ to coefficients.
- If $N$ is divisible by 4, then each point of $Y$ is a zero of one of

  $$f(x,-y), f(-x,y), f(-x,-y),$$
  $$f^\tau(x,y), f^\tau(x,-y), f^\tau(-x,y), f^\tau(-x,-y)$$

  where $f^\tau$ means apply the automorphism $\zeta_N \mapsto -\zeta_N$ to coefficients.

We thus compute a finite set containing the torsion closure. By univariate computations (as above), we reduce this to the actual torsion closure.

# Higher dimensions

Aliev-Smyth propose a similar algorithm in higher dimensions, using resultants at each step to eliminate one variable.

It seems more practical to reconceptualize this in terms of commutative algebra. Starting with an ideal $I$, we have a finite collection $S$ of ring endomorphisms with the properties that:

- every torsion point of $Z(I)$ belongs to $Z(I + f(I))$ for some $f \in S$;
- if $f(I) = I$ for some $f \in S$, either $Z(I)$ is its own torsion closure, or $I$ arises by base extension from a "simpler" ideal (as in the Bradford-Davenport recursion).

The relevant commutative algebra (using Gröbner bases) is available in standard software: Singular (via Sage), Magma, Macaulay2, etc.

Unfortunately, my experiments suggest that this is *barely* practical in three variables and *never* in four or more variables.

# Example: tetrahedra with rational dihedral angles

For a tetrahedron in $\mathbb{R}^3$ with faces labeled $1, \dots, 4$, if $\alpha_{jk}$ denotes the dihedral angle between faces $j$ and $k$, then

$$\det \begin{pmatrix} -2 & 2\cos\alpha_{12} & 2\cos\alpha_{13} & 2\cos\alpha_{14} \\ 2\cos\alpha_{12} & -2 & 2\cos\alpha_{23} & 2\cos\alpha_{24} \\ 2\cos\alpha_{13} & 2\cos\alpha_{23} & -2 & 2\cos\alpha_{34} \\ 2\cos\alpha_{14} & 2\cos\alpha_{24} & 2\cos\alpha_{34} & -2 \end{pmatrix} = 0.$$

When are all six angles rational multiples of $\pi$? This question could have been asked by Dehn in the early 20th century (or by the ancient Greeks), but was (apparently) first suggested by Conway-Jones.

# Example: tetrahedra with rational dihedral angles

By rewriting the equation in terms of $e^{2\pi i \alpha_{jk}}$, one gets a polynomial equation in six roots of unity (plus some positivity constraints which we ignore). This is the same sort of problem we have been considering, but it seems out of reach for either¶ of the techniques we have introduced so far.

- The determinant expands to a sum of 105 monomials in the $e^{2\pi i \alpha_{jk}}$. It is hopeless to analyze cyclotomic relations of that length.
- The commutative algebra approach seems to top out at three variables, whereas here we have six.

¶Conway-Jones wrote somewhat optimistically: "It seems quite probable that the general tetrahedron all of whose dihedral angles are rational can be found by our techniques."

# A new hope

The factors of 2 in the equation

$$\det \begin{pmatrix} -2 & 2\cos\alpha_{12} & 2\cos\alpha_{13} & 2\cos\alpha_{14} \\ 2\cos\alpha_{12} & -2 & 2\cos\alpha_{23} & 2\cos\alpha_{24} \\ 2\cos\alpha_{13} & 2\cos\alpha_{23} & -2 & 2\cos\alpha_{34} \\ 2\cos\alpha_{14} & 2\cos\alpha_{24} & 2\cos\alpha_{34} & -2 \end{pmatrix} = 0$$

were put in so that the matrix entries are algebraic integers. What if we quotient that ring by 2?

The resulting determinant then simplifies to a sum of only 12 monomials in the $e^{2\pi i \alpha_{jk}}$. Poonen has suggested classifying *mod-2 cyclotomic relations* using the method of Conway-Jones, to reduce the original six-variable problem to a collection of subproblems in fewer variables.

A similar idea can also be employed within the Aliev-Beukers-Smyth method to speed it up as well. The hope is that a combination of these ideas can be used to classify tetrahedra with rational dihedral angles.