On a Problem of Hajdu and Tengely

Samir Siksek
University of Warwick

Michael Stoll
Universität Bayreuth

ANTS IX
INRIA, Nancy

July 23, 2010

The Problem

In a recent paper, Hajdu and Tengely have studied (among other cases) arithmetic progressions in coprime integers whose terms are squares and fifth powers.

They showed that no non-trivial such APs with four terms exist, except possibly of the form

$$a^2,\ b^2,\ c^2,\ d^5 \qquad \text{or equivalently} \qquad a^5,\ b^2,\ c^2,\ d^2\,.$$

We will show that also in this case, the only solution is the trivial one.

Translation of the Problem

The first step is to reduce the problem
to a question about rational points on certain curves.

There are several ways in which this can be done here;

Construction of the Curves (1)

Recall that

$$(b + c\sqrt{2})(b - c\sqrt{2}) = (-d)^5 .$$

Since the factors on the left are coprime and $\mathbb{Z}[\sqrt{2}]$ is a PID, we must have that

$$b + c\sqrt{2} = (1 + \sqrt{2})^j (u + v\sqrt{2})^5$$

for some $j \in \{-2, -1, 0, 1, 2\}$ and integers u and v.

We expand and compare coefficients; this gives

$$b = g_j(u, v) \qquad \text{and} \qquad c = h_j(u, v)$$

with certain homogeneous polynomials $g_j, h_j \in \mathbb{Z}[u, v]$ of degree 5.

Construction of the Curves (2)

Recall

$$b = g_j(u,v) \qquad \text{and} \qquad c = h_j(u,v)\,.$$

Now we use the relation

$$a^2 = 2b^2 - c^2$$

and find that

$$a^2 = 2g_j(u,v)^2 - h_j(u,v)^2 =: f_j(u,v)$$

where $f_j \in \mathbb{Z}[u,v]$ is homogeneous of degree 10.

Setting $y = a/v^5$ and $x = u/v$, we obtain hyperelliptic curves of genus 4:

$$C_j : y^2 = f_j(x,1)\,.$$

Since $f_{-j}(x,1) = f_j(-x,1)$, the curves C_{-j} and C_j are isomorphic.

The Curves

$$C_0 : y^2 = 2x^{10} + 55x^8 + 680x^6 + 1160x^4 + 640x^2 - 16$$

$$C_1 : y^2 = x^{10} + 30x^9 + 215x^8 + 720x^7 + 1840x^6 + 3024x^5 + 3880x^4 + 2880x^3 + 1520x^2 + 480x + 112$$

$$C_2 : y^2 = 14x^{10} + 180x^9 + 1135x^8 + 4320x^7 + 10760x^6 + 18144x^5 + 21320x^4 + 17280x^3 + 9280x^2 + 2880x + 368$$

Any solution to the original problem gives rise to a rational point on one of these curves.

The trivial solution comes from the two points at infinity on C_1.

Dealing with C_0 and C_2

We first consider C_0 and C_2.

We do not expect any rational points on them, so we try to prove this.

This can be done by a 2-descent on these curves, which proves that they do not have 2-coverings with points everywhere locally. Since any rational point would have to lift to one of these coverings, this shows that rational points cannot exist.

This is implemented in MAGMA:

```
> TwoCoverDescent(HyperellipticCurve(Polynomial(
    [-16,0,640,0,1160,0,680,0,55,0,2])));
> TwoCoverDescent(HyperellipticCurve(Polynomial(
    [368,2880,9280,17280,21320,18144,10760,4320,1135,180,14])));
```

2-Descent on C_1

We can also perform a 2-descent on C_1.

We obvisouly cannot get a proof that there are no rational points,
but we do get the information
that there is only one 2-covering of C_1 that has rational points.

We can use one of the two rational points at infinity
to embed C_1 into its Jacobian J_1;
then the result tells us that the image in J_1 of any rational point of C_1
must be twice an element of the Mordell-Weil group $J_1(\mathbb{Q})$.

In order to make use of this information,
we need to know something about the Mordell-Weil group $J_1(\mathbb{Q})$.

2-Descent on J_1

We can do a 2-descent on J_1.

(For Jacobians of curves of genus 2, this is in MAGMA;
for hyperelliptic Jacobians of higher even genus, it will be at some point.)

This results in an upper bound of 2 for the rank of $J_1(\mathbb{Q})$.

On the other hand, we can find two independent points $Q_1, Q_2 \in J_1(\mathbb{Q})$ and show that there is no torsion, so

$$J_1(\mathbb{Q}) \cong \mathbb{Z}^2 \,,$$

and $G = \langle Q_1, Q_2 \rangle$ is a subgroup of finite index.

Restricting the Residue Classes

We can show that $J_1(\mathbb{Q})$ and G have the same image in $J_1(\mathbb{F}_7)$ and $J_1(\mathbb{F}_{13})$.

Considering the commutative diagrams

$$\begin{array}{ccc} C_1(\mathbb{Q}) & \longrightarrow & 2J_1(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C_1(\mathbb{F}_7) & \longrightarrow & J_1(\mathbb{F}_7) \end{array} \qquad \begin{array}{ccc} C_1(\mathbb{Q}) & \longrightarrow & 2J_1(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C_1(\mathbb{F}_{13}) & \longrightarrow & J_1(\mathbb{F}_{13}) \end{array}$$

we can show that any rational point on C_1 must reduce to a point at infinity in $C_1(\mathbb{F}_7)$.

It remains to show that there can be at most one rational point in each of these residue classes.

The Chabauty-Coleman Method

Let C be a curve of genus g, with Jacobian J,
and let $p > 2$ be a prime of good reduction.

There is an 'integration pairing'

$$J(\mathbb{Q}_p) \times \Omega^1_C(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p \,.$$

If the rank of $J_1(\mathbb{Q})$ is less than g,
then there is a differential $0 \neq \omega \in \Omega^1_C(\mathbb{Q}_p)$ that kills $J(\mathbb{Q})$.

Theorem.

Let $P \in C(\mathbb{F}_p)$ such that the reduction $\bar{\omega}$ of ω does not vanish at P.
Then there is at most one rational point on C that reduces to P.

Application

In our case, the rank is 2 and the genus is 4,
so we can hope to be able to apply the method.

We use $p = 7$ (it is usually a good idea to use a small prime).

After a somewhat involved computation,
we find the 2-dimensional space of differentials that kill $J_1(\mathbb{Q})$.

There is a differential in this space
whose reduction does not vanish at infinity.

This concludes the proof.