Integral point sets over $\mathbb{Z}_p^2$

Sascha Kurz
sascha.kurz@uni-bayreuth.de
www.wm.uni-bayreuth.de

Chair of Business Mathematics
University of Bayreuth

Kolloquium über Kombinatorik
Magdeburg 16.-18.11.2006
Integral point sets over $\mathbb{Z}_p^2$

Introduction

Integral point sets over rings

Definition

Let $\mathcal{R}$ be a commutative ring. For example $\mathcal{R} = \mathbb{Z}_p$ for a prime $p$ or $\mathcal{R} = \mathbb{Z}$.

- A point set $\mathcal{P}$ is a subset of the vector space $\mathcal{R} \times \mathcal{R}$.
- The squared distance $d^2\left((s_1, s_2), (t_1, t_2)\right)$ of two points $(s_1, s_2), (t_1, t_2) \in \mathcal{R}^2$ is given by

  $$d^2\left((s_1, s_2), (t_1, t_2)\right) = (s_1 - t_1)^2 + (s_2 - t_2)^2 \in \mathcal{R}.$$ 

- Two points $p_1, p_2$ are at integral distance if there exists an element $r \in \mathcal{R}$ with $d^2(p_1, p_2) = r^2$.
- A point set is called integral if all pairs of points are at integral distance.
An example of an integral point set

Figure: An integral point set for $\mathcal{R} = \mathbb{Z}$. 

$(546, 1120)$

$(132, -720)$

$(0, 0)$

$(546, -272)$

$(1155, 540)$

$(960, -720)$

$\pm 1886 \in \mathbb{Z}$
Maximum cardinality

**Definition**

For a finite commutative ring \( R \) we denote by \( \mathcal{I}(R, 2) \) the maximum cardinality of an integral point set over \( R^2 \).
Maximum cardinality

**Definition**
For a finite commutative ring \( R \) we denote by \( \mathcal{I}(R, 2) \) the maximum cardinality of an integral point set over \( R^2 \).

**Remark**
From the previous example we can derive \( \mathcal{I}(\mathbb{Z}_n, 2) \geq 6 \) for \( n \geq 2000 \).
Maximum cardinality

**Definition**
For a finite commutative ring $\mathcal{R}$ we denote by $\mathcal{I}(\mathcal{R}, 2)$ the maximum cardinality of an integral point set over $\mathcal{R}^2$.

**Remark**
From the previous example we can derive $\mathcal{I}(\mathbb{Z}_n, 2) \geq 6$ for $n \geq 2000$.

**Lemma**
For a commutative ring $\mathcal{R}$ with $1 + 1 = 0$ we have $\mathcal{I}(\mathcal{R}, 2) = |\mathcal{R}|^2$. 
Integral point sets over $\mathbb{Z}_p^2$

Maximum cardinality

**Definition**
For a finite commutative ring $\mathcal{R}$ we denote by $\mathcal{I}(\mathcal{R}, 2)$ the maximum cardinality of an integral point set over $\mathcal{R}^2$.

**Remark**
From the previous example we can derive $\mathcal{I}(\mathbb{Z}_n, 2) \geq 6$ for $n \geq 2000$.

**Lemma**
For a commutative ring $\mathcal{R}$ with $1 + 1 = 0$ we have $\mathcal{I}(\mathcal{R}, 2) = |\mathcal{R}|^2$.

**Proof**
$\mathcal{I}(\mathcal{R}, 2) \leq |\mathcal{R}|^2$ and $(s_1 - t_1)^2 + (s_2 - t_2)^2 = (s_1 + t_1 + s_2 + t_2)^2$. 
Lower bounds

Lemma

\[ \mathcal{I}(\mathcal{R}, 2) \geq \]

Proof

Consider the integral point set

\[ P = \{ (r, 0) | r \in \mathcal{R} \} \]

Proof

Consider the integral point set

\[ P = \{ (r, n) | r \in \mathcal{R}, n \in \mathcal{N} \} \]

Either

\[ r^2 + n^2 = (r + n)^2 \]

or

\[ r^2 + n^2 = (r^2 + n^2)^2 \]
Lower bounds

**Lemma**

\[ \mathcal{I}(\mathcal{R}, 2) \geq |\mathcal{R}|. \]

**Proof**

Consider the integral point set \( \mathcal{P} = \{(r, 0) \mid r \in \mathcal{R}\}. \)
### Lower bounds

**Lemma**

$$I(\mathcal{R}, 2) \geq |\mathcal{R}|.$$  

**Proof**

Consider the integral point set $\mathcal{P} = \{(r, 0) \mid r \in \mathcal{R}\}$.

---

**Lemma**

If $N$ is an additive subgroup of $\{r \in \mathcal{R} \mid r^2 = 0\}$ or of $\{r \in \mathcal{R} \mid 2r^2 = 0 \land r^2 = r^4\}$ then $I(\mathcal{R}, 2) \geq |N| \cdot |\mathcal{R}|.$
Lower bounds

Lemma
\[ I(\mathcal{R}, 2) \geq |\mathcal{R}|. \]

Proof
Consider the integral point set \( \mathcal{P} = \{(r, 0) \mid r \in \mathcal{R}\} \).

Lemma
If \( N \) is an additive subgroup of \( \{r \in \mathcal{R} \mid r^2 = 0\} \) or of \( \{r \in \mathcal{R} \mid 2r^2 = 0 \land r^2 = r^4\} \) then \( I(\mathcal{R}, 2) \geq |N| \cdot |\mathcal{R}| \).

Proof
Consider the integral point set \( \mathcal{P} = \{(r, n) \mid r \in \mathcal{R}, n \in N\} \).
Either \( r^2 + n^2 = (r + n)^2 \) or \( r^2 + n^2 = (r + n^2)^2 \).
Integral point sets over $\mathbb{Z}_p^2$

Maximum cardinality

Lower bounds

**Lemma**

For two commutative rings $\mathcal{R}_1$, $\mathcal{R}_2$ we have

$$I(\mathcal{R}_1 \times \mathcal{R}_2, 2) \geq I(\mathcal{R}_1, 2) \cdot I(\mathcal{R}_2, 2),$$

if addition and multiplication are componentwise defined.
Lower bounds

Lemma
For two commutative rings $\mathcal{R}_1$, $\mathcal{R}_2$ we have

$$\mathcal{I}(\mathcal{R}_1 \times \mathcal{R}_2, 2) \geq \mathcal{I}(\mathcal{R}_1, 2) \cdot \mathcal{I}(\mathcal{R}_2, 2),$$

if addition and multiplication are componentwise defined.

Proof
If the corresponding maximal integral point sets for $\mathcal{R}_1$, $\mathcal{R}_2$ are $\mathcal{P}_1$ and $\mathcal{P}_2$, then $\mathcal{P} := \mathcal{P}_1 \times \mathcal{P}_2$ is an integral point set over $\mathcal{R}_1 \times \mathcal{R}_2$. 
Exact numbers for $I(\mathbb{Z}_n, 2)$

Theorem
For an odd integer $n$ we have $I(\mathbb{Z}_{2n}, 2) = 4 \cdot I(\mathbb{Z}_n, 2)$. 
Integral point sets over $\mathbb{Z}_p^2$

$\mathcal{R} = \mathbb{Z}_n$

**Exact numbers for $\mathcal{I}(\mathbb{Z}_n, 2)$**

**Theorem**
For an odd integer $n$ we have $\mathcal{I}(\mathbb{Z}_{2n}, 2) = 4 \cdot \mathcal{I}(\mathbb{Z}_n, 2)$.

**Corollary**
- $\mathcal{I}(\mathbb{Z}_2, 2) = 4 = |\mathbb{Z}_2|^2$
- For coprime integers $a, b$: $\mathcal{I}(\mathbb{Z}_{ab}, 2) \geq \mathcal{I}(\mathbb{Z}_a, 2) \cdot \mathcal{I}(\mathbb{Z}_b, 2)$
- For a prime $p$: $\mathcal{I}(\mathbb{Z}_p, 2) \geq p$
- If $n = \prod_{i=1}^{s} p_i^{r_i}$, then $\mathcal{I}(\mathbb{Z}_n, 2) \geq n \cdot \prod_{i=1}^{s} p_i^{\left\lfloor \frac{r_i}{2} \right\rfloor}$
- If $n = 2 \cdot \prod_{i=2}^{s} p_i^{r_i}$, then $\mathcal{I}(\mathbb{Z}_n, 2) \geq 2n \cdot \prod_{i=2}^{s} p_i^{\left\lfloor \frac{r_i}{2} \right\rfloor}$
Integral point sets over $\mathbb{Z}_p^2$

$\mathcal{R} = \mathbb{Z}_n$

**Exact numbers for $\mathcal{I}(\mathbb{Z}_n, 2)$**

**Conjecture**

The bounds from the previous corollary are sharp.
Exact numbers for $I(\mathbb{Z}_n, 2)$

**Conjecture**

The bounds from the previous corollary are sharp.

**Computer aided verification**

Using a clique search approach we can prove the conjecture for $n \leq 100$ and $p \leq 229$. 
Classification of maximal integral point sets in $\mathbb{Z}_p'$

**Definition**

We utilize the bijection $\varrho : \mathbb{Z}_p^2 \rightarrow \mathbb{Z}_p' := \mathbb{Z}_p[x]/(x^2 + 1)$, $(a, b) \mapsto a + bx$. Two point sets $\mathcal{P}_1$ and $\mathcal{P}_2$ are isomorphic if there exists an isometry of $\mathbb{Z}_p'$ with respect to the integral-nonintegral-metric which maps $\mathcal{P}_1$ to $\mathcal{P}_2$. 
Classification of maximal integral point sets in $\mathbb{Z}_p'$

**Definition**

We utilize the bijection $\varrho : \mathbb{Z}_p^2 \rightarrow \mathbb{Z}_p' := \mathbb{Z}_p[x]/(x^2 + 1)$, $(a, b) \mapsto a + bx$. Two point sets $\mathcal{P}_1$ and $\mathcal{P}_2$ are isomorphic if there exists an isometry of $\mathbb{Z}_p'$ with respect to the integral-nonintegral-metric which maps $\mathcal{P}_1$ to $\mathcal{P}_2$.

**Lemma**

If $\mathcal{P}$ is an integral point set over $\mathbb{Z}_p'$, then there is an isomorphic copy $\varphi(\mathcal{P})$ with

- $0, 1 \in \varphi(\mathcal{P})$ or
- $0, 1 + \omega(p) \cdot x \in \varphi(\mathcal{P})$ where $\omega^2(p) = -1$. 

where $\omega(p)$ is a root of $x^2 + 1$ in $\mathbb{Z}_p$.
Classification of maximal integral point sets in $\mathbb{Z}'_p$

Conjecture
For $p \equiv 3 \mod 4$ all maximal integral point sets are isomorphic to the line $\{i \in \mathbb{Z}\}$. 

Remark
For $p \equiv 1 \mod 4$ we have the two non-isomorphic lines $\{i \in \mathbb{Z}\}$, $\{i + \omega(p) \in \mathbb{Z}\}$ and another nice construction...
Classification of maximal integral point sets in $\mathbb{Z}_p'$

**Conjecture**

For $p \equiv 3 \mod 4$ all maximal integral point sets are isomorphic to the line $\{i \in \mathbb{Z}\}$.

**Remark**

For the verification we have utilized a maximum clique search algorithm by predescribing the points $0, 1$ and excluding the point $2$. The conjecture is valid for $p \leq 307$. 
### Classification of maximal integral point sets in $\mathbb{Z}_p'$

#### Conjecture

For $p \equiv 3 \mod 4$ all maximal integral point sets are isomorphic to the line $\{i \in \mathbb{Z}\}$.

#### Remark

For the verification we have utilized a maximum clique search algorithm by predescribing the points 0, 1 and excluding the point 2. The conjecture is valid for $p \leq 307$.

#### Remark

For $p \equiv 1 \mod 4$ we have the two non-isomorphic lines $\{i \in \mathbb{Z}\}$, $\{i + \omega(p)i x \in \mathbb{Z}\}$ and another nice construction . . .
Integral point sets over $\mathbb{Z}_p^2$

Classification

Iligs

Definition

For a prime $p \equiv 1 \mod 4$ a set

$$S = \{(x_1, y_1), \ldots, (x_r, y_r)\} \subset \mathbb{Z}_p^2$$

is called an **integral line-intersecton generating set**, for short **iligs**, if

$$\mathcal{P} = \{(0, 0)\} \cup \{(\pm x_i, \pm y_i)\} \cup \{(\pm x_i, \mp y_i)\}$$

is an integral point set of cardinality $4 \cdot |S| + 1 = p$. 

Example

The sets $\tilde{S}_5 = \{(1, 2)\}$ and $\tilde{S}_{13} = \{(1, 5), (3, 2), (4, 6)\}$ are iligs.
**Integral point sets over \( \mathbb{Z}_p^2 \)**

**Classification**

### Iligs

**Definition**

For a prime \( p \equiv 1 \mod 4 \) a set

\[
S = \{(x_1, y_1), \ldots, (x_r, y_r)\} \subset \mathbb{Z}_p^2
\]

is called an **integral line-intersecton generating set**, for short **iligs**, if

\[
P = \{(0, 0)\} \cup \{(\pm x_i, \pm y_i)\} \cup \{(\pm x_i, \mp y_i)\}
\]

is an integral point set of cardinality \( 4 \cdot |S| + 1 = p \).

**Example**

The sets \( \tilde{S}_5 = \{(1, 2)\} \) and \( \tilde{S}_{13} = \{(1, 5), (3, 2), (4, 6)\} \) are iligs.
Lemma

If $Q$ denotes the set of squares in $\mathbb{Z}_p \setminus 0$ and $\omega(p)^2 = -1$, then

$$S_p := (1, \omega(p)) \cdot Q$$

is an iligs.
Integral point sets over $\mathbb{Z}_p^2$

Classification

Iligs

**Lemma**

If $Q$ denotes the set of squares in $\mathbb{Z}_p \setminus 0$ and $\omega(p)^2 = -1$, then

$$S_p := (1, \omega(p)) \cdot Q$$

is an iligs.

**Conjecture**

If $p \geq 5$ and $\tilde{S}_p$ is an arbitrary iligs, then $\mathcal{P}(\tilde{S}_p) \simeq \mathcal{P}(S_p)$. For $p > 5$, $p \equiv 1 \mod 4$ maximal integral point sets are either isomorphic to a line or generated by an iligs.
Integration point sets over $\mathbb{Z}_p^2$

Classification

Classification of maximal integral point sets in $\mathbb{Z}_p'$

Remark

We have verified the previous conjecture up to $p = 229$ utilizing clique search:

- Predescribe $0, 1 + \omega(p)x$, exclude $2 + 2\omega(p)x$, and join two nodes via an edge iff their squared distance equals 0.
Integral point sets over $\mathbb{Z}_p^2$

Classification

Classification of maximal integral point sets in $\mathbb{Z}_p'$

Remark

We have verified the previous conjecture up to $p = 229$ utilizing clique search:

- Predescribe $0, 1 + \omega(p)x$, exclude $2 + 2\omega(p)x$, and join two nodes via an edge iff their squared distance equals 0.
- Predescribe 0, 1 and exclude the point 2. We expect two isomorphic copies of the point set generated by $S_p$. 
A set of $r$ points $(x_i, y_i) \in \mathbb{R}^2$ is collinear if there are $a, b, t_1, t_2, w_i \in \mathbb{R}$ with $a + w_i t_1 = x_i$ and $a + w_i t_2 = y_i$. The maximum cardinality of an integral point set with no three collinear points is denoted by $\overline{I}(\mathcal{R}, 2)$. 
Further restrictions

Definition

A set of $r$ points $(x_i, y_i) \in \mathbb{R}^2$ is collinear if there are $a, b, t_1, t_2, w_i \in \mathbb{R}$ with $a + w_it_1 = x_i$ and $a + w_it_2 = y_i$. The maximum cardinality of an integral point set with no three collinear points is denoted by $\overline{I}(\mathcal{R}, 2)$.

Lemma

For a odd prime $p$ we have $\overline{I}(\mathbb{Z}_p, 2) \leq p + 1$. For $n$ with $p^a | n$ and $p^{a+1} \not| n$ we have

$$\overline{I}(\mathbb{Z}_n, 2) \leq n \cdot \left(1 + p^{-\left\lceil \frac{a+1}{2} \right\rceil} + p^{-a}\right).$$

Proof

Ignore the integrality condition \cite{Huizenga preprint}.
Lower bounds

Conjecture

For $p \neq 2, 5$ we have

$$\overline{I}(\mathbb{Z}_p, 2) = \begin{cases} \frac{p-1}{2} & \text{if } p \equiv 1 \mod 4, \\ \frac{p+1}{2} & \text{if } p \equiv 3 \mod 4. \end{cases}$$
Lower bounds

**Conjecture**
For $p \neq 2, 5$ we have

$$\overline{I}(\mathbb{Z}_p, 2) = \begin{cases} \frac{p-1}{2} & \text{if } p \equiv 1 \mod 4, \\ \frac{p+1}{2} & \text{if } p \equiv 3 \mod 4. \end{cases}$$

**Lemma**
For $p \neq 2, 5$ we have

$$\overline{I}(\mathbb{Z}_p, 2) \geq \begin{cases} \frac{p-1}{2} & \text{if } p \equiv 1 \mod 4, \\ \frac{p+1}{2} & \text{if } p \equiv 3 \mod 4. \end{cases}$$
Lower bounds

Proof

We consider the set $C := \{(a, b) \in \mathbb{Z}_p^2 \mid a^2 + b^2 = 1\}$. With the multiplication of $\mathbb{Z}_p'$ it is a multiplicative subgroup. It is indeed a cyclic subgroup.
Integral point sets over $\mathbb{Z}_p^2$

Further restrictions

Lower bounds

Proof

We consider the set $C := \{(a, b) \in \mathbb{Z}_p^2 \mid a^2 + b^2 = 1\}$. With the multiplication of $\mathbb{Z}_p'$ it is a multiplicative subgroup. It is indeed a cyclic subgroup. For $p \equiv 3 \mod 4$ we notice that $\mathbb{Z}_p' \cong \mathbb{F}_{p^2}$ and for $p \equiv 1 \mod 4$ we utilize the bijection

$$\alpha_p : \mathbb{Z}_p^* \to C, \quad t \mapsto \frac{1 + t^2}{2t} + \omega(p) \frac{1 - t^2}{2t} x.$$
Lower bounds

Proof

We consider the set $C := \{(a, b) \in \mathbb{Z}_p^2 \mid a^2 + b^2 = 1\}$. With the multiplication of $\mathbb{Z}_p'$ it is a multiplicative subgroup. It is indeed a cyclic subgroup. For $p \equiv 3 \mod 4$ we notice that $\mathbb{Z}_p' \simeq \mathbb{F}_{p^2}$ and for $p \equiv 1 \mod 4$ we utilize the bijection

$$\alpha_p : \mathbb{Z}_p^* \to C, \quad t \mapsto \frac{1 + t^2}{2t} + \omega(p)\frac{1 - t^2}{2t}x.$$

Now let $z$ be a generator of $C$. We choose $\mathcal{P} = \{z^{2i} \mid i \in \mathbb{N}\}$ and define $a + bx := a - bx$. With this we have

$$d^2(z^{2a}, z^{2b}) = (z^{2a} - z^{2b}) \cdot (z^{2a} - z^{2b}) = (\underbrace{z^{a-b}x - z^{a-b}x}_{\in \mathbb{Z}_p})^2.$$
Integral point sets over $\mathbb{Z}_p^2$

Further restrictions

No four points on a circle

Definition

The points $p_i = (x_i, y_i) \in \mathbb{R}^2$ are said to be situated on a circle if there exist $a, b \in \mathbb{R}$ and $r \in \mathbb{R}\{0\}$ with

$$(x_i - a)^2 + (y_i - b)^2 = r^2 \forall i.$$ 

By $\hat{I}(\mathbb{R}, 2)$ we denote the maximum cardinality of an integral point set over $\mathbb{R}^2$ where no four points are situated on a circle.
Integral point sets over $\mathbb{Z}_p^2$

Further restrictions

No four points on a circle

**Definition**

The points $p_i = (x_i, y_i) \in \mathcal{R}^2$ are said to be situated on a circle if there exist $a, b \in \mathcal{R}$ and $r \in \mathcal{R}\{0\}$ with

$$(x_i - a)^2 + (y_i - b)^2 = r^2 \forall i.$$  

By $\hat{I}(\mathcal{R}, 2)$ we denote the maximum cardinality of an integral point set over $\mathcal{R}^2$ where no four points are situated on a circle.

**Remark**

$\hat{I}(\mathbb{Z}_{50}, 2) \geq 12$ and $\hat{I}(\mathbb{Z}_{71}, 2) \geq 11$.  

Integral point sets over $\mathbb{Z}_p^2$

Further restrictions

**Erdős Problem**

Open Problem

Is $\mathcal{I}(\mathbb{Z}, 2)$ bounded?
Erdős Problem

Open Problem
Is \( \mathcal{I}(\mathbb{Z}, 2) \) bounded?

Partial answer
So far only configurations (also called \( n_2 \)-clusters) of at most \( n = 6 \) points in the plane are known with integral coordinates and pairwise integral distances. An example was given in the introduction.
Integral point sets over $\mathbb{Z}_p^2$

Further restrictions

Erdős Problem

Open Problem

Is $\mathcal{I}(\mathbb{Z}, 2)$ bounded?

Partial answer

So far only configurations (also called $n_2$-clusters) of at most $n = 6$ points in the plane are known with integral coordinates and pairwise integral distances. An example was given in the introduction. So far no $7_2$ cluster is known, but . . .
There are seven points in the plane, no three on a line, no four on a circle with pairwise integral distances.
Thank you very much for your attention.

<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. Dimiev: A setting for a Diophantine distance geometry, Tensor 66, 2005</td>
</tr>
<tr>
<td>J. Huizenga: The maximum size of caps in $\mathbb{Z}/n\mathbb{Z})^2$, preprint 2005</td>
</tr>
<tr>
<td>A. Kohnert and S. Kurz: Integral point sets over $\mathbb{Z}_n^m$, submitted, ODSA 2006</td>
</tr>
<tr>
<td>T. Kreisel and S. Kurz: There are integral heptagons, no three points on a line, no four on a circle, submitted</td>
</tr>
</tbody>
</table>