The $n$–squares conjecture and rational points on some algebraic surfaces

Jerzy Browkin and Juliusz Brzeziński

Institute of Mathematics
Polish Academy of Sciences
and
Mathematical Sciences
University of Gothenburg and Chalmers

GHENT UNIVERSITY

September 1, 2010
Each sequence of integers

\[ a_1, a_2, \ldots, a_n \]

whose squares

\[ a_1^2, a_2^2, \ldots, a_n^2 \]

have second differences equal 2 must be trivial if \( n \) is sufficiently large.
**n—SQUARES CONJECTURE**

**n—squares conjecture**

Each sequence of integers

\[ a_1, a_2, \ldots, a_n \]

whose squares

\[ a_1^2, a_2^2, \ldots, a_n^2 \]

have second differences equal 2 must be trivial if \( n \) is sufficiently large.

J. Richard Büchi about 1975.
See L. Lipshitz in “The collected works of J. Richard Büchi.”
**Example (trivial)**

<table>
<thead>
<tr>
<th>$1^2$</th>
<th>$2^2$</th>
<th>$3^2$</th>
<th>$4^2$</th>
<th>$5^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>7</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
What is trivial?

Example (non-trivial)
For \( n = 4 \) take the sequence 6, 23, 32, 39:

Theorem (Buell, 1987)
There exist infinitely many nontrivial (increasing) sequences of FOUR integers whose squares have second differences equal 2.
What is trivial? Provisionally: $a_1, a_2, \ldots, a_n$, an arithmetical sequence (with difference $\pm 1$).
What is trivial? Provisionally: \( a_1, a_2, \ldots, a_n \), an arithmetical sequence (with difference \( \pm 1 \)).

<table>
<thead>
<tr>
<th>Example (non-trivial)</th>
</tr>
</thead>
<tbody>
<tr>
<td>For ( n = 4 ) take the sequence 6, 23, 32, 39:</td>
</tr>
<tr>
<td>6^2</td>
</tr>
<tr>
<td>493</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

Theorem (Buell, 1987)
There exist infinitely many nontrivial (increasing) sequences of FOUR integers whose squares have second differences equal 2.
DO THEY EXIST NONTRIVIAL SEQUENCES?

What is trivial? Provisionally: \( a_1, a_2, \ldots, a_n \), an arithmetical sequence (with difference \( \pm 1 \)).

Example (non-trivial)

For \( n = 4 \) take the sequence 6, 23, 32, 39:

\[
\begin{array}{cccc}
6^2 & 23^2 & 32^2 & 39^2 \\
493 & 495 & 497 & \\
2 & 2 & \\
\end{array}
\]

Theorem (Buell, 1987)

There exist infinitely many nontrivial (increasing) sequences of FOUR integers whose squares have second differences equal 2.
LONGER SEQUENCES?

Büchi's five squares conjecture

Each sequence of FIVE positive integers whose squares have constant second differences equal 2 must be trivial.

This conjecture as well as Büchi's $n^s$-squares conjecture are open problems.

J. Browkin and J. Brzeziński
Büchi’s five squares conjecture

Each sequence of FIVE positive integers whose squares have constant second differences equal 2 must be trivial.
Büchi’s five squares conjecture

Each sequence of FIVE positive integers whose squares have constant second differences equal 2 must be trivial.

This conjecture as well as Büchi’s $n$–squares conjecture are open problems.
Hilbert's Tenth Problem

Let $a_{ij}, b_j \in \mathbb{Z}$, where $i = 1, \ldots, n$, $j = 1, \ldots, m$. Does there exists an algorithm to determine:

$$\exists x_1, \ldots, x_n \in \mathbb{Z}^n \sum_{i=1}^{n} a_{ij} x_i^2 = b_j,$$ $j = 1, \ldots, m$?

If the answer is NO, take corresponding $a_{ij}, b_j$ and $P(x_1, \ldots, x_n) = m \sum_{j=1}^{m} \left( \sum_{i=1}^{n} a_{ij} x_i^2 - b_j \right)^2$.

as a polynomial proving Matiyasevich's result.

Theorem (Büchi)

If the $n$-squares conjecture is true, then the Hilbert Tenth Problem can be reduced to Büchi's question.
Hilbert’s Tenth Problem

Let \( a_{ij}, b_j \in \mathbb{Z}, \) where \( i = 1, \ldots, n \), \( j = 1, \ldots, m \). Does there exist an algorithm to determine:

\[
\exists x_1, \ldots, x_n \in \mathbb{Z} \quad \sum_{i=1}^{n} a_{ij} x_i^2 = b_j, \quad j = 1, \ldots, m.
\]

If the answer is NO, take corresponding \( a_{ij}, b_j \) and \( P(x_1, \ldots, x_n) = \left( \sum_{j=1}^{m} \left( \sum_{i=1}^{n} a_{ij} x_i^2 - b_j \right) \right)^2. \)

as a polynomial proving Matiyasevich’s result.

Theorem (Büchi)

If the \( n \)-squares conjecture is true, then the Hilbert Tenth Problem can be reduced to Büchi’s question.
Hilbert’s Tenth Problem

Büchi’s question

Let $a_{ij}, b_j \in \mathbb{Z}$, where $i = 1, \ldots, n$, $j = 1, \ldots, m$. Does there exists an algorithm to determine:

$$\exists \ x_1, \ldots, x_n \in \mathbb{Z} \ \sum_{i=1}^{n} a_{ij}x_i^2 = b_j, \ j = 1, \ldots, m?$$
Hilbert’s Tenth Problem

Büchi’s question

Let \( a_{ij}, b_j \in \mathbb{Z} \), where \( i = 1, \ldots, n, j = 1, \ldots, m \). Does there exist an algorithm to determine:

\[
\exists x_1, \ldots, x_n \in \mathbb{Z} \sum_{i=1}^{n} a_{ij}x_i^2 = b_j, j = 1, \ldots, m
\]

If the answer is NO, take corresponding \( a_{ij}, b_j \) and

\[
P(x_1, \ldots, x_n) = \sum_{j=1}^{m} \left( \sum_{i=1}^{n} a_{ij}x_i^2 - b_j \right)^2
\]

as a polynomial proving Matiyasevich’s result.
THE SOURCE OF THE PROBLEM?

Hilbert’s Tenth Problem

Büchi’s question

Let $a_{ij}, b_j \in \mathbb{Z}$, where $i = 1, \ldots, n, j = 1, \ldots, m$. Does there exists an algorithm to determine:

$$\exists \ x_1, \ldots, x_n \in \mathbb{Z} \ \sum_{i=1}^{n} a_{ij}x_i^2 = b_j, \ j = 1, \ldots, m?$$

If the answer is NO, take corresponding $a_{ij}, b_j$ and

$$P(x_1, \ldots, x_n) = \sum_{j=1}^{m} \left( \sum_{i=1}^{n} a_{ij}x_i^2 - b_j \right)^2.$$

as a polynomial proving Matiyasevich’s result.

Theorem (Büchi)

*If the $n$–squares conjecture is true, then the Hilbert Tenth Problem can be reduced to Buchi’s question.*
\[
\begin{align*}
& a_1^2 \\ & a_2^2 - a_1^2 \\ & a_3^2 - a_2^2 \\ & a_4^2 - a_3^2 \\ & a_5^2 - a_4^2
\end{align*}
\]

\[
(a_3^2 - a_2^2) - (a_2^2 - a_1^2) = \ldots = (a_5^2 - a_4^2) - (a_4^2 - a_3^2) = D
\]

so

\[
a_i^2 - 2a_{i+1}^2 + a_{i+2}^2 = D
\]

for \( i = 1, \ldots, n-2, \ n \geq 3. \) The equations

\[
a_i^2 - 2a_{i+1}^2 + a_{i+2}^2 = Da_0^2
\]

define a projective surface \( X_{n,D} \subset \mathbb{P}^n, \) which depends on \( D \)
(intersection of \( n-2 \) quadrics). Denote \( X_{n,2} = X_n. \)
\[ a_i^2 - 2a_{i+1}^2 + a_{i+2}^2 = a_{i+1}^2 - 2a_{i+2}^2 + a_{i+3}^2 \]

for \( i = 1, \ldots, n - 3, \ n \geq 4 \), that is,

\[ a_i^2 - 3a_{i+1}^2 + 3a_{i+2}^2 - a_{i+3}^2 = 0 \]

define a projective surface \( X'_n \subset \mathbb{P}^{n-1} \), which does not depend on \( D \) (intersection of \( n - 3 \) quadrics).
Theorem (Vojta, 2000)

*If there exists an integer $k \geq 8$ such that Lang’s conjecture holds for $X_k(\mathbb{Q})$, then the $n$–squares conjecture holds for some $n \geq k$.**
Theorem (Vojta, 2000)

If there exists an integer $k \geq 8$ such that Lang’s conjecture holds for $X_k(\mathbb{Q})$, then the $n$–squares conjecture holds for some $n \geq k$.

Lang’s Conjecture 1986

Let $X$ be a smooth projective algebraic variety of general type defined over a number field $k$. Then there exists a proper Zariski-closed subset $Z$ of $X$ such that for all number fields $K \supseteq k$, the set $X(K) \setminus Z(K)$ is finite.
For all $n \geq 2$, $X_n$ is a nonsingular surface with canonical sheaf $\mathcal{O}(n - 5)$, so $X_n$ is a surface of general type if $n \geq 6$.

If $n \geq 8$, then the only curves of genus 0 or 1 on $X_n$ are the trivial lines (the set $Z$ may be chosen as a union of the trivial lines).

The surface $X_n$ in $\mathbb{P}^n$ is given by the equations:

$$a_i^2 - 2a_{i+1}^2 + a_{i+2}^2 = 2a_0^2$$

for $i = 1, \ldots, n - 2$. The trivial lines ($2^n$) corresponding to $(\varepsilon_1, \ldots, \varepsilon_n)$, where $\varepsilon_k = \pm 1$ and:

$$\varepsilon_ia_i = \varepsilon_1a_1 + (i - 1)a_0$$

for $i = 2, \ldots, n$
For all $n \geq 2$, $X_n$ is a nonsingular surface with canonical sheaf $\mathcal{O}(n - 5)$, so $X_n$ is a surface of general type if $n \geq 6$.

If $n \geq 8$, then the only curves of genus 0 or 1 on $X_n$ are the trivial lines (the set $Z$ may be chosen as a union of the trivial lines).

“Lang’s set” $Z$ is a union of a finite number of curves. Only curves of genus 0 or 1 may contribute with infinite number of rational points (according to Falting’s result). The trivial lines correspond to arithmetical sequences $a_1, \ldots, a_n$. 
NUMERICAL EVIDENCE OF $n$–SQUARES CONJECTURE?

Is the $n$–squares conjecture true?

Numerical study of $X_n$, $X'_n$ for $n = 5, 6, 7, 8, ...$

In particular,

- Nontrivial sequences of five or more rational squares with constant second differences equal 2 (description of $X_n(\mathbb{Q})$)?

- Nontrivial sequences of five or more integer squares with constant second differences not necessarily 2 (description of $X'_n(\mathbb{Z})$)?
Is the $n-$squares conjecture true?
Is the \( n \)-squares conjecture true?
Numerical study of \( X_n \), \( X'_n \) for \( n = 5, 6, 7, 8 \ldots \). In particular,
Is the $n$–squares conjecture true?
Numerical study of $X_n, X'_n$ for $n = 5, 6, 7, 8 \ldots$. In particular,

- Nontrivial sequences of five or more rational squares with constant second differences equal 2 (description of $X_n(\mathbb{Q})$)?

- Nontrivial sequences of five or more integer squares with constant second differences not necessarily 2 (description of $X'_n(\mathbb{Q})$)?
Is the $n$–squares conjecture true?

Numerical study of $X_n, X'_n$ for $n = 5, 6, 7, 8, \ldots$. In particular,

- Nontrivial sequences of five or more rational squares with constant second differences equal 2 (description of $X_n(\mathbb{Q})$)?

- Nontrivial sequences of five or more integer squares with constant second differences not necessarily 2 (description of $X'_n(\mathbb{Q})$)?
A sequence \( a_1, a_2, \ldots, a_n \) is called \textbf{trivial} if there exists an arithmetical progression \( b_1, b_2, \ldots, b_n \) such that \( a_i = \pm b_i \).
(ex. 1, 1, 3 since \(-1, 1, 3\) is an arithmetic progression.)
A sequence \( a_1, a_2, \ldots, a_n \) is called **trivial** if there exists an arithmetical progression \( b_1, b_2, \ldots, b_n \) such that \( a_i = \pm b_i \).

(ex. 1, 1, 3 since \(-1, 1, 3\) is an arithmetic progression.)

A sequence \( a_1, a_2, \ldots, a_n \) is called **symmetric** if \( a_i = a_{n-i+1} \) for \( i = 1, 2, \ldots, n \).
A sequence \( a_1, a_2, \ldots, a_n \) is called **trivial** if there exists an arithmetical progression \( b_1, b_2, \ldots, b_n \) such that \( a_i = \pm b_i \).

(ex. \( 1, 1, 3 \) since \( -1, 1, 3 \) is an arithmetic progression.)

A sequence \( a_1, a_2, \ldots, a_n \) is called **symmetric** if \( a_i = a_{n-i+1} \) for \( i = 1, 2, \ldots, n \).

A sequence of positive integers \( a_1, a_2, \ldots, a_n \) is called **Büchi’s sequence** if for \( i = 1, \ldots, n-2 \)

\[
D = (a_{i+2}^2 - a_{i+1}^2) - (a_{i+1}^2 - a_i^2) = a_i^2 - 2a_{i+1}^2 + a_{i+2}^2 = 2.
\]

We call such a sequence **rational Büchi’s sequence** if the numbers \( a_i \) are rational.
A sequence \( a_1, a_2, \ldots, a_n \) is called **trivial** if there exists an arithmetical progression \( b_1, b_2, \ldots, b_n \) such that \( a_i = \pm b_i \).

(ex. \( 1, 1, 3 \) since \(-1, 1, 3\) is an arithmetic progression.)

A sequence \( a_1, a_2, \ldots, a_n \) is called **symmetric** if \( a_i = a_{n-i+1} \) for \( i = 1, 2, \ldots, n \).

A sequence of positive integers \( a_1, a_2, \ldots, a_n \) is called **Büchi’s sequence** if for \( i = 1, \ldots, n - 2 \)

\[
D = (a_{i+2}^2 - a_{i+1}^2) - (a_{i+1}^2 - a_i^2) = a_i^2 - 2a_{i+1}^2 + a_{i+2}^2 = 2.
\]

We call such a sequence **rational Büchi’s sequence** if the numbers \( a_i \) are rational.

A sequence of positive integers \( a_1, a_2, \ldots, a_n \) will be called **primitive** if these numbers are relatively prime.
A FEW DEFINITIONS

- A sequence $a_1, a_2, \ldots, a_n$ is called **trivial** if there exists an arithmetical progression $b_1, b_2, \ldots, b_n$ such that $a_i = \pm b_i$. (ex. $1, 1, 3$ since $-1, 1, 3$ is an arithmetic progression.)

- A sequence $a_1, a_2, \ldots, a_n$ is called **symmetric** if $a_i = a_{n-i+1}$ for $i = 1, 2, \ldots, n$.

- A sequence of positive integers $a_1, a_2, \ldots, a_n$ is called **Büchi’s sequence** if for $i = 1, \ldots, n-2$

  $$D = (a_{i+2}^2 - a_{i+1}^2) - (a_{i+1}^2 - a_i^2) = a_i^2 - 2a_{i+1}^2 + a_{i+2}^2 = 2.$$ 

  We call such a sequence **rational Büchi’s sequence** if the numbers $a_i$ are rational.

- A sequence of positive integers $a_1, a_2, \ldots, a_n$ will be called **primitive** if these numbers are relatively prime.

Notice that the triviality and symmetry conditions are properties of $(a_1, a_2, \ldots, a_n)$ as a point of the projective space $\mathbb{P}^{n-1}(\mathbb{Q})$. 
EARLIER RESULTS

**Theorem (Allison 1986)**
There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.

Example
E.g.
17, 53, 67, 73, 73, 67, 53, 17
with \(D = -840\).

Two non-trivial integer points on \(X_7\) (not on trivial lines, not extendable to symmetric eighttuples):
53, 173, 217, 233, 227, 197, 127
with \(D = -9960\).

526, 337, 160, 113, 274, 461, 652
with \(D = 75138\).

**Theorem (Buell, 1987)**
There exist infinitely many nontrivial \(\text{(increasing)}\) sequences of FOUR integers whose squares have second differences equal 2 \(\text{(infinitely many integer points on }X_4)\).

**Bremner, Acta Arith. 2003**
There exist at least 14 non-trivial integer points on \(X_7\).

**Theorem (B.-B. 2006)**
There exist infinitely many nontrivial increasing sequences of six integer squares whose second differences are constant \(\text{(non-trivial rational points on }X_6)\).
Theorem (Allison 1986)

There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.

Example

E.g.

\[17, 53, 67, 73, 73, 67, 53, 17\]

with \(D = -840\).

Two non-trivial integer points on \(X^7\) (not on trivial lines, not extendable to symmetric eighttuples):

\[53, 173, 217, 233, 227, 197, 127\]

with \(D = -9960\).

\[526, 337, 160, 113, 274, 461, 652\]

with \(D = 75138\).

Theorem (Buell, 1987)

There exist infinitely many nontrivial (increasing) sequences of four integers whose squares have second differences equal 2 (infinitely many integer points on \(X^4\)).

Bremner, Acta Arith. 2003

There exist at least 14 non-trivial integer points on \(X^7\).

Theorem (B.-B. 2006)

There exist infinitely many nontrivial increasing sequences of six integer squares whose second differences are constant (non-trivial rational points on \(X^6\)).
Theorem (Allison 1986)

There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.

Example

E.g. 17, 53, 67, 73, 73, 67, 53, 17 with $D = -840$.
Two non-trivial integer points on $X'_7$ (not on trivial lines, not extendable to symmetric eighntuples):
53, 173, 217, 233, 227, 197, 127 with $D = -9960$
526, 337, 160, 113, 274, 461, 652 with $D = 75138$
Theorem (Allison 1986)

There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.

Example

E.g. 17, 53, 67, 73, 73, 67, 53, 17 with $D = -840$.
Two non-trivial integer points on $X_7^F$ (not on trivial lines, not extendable to symmetric eighhtuples):
53, 173, 217, 233, 227, 197, 127 with $D = -9960$
526, 337, 160, 113, 274, 461, 652 with $D = 75138$

Theorem (Buell, 1987)

There exist infinitely many nontrivial (increasing) sequences of FOUR integers whose squares have second differences equal 2 (infinitely many integer points on $X_4$).
**EARLIER RESULTS**

---

**Theorem (Allison 1986)**

There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.

**Example**

E.g. 17, 53, 67, 73, 73, 67, 53, 17 with $D = -840$.

Two non-trivial integer points on $X_7'$ (not on trivial lines, not extendable to symmetric eighttuples):

- 53, 173, 217, 233, 227, 197, 127 with $D = -9960$
- 526, 337, 160, 113, 274, 461, 652 with $D = 75138$

---

**Theorem (Buell, 1987)**

There exist infinitely many nontrivial (increasing) sequences of FOUR integers whose squares have second differences equal 2 (infinitely many integer points on $X_4$).

---

**Bremner, Acta Arith. 2003**

There exist at least 14 non-trivial integer points on $X_7'$. 

---
Theorem (Allison 1986)

There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.

Example

E.g. 17, 53, 67, 73, 73, 67, 53, 17 with $D = -840$.

Two non-trivial integer points on $X'_7$ (not on trivial lines, not extendable to symmetric eighthtuples):

53, 173, 217, 233, 227, 197, 127 with $D = -9960$

526, 337, 160, 113, 274, 461, 652 with $D = 75138$

Theorem (Buell, 1987)

There exist infinitely many nontrivial (increasing) sequences of FOUR integers whose squares have second differences equal 2 (infinitely many integer points on $X_4'$).

Bremner, Acta Arith. 2003

There exist at least 14 non-trivial integer points on $X'_7$.

Theorem (B.-B. 2006)

There exist infinitely many nontrivial increasing sequences of six integer squares whose second differences are constant (non-trivial rational points on $X'_6$).
Theorem (B-B)

There is a one-to-one correspondence between all rational non-symmetric points \((a_1, a_2, a_3, a_4, a_5)\) of \(X_5'(\mathbb{Q})\) and the strictly nonzero rational points on the del Pezzo surface in \(\mathbb{P}^3(\mathbb{Q})\):

\[
X_0^2X_1^2 + 4X_2^4 - 4X_0^2X_2^2 - 4X_1^2X_2^2 + 3X_0^2X_3^2 = 0.
\]

Quintuples – integer points on the intersection of 2 quadrics in \(\mathbb{P}^4\) (a del Pezzo surface):

\[
\begin{align*}
a_1^2 - 3a_2^2 + 3a_3^2 - a_4^2 &= 0 \\
a_2^2 - 3a_3^2 + 3a_4^2 - a_5^2 &= 0
\end{align*}
\]

A point \((X_0, X_1, X_2, X_3)\) is called strictly nonzero if \(X_0X_1X_2X_3 \neq 0\).
Theorem (B-B)

There is a one-to-one correspondence between all rational non-symmetric points \((a_1, a_2, a_3, a_4, a_5)\) of \(X'_5(\mathbb{Q})\) and the strictly nonzero rational points on the del Pezzo surface in \(\mathbb{P}^3(\mathbb{Q})\):

\[
X_0^2X_1^2 + 4X_2^4 - 4X_0^2X_2^2 - 4X_1^2X_2^2 + 3X_0^2X_3^2 = 0.
\]

\[
\begin{align*}
\lambda a_1 &= X_0X_1 - 2X_2^2, \\
\lambda a_2 &= X_0X_2 - X_1X_2, \\
\lambda a_3 &= X_0X_3, \\
\lambda a_4 &= X_0X_2 + X_1X_2, \\
\lambda a_5 &= X_0X_1 + 2X_2^2.
\end{align*}
\]
Del Pezzo surface in $\mathbb{P}^3(\mathbb{Q})$ is rational. In fact (in $A^3(\mathbb{Q})$):

$$X_1^2 + 4X_2^4 - 4X_2^2 - 4X_1^2X_2^2 + 3X_3^2 = 0,$$

can be rewritten in the form:

$$(1 - 4X_2^2)X_1^2 + 3X_3^2 = 4X_2^2 - 4X_2^4.$$

Consider the conic

$$(1 - 4X_2^2)X^2 + 3Y^2 = 4X_2^2 - 4X_2^4.$$

for a rational number $X_2$. There is a rational point on the conic $X = Y = X_2$. For the rational points $(X_1, X_3)$ on this conic, we have

$$X_1 = \frac{3st^2 - 6st - (1 - 4s^2)s}{1 - 4s^2 + 3t^2},$$

$$X_3 = \frac{(1 - 4s^2)s - 2(1 - 4s^2)st - 3st^2}{1 - 4s^2 + 3t^2},$$

where $s = X_2$ and $t \in \mathbb{Q}$. 
Proposition

There are infinitely many non-trivial increasing rational Büchi sequences of length 5.

Proof.

Choose $s = 2$ in the parametrization and express $a_i^{2i}$ by $X_i$:

- $a_{21} = (3t^2 + 2t - 25)^2t^4 + t^3 - 16t^2 + 5t + 25$,
- $a_{22} = (15 + t^2 - 4t)^2t^4 + t^3 - 16t^2 + 5t + 25$,
- $a_{23} = (5 - 10t + t^2)^2t^4 + t^3 - 16t^2 + 5t + 25$,
- $a_{24} = (3t^2 - 4t + 5)^2t^4 + t^3 - 16t^2 + 5t + 25$,
- $a_{25} = (5t^2 - 2t - 15)^2t^4 + t^3 - 16t^2 + 5t + 25$,

where $t$ is a rational number such that $(t, y)$ is a rational point on the corresponding elliptic curve $y^2 = t^4 + t^3 - 16t^2 + 5t + 25$. It's rank is 1. Do computations!
Proposition

There are infinitely many non-trivial increasing rational Büchi sequences of length 5.

Proof.

Choose \( s = 2 \) in the parametrization and express \( a_i^2 \) by \( X_i \):

\[
\begin{align*}
a_1^2 &= \frac{(3t^2 + 2t - 25)^2}{t^4 + t^3 - 16t^2 + 5t + 25}, \\
a_2^2 &= \frac{(15 + t^2 - 4t)^2}{t^4 + t^3 - 16t^2 + 5t + 25}, \\
a_3^2 &= \frac{(5 - 10t + t^2)^2}{t^4 + t^3 - 16t^2 + 5t + 25}, \\
a_4^2 &= \frac{(3t^2 - 4t + 5)^2}{t^4 + t^3 - 16t^2 + 5t + 25}, \\
a_5^2 &= \frac{(5t^2 - 2t - 15)^2}{t^4 + t^3 - 16t^2 + 5t + 25},
\end{align*}
\]

where \( t \) is a rational number such that \((t, y)\) is a rational point on the corresponding elliptic curve

\[
y^2 = t^4 + t^3 - 16t^2 + 5t + 25.
\]

It's rank is 1. Do computations!
### TABLE 1

Non-trivial rational Büchi’s sequences of length 5. Increasing sequences in bold face.

\[
\frac{1}{82} [135, 157, 211, 279, 353]
\]

\[
\frac{1}{211} [314, 135, 164, 353, 558]
\]

\[
\frac{1}{3764} [9273, 5813, 3151, 3795, 6871]
\]

\[
\frac{1}{2965} [6884, 4089, 1906, 2851, 5496]
\]

\[
\frac{1}{204878} [2202953, 1903119, 1573109, 1188037, 657375]
\]

\[
\frac{1}{403131} [2119580, 1785791, 1486778, 1247797, 1108384]
\]

\[
\frac{1}{1573109} [3806238, 2202953, 409756, 657375, 2376074]
\]

\[
\frac{1}{317048143} [109002572530, 10847694804, 10804184189, 10769835118, 10744735455]
\]
Proposition

There is a one-to-one correspondence between all non-symmetric points \((a_1, a_2, a_3, a_4, a_5, a_6)\) of \(X'_6(\mathbb{Q})\) and the strictly nonzero rational points on the \(K3\)-surface in \(\mathbb{P}^3(\mathbb{Q})\):

\[
X_0^2X_1^2 - 3X_0^2X_2^2 + 2X_0^2X_3^2 + 2X_1^2X_2^2 + 25X_2^2X_3^2 - 27X_1X_3^2 = 0.
\]

Intersection of 3 quadrics in \(\mathbb{P}^5\) : (a \(K3\)-surface):

\[
\begin{align*}
    a_1^2 - 3a_2^2 + 3a_3^2 - a_4^2 &= 0 \\
    a_2^2 - 3a_3^2 + 3a_4^2 - a_5^2 &= 0 \\
    a_3^2 - 3a_4^2 + 3a_5^2 - a_6^2 &= 0
\end{align*}
\]
Proposition

There is a one-to-one correspondence between all non-symmetric points \((a_1, a_2, a_3, a_4, a_5, a_6)\) of \(X'_6(\mathbb{Q})\) and the strictly nonzero rational points on the K3–surface in \(\mathbb{P}^3(\mathbb{Q})\):

\[
X_0^2X_1^2 - 3X_0^2X_2^2 + 2X_0^2X_3^2 + 2X_1^2X_2^2 + 25X_2^2X_3^2 - 27X_1^2X_3^2 = 0.
\]

\[
\begin{align*}
\lambda a_1 &= X_0X_1 - 5X_2X_3, \\
\lambda a_2 &= X_0X_2 - 3X_1X_3, \\
\lambda a_3 &= X_0X_3 - X_1X_2, \\
\lambda a_4 &= X_0X_3 + X_1X_2, \\
\lambda a_5 &= X_0X_2 + 3X_1X_3, \\
\lambda a_6 &= X_0X_1 + 5X_2X_3.
\end{align*}
\]
CONJECTURE 1

Extensive numerical computations allow to find only non-trivial symmetric rational Büchi’s sextuples (there are infinitely many and all correspond to the non-torsion rational points on a specific elliptic curve of rank one).

Conjecture 1

Every rational Büchi’s sequence of length 6 must be trivial or symmetric.

Conjecture 1 may be explained in terms of an “exceptional set” $Z(\mathbb{Q})$ on $X_6(\mathbb{Q})$: the set $Z(\mathbb{Q})$ may be described as the union (of projectivizations) of the trivial lines $\pm a_i = a_1 + (i-1)$, $\pm a_i = -a_1 + (i-1)$ for $i = 2, \ldots, 6$ and the elliptic curve $a_6 = a_1$, $a_5 = a_2$, $a_4 = a_3$, $a_2^2 = a_2^1 - 4$, $a_2^3 = a_2^1 - 6$. Moreover, it seems that the set $X_6(\mathbb{Q}) \setminus Z(\mathbb{Q})$ is empty.

Proposition

Conjecture 1 implies the $n$-squares conjecture with $n = 6$.

Proof.

Easy to check that there are no symmetric integer Büchi’s sequences of length 6.
Extensive numerical computations allow to find only non-trivial symmetric rational Büchi’s sextuples (there are infinitely many and all correspond to the non-torsion rational points on a specific elliptic curve of rank one).
Extensive numerical computations allow to find only non-trivial symmetric rational Büchi’s sextuples (there are infinitely many and all correspond to the non-torsion rational points on a specific elliptic curve of rank one).

Conjecture 1
Every rational Büchi’s sequence of length 6 must be trivial or symmetric.
Extensive numerical computations allow to find only non-trivial symmetric rational Büchi’s sextuples (there are infinitely many and all correspond to the non-torsion rational points on a specific elliptic curve of rank one).

Conjecture 1

Every rational Büchi’s sequence of length 6 must be trivial or symmetric.

Conjecture 1 may be explained in terms of an “exceptional set” $Z(\mathbb{Q})$ on $X_6(\mathbb{Q})$: the set $Z(\mathbb{Q})$ may be described as the union (of projectivizations) of the trivial lines $\pm a_i = a_1 + (i - 1)$, $\pm a_i = -a_1 + (i - 1)$ for $i = 2, \ldots, 6$ and the elliptic curve $a_6 = a_1$, $a_5 = a_2$, $a_4 = a_3$, $a_2^2 = a_1^2 - 4$, $a_3^2 = a_1^2 - 6$. Moreover, it seems that the set $X_6(\mathbb{Q}) \setminus Z(\mathbb{Q})$ is empty.
Extensive numerical computations allow to find only non-trivial symmetric rational Büchi’s sextuples (there are infinitely many and all correspond to the non-torsion rational points on a specific elliptic curve of rank one).

**Conjecture 1**

Every rational Büchi’s sequence of length 6 must be trivial or symmetric.

Conjecture 1 may be explained in terms of an “exceptional set” $Z(\mathbb{Q})$ on $X_6(\mathbb{Q})$: the set $Z(\mathbb{Q})$ may be described as the union (of projectivizations) of the trivial lines $\pm a_i = a_1 + (i - 1), \pm a_i = -a_1 + (i - 1)$ for $i = 2, \ldots, 6$ and the elliptic curve $a_6 = a_1, a_5 = a_2, a_4 = a_3, a_2^2 = a_1^2 - 4, a_3^2 = a_1^2 - 6$. Moreover, it seems that the set $X_6(\mathbb{Q}) \setminus Z(\mathbb{Q})$ is empty.

**Proposition**

*Conjecture 1 implies the $n$–squares conjecture with $n = 6$.***
Conjecture 1

Every rational Büchi’s sequence of length 6 must be trivial or symmetric.

Conjecture 1 may be explained in terms of an “exceptional set” $Z(\mathbb{Q})$ on $X_6(\mathbb{Q})$: the set $Z(\mathbb{Q})$ may be described as the union (of projectivizations) of the trivial lines $\pm a_i = a_1 + (i - 1)$, $\pm a_i = -a_1 + (i - 1)$ for $i = 2, \ldots, 6$ and the elliptic curve $a_6 = a_1$, $a_5 = a_2$, $a_4 = a_3$, $a_2^2 = a_1^2 - 4$, $a_3^2 = a_1^2 - 6$. Moreover, it seems that the set $X_6(\mathbb{Q}) \setminus Z(\mathbb{Q})$ is empty.

**Proposition**

Conjecture 1 implies the $n$–squares conjecture with $n = 6$.

**Proof.**

Easy to check that there are no symmetric integer Büchi’s sequences of length 6.
There are infinitely many symmetric rational Büchi sequences of length 6

Consider $a, b, c, c, b, a$. Then

$$a^2 = c^2 + 6 \quad \text{and} \quad b^2 = c^2 + 2.$$ 

Hence $(ab, c)$ is a point on the elliptic curve

$$y^2 = x^4 + 8x^2 + 12.$$ 

Reduced Weierstrass equation:

$$Y^2 = X^3 - X^2 - 4X - 2.$$ 

Rank 1, torsion group of order 2 generated by $(-1, 0)$ and a generator of the torsion free part $P = (3, 2)$. 

J. Browkin and J. Brzeziński
Proposition

There are infinitely many symmetric rational Büchi sequences of length 6.

**TABLE 2**

Symmetric rational Büchi’s sequences of length 6:

\[ a, b, c, c, b, a, \text{ for } a = \sqrt{x_n^2 + 6}, \quad b = \sqrt{x_n^2 + 2}, \quad c = x_n \]

where \((x_n, y_n)\) is on \(y^2 = x^4 + 8x^2 + 12\) and corresponds to \(nP\) for \(P = [3, 2]\) on \(Y^2 = X^3 - X^2 - 4X - 2\).

<table>
<thead>
<tr>
<th>(n)</th>
<th>(a)</th>
<th>(b)</th>
<th>(c)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(\frac{5}{2})</td>
<td>(\frac{3}{2})</td>
<td>(\frac{1}{2})</td>
</tr>
<tr>
<td>3</td>
<td>(\frac{241}{60})</td>
<td>(\frac{209}{60})</td>
<td>(\frac{191}{60})</td>
</tr>
<tr>
<td>4</td>
<td>(\frac{221285}{71162})</td>
<td>(\frac{169443}{71162})</td>
<td>(\frac{136319}{71162})</td>
</tr>
<tr>
<td>5</td>
<td>(\frac{3062362561}{1154457480})</td>
<td>(\frac{2011709761}{1154457480})</td>
<td>(\frac{1175343361}{1154457480})</td>
</tr>
<tr>
<td>6</td>
<td>(\frac{481304617823525}{58921278095882})</td>
<td>(\frac{466655405077923}{58921278095882})</td>
<td>(\frac{459155565210241}{58921278095882})</td>
</tr>
</tbody>
</table>
Proposition

There is a one-to-one correspondence between all non-symmetric points of $X'_7(\mathbb{Q})$ and the strictly non-zero rational points on the intersection of the hypersurfaces in $\mathbb{P}^5(\mathbb{Q})$:

$$X_0^2X_1^2 + 9X_2^2X_3^2 - 3X_0^2X_2^2 - 12X_1^2X_3^2 + 3X_0^2X_3^2 + 3X_1^2X_2^2 - X_0^2X_4^2 = 0$$

and

$$X_0^2X_2^2 + 4X_1^2X_3^2 - 4X_0^2X_3^2 - 4X_1^2X_2^2 + 3X_0^2X_4^2 = 0.$$
The intersection of the hypersurfaces in the above Proposition is isomorphic (as variety) to the projective closure of the affine surface in \( \mathbb{A}^3 \):

\[
AX_4^4 - BX_4^2 + C = 0,
\]

where

\[
A(s, t) = 9(-4t^2 + 4t^2s^2 + 8t - 8ts^2 + 4s^2 - 1)^2(4s^2 - 1 - 8ts^2 + 2t - 4t^2 + 4t^2s^2)^2
\]

\[
B(s, t) = (144s^6 - 56s^4 + s^2 + 1 - 576s^6 t + 144ts^4 + 144ts^2 - 36t + 864s^6 t^2 - 392s^4 t^2 - 320t^2 s^2 + 172t^2 - 576s^6 t^3 + 576ts^4 + 144t^3 s^2 - 144t^3 + 144s^6 t^4 - 272t^4 s^4 + 112t^4 s^2 + 16t^4)(-4s^2 + 1 - 4t^2 + 4t^2s^2)^2,
\]

\[
C(s, t) = s^2(-4s^2 + 1 - 4t^2 + 4t^2s^2)^4.
\]
Proposition

The intersection of the hypersurfaces in the above Proposition is isomorphic (as variety) to the projective closure of the affine surface in \( \mathbb{A}^3 \):

\[
AX_4^4 - BX_4^2 + C = 0,
\]

where

\[
A(s, t) = 9(-4t^2 + 4t^2s^2 + 8t - 8ts^2 + 4s^2 - 1)^2(4s^2 - 1 - 8ts^2 + 2t - 4t^2 + 4t^2s^2)^2
\]

\[
B(s, t) = (144s^6 - 56s^4 + s^2 + 1 - 576s^6t + 144ts^4 + 144ts^2 - 36t + 864s^6t^2 -
\]

\[
392s^4t^2 - 320t^2s^2 + 172t^2 - 576s^6t^3 + 576t^3s^4 + 144t^3s^2 - 144t^3 + 144s^6t^4 -
\]

\[
272t^4s^4 + 112t^4s^2 + 16t^4)(-4s^2 + 1 - 4t^2 + 4t^2s^2)^2,
\]

\[
C(s, t) = s^2(-4s^2 + 1 - 4t^2 + 4t^2s^2)^4.
\]

Not unsuitable for computations!
Extensive computations of non-trivial integer septuples on the surface in $\mathbb{A}^3$ lead to sequences of two types – one of them also “trivial”:

Theorem (Allison 1986)
There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences. Such a sequence gives 2 “trivial” septuples (septuples extendable to symmetric eighttuples). All given by the rational points of a specific elliptic curve of rank 1.

Proposition (Bremner 2003)
There are no symmetric sequences of seven integers whose squares have constant second differences. Moreover a number of very rare exceptional septuples (non-trivial and not extendable to symmetric eighttuples).
Extensive computations of non-trivial integer septuples on the surface in $\mathbb{A}^3$ lead to sequences of two types – one of them also “trivial”:

**Theorem (Allison 1986)**

*There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.*
Extensive computations of non-trivial integer septuples on the surface in $\mathbb{A}^3$ lead to sequences of two types – one of them also “trivial”:

Theorem (Allison 1986)

There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.

Such a sequence gives 2 “trivial” septuples (septuples extendable to symmetric eighttuples). All given by the rational points of a specific elliptic curve of rank 1.

No nontrivial and non-symmetric sequence of eight integers whose squares have constant second differences is known.
Extensive computations of non-trivial integer septuples on the surface in $\mathbb{A}^3$ lead to sequences of two types – one of them also “trivial”:

**Theorem (Allison 1986)**

*There exists infinitely many symmetric sequences of eight integers whose squares have constant second differences.*

Such a sequence gives 2 “trivial” septuples (septuples extendable to symmetric eighttuples). All given by the rational points of a specific elliptic curve of rank 1.
No nontrivial and non-symmetric sequence of eight integers whose squares have constant second differences is known.

**Proposition (Bremner 2003)**

*There are no symmetric sequences of seven integers whose squares have constant second differences.*

Moreover a number of very rare **exceptional septuples** is obtained (non-trivial and not extendable to symmetric eighttuples).
There are 20 known non-trivial integer septuples (not on the trivial lines and not extendable to symmetric eighttuples, that is, not on a specific elliptic curve) whose squares have constant second differences:

- D. Allison, (1986): 2 examples,
- A. Bremner, (2003): 12 examples,
- B-B (2010, unpublished): 6 examples
EXAMPLES OF EXCEPTIONAL SEPTUPELS

Allison 1986:

53, 173, 217, 233, 227, 197, 127
526, 337, 160, 113, 274, 461, 652

Bremner 2003:

3131, 2351, 1761, 1589, 1949, 2631, 3449
4630, 2713, 1544, 2551, 4442, 6485, 8572
5207, 3025, 337, 41, 2969, 5153, 7295
28621, 10460, 12651, 31162, 50423, 69816, 89255
40196, 80351, 98726, 107179, 108064, 101579, 86074
53331, 36943, 25885, 27567, 40429, 57391, 75747
572321, 1938531, 2969567, 3938125, 4881537, 5812061, 6735041
1237931, 826051, 436459, 238499, 530581, 929731, 1343701
16620, 12817, 11314, 12939, 16808, 21755, 27198
19920, 8527, 11074, 23379, 36668, 50165, 63738
87455, 81103, 79239, 82169, 89423, 100065, 113143

B-B 2010:

12515, 7459, 10143, 17273, 25339, 33675, 42121
12871, 9822, 9373, 11824, 15885, 20626, 25673
15621, 9075, 1011, 123, 8907, 15459, 21885
16620, 12817, 11314, 12939, 16808, 21755, 27198
19920, 8527, 11074, 23379, 36668, 50165, 63738
87455, 81103, 79239, 82169, 89423, 100065, 113143
The surface $X'_7$ (in $\mathbb{P}^6$), which is birationally isomorphic to the surface in $\mathbb{A}^3$ (given above) is probably of general type (which we have not proved). Denote by $Z \subset X'_7$ the union of the trivial lines and the elliptic curve whose rational points correspond to the septuples extendable to symmetric eightuples with constant second differences of squares. Our numerical results and Lang’s conjecture suggest that the following result may be true:
The surface $X_7'$ (in $\mathbb{P}^6$), which is birationally isomorphic to the surface in $\mathbb{A}^3$ (given above) is probably of general type (which we have not proved). Denote by $Z \subset X_7'$ the union of the trivial lines and the elliptic curve whose rational points correspond to the septuples extendable to symmetric eightuples with constant second differences of squares. Our numerical results and Lang’s conjecture suggest that the following result may be true:

**Conjecture 2**

The only curves on $X_7'$ with infinitely many rational points are the trivial lines and the elliptic curve whose rational points correspond to the septuples extendable to symmetric eightuples. The set $X_7'(\mathbb{Q}) \setminus Z(\mathbb{Q})$ is finite.
The surface $X_7'$ (in $\mathbb{P}^6$), which is birationally isomorphic to the surface in $\mathbb{A}^3$ (given above) is probably of general type (which we have not proved). Denote by $Z \subset X_7'$ the union of the trivial lines and the elliptic curve whose rational points correspond to the septuples extendable to symmetric eightuples with constant second differences of squares. Our numerical results and Lang’s conjecture suggest that the following result may be true:

**Conjecture 2**

The only curves on $X_7'$ with infinitely many rational points are the trivial lines and the elliptic curve whose rational points correspond to the septuples extendable to symmetric eightuples. The set $X_7'(\mathbb{Q}) \setminus Z(\mathbb{Q})$ is finite.

Accordingly to the Lang’s conjecture (if applicable here) the set $X_7'(\mathbb{Q}) \setminus Z(\mathbb{Q})$ is finite and contains at least the 20 known exceptional septuples listed before (found by Allison, Bremner and B.-B.).
Proof.

Assume that the number of exceptional septuples, that is, the elements of \( X'_7(\mathbb{Q}) \setminus \mathbb{Z}(\mathbb{Q}) \) equals \( N \). Then every Büchi’s sequence of length \( N + 9 \) must be trivial. In fact, if \( a_1, a_2, \ldots, a_{N+9} \) is a Büchi sequence, then multiplying all its terms by their greatest common denominator, we get a sequence \( b_1, b_2, \ldots, b_{N+9} \) of integers whose squares have constant second differences. If this sequence is trivial, then the sequence of \( a_i \) is also trivial. If it is not trivial, then we have \( N + 3 \) different septuples \( b_i, b_{i+1}, \ldots, b_{i+6} \) for \( i = 1, 2, \ldots, N + 3 \). The points \( (i, b_i) \) are on a parabola so all the septuples are different and non-trivial. At most two of them can be extended to (the same) symmetric eithttuple. Thus, we have at least \( N + 1 \) septuples which are non-trivial and non-symmetric – a contradiction. Hence the sequence \( a_1, a_2, \ldots, a_{N+9} \) must be trivial. \( \square \)
Conjecture 2 ⇒ $n$–Squares Conjecture

Proof.

Assume that the number of exceptional septuples, that is, the elements of $X'_7(\mathbb{Q}) \setminus \mathbb{Z}(\mathbb{Q})$ equals $N$. Then every Büchi’s sequence of length $N + 9$ must be trivial. In fact, if $a_1, a_2, \ldots, a_{N+9}$ is a Büchi sequence, then multiplying all its terms by their greatest common denominator, we get a sequence $b_1, b_2, \ldots, b_{N+9}$ of integers whose squares have constant second differences. If this sequence is trivial, then the sequence of $a_i$ is also trivial. If it is not trivial, then we have $N + 3$ different septuples $b_i, b_{i+1}, \ldots, b_{i+6}$ for $i = 1, 2, \ldots, N + 3$. The points $(i, b_i)$ are on a parabola so all the septuples are different and non-trivial. At most two of them can be extended to (the same) symmetric eighttuple. Thus, we have at least $N + 1$ septuples which are non-trivial and non-symmetric – a contradiction. Hence the sequence $a_1, a_2, \ldots, a_{N+9}$ must be trivial. \qed

Remark

Of course, the same argument as in the proof of the last Proposition applies to any $X'_n$ satisfying Lang’s conjecture when the set $Z$ has a similar description. The idea of the proof above is similar the idea behind Vojta’s proof of Theorem 3.1 in [V].
REFERENCES


Quadratic polynomials

Given a positive integer $n$, does there exist a function

$$f(x) = ax^2 + bx + c,$$

where $a, b, c$ are relatively prime integers and $b^2 - 4ac \neq 0$, which takes square values for $n$ consecutive integer values of $x$?

Proof. If $f(x) = ax^2 + bx + c$ takes square values for $x = 0, 1, 2, \ldots, n$, then we have a sequence of squares whose second differences are constant and equal $2a$:

$$c a + b x + c,$$

$$2a x^2 + 2b x + c,$$

$$3a x^2 + 3b x + c,$$

$$\ldots$$

Proof. Conversely, if $a^2, a^2 + 1, a^2 + 2, \ldots, a^2 + n$ is a sequence of squares whose second differences are constant and equal $\Delta$, then it is easy to check using the recurrence relation $a^2_i - 2a^2_{i+1} + a^2_{i+2} = \Delta$ for $i = 1, \ldots, n-2$ that $f(x) = \Delta x^2 - x^2 + (a^2 - a^2_1)x + a^2_1$ takes square values for $x = 0, 1, 2, \ldots, n-1$. 

J. Browkin and J. Brzeziński

The $n$—squares conjecture and rational points... 28/ 28
Quadratic polynomials

Given a positive integer \( n \), does there exist a function

\[
f(x) = ax^2 + bx + c,
\]

where \( a, b, c \) are relatively prime integers and \( b^2 - 4ac \neq 0 \), which takes square values for \( n \) consecutive integer values of \( x \)?

Proof.

If \( f(x) = ax^2 + bx + c \) takes square values for \( x = 0, 1, 2, 3, \ldots \), then we have a sequence of squares whose second differences are constant and equal \( 2a \):

\[
\begin{align*}
c & a+b+c & 4a+2b+c & 9a+3b+c & \ldots \\
 a+b & 3a+b & 5a+b, & + \ldots \\
 2a & 2a & 2a & \ldots 
\end{align*}
\]
Quadratic polynomials

Given a positive integer $n$, does there exist a function

$$f(x) = ax^2 + bx + c,$$

where $a$, $b$, $c$ are relatively prime integers and $b^2 - 4ac \neq 0$, which takes square values for $n$ consecutive integer values of $x$?

Proof.

If $f(x) = ax^2 + bx + c$ takes square values for $x = 0, 1, 2, 3, \ldots$, then we have a sequence of squares whose second differences are constant and equal $2a$:

$$
\begin{array}{ccccccc}
& c & a + b + c & 4a + 2b + c & 9a + 3b + c & \ldots \\
2a & a + b & 3a + b & 5a + b, & \ldots \\
& 2a & 2a & 2a & \ldots 
\end{array}
$$

Proof.

Conversely, if $a_1^2, a_2^2, a_3^2, \ldots, a_n^2$ is a sequence of squares whose second differences are constant and equal $\Delta$, then it is easy to check using the recurrence relation $a_i^2 - 2a_{i+1} + a_{i+2}^2 = \Delta$ for $i = 1, \ldots, n - 2$ that

$$f(x) = \Delta \frac{x^2 - x}{2} + (a_2^2 - a_1^2)x + a_1^2$$

takes square values for $x = 0, 1, 2, \ldots, n - 1$. 