Combinatorial Diophantine Equations

Szabolcs Tengely

Arctic Number Theory School, Helsinki

May 21, 2011

Integer sequences

Problem: find intersection of integer sequences

Some well-known sequences:

- perfect powers
- binomial coefficients
- Fibonacci sequence, recurrence sequences

We will consider the equation

$$L_n = \binom{x}{5}$$

Research supported by OTKA PD75264 and
János Bolyai Research Scholarship
of the Hungarian Academy of Sciences

Related results

- Cohn and independently Wyler: the only squares in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1, F_{12} = 144$.
- Alfred and independently Cohn: perfect squares in the Lucas sequence.
- Cohn and independently Pethő: perfect squares in the Pell sequence.
- London and Finkelstein and independently Pethő: the only cubes in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1$ and $F_6 = 8$.
- Bugeaud, Mignotte and Siksek: combination of Baker's method, modular approach and some classical techniques to show that the perfect powers in the Fibonacci sequence are 0,1,8 and 144, and the perfect powers in the Lucas sequence are 1 and 4.
- Szalay: solved the equations $F_n, L_n, P_n = \binom{x}{3}$ and $F_n, L_n = \binom{x}{4}$.
- Kovács: solved the equations $P_n = \binom{x}{4}$ and $F_n = \Pi_4(x)$.

Similar combinatorial Diophantine problems

Many results, we mention only a few mathematicians working on this subject: Bennett, Bilu, Bremner, Bugeaud, Győry, Hajdu, Hanrot, Kovács, Luca, Mignotte, Olajos, Pethő, Pintér, Rakaczki, Saradha, Shorey, Siksek, Stewart, Stoll, Stroeker, Szalay, Tijdeman, Tzanakis, De Weger.

Main result

We consider the Diophantine equation

$$L_n = \binom{x}{5}. \tag{1}$$

Theorem

The only positive solution of equation (1) is $(n, x) = (1, 5)$.

We will use the following well known property of the sequences F_n and L_n :

$$L_n^2 - 5F_n^2 = 4(-1)^n.$$

We have that

$$\binom{x}{5}^2 \pm 4 = 5F_n^2.$$

We will use the following well known property of the sequences F_n and L_n :

$$L_n^2 - 5F_n^2 = 4(-1)^n.$$

We have that

$$\binom{x}{5}^2 \pm 4 = 5F_n^2.$$

The above equation can be reduced to two genus two curves as follows

$$\mathcal{C}^+ : Y^2 = X^2(X+15)^2(X+20) + 180000000 \qquad (2)$$

and

$$\mathcal{C}^- : Y^2 = X^2(X+15)^2(X+20) - 180000000, \qquad (3)$$

where $Y = 5^3 5! F_n$ and $X = 5x^2 - 20x$.

Theorem

(a) The integral solutions of equation (2) are

$$(X, Y) \in \{(25, -15000), (25, 15000)\}.$$

(b) There are no integral solution of equation (3).

To prove the above results we will follow the paper by Bugeaud, Mignotte, Siksek, Stoll and Tengely. They combined Baker's method and the so-called Mordell-Weil sieve to solve

$$\binom{x}{2} = \binom{y}{5}$$

and

$$x^2 - x = y^5 - y.$$

Proof of part (a)

Using MAGMA (procedures based on Stoll's papers) we obtain that $J(\mathbb{Q})^+$ is free of rank 1 with Mordell-Weil basis given by

$$D = (25, 15000) - \infty.$$

Classical Chabauty's method can be applied.

$$\mathcal{C}^+(\mathbb{Q}) = \{\infty, (25, \pm 15000)\}.$$

Proof of part (b)

Using MAGMA we determine a Mordell-Weil basis which is given by

$$D_1 = (\omega_1, -200\omega_1) + (\overline{\omega}_1, -200\overline{\omega}_1) - 2\infty,$$
$$D_2 = (\omega_2, 120000) + (\overline{\omega}_2, 120000) - 2\infty,$$

where ω_1 is a root of the polynomial $x^2 - 5x + 1500$ and ω_2 is a root of $x^2 + 195x + 13500$.
Let $f = x^2(x+15)^2(x+20) - 180000000$ and α be a root of f.
We have

$$x - \alpha = \kappa\xi^2,$$

such that $\kappa \in \{1, \alpha^2 - 5\alpha + 1500, \alpha^2 + 195\alpha + 13500, \alpha^4 + 190\alpha^3 + 14025\alpha^2 + 225000\alpha + 20250000\}$.

By local arguments it is possible to restrict the set. In our case one can eliminate

$$\alpha^2 - 5\alpha + 1500, \quad \alpha^2 + 195\alpha + 13500$$

by local computations in $\mathbb{Q}_2$ and

$$\alpha^4 + 190\alpha^3 + 14025\alpha^2 + 225000\alpha + 20250000$$

by local computations in $\mathbb{Q}_3$. It remains to deal with the case $\kappa = 1$. By Baker's method we get a large upper bound for $\log |x|$:

$$1.58037 \times 10^{285}.$$

The set of known rational points on the curve (3) is $\{\infty\}$. Let W be the image of this set in $J(\mathbb{Q})^-$. Applying the Mordell-Weil sieve implemented by Bruin and Stoll we obtain that

$$\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})^-,$$

where

$$B = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 19 \cdot 23 \cdot 31 \cdot 41 \cdot \cdot 43 \cdot 47 \cdot 61 \cdot 67 \cdot 79 \cdot 83 \cdot 109 \cdot 113 \cdot 127,$$

that is

$$B = 6789572526810823287690653989488800.$$

Now we use an extension of the Mordell-Weil sieve due to Samir Siksek to obtain a very long decreasing sequence of lattices in $\mathbb{Z}^2$ to obtain a lower bound for possible unknown rational points.

If (x, y) is an unknown integral point, then

$$\log |x| \geq 7.38833 \times 10^{1076}.$$

This contradicts the bound for $\log |x|$ we obtained by Baker's method.

Proof of the main theorem

We have that $X = 25$ and we also have that $X = 5x^2 - 20x$. We obtain that $x \in \{-1, 5\}$.

$$1 = L_1 = \binom{5}{5}.$$

Research problem

Lucas sequence: $\{U_n(P,Q)\}$, where P, Q are non-zero integers, $U_0 = 0$, $U_1 = 1$ and

$$U_n = PU_{n-1} - QU_{n-2}, \quad n \geq 2.$$

Determine all (P, Q, n) such that $U_n(P,Q) = \pm 3\square$.
Joint work with László Szalay.

Some related results

Ljunggren (1942): if $(P, Q) = (-2, 1)$, then $U_n = \Box$ implies that $n = 7$, and $U_n = 2\Box$ implies that $n = 2$.
Cohn (1964): if $(P, Q) = (1, -1)$, (the Fibonacci sequence), then the only square in the sequence $U_n > 1$ is U_{12}.
Mignotte and Pethő (1993): $U_n(P, 1) = \Box, k\Box, P \geq 3$.
Nakamula and Pethő (1998): $U_n(P, -1) = \Box, k\Box, P \geq 1$.
Bremner, Tzanakis (2004): $U_9 = \Box, U_{12} = \Box$, assuming that $\gcd(P, Q) = 1$.
General finiteness results, results related to perfect powers:
Pethő (1982), Shorey and Stewart (1983), Shorey and Tijdeman (1986), Bugeaud, Mignotte and Siksek (2006).

Notation

$U_0(P,Q) = 0, U_1(P,Q) = 1$ and $U_n = PU_{n-1} - QU_{n-2}, \quad n \geq 2,$
associated sequence
$V_0(P,Q) = 2, V_1(P,Q) = P$ and $V_n = PV_{n-1} - QV_{n-2}, \quad n \geq 2,$
discriminant: $D = P^2 - 4Q$.
We assume that $PQ \neq 0, \gcd(P,Q) = 1$ and $D \neq 0$.
We have that

$$V_n(P,Q)^2 - DU_n(P,Q)^2 = 4Q^n$$

Problem by Bremner and Tzanakis

Let $k \neq 0$ and $n_0 > 1$ be fixed integers and $\mathcal{S}$ is a fixed set of primes. Find all (m, P, Q) for which

$$U_{n_0 m}(P, Q) = k\Box,$$

and all prime divisors of m are from $\mathcal{S}$.

Bremner and Tzanakis proved the following theorem.

Theorem. Let $k, n_0 \geq 8$ be fixed non-zero integers. Then

$$U_{n_0} = k\Box$$

can hold only for finitely many coprime integers P, Q.

The case $n_0 = 8, k = \pm 3, \mathcal{S} = \{2\}$

If $n_0 = 8, k = \pm 3, \mathcal{S} = \{2\}$, then the equation is in the form

$$U_{2^t}(P, Q) = k\square.$$

In case of $n_0 = 8$ and $k = \pm 3$ we get

$$\begin{aligned} P &= ax^2, \\ P^2 - 2Q &= by^2, \\ P^4 - 4P^2Q + 2Q^2 &= cz^2, \end{aligned}$$

where $a, b, c \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$.
The last equation can be written as $(P^2 - 2Q)^2 - 2Q^2 = cz^2$, which has no solution if $3|c$. Therefore $c \in \{\pm 1, \pm 2\}$. We also have that $\gcd(a, b) \in \{1, 2\}$ and $gcd(b, c) \in \{1, 2\}$. It remains to deal with 64 triples.

Eliminating triples

The previous system of equations leads to the hyperelliptic curve

$$-2cX^4 + 4bcX^2 + 2b^2c = Y^2.$$

```
Elim:=function(D)
 P<x>:=PolynomialRing(Rationals());
 C:=HyperellipticCurve(-2*D[3]*x^4+4*D[2]*D[3]*x^2+
    2*D[2]^2*D[3]);
 BP:=BadPrimes(C);
 return &and [IsLocallySolvable(C,p): p in BP];
end function;
```

After testing local solvability of these curves there remains only 40 triples to deal with.

Rank 0 elliptic curves

The hyperelliptic curve

$$-2cX^4 + 4bcX^2 + 2b^2c = Y^2$$

is a curve of genus 1, that is an elliptic curve. There are only finitely many rational points on elliptic curves of rank 0. The Birch and Swinnerton-Dyer conjecture is known for elliptic curves of rank 0, so we reduce the number of triples by using the Magma procedure `AnalyticRank`.

```
Elim2:=function(D)
 E:=EllipticCurve([0,4*D[2]*D[3],0,-4*D[2]^2*D[3]^2,0]);
 return AnalyticRank(E);
end function;
```

The number of remaining triples is 16.

Triples to deal with

The remaining triples are as follows

$$< -3, -2, -2 >, < -1, 6, -2 >, < 1, 6, -2 >, < 3, -2, -2 >,$$
$$< -3, -1, -1 >, < -1, 3, -1 >, < 1, 3, -1 >, < 3, -1, -1 >,$$
$$< -3, 1, 1 >, < -1, -3, 1 >, < 1, -3, 1 >, < 3, 1, 1 >,$$
$$< -3, 2, 2 >, < -1, -6, 2 >, < 1, -6, 2 >, < 3, 2, 2 > .$$

Important remark: $< -3, -2, -2 > \sim < 3, -2, -2 >$ etc.

Eliminating triples by elliptic Chabauty

We may also try to eliminate triples by the so-called elliptic Chabauty method, which is now implemented in Magma (work by Nils Bruin).
A few of them can be eliminated in this way.

Other direction

We have a conic:

$$-(a^2x^4)^2 + 2(a^2x^4)(by^2) + (by^2)^2 = 2cz^2$$

c	point	a^2x^4	by^2
-2	$(2,0,1)$	$2u^2 + 2v^2$	$4uv - 4v^2$
-1	$(1,-1,1)$	$3u^2 + 2uv + v^2$	$u^2 + 2uv - v^2$
1	$(1,1,1)$	$-u^2 - 2uv + v^2$	$-u^2 + 2uv - 3v^2$
2	$(0,2,1)$	$-4u^2 - 4uv$	$-2u^2 - 2v^2$

Parametrizations yields curves of genus 3 and genus 4 over the rational number field.

We have that $(P, Q) \in \{(\pm 3, 5), (\pm 1, 2)\}$. For given (P, Q) Bremner and Tzanakis reduced the problem to certain Thue-Mahler equation of degree 4. We do it in a different way.
$(P, Q) = (\pm 3, 5)$, we obtain that $D = -11$, therefore

$$V_n^2 + 11U_n^2 = 4 \cdot 5^n,$$

and we also have that $U_n = \pm 3\square$.

$$V_n^2 = -99x^4 + 4 \cdot 5^n.$$

That is we have to determine S-integral points on elliptic curves. That can be done by the Magma procedure `SIntegralLjunggrenPoints`.
if $(P, Q) = (\pm 1, 2)$, then the curve is given by $V_n^2 = -63x^4 + 2^{n+2}$.