# Hinges in $\mathbb{Z}_q^2$ and $\mathbb{F}_q^2$

David Lin & Allisun Thomas

This work was supported in part by NSF Grant DMS 1559911.

August 2, 2018

# Definitions

- Finite sets (e.g. $\mathbb{Z}_5$)

# Definitions: Groups

Groups (e.g. $\langle \mathbb{Z}, + \rangle$)
A set (not necessarily finite) that holds four properties:

- Closed under an operation
- Associative Property
- Identities
- Inverses

# Definitions: Groups

Groups (e.g. $\langle \mathbb{Z}, + \rangle$)
A set (not necessarily finite) that holds four properties:

- Closed under an operation
- Associative Property
- Identities
- Inverses
- A special type of group: Abelian Groups

# Definitions: Rings

Rings (e.g. $\langle \mathbb{Z}, +, \cdot \rangle$)
Sets with 2 operations (addition and multiplication) that hold the following properties:

- Abelian group under addition
- Multiplication is associative
- Distributive law

# Definitions: Rings

Rings (e.g. $\langle \mathbb{Z}, +, \cdot \rangle$)
Sets with 2 operations (addition and multiplication) that hold the following properties:

- Abelian group under addition
- Multiplication is associative
- Distributive law
- A special type of ring: Fields

# Definition: Fields

Fields (e.g. $\langle \mathbb{R}, +, \times \rangle$)
A ring that holds the following properties:

- Multiplication is commutative (commutative ring)
- The ring contains a multiplicative identity (ring with unity)
- All nonzero elements have a multiplicative inverse

# Definition: Division Ring

A division ring is a ring with unity where all the the nonzero elements have a multiplicative inverse.

# Definitions: Notation

$\gtrsim$ or $\lesssim$: "Approximately" less (greater) than or equal to

- If $X(n)$ and $Y(n)$ depend on some parameter $n$, then if there exists constants $C, N > 0 : \forall n \geq N$,

$$|X(n)| \leq C|Y(n)|$$

We write $X \lesssim Y$.

# Definitions: k-chains

- 1-chain: The pairs that are a certain $\alpha$ distance apart $((x_1, x_2) \in \mathbb{R}^2 : |x_1 - x_2| = \alpha)$.

# Definitions: k-chains

- 1-chain: The pairs that are a certain $\alpha$ distance apart $((x_1, x_2) \in \mathbb{R}^2 : |x_1 - x_2| = \alpha)$.
- 2-chain (**hinge**): The triples such that the $i$th and $(i+1)$th terms are specific distances apart. $((x_1, x_2, x_3) \in \mathbb{R}^2 : |x_1 - x_2| = \alpha_1, |x_2 - x_3| = \alpha_2)$

# Definitions: k-chains

- 1-chain: The pairs that are a certain $\alpha$ distance apart $((x_1, x_2) \in \mathbb{R}^2 : |x_1 - x_2| = \alpha)$.
- 2-chain (**hinge**): The triples such that the $i$th and $(i+1)$th terms are specific distances apart. $((x_1, x_2, x_3) \in \mathbb{R}^2 : |x_1 - x_2| = \alpha_1, |x_2 - x_3| = \alpha_2)$
- k-chain: The set of $k$-tuples such that the $i$th and $(i+1)$th terms are specific distances apart. $((x_1, ..., x_k) \in \mathbb{R}^2 : |x_1 - x_2| = \alpha_1, ...|x_k - x_{k+1}| = \alpha_k)$

# Background: Unit Distance Problem

Erdős unit distance problem:
Estimates the maximum number of pairs of points the are a unit distance away from each other in a finite set.

- Conjecture: *n logn* (1946)

# Background: Unit Distance Problem

Erdős unit distance problem:
Estimates the maximum number of pairs of points the are a unit distance away from each other in a finite set.

- Conjecture: $n\ logn$ (1946)
- The trivial result: $\binom{n}{2} = n^2$

# Background: Unit Distance Problem

Erdős unit distance problem:
Estimates the maximum number of pairs of points the are a unit distance away from each other in a finite set.

- Conjecture: $n\ logn$ (1946)
- The trivial result: $\binom{n}{2} = n^2$
- Best result: $n^{4/3}$ (1984)

# Background: Hinges

What's the connection?

- Like with the unit distance problem, we can set positions for 2 points to limit our possibilities when counting hinges.

## Background: Hinges

What's the connection?

- Like with the unit distance problem, we can set positions for 2 points to limit our possibilities when counting hinges.
- A proof on how to find hinges in $\mathbb{R}^2$ for a set $E$ with $n$ elements.

## Background: $\mathbb{Z}_q^2$

What happens when we switch from $\mathbb{R}^2$ to integer modulo $q$ sets $(\mathbb{Z}_q^2)$?

- Circles are geometrically different, containing approximately $q$ points (Covert, Iosevich, Pakianathan, 2018).

## Background: $\mathbb{Z}_q^2$

What happens when we switch from $\mathbb{R}^2$ to integer modulo $q$ sets $(\mathbb{Z}_q^2)$?

- Circles are geometrically different, containing approximately $q$ points (Covert, Iosevich, Pakianathan, 2018).
- Intersections between circles can be at more than 2 points, even if the circles are not necessarily the same.

# Background: $\mathbb{Z}_q^2$

What happens when we switch from $\mathbb{R}^2$ to integer modulo $q$ sets $(\mathbb{Z}_q^2)$?

- Circles are geometrically different, containing approximately $q$ points (Covert, Iosevich, Pakianathan, 2018).
- Intersections between circles can be at more than 2 points, even if the circles are not necessarily the same.
- Thus, we let $q = p^2$, $p$ a prime, to keep things more manageable.

# Background: $\mathbb{F}_q^2$

We will also be working with hinges in $\mathbb{F}_q^2$. This time $q = p^l$ where $l \geq 2$.

$\mathbb{F}_q \cong$

$$\{0, 1, ..., p-1\} \cup \{x, 2x, ..., (p-1)x\} \cup ... \cup \{x^{l-1}, 2x^{l-1}, ...(p-1)^{l-1}\}/f(x)$$

Where $f(x)$ is an irreducible polynomial of degree $l$ in $\mathbb{F}_p[x]$.

# Background: Other work

We study $\mathbb{F}_q$ and $\mathbb{Z}_q$ because:

- Researchers are exploring these sets: Finding solutions to the diagonal equations

$$\alpha_1 x_1^2 + ...\alpha_n x_n^2 = \alpha$$

in $\mathbb{F}_q$

## Background

We study $\mathbb{F}_q$ and $\mathbb{Z}_q$ because:

- They help us learn more information about larger fields and rings such as $\mathbb{Q}$ (Iosevich, Rudnev, 2008).

# $\mathbb{Z}_q^2$ Main Theorem

- In $\mathbb{Z}_q^2$, our definition of distance is as follows: $|x-y| = (x_1 - y_1)^2 + (x_2 - y_2)^2$.

# $\mathbb{Z}_q^2$ Main Theorem

- In $\mathbb{Z}_q^2$, our definition of distance is as follows: $|x-y| = (x_1 - y_1)^2 + (x_2 - y_2)^2$.
- We define $H(E)$ to be the set of hinges defined by our set $E \subseteq \mathbb{Z}_q^2$.

# $\mathbb{Z}_q^2$ Main Theorem

- In $\mathbb{Z}_q^2$, our definition of distance is as follows: $|x-y| = (x_1-y_1)^2 + (x_2-y_2)^2$.
- We define $H(E)$ to be the set of hinges defined by our set $E \subseteq \mathbb{Z}_q^2$.

**Theorem**

*For some $E \subseteq \mathbb{Z}_q^2$, where $q = p^2$ and $p$ is an odd prime,*

$$|H(E)| \lesssim p|E|^2$$

# $\mathbb{Z}_q^2$ Main Theorem

- In $\mathbb{Z}_q^2$, our definition of distance is as follows: $|x - y| = (x_1 - y_1)^2 + (x_2 - y_2)^2$.
- We define $H(E)$ to be the set of hinges defined by our set $E \subseteq \mathbb{Z}_q^2$.

**Theorem**

*For some $E \subseteq \mathbb{Z}_q^2$, where $q = p^2$ and $p$ is an odd prime,*

$$|H(E)| \lesssim p|E|^2$$

Note that this is a nontrivial bound for $|E| \gtrsim p$

## $\mathbb{Z}_q^2$ Basics

- Basic question: How many times do two unit circles in $\mathbb{Z}_q^2$ intersect?

## $\mathbb{Z}_q^2$ Basics

- Basic question: How many times do two unit circles in $\mathbb{Z}_q^2$ intersect?
- Because this property is translation invariant, we just look at unit circles intersecting the unit circle centered at the origin.

# $\mathbb{Z}_q^2$ Circles

- First, let us just count points on one circle. We define a function similar to an indicator function, $C(x)$, such that when $x$ lies on the circle, $C(x) = 0$ but is nonzero otherwise.

# $\mathbb{Z}_q^2$ Circles

- First, let us just count points on one circle. We define a function similar to an indicator function, $C(x)$, such that when $x$ lies on the circle, $C(x) = 0$ but is nonzero otherwise.
- To count the zeros, we use the following equation:

$$|C| = q^{-1} \sum_{m \in \mathbb{Z}_q} \sum_{x \in \mathbb{Z}_q^2} \chi(m(C(x)))$$

# $\mathbb{Z}_q^2$ Circles

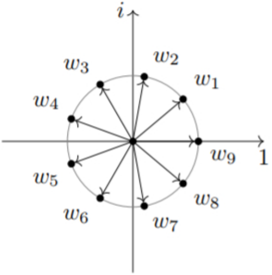
- First, let us just count points on one circle. We define a function similar to an indicator function, $C(x)$, such that when $x$ lies on the circle, $C(x) = 0$ but is nonzero otherwise.
- To count the zeros, we use the following equation:

$$|C| = q^{-1} \sum_{m \in \mathbb{Z}_q} \sum_{x \in \mathbb{Z}_q^2} \chi(m(C(x)))$$

- Here $\chi(m) = e^{\frac{2\pi i m}{q}}$, which are the $q^{\text{th}}$ roots of unity.

# $\mathbb{Z}_q^2$ Roots of Unity

$$|C| = q^{-1} \sum_{m \in \mathbb{Z}_q} \sum_{x \in \mathbb{Z}_q^2} \chi(m(C(x)))$$



# $\mathbb{Z}_q^2$ Main equation

- If $C(x)$ is the function for the unit circle centered at the origin, it's easy to see that $C(x) = x_1^2 + x_2^2 - 1$. So, we want to intersect this with a unit circle centered at $(h, k) \in \mathbb{Z}_q^2$. Hence the function for that is $D(x) = (x_1 - h)^2 + (x_2 - k)^2 - 1$.

## $\mathbb{Z}_q^2$ Main equation

- If $C(x)$ is the function for the unit circle centered at the origin, it's easy to see that $C(x) = x_1^2 + x_2^2 - 1$. So, we want to intersect this with a unit circle centered at $(h,k) \in \mathbb{Z}_q^2$. Hence the function for that is $D(x) = (x_1 - h)^2 + (x_2 - k)^2 - 1$.

$$|I| = q^{-2} \sum_{m \in \mathbb{Z}_q} \sum_{m' \in \mathbb{Z}_q} \sum_{x \in \mathbb{Z}_q^2} \chi(m(C(x)))\chi(m'(D(x)))$$

# $\mathbb{Z}_q^2$ Roots of Unity

- Note that taking $\sum_{x\in\mathbb{Z}_q}\chi(ux)$, where $u \in \mathbb{Z}_q^\times$, will still sum to zero as we are just permuting the roots of unity.

# $\mathbb{Z}_q^2$ Roots of Unity

- Note that taking $\sum_{x\in\mathbb{Z}_q}\chi(ux)$, where $u\in\mathbb{Z}_q^\times$, will still sum to zero as we are just permuting the roots of unity.
- Furthermore, if $u\in p\mathbb{Z}_p^\times$, the sum is still zero because we are just now summing over the $p^{\text{th}}$ roots of unity.

## $\mathbb{Z}_q^2$ Roots of Unity

- Note that taking $\sum_{x \in \mathbb{Z}_q} \chi(ux)$, where $u \in \mathbb{Z}_q^\times$, will still sum to zero as we are just permuting the roots of unity.
- Furthermore, if $u \in p\mathbb{Z}_p^\times$, the sum is still zero because we are just now summing over the $p^{\text{th}}$ roots of unity.
- Also, since our sums are finite, we can exchange the order.

# $\mathbb{Z}_q^2$ Key Tools

- Our main tool is Quadratic Gauss Sums:
- For positive integers $a, b, n$, the following is called a Gauss Sum:

$$G(a, b, n) = \sum_{x \in \mathbb{Z}_n} \chi(ax^2 + bx)$$

For ease, we will write $G(a, n)$ in place of $G(a, 0, n)$.

# $\mathbb{Z}_q^2$ Legendre Symbol

- In order to understand Gauss Sums, we need to understand the Jacobi symbol, which is a generalization to the Legendre symbol.

# $\mathbb{Z}_q^2$ Legendre Symbol

- In order to understand Gauss Sums, we need to understand the Jacobi symbol, which is a generalization to the Legendre symbol.

## Definition

Let $p$ be a prime and $a \in \mathbb{Z}$, then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ 0 & a | p \\ -1 & \text{otherwise} \end{cases}$$

# $\mathbb{Z}_q^2$ Legendre Symbol

## Theorem

*(Euler) Let $a \in \mathbb{Z}$ and $p$ be an odd prime. Then,*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$$

## Proposition

*Let $a, b \in \mathbb{Z}$ and $p$ be an odd prime. Then,* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

# $\mathbb{Z}_q^2$ Jacobi Symbol

## Definition

The Jacobi symbol is defined on $n \in \mathbb{Z}$ and $a \in \mathbb{Z}_n$, as follows:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_n}\right)^{\alpha_n}$$

where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$.

# $\mathbb{Z}_q^2$ Gauss Sums

- If we have $a \in \mathbb{Z}_n^\times$ and $n$ is odd, then:

$$G(a,n) = \epsilon_n \left(\frac{a}{n}\right) \sqrt{n}$$

## $\mathbb{Z}_q^2$ Gauss Sums

- If we have $a \in \mathbb{Z}_n^\times$ and $n$ is odd, then:

$$G(a,n) = \epsilon_n \left(\frac{a}{n}\right) \sqrt{n}$$

- Here, we have that $\left(\frac{\cdot}{n}\right)$ defines the Jacobi symbol. Furthermore,

$$\epsilon_n = \begin{cases} 1 & n \equiv 1 \mod 4 \\ i & n \equiv 3 \mod 4 \end{cases}$$

# $\mathbb{Z}_q^2$ Gauss Sums

**Proposition**

*For any $a \in \mathbb{Z}_n$, we have that:*

$$G(a,b,n) = \begin{cases} (a,n)G\left(\frac{a}{(a,n)}, \frac{b}{(a,n)}, \frac{n}{(a,n)}\right) & (a,n)|b \\ 0 & otherwise \end{cases}$$

# $\mathbb{Z}_q^2$ Gauss Sums

## Proposition

*Suppose that $a \in \mathbb{Z}_n^\times$, where $n$ is odd. Then, we have that:*

$$G(a, b, n) = (a, n) G(a, n) \chi\left(\frac{-b^2}{4a}\right)$$

## Proposition

$$G(1, q) = \sum_{d \in \mathbb{Z}_q} \chi(d) \left(\frac{d}{q}\right)$$

# $\mathbb{Z}_q^2$ Intersection Bound

- Using these techniques and splitting up our sums over $m$ and $m'$ by looking at $(m+m', q)$, we reached the following bounds, as of now.

## $\mathbb{Z}_q^2$ Intersection Bound

- Using these techniques and splitting up our sums over $m$ and $m'$ by looking at $(m + m', q)$, we reached the following bounds, as of now.
- If $h, k = 0$, we have $|I| = |q + 0 - p(\epsilon_p)^2| = q - p(\epsilon_p)^2$.

# $\mathbb{Z}_q^2$ Intersection Bound

- Using these techniques and splitting up our sums over $m$ and $m'$ by looking at $(m+m', q)$, we reached the following bounds, as of now.
- If $h, k = 0$, we have $|I| = |q + 0 - p(\epsilon_p)^2| = q - p(\epsilon_p)^2$.
- If $h = 0$ and $k \in p\mathbb{Z}_p^\times$, we get $|I| = |p + 0 + p| = 2p$.

# $\mathbb{Z}_q^2$ Intersection Bound

- Using these techniques and splitting up our sums over $m$ and $m'$ by looking at $(m+m', q)$, we reached the following bounds, as of now.
- If $h, k = 0$, we have $|I| = |q + 0 - p(\epsilon_p)^2| = q - p(\epsilon_p)^2$.
- If $h = 0$ and $k \in p\mathbb{Z}_p^\times$, we get $|I| = |p + 0 + p| = 2p$.
- If $h = sp, k = tp$, we have

$$|I| = \begin{cases} |p + 0 - \epsilon_p^2 p| & s^2 + t^2 \in p\mathbb{Z}_p \\ |p + 0 + \left(\frac{s^2+t^2}{p}\right) p| & s^2 + t^2 \in \mathbb{Z}_q^\times \end{cases}$$

# $\mathbb{Z}_q^2$ Intersection Bound

- Now, if $h \in \mathbb{Z}_q^\times$ and $k \in p\mathbb{Z}_p$, we have multiple cases:

$$|I| = \begin{cases} |1 + p - 1 + 0| = p & h^2 \equiv 4 \mod q \\ |1 - 1 + 0| = 0 & h^2 \equiv 4 + dp \mod q, d \in \mathbb{Z}_p^\times \\ |1 + 0 + \left(\frac{1 - \frac{h^2}{4}}{p}\right)| & h^2 \not\equiv 4 \mod p \end{cases}$$

# $\mathbb{Z}_q^2$ Intersection Bound

- Lastly, if $h, k \in \mathbb{Z}_q^\times$:

$$|I| \leq \begin{cases} |1 + 0 - \epsilon_p^2| & (h^2 + k^2, q) = q \\ |1 + \phi| & (h^2 + k^2, q) = 1 \\ |1 + \sqrt{p} - \epsilon_p^2| & (h^2 + k^2, q) = p \end{cases}$$

Define:

$$\phi = \begin{cases} p - 1 + 0 & h^2 + k^2 \equiv 4 \mod q \\ -1 + 0 & h^2 + l^2 \equiv 4 + dp \mod q, d \in \mathbb{Z}_p^\times \\ \left(\frac{h^2+k^2}{p}\right)\left(\frac{1-\frac{h^2+k^2}{4}}{p}\right) & \text{otherwise} \end{cases}$$

# $\mathbb{Z}_q^2$ Sharpness Example

- To show that our bound is sharp, it is sufficient to find a set, $E \subseteq \mathbb{Z}_q^2$, with $|E|^2 p$ hinges.

# $\mathbb{Z}_q^2$ Sharpness Example

- To show that our bound is sharp, it is sufficient to find a set, $E \subseteq \mathbb{Z}_q^2$, with $|E|^2 p$ hinges.
- To do this consider the following two sets:

$$A = \{(0,0),(0,p),(0,2p),...,(0,(p-1)p)\}$$

$$B = \{(1,0),(1,p),(1,2p),...,(1,(p-1)p)\}$$

Take $x, z \in A$ and $y \in B$. All of the unit circles centered at points in $A$ intersect at the points in $B$.

# $\mathbb{Z}_q^2$ Sharpness Example

- To show that our bound is sharp, it is sufficient to find a set, $E \subseteq \mathbb{Z}_q^2$, with $|E|^2 p$ hinges.
- To do this consider the following two sets:

$$A = \{(0,0),(0,p),(0,2p),...,(0,(p-1)p)\}$$

$$B = \{(1,0),(1,p),(1,2p),...,(1,(p-1)p)\}$$

  Take $x, z \in A$ and $y \in B$. All of the unit circles centered at points in $A$ intersect at the points in $B$.
- Note that this gives $|E|^3$ possible hinges when $|E| < p$.

# $\mathbb{Z}_q^2$ Averaging

$$
\begin{aligned}
|H(E)| &= \sum_{x,y,z \in \mathbb{Z}_q^2} I(y) \\
&\lesssim \sum_{\substack{x,z \in E \\ (z_1,z_2)=(x_1+h,x_2+k) \text{ s.t.} \\ h,k \in p\mathbb{Z}_p \vee h^2+k^2 \equiv 4 \mod q}} p + \sum_{\substack{x,z \in E \\ (z_1,z_2)=(x_1+h,x_2+k) \text{ s.t.} \\ h,k \in \mathbb{Z}_q^\times \wedge h^2+k^2 \equiv dp \mod q \\ d \in \mathbb{Z}_p^\times}} \sqrt{p} \\
&+ \sum_{x,z \text{ in the rest of } E} 1 \\
&= T_1 + T_2 + T_3
\end{aligned}
$$

# $\mathbb{Z}_q^2$ Averaging

- Now, we examine each of these terms. $T_1$. We clearly have $|E|$ choices for $x$. The choices for $z$ are more complicated. It comes out to:

$$\text{Choices for } z \lesssim p^2 + 2p + 2 \cdot p(p-1) \lesssim p^2$$

Hence, our bound on this term is $|E| \cdot |p| \cdot \min\{p^2, |E|\}$.

## $\mathbb{Z}_q^2$ Averaging

- Now, we examine each of these terms. $T_1$. We clearly have $|E|$ choices for $x$. The choices for $z$ are more complicated. It comes out to:

$$\text{Choices for } z \lesssim p^2 + 2p + 2 \cdot p(p-1) \lesssim p^2$$

  Hence, our bound on this term is $|E| \cdot |p| \cdot \min\{p^2, |E|\}$.
- For $T_2$, we have $|E|$ choices for $x$. For $z$, we get $p^3$. Hence,

$$T_2 \lesssim |E| \cdot |\sqrt{p}| \cdot \min\{p^3, |E|\}$$

# $\mathbb{Z}_q^2$ Averaging

- Now, we examine each of these terms. $T_1$. We clearly have $|E|$ choices for $x$. The choices for $z$ are more complicated. It comes out to:

$$\text{Choices for } z \lesssim p^2 + 2p + 2 \cdot p(p-1) \lesssim p^2$$

  Hence, our bound on this term is $|E| \cdot |p| \cdot \min\{p^2, |E|\}$.
- For $T_2$, we have $|E|$ choices for $x$. For $z$, we get $p^3$. Hence,

$$T_2 \lesssim |E| \cdot |\sqrt{p}| \cdot \min\{p^3, |E|\}$$

- Finally, $T_3 \lesssim |E|^2$. So, in total:

$$|H(E)| \lesssim |E| p \min\{p^2, |E|\} + |E| \cdot |\sqrt{p}| \cdot \min\{p^3, |E|\} + |E|^2$$

# $\mathbb{Z}_q^2$ Averaging

- With a little bit of work we get the following bounds:

$$|H(E)| \lesssim \begin{cases} |E|^3 & |E| < p \\ |E|^2 p & p \leq |E| < p^2 \\ |E| p^3 & p^2 \leq |E| < p^2\sqrt{p} \\ |E|^2\sqrt{p} & p^2\sqrt{p} \leq |E| < p^3 \\ |E| p^3\sqrt{p} & p^3 \leq |E| \end{cases}$$

# $\mathbb{Z}_q^2$ $k$-chains

- The maximum number of $k$-chains in a finite set $E$, is bounded by the following piecewise equation, which uses both our hinge bound and our intersection bound. Note that this requires $k \geq 2$.

$$\#_k \lesssim \begin{cases} |H(E)|^m & k = 3m \\ |H(E)|^m \cdot |E| & k = 3m+1 \\ |H(E)|^m \cdot p \cdot |E| & k = 3m+2 \end{cases}$$

# $\mathbb{F}_q^2$ Main Question

- Now, we want to look at intersections in $\mathbb{F}_q$ for $q = p^l$.

# $\mathbb{F}_q^2$ Main Question

- Now, we want to look at intersections in $\mathbb{F}_q$ for $q = p^l$.
- $|I| = q^{-2} \sum_{m,m' \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \chi(-m(x^2 + y^2 - 1))\chi(-m'((x - h)^2 + (y - k)^2 - 1))$

# $\mathbb{F}_q^2$ Main Question

- Now, we want to look at intersections in $\mathbb{F}_q$ for $q = p^l$.
- $|I| = q^{-2} \sum_{m,m' \in \mathbb{F}_q} \sum_{x,y \in \mathbb{F}_q} \chi(-m(x^2 + y^2 - 1))\chi(-m'((x - h)^2 + (y - k)^2 - 1))$
- Note that we have to change our definition of $\chi$ because it doesn't make any sense to take $e^x$ for $x \in \mathbb{F}_q$.

# $\mathbb{F}_q^2$ Trace

- For $\alpha \in \mathbb{F}_q$, $\chi(\alpha) = e^{2\pi i \mathrm{tr}(\alpha)}$.

# $\mathbb{F}_q^2$ Trace

- For $\alpha \in \mathbb{F}_q$, $\chi(\alpha) = e^{2\pi i \mathrm{tr}(\alpha)}$.
- $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{l-1}}$.

# $\mathbb{F}_q^2$ Trace

- For $\alpha \in \mathbb{F}_q$, $\chi(\alpha) = e^{2\pi i \mathrm{tr}(\alpha)}$.
- $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{l-1}}$.
- tr:$\mathbb{F}_q \to \mathbb{F}_p$.

# $\mathbb{F}_q^2$ Trace

- For $\alpha \in \mathbb{F}_q$, $\chi(\alpha) = e^{2\pi i \text{tr}(\alpha)}$.
- $\text{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{l-1}}$.
- tr:$\mathbb{F}_q \to \mathbb{F}_p$.
- Note that this equation permutes everything in a nontrivial way, but does make our equation work as intended.

# $\mathbb{F}_q^2$ Gauss Sums

- Let $\beta \in \mathbb{F}_q$, and let $q = p^l$. Then the Gauss sum $g_l(\beta, k)$ over $\mathbb{F}_q$ is defined by

$$g_r(\beta, k) = \sum_{\alpha \in \mathbb{F}_q} e^{2\pi i \mathrm{tr}(\beta \alpha^k)/p}$$

# $\mathbb{F}_q^2$ Gauss Sums

- Let $\beta \in \mathbb{F}_q$, and let $q = p^l$. Then the Gauss sum $g_l(\beta, k)$ over $\mathbb{F}_q$ is defined by

$$g_r(\beta, k) = \sum_{\alpha \in \mathbb{F}_q} e^{2\pi i \mathrm{tr}(\beta\alpha^k)/p}$$

- When we let $k = 2$, which is what we need for our question, we have that

$$g_l(\beta, 2) = \rho(\beta^{-1}) g_l(1, 2)$$

Here, $\rho$ is the canonical quadratic character in $\mathbb{F}_q$.

# $\mathbb{F}_q^2$ Gauss Sums

- Let $\beta \in \mathbb{F}_q$, and let $q = p^l$. Then the Gauss sum $g_l(\beta, k)$ over $\mathbb{F}_q$ is defined by

$$g_r(\beta, k) = \sum_{\alpha \in \mathbb{F}_q} e^{2\pi i \mathrm{tr}(\beta\alpha^k)/p}$$

- When we let $k = 2$, which is what we need for our question, we have that

$$g_l(\beta, 2) = \rho(\beta^{-1}) g_l(1, 2)$$

Here, $\rho$ is the canonical quadratic character in $\mathbb{F}_q$.

- $g_l(1, 2) = (-1)^{l-1} i^{\frac{r(p-1)^2}{4}} q^{\frac{1}{2}}$.

# $\mathbb{F}_q^2$ Intersection Bound

- $$|I| = \begin{cases} 1 + 0 + -1 = 0 & h^2 + k^2 = 0 \\ 1 + 0 + \rho(h^2 + k^2)\rho\left(1 - \frac{h^2+k^2}{4}\right) & 1 + \frac{h^2+k^2}{4} \neq 0 \\ 1 + 0 + 0 = 1 & 1 + \frac{h^2+k^2}{4} = 0 \end{cases}$$

# $\mathbb{F}_q^2$ Intersection Bound

- $$|I| = \begin{cases} 1 + 0 + -1 = 0 & h^2 + k^2 = 0 \\ 1 + 0 + \rho(h^2 + k^2)\rho\left(1 - \frac{h^2+k^2}{4}\right) & 1 + \frac{h^2+k^2}{4} \neq 0 \\ 1 + 0 + 0 = 1 & 1 + \frac{h^2+k^2}{4} = 0 \end{cases}$$
- $|H(E)| \lesssim |E|^2$

# References


- Erdős, Paul (1946), "On sets of distances of n points", American Mathematical Monthly, 53 (5): pp. 248–250, doi:10.2307/2305092.
- Spencer, Joel; Szemerédi, Endre; Trotter, William T. (1984), "Unit distances in the Euclidean plane", in Bollobás, Béla, Graph Theory and Combinatorics, London: Academic Press, pp. 293–308, ISBN 0-12-111760-X, MR 0777185.
- Covert, David; Iosevich, Alex; Pakianathan, Jonathan (2012), "Geometric Configurations in the Ring of Integers Modulo $p^l$", Indiana University Mathematics Journal, 61 (5): pp. 1949–1969.

# References


- Iosevich, Alex; Morgan, Hannah; Pakianathan, Jonathan (2011), "On Directions Determined by Subsets of Vector Spaces Over Finite Fields", Integers, 11 (6): pp. 815-825,doi: https://doi.org/10.1515/INTEG.2011.063.
- Iosevich, Alex; Rudnev, Misha, (2007) "Erdős Distance Problem in Vector Spaces Over Finite Fields", Transactions of the Mathematical Society, 359 (12): pp. 6127–6142.
- Berndt, Bruce C.; Evans, Ronald J.; Williams, Kenneth S. (1998),*Gauss and Jacobi Sums*, John Wiley & Sons Inc., Canada, pp. 9–11, 303, 362.

# Acknowledgments

We'd like to thank Steve for teaching and helping us extensively with this project ☺