# Rational Diophantine Quintuples and Diagonal Genus 5 Curves

Michael Stoll
Universität Bayreuth

**Diophantine Problems**
University of Manchester
15 September 2017

# Diophantine $m$-Tuples

**Definition.**
A (rational) Diophantine $m$-tuple is an $m$-tuple $(a_1, \ldots, a_m)$ of distinct nonzero integers (rational numbers) such that $a_i a_j + 1$ is a square for all $1 \le i < j \le m$.

**Examples.**
$(1, 3, 8, 120)$ is a Diophantine quadruple (found by Fermat):

$$1 \cdot 3 + 1 = 2^2, \quad 1 \cdot 8 + 1 = 3^2, \quad 1 \cdot 120 + 1 = 11^2$$
$$3 \cdot 8 + 1 = 5^2, \quad 3 \cdot 120 + 1 = 19^2, \quad 8 \cdot 120 + 1 = 31^2$$

In fact, this is just the case $t = 2$ in the family

$$\bigl(t-1, t+1, 4t, 4t(4t^2-1)\bigr)$$

of Diophantine quadruples.

(See Andrej Dujella's homepage for exhaustive information.)

# A Diophantine Problem

Consider a given rational Diophantine quadruple $(a_1, a_2, a_3, a_4)$, for example Fermat's quadruple $(1, 3, 8, 120)$.

**Problem.**
Find all rational numbers $a_5$
such that $(a_1, a_2, a_3, a_4, a_5)$ is a rational Diophantine quintuple.

**Fact.**
We can always take (the "regular extensions")

$$a_5 = z_\pm = \frac{(a_1+a_2+a_3+a_4)(a_1a_2a_3a_4+1)+2(a_1a_2a_3+a_1a_2a_4+a_1a_3a_4+a_2a_3a_4)\pm 2s}{(a_1a_2a_3a_4-1)^2},$$

where $s = \sqrt{(a_1a_2+1)(a_1a_3+1)(a_1a_4+1)(a_2a_3+1)(a_2a_4+1)(a_3a_4+1)}$
(unless $z_\pm \in \{0, a_1, a_2, a_3, a_4\}$).

Are there more possibilities in our concrete case?

# Extending Fermat's Quadruple

For all quadruples in the family shown before, we have $z_- = 0$, so there is only one regular extension.

For Fermat's quadruple $(1, 3, 8, 120)$, this is $z_+ = \frac{777\,480}{8\,288\,641}$. We will show that this is the only extension.

Any extension $z \in \mathbb{Q}^\times$ gives rise to a bunch of rational points on the curve

$$z + 1 = u_1^2, \quad 3z + 1 = u_2^2, \quad 8z + 1 = u_3^2, \quad 120z + 1 = u_4^2.$$

This curve has genus 5, so there are only finitely many solutions.

With $x = u_4$, this gives $x^2 + 119 = 120u_1^2$, $x^2 + 39 = 40u_2^2$, $x^2 + 14 = 15u_3^2$, hence

$$y^2 = 5(x^2 + 119)(x^2 + 39)(x^2 + 14)$$

with $y = 600u_1u_2u_3$.

# Rational Points on a Curve of Genus 2

The curve

$$C\colon y^2 = 5(x^2+119)(x^2+39)(x^2+14)$$

has genus 2. We want to find its rational points.

A search turns up points with $x$-coordinates $\pm 1$ and $\pm\frac{10\,079}{2\,879}$:

```
> P<x> := PolynomialRing(Rationals());
> C := HyperellipticCurve(5*(x^2+119)*(x^2+39)*(x^2+14));
> ptsC := Points(C : Bound := 10^5); ptsC;
{@ (-1 : -600 : 1), (-1 : 600 : 1), (1 : -600 : 1), (1 : 600 : 1),
(-10079 : -22426285104600 : 2879), (-10079 : 22426285104600 : 2879),
(10079 : -22426285104600 : 2879), (10079 : 22426285104600 : 2879) @}
```

They correspond to $z = 0$ and $z = \frac{777\,480}{8\,288\,641}$.

# Standard Chabauty Does not Work

The differences of the points we found
generate a subgroup of rank $2$ in the Mordell-Weil group of $C$
(which actually does have rank $2$ itself),
so the standard version of Chabauty's method does not apply.

```
> bas := ReducedBasis([pt - ptsC[1] : pt in ptsC]); bas;
[ (x^2 - 1, 600, 2), (x^2 - 1, 600*x, 2) ]
> J := Jacobian(C);
> RankBound(J);
2
```

("Quadratic Chabauty" would apply here, since $C$ is bielliptic.)

So we need to do something else.

# Two-Cover Descent

We compute the "fake 2-Selmer set" $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C)$ of $C$.

```
> Sel, mSel := TwoCoverDescent(C);
> #Sel;
2
> A<th> := Domain(mSel);
> Sel eq {mSel(x0 - th) : x0 in {1,-1}};
true
```

The last line verifies that the points $(\pm 1, \pm 600)$ account for all of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C)$.
So if $(\xi, \eta) \in C(\mathbb{Q})$, then (for one choice of sign and some $a \in \mathbb{Q}^\times$)

$$\frac{\xi - \sqrt{-119}}{\pm 1 - \sqrt{-119}} \in a\mathbb{Q}(\sqrt{-119})^{\times 2}, \quad \frac{\xi - \sqrt{-39}}{\pm 1 - \sqrt{-39}} \in a\mathbb{Q}(\sqrt{-39})^{\times 2}, \quad \frac{\xi - \sqrt{-14}}{\pm 1 - \sqrt{-14}} \in a\mathbb{Q}(\sqrt{-14})^{\times 2}$$

The automorphism $x \mapsto -x$ of $C$ swaps the two elements,
hence it suffices to consider one of them. We take the image of $(1, \pm 600)$.

# An Elliptic Curve

Recall that we have (w.l.o.g.)

$$\frac{\xi-\sqrt{-119}}{1-\sqrt{-119}} \in a\mathbb{Q}(\sqrt{-119})^{\times 2}, \qquad \frac{\xi-\sqrt{-39}}{1-\sqrt{-39}} \in a\mathbb{Q}(\sqrt{-39})^{\times 2}, \qquad \frac{\xi-\sqrt{-14}}{1-\sqrt{-14}} \in a\mathbb{Q}(\sqrt{-14})^{\times 2}.$$

This implies in particular that there is $\tau \in K = \mathbb{Q}(\sqrt{-119}, \sqrt{-39})$ such that

$$\tau^2 = 15(1-\sqrt{-119})(1-\sqrt{-39}) \cdot (\xi^2+14)(\xi-\sqrt{-119})(\xi-\sqrt{-39}),$$

so we get a K-rational point with rational X-coordinate
on the elliptic curve

$$E\colon Y^2 = 15(1-\sqrt{-119})(1-\sqrt{-39}) \cdot (X^2+14)(X-\sqrt{-119})(X-\sqrt{-39}).$$

This is the setting for Elliptic Curve Chabauty.

# Elliptic Curve Chabauty

We want to find all points $(\xi, \tau) \in E(K)$ with $\xi \in \mathbb{Q}$.

This works when rank $E(K) < [K : \mathbb{Q}] = 4$.

```
> K := AbsoluteField(ext<Rationals() | x^2 + 119, x^2 + 39>);
> w119 := Roots(x^2 + 119, K)[1,1]; w39 := Roots(x^2 + 39, K)[1,1];
> PK<X> := PolynomialRing(K);
> E := HyperellipticCurve(15*(1-w119)*(1-w39)*(X^2+14)*(X-w119)*(X-w39));
> EE, EtoEE := EllipticCurve(E, E![1, 15*(1-w119)*(1-w39)]);
> Invariants(TorsionSubgroup(EE)); Invariants(TwoSelmerGroup(EE));
[ 2 ]
[ 2, 2, 2 ]
> bas := Saturation(ReducedBasis([EtoEE(pt) : pt in Points(E, 10079/2879)]), 7); #bas;
3
> MW := AbelianGroup([2,0,0]);
> MWmap := map<MW -> EE | m :-> &+[s[i]*bas[i] : i in [1..3]] where s := Eltseq(m)>;
> P1 := ProjectiveSpace(Rationals(), 1);
> pi := Expand(Inverse(EtoEE)*map<E -> P1 | [E.1, E.3]>);
> chab := Chabauty(MWmap, pi : IndexBound := 2*3*5*7);
> {pi(MWmap(pt)) : pt in chab};
{ (1 : 1), (10079/2879 : 1) }
```

This finishes the proof.

# What is Going on Here?

Given a Diophantine quadruple $(a_1, a_2, a_3, a_4)$, the equations

$$a_1 z + 1 = u_1^2, \quad a_2 z + 1 = u_2^2, \quad a_3 z + 1 = u_3^2, \quad a_4 z + 1 = u_4^2$$

define (after homogenising via $1 = u_0^2$ and eliminating $z$)
a diagonal curve $X \subset \mathbb{P}^4$ of genus 5:

$$\begin{aligned}
(a_4 - a_1)u_0^2 - a_4 u_1^2 \qquad\qquad\qquad\qquad &+ a_1 u_4^2 = 0 \\
(a_4 - a_2)u_0^2 \qquad\qquad - a_4 u_2^2 \qquad\qquad &+ a_2 u_4^2 = 0 \\
(a_4 - a_3)u_0^2 \qquad\qquad\qquad\qquad - a_4 u_3^2 &+ a_3 u_4^2 = 0
\end{aligned}$$

Eliminating $u_i$ gives a double cover $X \to F_i$ with $F_i$ of genus 1.
Eliminating $u_i$ and $u_j$ gives a degree 4 map $X \to Q_{ij}$ with a conic $Q_{ij}$.

# Isogeny and 2-Torsion

There is a "Richelot-type isogeny" $\varphi\colon \mathrm{Jac}(X) \to \prod_{i=0}^{4} \mathrm{Jac}(F_i)$.

Its kernel is $\ker\varphi \simeq (\mathbb{Z}/2\mathbb{Z})^5$; all points are defined over $\mathbb{Q}$.
So we can easily compute the $\hat{\varphi}$-Selmer set $\mathrm{Sel}^{\hat{\varphi}}(X)$.

The kernel gives us $31$ distinct étale double covers $A_T \to \mathrm{Jac}(X)$,
which we can pull back to étale double covers $Y_T \to X$.

$30$ of these have a nice explicit description.
For each $\xi \in \mathrm{Sel}^{\hat{\varphi}}(X)$ there is a twist $Y_{T,\xi} \to X$;
each point $P \in X(\mathbb{Q})$ lifts to one of these twists (same $\xi$ for all $T$).

The Prym variety of $Y_{T,\xi} \to X$ is (generically) the Weil restriction
of an elliptic curve $E_{T,\xi}$ over a biquadratic field $K_T$.
There are morphisms $Y_{T,\xi} \to E_{T,\xi}$ and $E_{T,\xi} \to \mathbb{P}^1$
whose composition is defined over $\mathbb{Q}$.

In this setting, Elliptic Curve Chabauty can be used to find $Y_{T,\xi}(\mathbb{Q})$.

# "Algorithm"

Given a diagonal genus 5 curve $X$ with $X(\mathbb{Q}) \neq \emptyset$:

1. Compute $S = \mathrm{Sel}^{\hat{\varphi}}(X)$.
2. For each $\xi \in S$ (modulo action of $\mathrm{Aut}(X)$) do:

   2a. Find $0 \neq T \in \ker \varphi$ such that
   - $E_{T,\xi}(K_T)$ can be determined (up to finite index), and
   - $\mathrm{rank}\, E_{T,\xi}(K_T) < 4$.

   2b. Apply Elliptic Curve Chabauty to find $Y_{T,\xi}(\mathbb{Q})$ and its image $X(\mathbb{Q})_\xi$ in $X(\mathbb{Q})$.
3. If Step 2 was successful, then $X(\mathbb{Q}) = \mathrm{Aut}(X) \cdot \bigcup_{\xi \in S} X(\mathbb{Q})_\xi$.

(This extends and improves on recent work by Gonzáles-Jiménez.)

# Further Results

We have applied this "algorithm" to quadruples from the family

$$\big(t-1, t+1, 4t, 4t(4t^2-1)\big)$$

(where $\pm t \neq 0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}$).

In this way, we could show that the regular extension is the only one for

$$t = 2 \text{ (see above)},\ 3,\ \tfrac{2}{3},\ \tfrac{3}{2},\ 4,\ \tfrac{3}{4},\ \tfrac{4}{3},\ 5,\ \tfrac{1}{5},\ \tfrac{2}{5},\ \tfrac{3}{5},\ \tfrac{5}{4},\ \tfrac{4}{5}\,.$$

(For $t = \frac{3}{5}$, there is a second "illegal" extension besides $0$ given by $\frac{12}{5}$, which is already present. Note that $\left(\frac{12}{5}\right)^2 + 1 = \left(\frac{13}{5}\right)^2$.)

Thank You!