Diophantine Equations Related to Arithmetic Progressions

Szabolcs Tengely

May 14, 2007
$x^2 + q^m = 2^r y^p$ (joint work with Samir Siksek)
\[ x^2 + q^m = 2^r y^p \] (joint work with Samir Siksek)

- Special cases
- Modular approach
Special cases

Modular approach

\[ x^2 + q^m = 2^r y^p \] (joint work with Samir Siksek)

\[ n(n + d) \cdots (n + (k - 1)d) = by^m \]
\[ x^2 + q^m = 2^r y^p \] (joint work with Samir Siksek)

- Special cases
- Modular approach

\[ n(n + d) \cdots (n + (k - 1)d) = by^m \]

- \( m = 2 \), the cases \( k = 5, 7 \) (lecture by Rob Tijdeman and lecture by Shanta Laisram)
- \( m = 3 \), lecture by Lajos Hajdu
\[ x^2 + q^m = 2^r y^p \] (joint work with Samir Siksek)

- Special cases
- Modular approach

\[ n(n + d) \cdots (n + (k - 1)d) = by^m \]

- \( m = 2 \), the cases \( k = 5, 7 \) (lecture by Rob Tijdeman and lecture by Shanta Laisram)
- \( m = 3 \), lecture by Lajos Hajdu

- squares and cubes in arithmetic progressions, paper by Nils Bruin, Kálmán Győry, Lajos Hajdu, Szabolcs Tengely
BHV works in many cases
BHV works in many cases

- $x^2 + 2^a 3^b = y^p$  Luca (2002)
- $x^2 + p^{2k+1} = 4y^n$  Arif and Al-Ali (2002)
- $x^2 + 5^{2k} = y^n$  Muriefah (2006)
Special cases

- BHV works in many cases
  - $x^2 + 2^a3^b = y^p$ Luca (2002)
  - $x^2 + p^{2k+1} = 4y^n$ Arif and Al-Ali (2002)
  - $x^2 + 5^{2k} = y^n$ Muriefah (2006)

- $p = 3$, $S$-integral points on elliptic curves
  
  $$\left(\frac{x}{q^{3t}}\right)^2 + q^s = 2^r \left(\frac{y}{q^{2t}}\right)^3$$
BHV works in many cases

\[ x^2 + 2^{a}3^{b} = y^p \] Luca (2002)

\[ x^2 + p^{2k+1} = 4y^n \] Arif and Al-Ali (2002)

\[ x^2 + 5^{2k} = y^n \] Muriefah (2006)

\[ p = 3, \text{ } S\text{-integral points on elliptic curves} \]

\[
\left( \frac{x}{q^{3t}} \right)^2 + q^s = 2^r \left( \frac{y}{q^{2t}} \right)^3
\]

\[ p = 5, \text{ algebraic number theory, Thue-equations (lecture by Yann Bugeaud)} \]
Lucas sequence: \( u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \), \( p \) is a primitive divisor of \( u_n(\alpha, \beta) \) if \( p \) divides \( u_n \), but does not divide \((\alpha - \beta)^2u_1u_2\cdots u_{n-1}\).

Arif and Al-Ali (2002):

\[
x^2 + 3^{2k+1} = 4y^p
\]

We obtain

\[
\frac{x + 3^k \sqrt{-3}}{2} = \left( \frac{a + b \sqrt{-3}}{2} \right)^p.
\]

Let \( \alpha = \frac{a+b\sqrt{-3}}{2}, \beta = \frac{a-b\sqrt{-3}}{2} \). We have

\[
u_n(\alpha, \beta) = \begin{cases} 
\pm 1 & \text{if } p \neq 3, \\
\pm 3 & \text{if } p = 3.
\end{cases}
\]
\[ x^2 + 5^k = 2y^3, \]

here \( S = \{5\} \),

\[
\left( \frac{2x}{5^{3t}} \right)^2 = \left( \frac{2y}{5^{2t}} \right)^3 - 4 \cdot 5^s, \quad s \in \{0, 1, \ldots, 5\}
\]

using MAGMA one obtains all the \( S \)-integral points on the curve. The solutions of the original problem:

\[
(x, y) \in \{(\pm1, 1), (\pm7, 3), (\pm99, 17)\}.
\]
\[ x^2 + 3^{2m} = 2y^3, \] factor the LHS \[ 3^m = (u - v)(u^2 + 4uv + v^2), \] hence there exists \( k \in \{0, \ldots, m\} \) such that
$x^2 + 3^{2m} = 2y^3$, factor the LHS $3^m = (u - v)(u^2 + 4uv + v^2)$, hence there exists $k \in \{0, \ldots, m\}$ such that

$$u - v = \pm 3^k,$$

$$u^2 + 4uv + v^2 = \pm 3^{m-k}.$$
\[ x^2 + 3^{2m} = 2y^3, \] factor the LHS \[ 3^m = (u - v)(u^2 + 4uv + v^2), \] hence there exists \( k \in \{0, \ldots, m\} \) such that

\[
\begin{align*}
u - v &= \pm 3^k, \\
u^2 + 4uv + v^2 &= \pm 3^{m-k}.
\end{align*}
\]

That is

\[
6v^2 \pm 6(3^k)v + 3^{2k} = \pm 3^{m-k}.
\]

If \( k = 0 \) or \( k = m \), then \((x, y) = (\pm 1, 1)\).

If \( k = m - 1 > 0 \), then \( 3 \mid 2v^2 \pm 1 \).
\[ x^2 + 3^{2m} = 2y^3, \]  

factor the LHS \( 3^m = (u - v)(u^2 + 4uv + v^2) \), hence there exists \( k \in \{0, \ldots, m\} \) such that

\[
\begin{align*}
    u - v &= \pm 3^k, \\
    u^2 + 4uv + v^2 &= \pm 3^{m-k}.
\end{align*}
\]

That is

\[ 6v^2 \pm 6(3^k)v + 3^{2k} = \pm 3^{m-k}. \]

If \( k = 0 \) or \( k = m \), then \((x, y) = (\pm 1, 1)\).

If \( k = m - 1 > 0 \), then \( 3 \mid 2v^2 \pm 1 \).

\[
\begin{align*}
    u - v &= -3^{m-1}, \\
    u^2 + 4uv + v^2 &= -3.
\end{align*}
\]
\[ u = \frac{-\varepsilon}{2} \left( (2 + \sqrt{3})^{t-1} + (2 - \sqrt{3})^{t-1} \right), \]
\[ v = \frac{\varepsilon}{2} \left( (2 + \sqrt{3})^t + (2 - \sqrt{3})^t \right), \]

where \( t \in \mathbb{N}, \varepsilon \in \{-1, 1\}. \]
where $t \in \mathbb{N}$, $\varepsilon \in \{-1, 1\}$.

$$\frac{1}{2} \left( (3 + \sqrt{3})(2 + \sqrt{3})^{t-1} + (3 - \sqrt{3})(2 - \sqrt{3})^{t-1} \right) = \pm 3^{m-1}. $$
\[ u = \frac{-\varepsilon}{2} \left( (2 + \sqrt{3})^{t-1} + (2 - \sqrt{3})^{t-1} \right), \]
\[ v = \frac{\varepsilon}{2} \left( (2 + \sqrt{3})^t + (2 - \sqrt{3})^t \right), \]

where \( t \in \mathbb{N}, \varepsilon \in \{-1, 1\}. \)

\[ \frac{1}{2} \left( (3 + \sqrt{3})(2 + \sqrt{3})^{t-1} + (3 - \sqrt{3})(2 - \sqrt{3})^{t-1} \right) = \pm 3^{m-1}. \]

Recurrence sequence \( r_0 = r_1 = 3, r_t = 4r_{t-1} - r_{t-2}, t \geq 2. \)
$u = \frac{-\varepsilon}{2} \left( (2 + \sqrt{3})^{t-1} + (2 - \sqrt{3})^{t-1} \right),$

$v = \frac{\varepsilon}{2} \left( (2 + \sqrt{3})^t + (2 - \sqrt{3})^t \right),$

where $t \in \mathbb{N}$, $\varepsilon \in \{-1, 1\}$.

$$\frac{1}{2} \left( (3 + \sqrt{3})(2 + \sqrt{3})^{t-1} + (3 - \sqrt{3})(2 - \sqrt{3})^{t-1} \right) = \pm 3^{m-1}.$$ 

Recurrence sequence $r_0 = r_1 = 3, r_t = 4r_{t-1} - r_{t-2}, t \geq 2$.

$r_t \equiv 0 \pmod{27} \iff t \equiv 5 \text{ or } 14 \pmod{18}$,

$r_t \equiv 0 \pmod{17} \iff t \equiv 5 \text{ or } 14 \pmod{18}$. 
\[ u = \frac{-\varepsilon}{2} \left( (2 + \sqrt{3})^{t-1} + (2 - \sqrt{3})^{t-1} \right), \]
\[ v = \frac{\varepsilon}{2} \left( (2 + \sqrt{3})^t + (2 - \sqrt{3})^t \right), \]

where \( t \in \mathbb{N}, \varepsilon \in \{-1, 1\} \).

\[ \frac{1}{2} \left( (3 + \sqrt{3})(2 + \sqrt{3})^{t-1} + (3 - \sqrt{3})(2 - \sqrt{3})^{t-1} \right) = \pm 3^{m-1}. \]

Recurrence sequence \( r_0 = r_1 = 3, r_t = 4r_{t-1} - r_{t-2}, t \geq 2 \).

\[ r_t \equiv 0 \pmod{27} \iff t \equiv 5 \text{ or } 14 \pmod{18}, \]
\[ r_t \equiv 0 \pmod{17} \iff t \equiv 5 \text{ or } 14 \pmod{18}. \]

There are two possible cases: \( m = 2, k = 1 : (x, y) = (13, 5) \), and \( m = 3, k = 2 : (x, y) = (545, 53) \).
If $r > 1$ then $x^2 + 13^m \equiv 2 \pmod{4}$ and $2^r y^p \equiv 0 \pmod{4}$, a contradiction.

\[
\begin{align*}
    r = 0 : & \quad x^2 + 13^m = y^p, \quad x \text{ is even, } y \text{ odd.} \\
    r = 1 : & \quad x^2 + 13^m = 2y^p, \quad x \text{ is odd, } y \text{ is odd.}
\end{align*}
\]
If $r > 1$ then $x^2 + 13^m \equiv 2 \pmod{4}$ and $2^r y^p \equiv 0 \pmod{4}$, a contradiction.

\[r = 0 : \quad x^2 + 13^m = y^p, \quad x \text{ is even , } y \text{ odd.}\]
\[r = 1 : \quad x^2 + 13^m = 2y^p, \quad x \text{ is odd , } y \text{ is odd.}\]

The case $r = 0$. We have the following two Frey curves (Ivorra and Kraus (2006), lecture by Ivorra)

\[E_1 : \quad Y^2 = X^3 + 2xX^2 + y^p X,\]
\[E_2 : \quad Y^2 = X^3 + 2xX^2 + (x^2 - y^p)X.\]
By Ribet’s level-lowering one gets

\[ N_p(E_1) = 2^s \cdot 13 \quad \text{where} \quad s = \begin{cases} 6 & \text{if } x \equiv 1 \pmod{4}, \\ 5 & \text{if } x \equiv -1 \pmod{4}, \end{cases} \]

and

\[ N_p(E_2) = 2^t \cdot 13 \quad \text{where} \quad t = \begin{cases} 5 & \text{if } x \equiv 1 \pmod{4}, \\ 6 & \text{if } x \equiv -1 \pmod{4}. \end{cases} \]

There are 6 newforms at level \(2^5 \cdot 13\) and 16 at level \(2^6 \cdot 13\).
It is often possible to obtain bound for the exponent $p$. (Samir’s notes, section 6). Let $E_1 \sim_p f_1$ and $E_2 \sim_p f_2$. Let $c_l$ be the $l$-th coefficient of $f_1$ and $d_l$ be the $l$-th coefficient of $f_2$. Define

$$B'_l(f_1) = \text{Norm}_{K/\mathbb{Q}}((l + 1)^2 - c_l^2) \prod_{x,y \in \mathbb{F}_l} \text{Norm}_{K/\mathbb{Q}}(a_l(E_1) - c_l),$$

and

$$B_l(f_1) = \begin{cases} l \cdot B'_l(f_1) & \text{if } f \text{ is not rational,} \\ B'_l(f_1) & \text{if } f \text{ is rational.} \end{cases}$$

Similarly for $f_2$. We have $p \mid \gcd(B_l(f_1), B_l(f_2))$. The above argument implies that if there exists a solution of $x^2 + 13^m = y^p$ then $p \in \{3, 5\}$. 
Here we have the following two Frey curves

\[ E_1 : \quad Y^2 = X^3 + 2xX^2 + 2y^p X, \]
\[ E_2 : \quad Y^2 = X^3 + 2xX^2 + (x^2 - 2y^p) X, \]

and \( N_p(E_1) = N_p(E_2) = 2^7 \cdot 13 \). There are 28 newforms at level \( 2^7 \cdot 13 \). The previous argument does not provide bound for the exponent \( p \) in this case. There are only a few pairs of newforms for which it happens.
Here we have the following two Frey curves

\( E_1 : \quad Y^2 = X^3 + 2xX^2 + 2y^p X, \)

\( E_2 : \quad Y^2 = X^3 + 2xX^2 + (x^2 - 2y^p) X, \)

and \( N_p(E_1) = N_p(E_2) = 2^7 \cdot 13 \). There are 28 newforms at level \( 2^7 \cdot 13 \). The previous argument does not provide bound for the exponent \( p \) in this case. There are only a few pairs of newforms for which it happens.

Rewrite the Frey curves as follows

\( E_1 : \quad Y^2 = X^3 + 2xX^2 + (x^2 + 13^m) X, \)

\( E_2 : \quad Y^2 = X^3 + 2xX^2 + (-13^m) X. \)

We get congruence conditions for \( m \). We have \( \text{ord}_7(13) = 2 \) and \( \text{ord}_{11}(13) = 10 \). 

\[ x^2 + 13^m = 2y^p \]
Therefore $m \equiv 0 \pmod{2}$.

\[ x^2 + 13^{2k} = 2y^p \]
The equation \( x^2 + q^{2k} = 2y^p \).

\[
\delta_4 = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}, \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

\[
\delta_8 = \begin{cases} 
1 & \text{if } p \equiv 1 \text{ or } 3 \pmod{8}, \\
-1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{8}.
\end{cases}
\]

\[
y = u^2 + v^2,
\]

\[
x = \Re((1 + i)(u + iv)^p) =: F_p(u, v),
\]

\[
q^k = \Im((1 + i)(u + iv)^p) =: G_p(u, v).
\]
\[(u - \delta_4 v) \mid F_p(u, v), \]
\[(u + \delta_4 v) \mid G_p(u, v).\]
Reducibility

\[(u - \delta_4 v) \mid F_p(u, v),\]
\[(u + \delta_4 v) \mid G_p(u, v).\]

Example: \(p = 5\).

\[F_5(u, v) = (u - v)(u^4 - 4u^3v - 14u^2v^2 - 4uv^3 + v^4),\]
\[G_5(u, v) = (u + v)(u^4 + 4u^3v - 14u^2v^2 + 4uv^3 + v^4).\]
There exists \( s \in \{0, 1, \ldots, k\} \) such that

\[
\begin{align*}
    u + \delta_4 v &= q^s, \\
    H_p(u, v) &= q^{k-s},
\end{align*}
\]

or

\[
\begin{align*}
    u + \delta_4 v &= -q^s, \\
    H_p(u, v) &= -q^{k-s},
\end{align*}
\]

where \( H_p(u, v) = \frac{G_p(u,v)}{u+\delta_4 v} \).
We have \( \deg H_p(\pm q^s - \delta_4 v, v) = p - 1 \) and

\[
H_p(\pm q^s - \delta_4 v, v) = \pm \delta_8 2^{\frac{p-1}{2}} pv^{p-1} + q^s p \hat{H}_p(v) + q^s(p-1),
\]

where \( \hat{H}_p \in \mathbb{Z}[X] \).
We have \( \deg H_p(\pm q^s - \delta_4 v, v) = p - 1 \) and

\[
H_p(\pm q^s - \delta_4 v, v) = \pm \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^s p \hat{H}_p(v) + q^{s(p-1)},
\]

where \( \hat{H}_p \in \mathbb{Z}[X] \).

Equations (1) and (2) imply

\[
\pm \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^s p \hat{H}_p(v) + q^{s(p-1)} = \pm q^{k-s}.
\]
We have \( \deg H_p(\pm q^s - \delta_4 v, v) = p - 1 \) and

\[
H_p(\pm q^s - \delta_4 v, v) = \pm \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^s p \hat{H}_p(v) + q^s(p-1),
\]

where \( \hat{H}_p \in \mathbb{Z}[X] \).

Equations (1) and (2) imply

\[
\pm \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^s p \hat{H}_p(v) + q^s(p-1) = \pm q^{k-s}.
\]

The following cases are possible
We have \( \deg H_p(\pm q^s - \delta_4 v, v) = p - 1 \) and

\[
H_p(\pm q^s - \delta_4 v, v) = \pm \delta_8 2^{\frac{p-1}{2}} pv^{p-1} + q^s p \hat{H}_p(v) + q^s(p-1),
\]

where \( \hat{H}_p \in \mathbb{Z}[X] \).

Equations (1) and (2) imply

\[
\pm \delta_8 2^{\frac{p-1}{2}} pv^{p-1} + q^s p \hat{H}_p(v) + q^s(p-1) = \pm q^{k-s}.
\]

The following cases are possible

- \( p = q, s = k - 1 \),
We have $\deg H_p(\pm q^s - \delta_4 v, v) = p - 1$ and

$$H_p(\pm q^s - \delta_4 v, v) = \pm \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^s p \hat{H}_p(v) + q^s(p-1),$$

where $\hat{H}_p \in \mathbb{Z}[X]$.
Equations (1) and (2) imply

$$\pm \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^s p \hat{H}_p(v) + q^s(p-1) = \pm q^{k-s}.$$  

The following cases are possible

- $p = q, s = k - 1$,
- $p \neq q, s = 0$ or $s = k$.  

All solutions of the equation $x^2 + q^{2k} = 2y^p$ with $3 \leq q^k \leq 501$ are as follows

$$(x, y, q, k, p) \in \{(3, 5, 79, 1, 5), (9, 5, 13, 1, 3), (13, 5, 3, 2, 3), (55, 13, 37, 1, 3), (79, 5, 3, 1, 5), (99, 17, 5, 1, 3), (161, 25, 73, 1, 3), (249, 5, 307, 1, 7), (351, 41, 11, 2, 3), (545, 53, 3, 3, 3), (649, 61, 181, 1, 3), (1665, 113, 337, 1, 3), (2431, 145, 433, 1, 3), (5291, 241, 19, 1, 3), (275561, 3361, 71, 1, 3)\}.$$

It remains to deal with

$$x^2 + 13^{2k} = 2y^p,$$

with $k \geq 3$. 
Theorem. If \( x^2 + 13^{2k} = 2y^p \) admits a relatively prime solution \( (x, y) \in \mathbb{N}^2 \) then we have \( p \leq 3203 \) if \( u + \delta_4 v = \pm 13^k, k \geq 3 \).

We get
\[
\frac{13^k}{2} \leq \frac{|u| + |v|}{2} \leq \sqrt{\frac{u^2 + v^2}{2}} = \sqrt{\frac{y}{2}}.
\]

We have
\[
\left| \frac{x + 13^k i}{x - 13^k i} - 1 \right| = \frac{2 \cdot 13^k}{\sqrt{x^2 + 13^{2k}}} \leq \frac{2 \sqrt{y}}{y^{p/2}} = \frac{2}{y^{p-1}/2},
\]

and
\[
\frac{x + 13^k i}{x - 13^k i} = \frac{(1 + i)(u + iv)^p}{(1 - i)(u - iv)^p} = i \left( \frac{u + iv}{u - iv} \right)^p.
\]

Finally
\[
\left| i \left( \frac{u + iv}{u - iv} \right)^p - 1 \right| \geq \frac{1}{2} \left| \log i \left( \frac{u + iv}{u - iv} \right)^p \right|.
\]
**Lemma.** In case of $p > 3$ there is no solution of (1) and (2) with $s = 0$. 

---

Outline
Special cases

Parameterization
Reducibility
System of equations

Small solutions
Linear forms in two logs

Back to Frey curves
Product of terms in AP
Eliminate tuples
Elliptic curves
Magma computation
Powers in AP
Lemma. In case of $p > 3$ there is no solution of (1) and (2) with $s = 0$.

Proof. In case of (1) if $s = 0$, then $u = 1 - \delta_4 v$. Observe that by the definition of $H_p$

- if $v \equiv 0 \pmod{13}$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod{13}$,
- if $v \equiv 1 \pmod{13}$ and $p \equiv 1 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod{13}$,
- if $v \equiv 1 \pmod{13}$ and $p \equiv 3 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv \pm 5 \pmod{13}$,
- if $v \equiv 2 \pmod{13}$ and $p \equiv 1 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv \pm 1 \pmod{13}$,
- if $v \equiv 2 \pmod{13}$ and $p \equiv 3 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv 7, 8 \pmod{13}$,
- if $v \equiv 3 \pmod{13}$ and $p \equiv 1 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv 1, 9 \pmod{13}$,
- if $v \equiv 3 \pmod{13}$ and $p \equiv 3 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv 6, 12 \pmod{13}$.
- if $v \equiv 4 \pmod{13}$ and $p \equiv 1 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv 1, 7 \pmod{13}$,
- if $v \equiv 4 \pmod{13}$ and $p \equiv 3 \pmod{4}$, then $H_p(1 - \delta_4 v, v) \equiv 7, 8 \pmod{13}$.
- etc.

Thus if $p > 3$ then $H_p(1 - \delta_4 v, v) \not\equiv 0 \pmod{13}$. We remark that $u + \delta_4 v = -13^k$ is not possible because $-1 \equiv H_p(-13^k - \delta_4 v, v) \equiv 13^k(p-1) \equiv 1 \pmod{p}$. \qed
Remaining possibility

\[ u + \delta_4 v = 13^k, \]
\[ H_p(u, v) = 1, \]
\[ x = F_p(13^k - \delta_4 v, v). \]

Corresponding Frey curves

\[ E_1 : \quad Y^2 = X^3 + 2F_p(13^k - \delta_4 v)X^2 + (F_p(13^k - \delta_4 v)^2 + 13^{2k})X, \]
\[ E_2 : \quad Y^2 = X^3 + 2F_p(13^k - \delta_4 v)X^2 + (-13^{2k})X. \]
Remaining possibility

\[ u + \delta_4 v = 13^k, \]
\[ H_p(u, v) = 1, \]
\[ x = F_p(13^k - \delta_4 v, v). \]

Corresponding Frey curves

\[ E_1 : \quad Y^2 = X^3 + 2F_p(13^k - \delta_4 v)X^2 + (F_p(13^k - \delta_4 v)^2 + 13^{2k})X, \]
\[ E_2 : \quad Y^2 = X^3 + 2F_p(13^k - \delta_4 v)X^2 + (-13^{2k})X. \]

"Good" primes: primes of the form \( l = np + 1 \) or primes \( l \) for which \( \text{ord}_l(13) \) is "small". Using such primes and the method of Kraus we can exclude all primes \( p \in \{7, \ldots, 3203\} \).
\[ n(n + d) \cdots (n + (k - 1)d) = by^2 \]

where \( \gcd(n, d) = 1 \) and \( P(b) \leq k \).

We have

\[ n + id = a_i x_i^2 \text{ for } 0 \leq i < k. \]
\[ n(n + d) \cdots (n + (k - 1)d) = by^2 \]

where \( \gcd(n, d) = 1 \) and \( P(b) \leq k \).

We have

\[ n + id = a_i x_i^2 \text{ for } 0 \leq i < k. \]

**Theorem** (Hirata-Kohno, Laishram, Shorey, Tijdeman). *The above equation with \( d > 1 \), \( P(b) = k \) and \( 7 \leq k \leq 100 \) implies that \((a_0, a_1, \ldots, a_{k-1})\) is among the following tuples or their mirror images.*

- \( k = 7 \): (2, 3, 1, 5, 6, 7, 2), (3, 1, 5, 6, 7, 2, 1), (1, 5, 6, 7, 2, 1, 10),
- \( k = 13 \): (3, 1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15),
  (1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1),
- \( k = 19 \): (1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22),
- \( k = 23 \): (5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22, 23, 6, 1, 26, 3),
  (6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22, 23, 6, 1, 26, 3, 7).
The cases \( k = 5, P(b) = 5 \) and
\( k = 7, (2, 3, 1, 5, 6, 7, 2), (3, 1, 5, 6, 7, 2, 1), (1, 5, 6, 7, 2, 1, 10) \).

**Theorem** (Bennett). *If \( n \) and \( d \) are coprime nonzero integers, then the Diophantine equation*

\[
  n(n + d)(n + 2d)(n + 3d)(n + 4d) = by^l
\]

*has no solutions in nonzero integers \( b, y \) and \( l \) with \( l \geq 2 \) and \( P(b) \leq 3 \).*

\[
  T = \{(a_0, a_1, a_2, a_3, a_4) | a_i = 2^\alpha 3^\beta 5^\gamma \}.
\]

WLOG \( 5|a_1 \) or \( 5|a_2 \).
(6, −5, 1, 3, 2).

Congruence arguments.

Rank 0 elliptic curves.
Eliminate tuples

- $(6, -5, 1, 3, 2)$.
- Congruence arguments.
- Rank 0 elliptic curves.

The only possible tuples are

$$(2, 5, 2, -1, -1), (2, 5, -3, -1, -1), (3, 5, -2, -1, -1), (6, 5, 1, 3, 2).$$

Using $n + 2d = 2x_2^2$ and $n + 3d = -x_3^2$ we obtain

$$x_3^2 + 3x_2^2 = x_0^2,$$
$$x_3^2 + 4x_2^2 = 5x_1^2,$$
$$2x_3^2 + 2x_2^2 = x_4^2.$$ 

Remark: $\text{Rank}(J) = 2$. 

[Leiden 2007 tengely@math.klte.hu – slide 23]
After factorization we get

\[(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \Box,\]

where \(\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}\).
After factorization we get

\[(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \Box,\]

where \(\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}\).

Elliptic Chabauty’s method: implemented in MAGMA by Nils Bruin.
(lecture by Nils Bruin)
After factorization we get

\[(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \Box,
\]

where \( \delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\} \).

Elliptic Chabauty’s method: implemented in MAGMA by Nils Bruin.
(lecture by Nils Bruin)

-3 ± i, 3 ± i: RankBound = 0.
After factorization we get

\[(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \Box,\]

where \(\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}\).

Elliptic Chabauty’s method: implemented in MAGMA by Nils Bruin.

(lecture by Nils Bruin)

- \(-3 \pm i, 3 \pm i\) : \text{RankBound} = 0.
- \(-1 - 3i\) : \text{RankBound} = 1. Using \(p = 13\) we obtain that the only solution with \(x_3/x_2 \in \mathbb{Q}\) is -1.
After factorization we get

\[(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \Box,
\]

where \(\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}\).

Elliptic Chabauty’s method: implemented in MAGMA by Nils Bruin.

(lecture by Nils Bruin)

- \(-3 \pm i, 3 \pm i\): \(\text{RankBound} = 0\).
- \(-1 - 3i\): \(\text{RankBound} = 1\). Using \(p = 13\) we obtain that the only solution with \(x_3/x_2 \in \mathbb{Q}\) is \(-1\).
- \(-1 + 3i\): \(\text{RankBound} = 1\). Using again \(p = 13\) it follows that \(x_3/x_2 = 1\).
After factorization we get

\[(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \Box,\]

where \(\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}\).

Elliptic Chabauty’s method: implemented in MAGMA by Nils Bruin.
(lecture by Nils Bruin)

- \(-3 \pm i, 3 \pm i\): RankBound = 0.
- \(-1 - 3i\): RankBound = 1. Using \(p = 13\) we obtain that the only solution with \(x_3/x_2 \in \mathbb{Q}\) is -1.
- \(-1 + 3i\): RankBound = 1. Using again \(p = 13\) it follows that \(x_3/x_2 = 1\).
- \(1 - 3i\): RankBound = 1. Here we have \(x_3/x_2 = 1\).
After factorization we get

$$(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \Box,$$

where $\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}$.

Elliptic Chabauty’s method: implemented in MAGMA by Nils Bruin.
(lecture by Nils Bruin)

- $-3 \pm i, 3 \pm i$ : RankBound = 0.
- $-1 - 3i$ : RankBound = 1. Using $p = 13$ we obtain that the only solution with $x_3/x_2 \in \mathbb{Q}$ is -1.
- $-1 + 3i$ : RankBound = 1. Using again $p = 13$ it follows that $x_3/x_2 = 1$.
- $1 - 3i$ : RankBound = 1. Here we have $x_3/x_2 = 1$.
- $1 + 3i$ : RankBound = 1. In this case $x_3/x_2 = -1$. 
After factorization we get

\[(x_3 + ix_2)(x_3 + 2ix_2)(x_3^2 + 3x_2^2) = \delta \square,\]

where \(\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}\).

Elliptic Chabauty’s method: implemented in MAGMA by Nils Bruin.
(lecture by Nils Bruin)

-\( -3 \pm i, 3 \pm i \): RankBound = 0.

-\( -1 - 3i \): RankBound = 1. Using \(p = 13\) we obtain that the only solution with \(x_3/x_2 \in \mathbb{Q}\) is -1.

-\( -1 + 3i \): RankBound = 1. Using again \(p = 13\) it follows that \(x_3/x_2 = 1\).

-\( 1 - 3i \): RankBound = 1. Here we have \(x_3/x_2 = 1\).

-\( 1 + 3i \): RankBound = 1. In this case \(x_3/x_2 = -1\).

The AP is \([8, 5, 2, -1, -4]\), that is \(n = 8\) and \(d = -3\).
\[ P \quad \begin{equation} \begin{aligned} \langle x \rangle &:= \text{PolynomialRing}(\text{Rationals}()) \\ N \quad \begin{equation} \begin{aligned} i &:= \text{NumberField}(x^2 + 1) \\ R \quad \begin{equation} \begin{aligned} X &:= \text{PolynomialRing}(N) \\ P &:= \text{ProjectiveSpace}(\text{Rationals}(), 1) \\ C &:= \text{HyperellipticCurve}((1 + 3 \ast i) \ast (X + i) \ast (X + 2 \ast i) \ast (X^2 + 3)) \\ E, toE &:= \text{EllipticCurve}(C) \\ Em, EtoEm &:= \text{MinimalModel}(E) 
\end{aligned} \end{aligned} \end{equation} \end{aligned} \]
\( P < x > := PolynomialRing(Rationals()); \)
\( N < i > := NumberField(x^2 + 1); \)
\( R < X > := PolynomialRing(N); \)
\( P1 := ProjectiveSpace(Rationals(), 1); \)
\( C := HyperellipticCurve((1 + 3 \cdot i) \cdot (X + i) \cdot (X + 2 \cdot i) \cdot (X^2 + 3)); \)
\( E, toE := EllipticCurve(C); \)
\( Em, EtoEm := MinimalModel(E); \)
\( y^2 = x^3 + i \cdot x^2 + (5 \cdot i - 7) \cdot x + (4 \cdot i - 6) \)
\( umap := map < C \rightarrow P1|[C.1, C.3]>; \)
\( U := Expand(Inverse(toE \cdot EtoEm) \cdot umap); \)
\( success, G, mwmap := PseudoMordellWeilGroup(Em); \)
\( NC, VC, RC, CC := Chabauty(mwmap, U, 13); \)
\begin{verbatim}
P < x > := PolynomialRing(Rationals());
N < i > := NumberField(x^2 + 1);
R < X > := PolynomialRing(N);
P1 := ProjectiveSpace(Rationals(), 1);
C := HyperellipticCurve((1 + 3 * i) * (X + i) * (X + 2 * i) * (X^2 + 3));
E, toE := EllipticCurve(C);
Em, EtoEm := MinimalModel(E);
y^2 = x^3 + i * x^2 + (5 * i - 7) * x + (4 * i - 6)
umap := map < C - > P1|[C.1, C.3] >;
U := Expand(Inverse(toE * EtoEm) * umap);
success, G, mwmap := PseudoMordellWeilGroup(Em);
NC, VC, RC, CC := Chabauty(mwmap, U, 13);
NC = 2, VC = {G.1 ± G.2}, RC = 2
forall{pr : pr in PrimeDivisors(RC)|IsPSaturated(mwmap, pr)};
{EvaluateByPowerSeries(U, mwmap(gp)) : gp in VC};
{(−1 : 1)}
\end{verbatim}

**Theorem.** Let $k \geq 4$ and $L \geq 2$. There are only finitely many $k$-term integral arithmetic progressions $(h_0, h_1, \ldots, h_{k-1})$ such that $\gcd(h_0, h_1) = 1$ and $h_i = x_i^{l_i}$ with some $x_i \in \mathbb{Z}$ and $2 \leq l_i \leq L$ for $i = 0, 1, \ldots, k - 1$.

In case of $(l_0, l_1, l_2, l_3) = (2, 2, 2, 3)$

\[
((u^2 - 2uv - v^2)f(u, v))^2, ((u^2 + v^2)f(u, v))^2, ((u^2 + 2uv - v^2)f(u, v))^2, (f(u, v))^3
\]

is an arithmetic progression for any $u, v \in \mathbb{Z}$, where

\[f(u, v) = u^4 + 8u^3v + 2u^2v^2 - 8uv^3 + v^4.\]
Let \( x_0^3, x_1^2, x_2^3, x_3^2 \) be consecutive terms of an arithmetic progression with \( \gcd(x_0, x_1, x_2, x_3) = 1 \). We have

\[
x_1^2 = \frac{x_0^3 + x_2^3}{2},
\]

\[
x_3^2 = \frac{-x_0^3 + 3x_2^3}{2}.
\]

**Theorem.** Let \( C \) be the curve given by

\[
Y^2 = -X^6 + 2X^3 + 3.
\]

Then \( C(\mathbb{Q}) = \{(-1, 0), (1, \pm 2)\} \).

Solutions are given by

\[
(x_0, x_1, x_2, x_3) \in \{(-2t^2, 0, 2t^2, \pm 4t^3), (t^2, \pm t^3, t^2, \pm t^3)\} \text{ for some } t \in \mathbb{Z}.
\]