There Is a 2-Coloring Of the Plane Without a mono Red 3-Stick or a mono Blue Big-Stick

Exposition by William Gasarch-U of MD

Credit Where Credit is Due

The main result in these slides is due to Conlon and Wu (2022).

Recall the Notation $\mathbb{R}^2 \to (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \geq 2$. $\mathbb{R}^2 \to (\ell_n, \ell_m)$ means

Recall the Notation $\mathbb{R}^2 \to (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \ge 2$. $\mathbb{R}^2 \to (\ell_n, \ell_m)$ means
For all $\mathrm{COL}\colon \mathbb{R}^2 \to [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Recall the Notation $\mathbb{R}^2 \to (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \ge 2$. $\mathbb{R}^2 \to (\ell_n, \ell_m)$ means

For all $\mathrm{COL}\colon \mathbb{R}^2 \to [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Last lecture we proved $\mathbb{R}^2 \to (\ell_2, \ell_3)$.

Recall the Notation $\mathbb{R}^2 \to (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \ge 2$. $\mathbb{R}^2 \to (\ell_n, \ell_m)$ means

For all $\mathrm{COL}\colon \mathbb{R}^2 \to [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Last lecture we proved $\mathbb{R}^2 \to (\ell_2, \ell_3)$.

What about $\mathbb{R}^2 \to (\ell_3, \ell_b)$ with $b \ge 3$.

Recall the Notation $\mathbb{R}^2 \to (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \ge 2$. $\mathbb{R}^2 \to (\ell_n, \ell_m)$ means

For all $\mathrm{COL}\colon \mathbb{R}^2 \to [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Last lecture we proved $\mathbb{R}^2 \to (\ell_2, \ell_3)$.

What about $\mathbb{R}^2 \to (\ell_3, \ell_b)$ with $b \ge 3$.

The following are known:

Recall the Notation $\mathbb{R}^2 \rightarrow (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \geq 2$. $\mathbb{R}^2 \rightarrow (\ell_n, \ell_m)$ means

For all $\mathrm{COL}\colon \mathbb{R}^2 \rightarrow [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Last lecture we proved $\mathbb{R}^2 \rightarrow (\ell_2, \ell_3)$.

What about $\mathbb{R}^2 \rightarrow (\ell_3, \ell_b)$ with $b \geq 3$.

The following are known:

$\mathbb{R}^2 \rightarrow (\ell_3, \ell_3)$ (Currier-Moore-Yip, 2024).

Recall the Notation $\mathbb{R}^2 \to (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \ge 2$. $\mathbb{R}^2 \to (\ell_n, \ell_m)$ means

For all $\mathrm{COL}\colon \mathbb{R}^2 \to [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Last lecture we proved $\mathbb{R}^2 \to (\ell_2, \ell_3)$.

What about $\mathbb{R}^2 \to (\ell_3, \ell_b)$ with $b \ge 3$.

The following are known:

$\mathbb{R}^2 \to (\ell_3, \ell_3)$ (Currier-Moore-Yip, 2024). Won't do here.

Recall the Notation $\mathbb{R}^2 \to (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \ge 2$. $\mathbb{R}^2 \to (\ell_n, \ell_m)$ means

For all $\mathrm{COL}\colon \mathbb{R}^2 \to [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Last lecture we proved $\mathbb{R}^2 \to (\ell_2, \ell_3)$.

What about $\mathbb{R}^2 \to (\ell_3, \ell_b)$ with $b \ge 3$.

The following are known:

$\mathbb{R}^2 \to (\ell_3, \ell_3)$ (Currier-Moore-Yip, 2024). Won't do here.

$\mathbb{R}^2 \not\to (\ell_3, \ell_{10^{50}})$ (Conlon-Wu, 2022).

Recall the Notation $\mathbb{R}^2 \rightarrow (\ell_{\mathbf{a}}, \ell_{\mathbf{b}})$

Notation Let $a, b \ge 2$. $\mathbb{R}^2 \rightarrow (\ell_n, \ell_m)$ means

For all $\mathrm{COL}\colon \mathbb{R}^2 \rightarrow [2]$ there exists **Red** ℓ_n or **Blue** ℓ_m.

Last lecture we proved $\mathbb{R}^2 \rightarrow (\ell_2, \ell_3)$.

What about $\mathbb{R}^2 \rightarrow (\ell_3, \ell_b)$ with $b \ge 3$.

The following are known:

$\mathbb{R}^2 \rightarrow (\ell_3, \ell_3)$ (Currier-Moore-Yip, 2024). Won't do here.

$\mathbb{R}^2 \not\rightarrow (\ell_3, \ell_{10^{50}})$ (Conlon-Wu, 2022). Will do here.

Main Theorem

Full Statement

Thm There exists $\mathrm{COL}\colon \mathbb{R}^n \to [2]$ such that

Full Statement

Thm There exists $\mathrm{COL}\colon \mathbb{R}^n \to [2]$ such that there is no a **R** ℓ_3, and

Full Statement

Thm There exists $\mathrm{COL}\colon \mathbb{R}^n \to [2]$ such that

there is no a **R** ℓ_3, and

there is no **B** ℓ_m where m will be determined later.

Full Statement

Thm There exists $\mathrm{COL}\colon \mathbb{R}^n \to [2]$ such that

there is no a **R** ℓ_3, and

there is no **B** ℓ_m where m will be determined later.

m will be around 10^{50}.

Full Statement

Thm There exists $\mathrm{COL}\colon \mathbb{R}^n \rightarrow [2]$ such that

there is no a **R** ℓ_3, and

there is no **B** ℓ_m where m will be determined later.

m will be around 10^{50}.

The proof for $\mathbb{R}^n$ and $\mathbb{R}^2$ are identical.

Full Statement

Thm There exists $\mathrm{COL}\colon \mathbb{R}^n \to [2]$ such that

there is no a **R** ℓ_3, and

there is no **B** ℓ_m where m will be determined later.

m will be around 10^{50}.

The proof for $\mathbb{R}^n$ and $\mathbb{R}^2$ are identical.

Open Find an easier proof of $\mathbb{R}^2$ case.

Algebraic Implications of ℓ_3. No Coloring Involved

Algebraic Implications of ℓ_3. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.

Algebraic Implications of ℓ_3. No Coloring Involved

Let $\vec{0}$ be $(0, 0)$.
Let $\vec{a}_1, \vec{a}_2, \vec{a}_3$ be an ℓ_3.

Algebraic Implications of ℓ_3. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.
Let $\vec{a}_1, \vec{a}_2, \vec{a}_3$ be an ℓ_3.

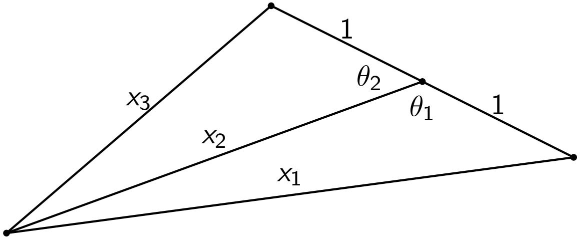
Let
$x_1 = d(\vec{0}, \vec{a}_1)$,
$x_2 = d(\vec{0}, \vec{a}_2)$,
$x_3 = d(\vec{0}, \vec{a}_3)$

Algebraic Implications of ℓ_3. No Coloring Involved

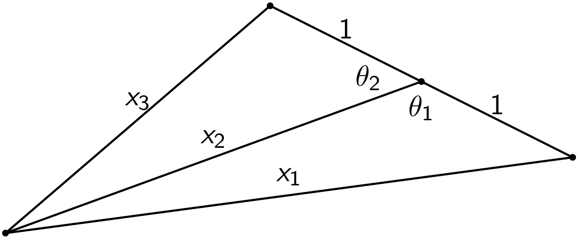
Let $\vec{0}$ be $(0, 0)$.
Let $\vec{a}_1, \vec{a}_2, \vec{a}_3$ be an ℓ_3.

Let
$x_1 = d(\vec{0}, \vec{a}_1)$,
$x_2 = d(\vec{0}, \vec{a}_2)$,
$x_3 = d(\vec{0}, \vec{a}_3)$
And we know
$1 = d(\vec{a}_1, \vec{a}_2)$,
$1 = d(\vec{a}_2, \vec{a}_3)$,

Algebra and Trigonometry

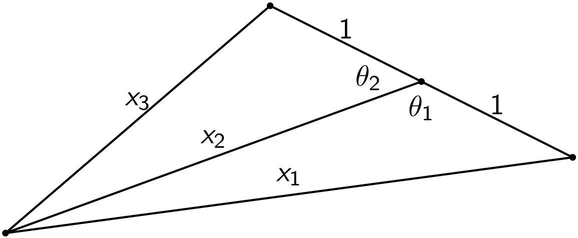


Algebra and Trigonometry



Bottom Triangle:

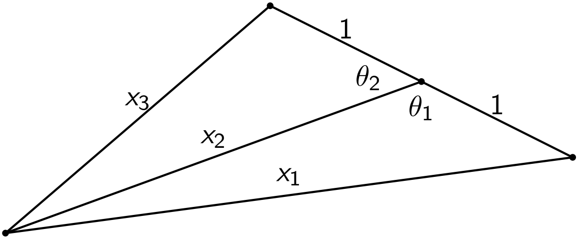
Algebra and Trigonometry



Bottom Triangle:

Law of cosines: $x_1^2 = x_2^2 + 1 - 2x_2 \cos(\theta_1)$.

Algebra and Trigonometry

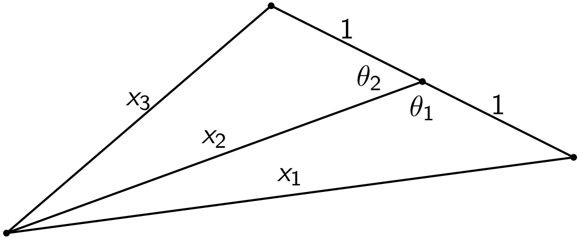


Bottom Triangle:

Law of cosines: $x_1^2 = x_2^2 + 1 - 2x_2 \cos(\theta_1)$.

Top Triangle:

Algebra and Trigonometry



Bottom Triangle:

Law of cosines: $x_1^2 = x_2^2 + 1 - 2x_2 \cos(\theta_1)$.

Top Triangle:

Law of cosines: $x_3^2 = x_2^2 + 1 - 2x_2 \cos(\theta_2)$.

Algebra and Trigonometry

Algebra and Trigonometry

$\theta_2 = \pi - \theta_2$. Hence $\cos(\theta_2) = -\cos(\theta_1)$.

Algebra and Trigonometry

$\theta_2 = \pi - \theta_2$. Hence $\cos(\theta_2) = -\cos(\theta_1)$.

Law of cosines: $x_1^2 = x_2^2 + 1 - 2x_2 \cos(\theta_1)$.

Algebra and Trigonometry

$\theta_2 = \pi - \theta_2$. Hence $\cos(\theta_2) = -\cos(\theta_1)$.

Law of cosines: $x_1^2 = x_2^2 + 1 - 2x_2\cos(\theta_1)$.

Law of cosines: $x_3^2 = x_2^2 + 1 - 2x_2\cos(\theta_2) = x_2^2 + 1 + 2x_2\cos(\theta_1)$.

Algebra and Trigonometry

$\theta_2 = \pi - \theta_2$. Hence $\cos(\theta_2) = -\cos(\theta_1)$.

Law of cosines: $x_1^2 = x_2^2 + 1 - 2x_2 \cos(\theta_1)$.

Law of cosines: $x_3^2 = x_2^2 + 1 - 2x_2 \cos(\theta_2) = x_2^2 + 1 + 2x_2 \cos(\theta_1)$.

Add to get

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

First Plan On How to Avoid R ℓ_3

First Plan On How to Avoid R ℓ_3

First Plan

First Plan On How to Avoid **R** ℓ_3

First Plan

1) Find $\mathrm{COL}'\colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

First Plan On How to Avoid R ℓ_3

First Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \rightarrow [2]$ such that there is no **R** solution to

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \rightarrow [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

First Plan On How to Avoid **R** ℓ_3

First Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \rightarrow [2]$ such that there is no **R** solution to

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \rightarrow [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Easy COL has **R** $\ell_3 \implies \mathrm{COL}'$ has **R** sol to $x_1^2 + x_3^2 = 2x_2^2 + 2$.

First Plan On How to Avoid R ℓ_3

First Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \rightarrow [2]$ such that there is no **R** solution to

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \rightarrow [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Easy COL has **R** $\ell_3 \implies$ COL' has **R** sol to $x_1^2 + x_3^2 = 2x_2^2 + 2$.
Hence COL does not have a **R** ℓ_3.

First Plan On How to Avoid R ℓ_3

First Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Easy COL has **R** $\ell_3 \implies \mathrm{COL}'$ has **R** sol to $x_1^2 + x_3^2 = 2x_2^2 + 2$.
Hence COL does not have a **R** ℓ_3.

This plan works but there is an even easier one.

First Plan On How to Avoid **R** ℓ_3

First Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Easy COL has **R** $\ell_3 \implies \mathrm{COL}'$ has **R** sol to $x_1^2 + x_3^2 = 2x_2^2 + 2$.
Hence COL does not have a **R** ℓ_3.

This plan works but there is an even easier one.

The fact that x_1, x_2, x_3 are squared is not important.

First Plan On How to Avoid R ℓ_3

First Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$x_1^2 + x_3^2 = 2x_2^2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Easy COL has **R** $\ell_3 \implies \mathrm{COL}'$ has **R** sol to $x_1^2 + x_3^2 = 2x_2^2 + 2$.
Hence COL does not have a **R** ℓ_3.

This plan works but there is an even easier one.

The fact that x_1, x_2, x_3 are squared is not important.
Can get rid of squares.

Second Plan On How to Avoid **R** ℓ_3

Second Plan On How to Avoid R ℓ_3

Second Plan

Second Plan On How to Avoid R ℓ_3

Second Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

Second Plan On How to Avoid **R** ℓ_3

Second Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Second Plan On How to Avoid **R** ℓ_3

Second Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Easy COL has **R** $\ell_3 \implies \mathrm{COL}'$ has **R** sol to $x_1^2 + x_3^2 = 2x_2^2 + 2$
$\implies \mathrm{COL}'$ has **R** sol to $y_1 + y_3 = 2y_2 + 2$.

Upshot on **R** ℓ_3

We will define $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

Upshot on **R** ℓ_3

We will define $\mathrm{COL}'\colon \mathbb{R} \to [2]$ such that there is no **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

Will then define $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$

Upshot on **R** ℓ_3

We will define $\mathrm{COL}' \colon \mathbb{R} \rightarrow [2]$ such that there is no **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

Will then define $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$

We will also have a condition on COL' that will make $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$ not have any **B** ℓ_m

Algebraic Implications of ℓ_m. No Coloring Involved

Algebraic Implications of $\ell_{\mathbf{m}}$. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.

Algebraic Implications of ℓ_m. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.
Let $\vec{a}_1, \ldots, \vec{a}_m$ be an ℓ_m.

Algebraic Implications of $\ell_{\mathbf{m}}$. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.
Let $\vec{a}_1,\ldots,\vec{a}_m$ be an ℓ_m.
For all $1 \le i \le m$ let $x_i = d(\vec{0},\vec{a}_i)$.

Algebraic Implications of ℓ_m. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.
Let $\vec{a}_1, \ldots, \vec{a}_m$ be an ℓ_m.

For all $1 \le i \le m$ let $x_i = d(\vec{0}, \vec{a}_i)$.
For all $1 \le i \le m-1$ we know $1 = d(\vec{a}_i, \vec{a}_{i+1})$.

Algebraic Implications of $\ell_{\mathbf{m}}$. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.
Let $\vec{a}_1, \ldots, \vec{a}_m$ be an ℓ_m.

For all $1 \le i \le m$ let $x_i = d(\vec{0}, \vec{a}_i)$.
For all $1 \le i \le m-1$ we know $1 = d(\vec{a}_i, \vec{a}_{i+1})$.
By using the prior reasoning about ℓ_3, applied to all ℓ_3's, we get

Algebraic Implications of ℓ_m. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.
Let $\vec{a}_1, \ldots, \vec{a}_m$ be an ℓ_m.
For all $1 \le i \le m$ let $x_i = d(\vec{0}, \vec{a}_i)$.
For all $1 \le i \le m-1$ we know $1 = d(\vec{a}_i, \vec{a}_{i+1})$.
By using the prior reasoning about ℓ_3, applied to all ℓ_3's, we get
For all $2 \le i \le m-1$,

Algebraic Implications of ℓ_m. No Coloring Involved

Let $\vec{0}$ be $(0,0)$.
Let $\vec{a}_1, \ldots, \vec{a}_m$ be an ℓ_m.
For all $1 \le i \le m$ let $x_i = d(\vec{0}, \vec{a}_i)$.
For all $1 \le i \le m-1$ we know $1 = d(\vec{a}_i, \vec{a}_{i+1})$.
By using the prior reasoning about ℓ_3, applied to all ℓ_3's, we get
For all $2 \le i \le m-1$,

$$x_{i-1}^2 + x_{i+1}^2 = 2x_i^2 + 2.$$

Real Plan On How to Avoid B ℓ_m

Real Plan On How to Avoid B ℓ_m

Real Plan

Real Plan On How to Avoid B ℓ_m

Real Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **B** solution to:
For all $2 \le i \le m-1$,

$$y_1 + y_3 = 2y_2 + 2.$$

Real Plan On How to Avoid **B** ℓ_m

Real Plan

1) Find $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that there is no **B** solution to:
For all $2 \le i \le m-1$,

$$y_1 + y_3 = 2y_2 + 2.$$

2) Define $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ by $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(\vec{0}, \vec{a}))$.

Third Plan

We need $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that

Third Plan

We need $\mathrm{COL}'\colon \mathbb{R} \to [2]$ such that
1) No **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

Third Plan

We need $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that
1) No **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

2) No **B** solution to

Third Plan

We need $\mathrm{COL}' \colon \mathbb{R} \to [2]$ such that
1) No **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

2) No **B** solution to
forall $2 \le i \le m-1$,

$$y_{i-1} + y_{i+1} = 2y_i + 2.$$

We Color Mod q

We have not determined m yet. We will later.

We Color Mod q

We have not determined m yet. We will later.
However we will require that $m = q^3$ where q is prime.

We Color Mod q

We have not determined m yet. We will later.
However we will require that $m = q^3$ where q is prime.
We will define $\mathrm{COL}''\colon \mathbb{Z}_q \to [2]$.

We Color Mod q

We have not determined m yet. We will later.
However we will require that $m = q^3$ where q is prime.
We will define $\mathrm{COL}''\colon \mathbb{Z}_q \to [2]$.
We will then define $\mathrm{COL}'\colon \mathbb{R} \to [2]$ by

We Color Mod q

We have not determined m yet. We will later.
However we will require that $m = q^3$ where q is prime.
We will define $\mathrm{COL}'': \mathbb{Z}_q \rightarrow [2]$.
We will then define $\mathrm{COL}': \mathbb{R} \rightarrow [2]$ by

$$\mathrm{COL}'(y) = \mathrm{COL}''(\lfloor y \rfloor \pmod{q}).$$

An Example of A Coloring with $q = 5$

$\mathrm{COL}''(0) = \mathbf{R}$
$\mathrm{COL}''(1) = \mathbf{B}$
$\mathrm{COL}''(2) = \mathbf{B}$
$\mathrm{COL}''(3) = \mathbf{R}$
$\mathrm{COL}''(4) = \mathbf{R}$

An Example of A Coloring with q = 5

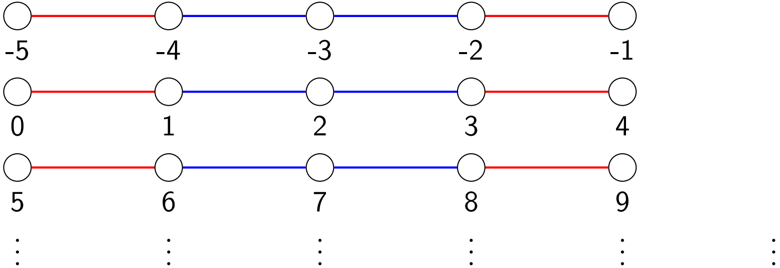
$\mathrm{COL}''(0) = $ **R**
$\mathrm{COL}''(1) = $ **B**
$\mathrm{COL}''(2) = $ **B**
$\mathrm{COL}''(3) = $ **R**
$\mathrm{COL}''(4) = $ **R**

$$\mathrm{COL}'(y) = \mathrm{COL}''(\lfloor y \rfloor \pmod{q})$$

An Example of A Coloring with q = 5

$\mathrm{COL}''(0) = $ **R**
$\mathrm{COL}''(1) = $ **B**
$\mathrm{COL}''(2) = $ **B**
$\mathrm{COL}''(3) = $ **R**
$\mathrm{COL}''(4) = $ **R**

$$\mathrm{COL}'(y) = \mathrm{COL}''(\lfloor y \rfloor \pmod q)$$



Final Plan

We need $\mathrm{COL}''\colon \mathbb{Z}_q \to [2]$ such that

Final Plan

We need $\mathrm{COL}'' \colon \mathbb{Z}_q \to [2]$ such that
1) No **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

Final Plan

We need $\mathrm{COL}'' \colon \mathbb{Z}_q \to [2]$ such that
1) No **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

2) No **B** solution to
for all $2 \leq i \leq m-1$

$$y_{i-1} + y_{i+1} = 2y_i + 2.$$

Final Plan

We need $\mathrm{COL}'' \colon \mathbb{Z}_q \to [2]$ such that
1) No **R** solution to

$$y_1 + y_3 = 2y_2 + 2.$$

2) No **B** solution to
for all $2 \le i \le m-1$

$$y_{i-1} + y_{i+1} = 2y_i + 2.$$

The next slide recaps where we are and says why COL'' helps us.

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \to [2]$:

COL'' and COL' and COL

Assume $\mathrm{COL}'' : \mathbb{Z}_q \rightarrow [2]$:
1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \rightarrow [2]$:
1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.
2) COL'' has no **B** solution (in $\mathbb{Z}_q$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \rightarrow [2]$:
1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.
2) COL'' has no **B** solution (in $\mathbb{Z}_q$) to

$$\text{For all } 2 \leq i \leq m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL}' \colon \mathbb{Z} \rightarrow [2]$ be $\mathrm{COL}''(\lfloor y \rfloor \pmod{q})$. Can show

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \rightarrow [2]$:
1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.
2) COL'' has no **B** solution (in $\mathbb{Z}_q$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL}' \colon \mathbb{Z} \rightarrow [2]$ be $\mathrm{COL}''(\lfloor y \rfloor \pmod q)$. Can show
1) COL' has no **R** solution (in $\mathbb{Z}$) to $y_1 + y_3 = 2y_2 + 2$.

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \rightarrow [2]$:
1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.
2) COL'' has no **B** solution (in $\mathbb{Z}_q$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL}' \colon \mathbb{Z} \rightarrow [2]$ be $\mathrm{COL}''(\lfloor y \rfloor \pmod{q})$. Can show
1) COL' has no **R** solution (in $\mathbb{Z}$) to $y_1 + y_3 = 2y_2 + 2$.
2) Has no **B** solution (in $\mathbb{Z}$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \to [2]$:
1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.
2) COL'' has no **B** solution (in $\mathbb{Z}_q$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL}' \colon \mathbb{Z} \to [2]$ be $\mathrm{COL}''(\lfloor y \rfloor \pmod{q})$. Can show
1) COL' has no **R** solution (in $\mathbb{Z}$) to $y_1 + y_3 = 2y_2 + 2$.
2) Has no **B** solution (in $\mathbb{Z}$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ be $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(0, \vec{a}))$. Did show

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \rightarrow [2]$:
1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.
2) COL'' has no **B** solution (in $\mathbb{Z}_q$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL}' \colon \mathbb{Z} \rightarrow [2]$ be $\mathrm{COL}''(\lfloor y \rfloor \pmod q)$. Can show
1) COL' has no **R** solution (in $\mathbb{Z}$) to $y_1 + y_3 = 2y_2 + 2$.
2) Has no **B** solution (in $\mathbb{Z}$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL} \colon \mathbb{R}^2 \rightarrow [2]$ be $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(0,\vec{a}))$. Did show
1) COL has no **R** ℓ_3 (in $\mathbb{R}^2$).

COL'' and COL' and COL

Assume $\mathrm{COL}'' \colon \mathbb{Z}_q \to [2]$:

1) COL'' has no **R** solution (in $\mathbb{Z}_q$) to $y_1 + y_3 = 2y_2 + 2$.
2) COL'' has no **B** solution (in $\mathbb{Z}_q$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL}' \colon \mathbb{Z} \to [2]$ be $\mathrm{COL}''(\lfloor y \rfloor \pmod{q})$. Can show

1) COL' has no **R** solution (in $\mathbb{Z}$) to $y_1 + y_3 = 2y_2 + 2$.
2) Has no **B** solution (in $\mathbb{Z}$) to

$$\text{For all } 2 \le i \le m-1,\ y_{i-1} + y_{i+1} = 2y_i + 2$$

Let $\mathrm{COL} \colon \mathbb{R}^2 \to [2]$ be $\mathrm{COL}(\vec{a}) = \mathrm{COL}'(d(0, \vec{a}))$. Did show

1) COL has no **R** ℓ_3 (in $\mathbb{R}^2$).
2) COL has no **B** ℓ_m (in $\mathbb{R}^2$).

We Define COL''

TO define COL'' we'll need some hard math. Or will we?

We Define COL''

TO define COL'' we'll need some hard math. Or will we?
See next slide.

That's Bullshit Man: Performed by Erin and Bill

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man!

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty!

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

ERIN: About picking randomly or about you being a moron?

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

ERIN: About picking randomly or about you being a moron?

BILL: Both.

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

ERIN: About picking randomly or about you being a moron?

BILL: Both. Now back to Math.

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

ERIN: About picking randomly or about you being a moron?

BILL: Both. Now back to Math.

ERIN: Math is bullshit man!

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

ERIN: About picking randomly or about you being a moron?

BILL: Both. Now back to Math.

ERIN: Math is bullshit man!

BILL: A catchphrase should be used exactly twice.

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

ERIN: About picking randomly or about you being a moron?

BILL: Both. Now back to Math.

ERIN: Math is bullshit man!

BILL: A catchphrase should be used exactly twice.

ERIN: That's bullshit man!

That's Bullshit Man: Performed by Erin and Bill

Bill is playing a slightly dumber version of Bill.
Erin is playing Erin.

BILL: We need to find a coloring. This requires hard math.

ERIN: That's bullshit man!

BILL: (ignoring Erin) We need topological algebraic topology.

ERIN: That's bullshit man! Pick the colors randomly moron!

BILL: Well pierce my ears and call me drafty! She's right!

ERIN: About picking randomly or about you being a moron?

BILL: Both. Now back to Math.

ERIN: Math is bullshit man!

BILL: A catchphrase should be used exactly twice.

ERIN: That's bullshit man!
The End

Pick a Coloring Randomly

We will pick $\mathrm{COL}\colon \mathbb{Z}_q \rightarrow [2]$ randomly.

Pick a Coloring Randomly

We will pick $\mathrm{COL}\colon \mathbb{Z}_q \to [2]$ randomly.

We will **not** color each element **R** or **B** with equal probability.

Pick a Coloring Randomly

We will pick $\mathrm{COL}\colon \mathbb{Z}_q \to [2]$ randomly.

We will **not** color each element **R** or **B** with equal probability.

We want **R** to be far rarer than **B**.

Pick a Coloring Randomly

We will pick $\mathrm{COL}\colon \mathbb{Z}_q \to [2]$ randomly.

We will **not** color each element **R** or **B** with equal probability.

We want **R** to be far rarer than **B**.

We pick

Pick a Coloring Randomly

We will pick $\mathrm{COL}\colon \mathbb{Z}_q \to [2]$ randomly.

We will **not** color each element **R** or **B** with equal probability.

We want **R** to be far rarer than **B**.

We pick
Prob of a **R** to be $p = q^{-1/2}$

Pick a Coloring Randomly

We will pick $\mathrm{COL}\colon \mathbb{Z}_q \to [2]$ randomly.

We will **not** color each element **R** or **B** with equal probability.

We want **R** to be far rarer than **B**.

We pick
Prob of a **R** to be $p = q^{-1/2}$
One can show prob of **R**sol to $y_1 + y_3 = 2y_2 + 2$ is $< \frac{1}{2}$.

Pick a Coloring Randomly

We will pick $\mathrm{COL}\colon \mathbb{Z}_q \to [2]$ randomly.

We will **not** color each element **R** or **B** with equal probability.

We want **R** to be far rarer than **B**.

We pick
Prob of a **R** to be $p = q^{-1/2}$
One can show prob of **R**sol to $y_1 + y_3 = 2y_2 + 2$ is $< \frac{1}{2}$.
Prob of a **B** to be $1 - p$

Lemmas and a Theorem of Independent Interest

Consider $\mathbf{p(x)} \in \mathbb{R}[\mathbf{x}] \pmod{\mathbf{q}}$

What does $p(x) = x^2 + \pi x + e \pmod{13}$ mean?

Consider $\mathbf{p}(\mathbf{x}) \in \mathbb{R}[\mathbf{x}] \pmod{\mathbf{q}}$

What does $p(x) = x^2 + \pi x + e \pmod{13}$ mean?

What is $p(10) = 100 + 10\pi + e \pmod{13}$?

Consider $\mathbf{p(x)} \in \mathbb{R}[\mathbf{x}] \pmod{\mathbf{q}}$

What does $p(x) = x^2 + \pi x + e \pmod{13}$ mean?

What is $p(10) = 100 + 10\pi + e \pmod{13}$?
subtract multiples of 13 until this is in $[0, 13)$.

Consider $\mathbf{p}(\mathbf{x}) \in \mathbb{R}[\mathbf{x}] \pmod{\mathbf{q}}$

What does $p(x) = x^2 + \pi x + e \pmod{13}$ mean?

What is $p(10) = 100 + 10\pi + e \pmod{13}$?
subtract multiples of 13 until this is in $[0, 13)$.

Lets say $p(10) = 134.1325$ (thats not true but its a good approx).

Consider $\mathbf{p(x)} \in \mathbb{R}[\mathbf{x}] \pmod{\mathbf{q}}$

What does $p(x) = x^2 + \pi x + e \pmod{13}$ mean?

What is $p(10) = 100 + 10\pi + e \pmod{13}$?
subtract multiples of 13 until this is in $[0, 13)$.

Lets say $p(10) = 134.1325$ (thats not true but its a good approx).
$134.1324 \pmod{13} = 4.1324$.

Consider $\mathbf{p}(\mathbf{x}) \in \mathbb{R}[\mathbf{x}] \pmod{\mathbf{q}}$

What does $p(x) = x^2 + \pi x + e \pmod{13}$ mean?

What is $p(10) = 100 + 10\pi + e \pmod{13}$?
subtract multiples of 13 until this is in $[0, 13)$.

Lets say $p(10) = 134.1325$ (thats not true but its a good approx).
$134.1324 \pmod{13} = 4.1324$.

So it makes sense to consider $p(x) \pmod{q}$ where $p(x) \in \mathbb{R}[x]$.

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \geq q$.

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \geq q$.
Let $f(x) = p(x) \pmod{q}$. Each element of

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \geq q$. Let $f(x) = p(x) \pmod{q}$. Each element of

$$\{f(1), f(2), \ldots, f(m)\}$$

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \geq q$.
Let $f(x) = p(x) \pmod{q}$. Each element of

$$\{f(1), f(2), \ldots, f(m)\}$$

is in one of $[0, 1)$, $[1, 2)$, …, $[q - 1, q)$.

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \geq q$. Let $f(x) = p(x) \pmod{q}$. Each element of

$$\{f(1), f(2), \ldots, f(m)\}$$

is in one of $[0, 1)$, $[1, 2)$, ..., $[q-1, q)$.

Informal Question How many interval are hit?

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \geq q$.
Let $f(x) = p(x) \pmod q$. Each element of

$$\{f(1), f(2), \ldots, f(m)\}$$

is in one of $[0, 1)$, $[1, 2)$, ..., $[q - 1, q)$.

Informal Question How many interval are hit?

Formal Question Given $p(x)$, q, m, give a lower bound on how many intervals are hit.

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \ge q$.
Let $f(x) = p(x) \pmod{q}$. Each element of

$$\{f(1), f(2), \ldots, f(m)\}$$

is in one of $[0, 1)$, $[1, 2)$, ..., $[q - 1, q)$.

Informal Question How many interval are hit?

Formal Question Given $p(x)$, q, m, give a lower bound on how many intervals are hit.

Meta Question We consider this question for the (ℓ_3, ℓ_b) result. Is it interesting in its own right?

How Concentrated Are The Elements In the Image?

Set Up Let $p(x) \in \mathbb{R}[x]$. Let q be a prime. Let $m \geq q$.
Let $f(x) = p(x) \pmod{q}$. Each element of

$$\{f(1), f(2), \ldots, f(m)\}$$

is in one of $[0, 1)$, $[1, 2)$, ..., $[q-1, q)$.

Informal Question How many interval are hit?

Formal Question Given $p(x)$, q, m, give a lower bound on how many intervals are hit.

Meta Question We consider this question for the (ℓ_3, ℓ_b) result. Is it interesting in its own right? I leave that to the reader.

The Lemma

Lemma Let $p(x) = x^2 + \alpha x + \beta$ where $\alpha, \beta \in \mathbb{R}$.

The Lemma

Lemma Let $p(x) = x^2 + \alpha x + \beta$ where $\alpha, \beta \in \mathbb{R}$.

Let q be a prime.

The Lemma

Lemma Let $p(x) = x^2 + \alpha x + \beta$ where $\alpha, \beta \in \mathbb{R}$.

Let q be a prime.

Let $f(x) = p(x) \pmod{q}$.

The Lemma

Lemma Let $p(x) = x^2 + \alpha x + \beta$ where $\alpha, \beta \in \mathbb{R}$.

Let q be a prime.

Let $f(x) = p(x) \pmod{q}$.

Let $m \geq q^3$.

The Lemma

Lemma Let $p(x) = x^2 + \alpha x + \beta$ where $\alpha, \beta \in \mathbb{R}$.

Let q be a prime.

Let $f(x) = p(x) \pmod{q}$.

Let $m \geq q^3$.

$$\text{Let } X = \{f(1), f(2), \ldots, f(m)\}.$$

The Lemma

Lemma Let $p(x) = x^2 + \alpha x + \beta$ where $\alpha, \beta \in \mathbb{R}$.
Let q be a prime.
Let $f(x) = p(x) \pmod{q}$.
Let $m \geq q^3$.

$$\text{Let } X = \{f(1), f(2), \ldots, f(m)\}.$$

Then

The Lemma

Lemma Let $p(x) = x^2 + \alpha x + \beta$ where $\alpha, \beta \in \mathbb{R}$.

Let q be a prime.

Let $f(x) = p(x) \pmod{q}$.

Let $m \geq q^3$.

$$\text{Let } X = \{f(1), f(2), \ldots, f(m)\}.$$

Then

X hits at least $q/6$ of the intervals $[0,1)$, $[1,2)$, ..., $[q-1,q)$.

Proof of Lemma: Two Cases

Consider $\alpha \pmod{q}$, $2\alpha \pmod{q}$, …, $q^2\alpha \pmod{q}$.

Proof of Lemma: Two Cases

Consider $\alpha \pmod{q}$, $2\alpha \pmod{q}$, ..., $q^2\alpha \pmod{q}$.

Map each one to which interval $[0, 1)$, ..., $[q-1, q)$ that it is in.

Proof of Lemma: Two Cases

Consider $\alpha \pmod q$, $2\alpha \pmod q$, …, $q^2\alpha \pmod q$.

Map each one to which interval $[0, 1)$, …, $[q - 1, q)$ that it is in.

Some intervals has $\geq q$ of these values.

Proof of Lemma: Two Cases

Consider $\alpha \pmod{q}$, $2\alpha \pmod{q}$, ..., $q^2\alpha \pmod{q}$.

Map each one to which interval $[0, 1)$, ..., $[q - 1, q)$ that it is in.

Some intervals has $\geq q$ of these values.

Two of those values are $\leq 1/q$ apart.

Proof of Lemma: Two Cases

Consider $\alpha \pmod{q}$, $2\alpha \pmod{q}$, …, $q^2\alpha \pmod{q}$.

Map each one to which interval $[0, 1)$, …, $[q-1, q)$ that it is in.

Some intervals has $\geq q$ of these values.

Two of those values are $\leq 1/q$ apart.

So there exists i, j such that $|i\alpha \pmod{q} - j\alpha \pmod{q}| \leq \frac{1}{q}$.

Proof of Lemma: Two Cases

Consider $\alpha \pmod q$, $2\alpha \pmod q$, …, $q^2\alpha \pmod q$.

Map each one to which interval $[0,1)$, …, $[q-1,q)$ that it is in.

Some intervals has $\geq q$ of these values.

Two of those values are $\leq 1/q$ apart.

So there exists i,j such that $|i\alpha \pmod q - j\alpha \pmod q| \leq \frac{1}{q}$.

Upshot There exists $k \leq q^2$ such that $|k\alpha \pmod q| \leq \frac{1}{q}$.

Proof of Lemma: Two Cases

Consider $\alpha \pmod q$, $2\alpha \pmod q$, ..., $q^2\alpha \pmod q$.

Map each one to which interval $[0, 1)$, ..., $[q-1, q)$ that it is in.

Some intervals has $\geq q$ of these values.

Two of those values are $\leq 1/q$ apart.

So there exists i, j such that $|i\alpha \pmod q - j\alpha \pmod q| \leq \frac{1}{q}$.

Upshot There exists $k \leq q^2$ such that $|k\alpha \pmod q| \leq \frac{1}{q}$.

We will consider two cases:

Proof of Lemma: Two Cases

Consider $\alpha \pmod{q}$, $2\alpha \pmod{q}$, …, $q^2\alpha \pmod{q}$.

Map each one to which interval $[0, 1)$, …, $[q-1, q)$ that it is in.

Some intervals has $\geq q$ of these values.

Two of those values are $\leq 1/q$ apart.

So there exists i, j such that $|i\alpha \pmod{q} - j\alpha \pmod{q}| \leq \frac{1}{q}$.

Upshot There exists $k \leq q^2$ such that $|k\alpha \pmod{q}| \leq \frac{1}{q}$.

We will consider two cases:

Case 1 $k \not\equiv 0 \pmod{q}$.

Proof of Lemma: Two Cases

Consider $\alpha \pmod{q}$, $2\alpha \pmod{q}$, …, $q^2\alpha \pmod{q}$.

Map each one to which interval $[0,1)$, …, $[q-1,q)$ that it is in.

Some intervals has $\geq q$ of these values.

Two of those values are $\leq 1/q$ apart.

So there exists i,j such that $|i\alpha \pmod{q} - j\alpha \pmod{q}| \leq \frac{1}{q}$.

Upshot There exists $k \leq q^2$ such that $|k\alpha \pmod{q}| \leq \frac{1}{q}$.

We will consider two cases:

Case 1 $k \not\equiv 0 \pmod{q}$.

Case 2 $k \equiv 0 \pmod{q}$.

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \leq \frac{1}{q}$.

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \leq \frac{1}{q}$.

Plan

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \leq \frac{1}{q}$.

Plan

1) Show $x^2 + \beta \pmod{q}$ hits $\geq (q+1)/2$ intervals.

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \leq \frac{1}{q}$.

Plan

1) Show $x^2 + \beta \pmod{q}$ hits $\geq (q+1)/2$ intervals.
2) Show that adding αx has a small effect since $|k\alpha \pmod{q}| \leq \frac{1}{q}$.

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \le \frac{1}{q}$.

Plan

1) Show $x^2 + \beta \pmod{q}$ hits $\ge (q+1)/2$ intervals.
2) Show that adding αx has a small effect since $|k\alpha \pmod{q}| \le \frac{1}{q}$.

We consider several sets and see how many intervals they hit.

Case 1: $\mathbf{k \not\equiv 0 \pmod{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \le \frac{1}{q}$.

Plan

1) Show $x^2 + \beta \pmod{q}$ hits $\ge (q+1)/2$ intervals.
2) Show that adding αx has a small effect since $|k\alpha \pmod{q}| \le \frac{1}{q}$.

We consider several sets and see how many intervals they hit.

$\mathrm{SQ}_q = \{1^2 \pmod{q}, 2^2 \pmod{q}, \ldots, q^2 \pmod{q}\}$.

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \le \frac{1}{q}$.

Plan

1) Show $x^2 + \beta \pmod{q}$ hits $\ge (q+1)/2$ intervals.
2) Show that adding αx has a small effect since $|k\alpha \pmod{q}| \le \frac{1}{q}$.

We consider several sets and see how many intervals they hit.

$\mathrm{SQ}_q = \{1^2 \pmod{q}, 2^2 \pmod{q}, \ldots, q^2 \pmod{q}\}$.
q is a prime so squaring is 2-to-1. Hence $|\mathrm{SQ}_q| = (q+1)/2$.

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$

Recap There is a $k \not\equiv 0 \pmod{q}$ such that $|k\alpha \mod q| \le \frac{1}{q}$.

Plan

1) Show $x^2 + \beta \pmod{q}$ hits $\ge (q+1)/2$ intervals.
2) Show that adding αx has a small effect since $|k\alpha \pmod{q}| \le \frac{1}{q}$.

We consider several sets and see how many intervals they hit.

$\mathrm{SQ}_q = \{1^2 \pmod{q}, 2^2 \pmod{q}, \ldots, q^2 \pmod{q}\}$.
q is a prime so squaring is 2-to-1. Hence $|\mathrm{SQ}_q| = (q+1)/2$.
Since every element in SQ_q is an integer, hits $(q+1)/2$ intervals.

Case 1: $k \not\equiv 0 \pmod{q}$ (cont)

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$ (cont)

We consider $f_1(x) = x^2 + \beta \pmod{q}$.

Case 1: $k \not\equiv 0 \pmod{q}$ (cont)

We consider $f_1(x) = x^2 + \beta \pmod{q}$.

$$X = \{f_1(1), f_1(2), \ldots, f_1(q)\} = \{1^2 + \beta, 2^2 + \beta, \ldots, q^2 + \beta\}$$

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$ (cont)

We consider $f_1(x) = x^2 + \beta \pmod{q}$.

$$X = \{f_1(1), f_1(2), \ldots, f_1(q)\} = \{1^2 + \beta, 2^2 + \beta, \ldots, q^2 + \beta\}$$

Since X is the squares all shifted by β, $|X_1| = (q+1)/2$.

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$ (cont)

We consider $f_1(x) = x^2 + \beta \pmod{q}$.

$$X = \{f_1(1), f_1(2), \ldots, f_1(q)\} = \{1^2 + \beta, 2^2 + \beta, \ldots, q^2 + \beta\}$$

Since X is the squares all shifted by β, $|X_1| = (q+1)/2$.

$$Y = \{f_1(k), f_1(2k), \ldots, f_1(qk)\} = \{k^2+\beta, (2k)^2+\beta, \ldots, (qk)^2+\beta\}$$

Case 1: $\mathbf{k} \not\equiv \mathbf{0} \pmod{\mathbf{q}}$ (cont)

We consider $f_1(x) = x^2 + \beta \pmod{q}$.

$$X = \{f_1(1), f_1(2), \ldots, f_1(q)\} = \{1^2 + \beta, 2^2 + \beta, \ldots, q^2 + \beta\}$$

Since X is the squares all shifted by β, $|X_1| = (q+1)/2$.

$$Y = \{f_1(k), f_1(2k), \ldots, f_1(qk)\} = \{k^2 + \beta, (2k)^2 + \beta, \ldots, (qk)^2 + \beta\}$$

Since $k \not\equiv 0 \pmod{q}$, $\{k, 2k, \ldots, qk\} = \{1, 2, \ldots, q\}$. Hence $X = Y$.

Why $\mathbf{m = q^3}$?

We have shown that

$$\{f_1(k), f_1(2k), \ldots, f_1(qk)\}.$$

hits $(q+1)/2$ intervals. Note that $qk \leq q^3 = m$. This is why we needed $m = q^3$ in the hypothesis.

Why $\mathbf{m = q^3}$?

We have shown that

$$\{f_1(k), f_1(2k), \ldots, f_1(qk)\}.$$

hits $(q+1)/2$ intervals. Note that $qk \le q^3 = m$. This is why we needed $m = q^3$ in the hypothesis.

We need to show that $Z = \{f(1), f(2), \ldots, f(q^3)\}$
hits $\ge q/6$ intervals.

Why $\mathbf{m = q^3}$?

We have shown that

$$\{f_1(k), f_1(2k), \ldots, f_1(qk)\}.$$

hits $(q+1)/2$ intervals. Note that $qk \le q^3 = m$. This is why we needed $m = q^3$ in the hypothesis.

We need to show that $Z = \{f(1), f(2), \ldots, f(q^3)\}$
hits $\ge q/6$ intervals.

We will do this on the next slide.

Finishing Up Case 1

Finishing Up Case 1

$\{f_1(k), f_1(2k), \ldots, f_1(qk)\}$ hits $(q+1)/2$ intervals.

Finishing Up Case 1

$\{f_1(k), f_1(2k), \ldots, f_1(qk)\}$ hits $(q+1)/2$ intervals.

We show that $\{f(1), \ldots, f(q^3)\}$ hits $\geq q/6$ intervals by just looking at the subset $\{f(k), f(2k), \ldots, f(qk)\}$.

Finishing Up Case 1

$\{f_1(k), f_1(2k), \ldots, f_1(qk)\}$ hits $(q+1)/2$ intervals.

We show that $\{f(1), \ldots, f(q^3)\}$ hits $\geq q/6$ intervals by just looking at the subset $\{f(k), f(2k), \ldots, f(qk)\}$.

$\{f(k), f(2k), \ldots, f(qk)\}$:
$f(k) = f_1(k) + k\alpha$. **Key** Recall $k\alpha \pmod q)| \leq \frac{1}{q} \leq 1$.
$f(2k) = f_1(2k) + 2k\alpha$. **Key** Recall $2k\alpha \pmod q)| \leq \frac{2}{q} \leq 1$.

$\vdots \qquad \vdots$

$f(qk) = f_1(2k) + qk\alpha$. **Key** Recall $qk\alpha \pmod q)| \leq \frac{q}{q} \leq 1$.

Finishing Up Case 1

$\{f_1(k), f_1(2k), \ldots, f_1(qk)\}$ hits $(q+1)/2$ intervals.

We show that $\{f(1), \ldots, f(q^3)\}$ hits $\geq q/6$ intervals by just looking at the subset $\{f(k), f(2k), \ldots, f(qk)\}$.

$\{f(k), f(2k), \ldots, f(qk)\}$:
$f(k) = f_1(k) + k\alpha$. **Key** Recall $k\alpha \pmod{q})| \leq \frac{1}{q} \leq 1$.
$f(2k) = f_1(2k) + 2k\alpha$. **Key** Recall $2k\alpha \pmod{q})| \leq \frac{2}{q} \leq 1$.

$\vdots \qquad \vdots$

$f(qk) = f_1(2k) + qk\alpha$. **Key** Recall $qk\alpha \pmod{q})| \leq \frac{q}{q} \leq 1$.

Recap The set $Y = \{f_1(k), \ldots, f_1(qk)\}$ hits $(q+1)/2$ intervals of length 1.
$Z = \{f(k), \ldots, f(qk)\}$ can be viewed as taking every element in Y and adding or subtracting ≤ 1 to it. It is easy to show that Z hits $\geq q/6$ intervals.

Case 2: $\mathbf{k} \equiv \mathbf{0} \pmod{\mathbf{q}}$

OMITTED FOR NOW.

Another Lemma Of Independent Interest

The Sign Function and Other Notation

Def if $a \in \mathbb{R}$ then

The Sign Function and Other Notation

Def if $a \in \mathbb{R}$ then

$$\text{sign}(a) = \begin{cases} -1 & \text{if } a < 0 \\ 0 & \text{if } a = 0 \\ 1 & \text{if } a > 0 \end{cases} \tag{1}$$

The Sign Function and Other Notation

Def if $a \in \mathbb{R}$ then

$$\text{sign}(a) = \begin{cases} -1 & \text{if } a < 0 \\ 0 & \text{if } a = 0 \\ 1 & \text{if } a > 0 \end{cases} \tag{1}$$

Notation If $\eta \in \{-1, 0, 1\}^*$ then $\eta(i)$ is the ith character in η.

The Sign Pattern of a Polynomial: Intuitively

The Sign Pattern of a Polynomial: Intuitively

$$p_1(x, y) = x + 2y - 3 \qquad p_2(x, y) = -2x + 3y - 7$$
$$p_3(x, y) = 4x - y$$

The Sign Pattern of a Polynomial: Intuitively

$p_1(x, y) = x + 2y - 3 \qquad p_2(x, y) = -2x + 3y - 7$
$p_3(x, y) = 4x - y$

We care about $(\text{sign}(p_1(x, y)), \text{sign}(p_2(x, y)), \text{sign}(p_3(x, y)))$.

The Sign Pattern of a Polynomial: Intuitively

$p_1(x, y) = x + 2y - 3 \qquad p_2(x, y) = -2x + 3y - 7$
$p_3(x, y) = 4x - y$

We care about $(\mathrm{sign}(p_1(x, y)), \mathrm{sign}(p_2(x, y)), \mathrm{sign}(p_3(x, y)))$.

(x, y)	$(p_1(x, y), p_2(x, y), p_3(x, y))$	sign pattern
$(0, 0)$	$(-3, -7, 0)$	$(-, -, 0)$
$(10, 0)$	$(7, -27, 40)$	$(+, -, +)$
$(0, 10)$	$(17, 23, -10)$	$(+, +, -)$
$(1, 1)$	$(0, -6, 3)$	$(0, -, +)$
$(5, 10)$	$(22, 13, 30)$	$(+, +, +)$

There are $3^3 = 27$ sign patterns. (p_1, p_2, p_3) has at least 5.

The Sign Pattern of a Polynomial: Intuitively

$p_1(x, y) = x + 2y - 3 \qquad p_2(x, y) = -2x + 3y - 7$
$p_3(x, y) = 4x - y$

We care about $(\text{sign}(p_1(x, y)), \text{sign}(p_2(x, y)), \text{sign}(p_3(x, y)))$.

(x, y)	$(p_1(x, y), p_2(x, y), p_3(x, y))$	sign pattern
$(0, 0)$	$(-3, -7, 0)$	$(-, -, 0)$
$(10, 0)$	$(7, -27, 40)$	$(+, -, +)$
$(0, 10)$	$(17, 23, -10)$	$(+, +, -)$
$(1, 1)$	$(0, -6, 3)$	$(0, -, +)$
$(5, 10)$	$(22, 13, 30)$	$(+, +, +)$

There are $3^3 = 27$ sign patterns. (p_1, p_2, p_3) has at least 5.
I doubt it has anywhere near 27.

The Sign Pattern of a Polynomial: Formally

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.
Let $X = (p_1, \ldots, p_M)$.

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.
Let $X = (p_1, \ldots, p_M)$.
$\eta \in \{-, 0, +\}^M$ is a **sign pattern for** X if

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.
Let $X = (p_1, \ldots, p_M)$.
$\eta \in \{-, 0, +\}^M$ is a **sign pattern for X** if
there exists $a_1, a_2 \in \mathbb{R}$ such that for all $1 \le i \le M$

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.
Let $X = (p_1, \ldots, p_M)$.
$\eta \in \{-, 0, +\}^M$ is a **sign pattern for X** if
there exists $a_1, a_2 \in \mathbb{R}$ such that for all $1 \le i \le M$

$$\text{sign}(p_i(a_1, a_2)) = \eta(i).$$

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.
Let $X = (p_1, \ldots, p_M)$.
$\eta \in \{-, 0, +\}^M$ is a **sign pattern for** X if
there exists $a_1, a_2 \in \mathbb{R}$ such that for all $1 \le i \le M$

$$\mathrm{sign}(p_i(a_1, a_2)) = \eta(i).$$

Note Obvious bound on number of sign patterns: 3^M

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.
Let $X = (p_1, \ldots, p_M)$.
$\eta \in \{-, 0, +\}^M$ is a **sign pattern for X** if
there exists $a_1, a_2 \in \mathbb{R}$ such that for all $1 \le i \le M$

$$\text{sign}(p_i(a_1, a_2)) = \eta(i).$$

Note Obvious bound on number of sign patterns: 3^M
Question Is there a better bound?

The Sign Pattern of a Polynomial: Formally

Def Let $p_1, \ldots, p_M \in \mathbb{R}[x, y]$.
Let $X = (p_1, \ldots, p_M)$.
$\eta \in \{-, 0, +\}^M$ is a **sign pattern for X** if
there exists $a_1, a_2 \in \mathbb{R}$ such that for all $1 \leq i \leq M$

$$\text{sign}(p_i(a_1, a_2)) = \eta(i).$$

Note Obvious bound on number of sign patterns: 3^M
Question Is there a better bound? Yes!

Lemma About Sign Patterns

Lemma Let $M \in \mathbb{N}$. Let $p_1, \ldots, p_M \in \mathbb{Z}[x, y]$.

Lemma About Sign Patterns

Lemma Let $M \in \mathbb{N}$. Let $p_1, \ldots, p_M \in \mathbb{Z}[x, y]$.
The number of sign patterns is $\leq 25M^2$.

Lemma About Sign Patterns

Lemma Let $M \in \mathbb{N}$. Let $p_1, \ldots, p_M \in \mathbb{Z}[x, y]$.
The number of sign patterns is $\leq 25M^2$.
Proof Omitted thought it is not hard.

Lemma About Sign Patterns

Lemma Let $M \in \mathbb{N}$. Let $p_1, \ldots, p_M \in \mathbb{Z}[x, y]$.
The number of sign patterns is $\leq 25M^2$.
Proof Omitted thought it is not hard.

Lemma also a corollary of a theorem by
Olenik-Petrovsky-Thom-Milnor.

Image-Solution

Let $p_1(z_1, z_2)$, . . ., $p_m(z_1.z_2) \in \mathbb{Z}[z_1, z_2]$. We denote this set of polynomials by F.

Image-Solution

Let $p_1(z_1, z_2)$, ..., $p_m(z_1.z_2) \in \mathbb{Z}[z_1, z_2]$. We denote this set of polynomials by F.

1) An **image-solution of F** is just $(a, d; y_1, \ldots, y_m)$ where $(\forall 1 \leq i \leq m)[y_i = p_i(a, d)]$.

Image-Solution

Let $p_1(z_1, z_2)$, ..., $p_m(z_1.z_2) \in \mathbb{Z}[z_1, z_2]$. We denote this set of polynomials by F.

1) An **image-solution of F** is just $(a, d; y_1, \ldots, y_m)$ where $(\forall 1 \le i \le m)[y_i = p_i(a, d)]$.

2) Assume the reals are 2-colored. Then a **mono image-solution of F** is an image-solution $(a, d; y_1, \ldots, y_m)$ where $y_1, \ldots, y_m$ are all the same color. Note that a, d need not be that color.

Image-Solution

Let $p_1(z_1, z_2)$, ..., $p_m(z_1.z_2) \in \mathbb{Z}[z_1, z_2]$. We denote this set of polynomials by F.

1) An **image-solution of F** is just $(a, d; y_1, \ldots, y_m)$ where $(\forall 1 \le i \le m)[y_i = p_i(a, d)]$.

2) Assume the reals are 2-colored. Then a **mono image-solution of F** is an image-solution $(a, d; y_1, \ldots, y_m)$ where $y_1, \ldots, y_m$ are all the same color. Note that a, d need not be that color.

3) A **Red image-solution of F** and a **Blue image-solution of F** obvious.

We Skip Lots of Steps To Get To

We show that if prob of **B** is $1 - q^{-1/2}$ then an no BLUE solution to a set of m equations.

We Skip Lots of Steps To Get To

We show that if prob of **B**is $1 - q^{-1/2}$ then an no BLUE solution to a set of m equations.

We skip a lot of steps.

We Skip Lots of Steps To Get To

We show that if prob of **B**is $1 - q^{-1/2}$ then an no BLUE solution to a set of m equations.

We skip a lot of steps.

We find a bound on a prob so that there is no **blue image-solution** to a set of polys.

We Skip Lots of Steps To Get To

We show that if prob of **B**is $1 - q^{-1/2}$ then an no BLUE solution to a set of m equations.

We skip a lot of steps.

We find a bound on a prob so that there is no **blue image-solution** to a set of polys.

This turns out to be equivalent.

We Skip Lots of Steps To Get To

We show that if prob of **B**is $1 - q^{-1/2}$ then an no BLUE solution to a set of m equations.

We skip a lot of steps.

We find a bound on a prob so that there is no **blue image-solution** to a set of polys.

This turns out to be equivalent.

I am skipping some stuff of interest to get to some stuff that is of more interest.

The Important Lemma

Let q be a prime and let $m = q^3$.

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

2) Coefficients of $p_i(z_1, z_2)$ are quadratic polynomials in i over $\mathbb{Z}$.

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

2) Coefficients of $p_i(z_1, z_2)$ are quadratic polynomials in i over $\mathbb{Z}$.

3) If $a, d \in [0, q]$ then, for all i, $0 \le p_i(a, d) \le 2m^2$

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

2) Coefficients of $p_i(z_1, z_2)$ are quadratic polynomials in i over $\mathbb{Z}$.

3) If $a, d \in [0, q]$ then, for all i, $0 \leq p_i(a, d) \leq 2m^2$

Let b, r be such that $0 \leq b, r \leq 1$ and $b + r = 1$.

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

2) Coefficients of $p_i(z_1, z_2)$ are quadratic polynomials in i over $\mathbb{Z}$.

3) If $a, d \in [0, q]$ then, for all i, $0 \le p_i(a, d) \le 2m^2$

Let b, r be such that $0 \le b, r \le 1$ and $b + r = 1$.

Let COL' be a rand 2-col of $\mathbb{Z}_q$: prob(BLUE)=b, prob(RED)=r.

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

2) Coefficients of $p_i(z_1, z_2)$ are quadratic polynomials in i over $\mathbb{Z}$.

3) If $a, d \in [0, q]$ then, for all i, $0 \le p_i(a, d) \le 2m^2$

Let b, r be such that $0 \le b, r \le 1$ and $b + r = 1$.

Let COL' be a rand 2-col of $\mathbb{Z}_q$: prob(BLUE)=b, prob(RED)=r.
Let $\mathrm{COL}(z) = \mathrm{COL}'(z \bmod q)$.

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

2) Coefficients of $p_i(z_1, z_2)$ are quadratic polynomials in i over $\mathbb{Z}$.

3) If $a, d \in [0, q]$ then, for all i, $0 \le p_i(a, d) \le 2m^2$

Let b, r be such that $0 \le b, r \le 1$ and $b + r = 1$.

Let COL' be a rand 2-col of $\mathbb{Z}_q$: prob(BLUE)=b, prob(RED)=r.
Let $\mathrm{COL}(z) = \mathrm{COL}'(z \bmod q)$.
THEN

The Important Lemma

Let q be a prime and let $m = q^3$.

Let $p_1(z_1, z_2), \ldots, p_m(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$ be such that:

1) For all i, $p_i(z_1, z_2)$ is linear in z_1, z_2.

2) Coefficients of $p_i(z_1, z_2)$ are quadratic polynomials in i over $\mathbb{Z}$.

3) If $a, d \in [0, q]$ then, for all i, $0 \le p_i(a, d) \le 2m^2$

Let b, r be such that $0 \le b, r \le 1$ and $b + r = 1$.

Let COL' be a rand 2-col of $\mathbb{Z}_q$: prob(BLUE)=b, prob(RED)=r.
Let $\mathrm{COL}(z) = \mathrm{COL}'(z \bmod q)$.
THEN
prob there is a **blue image-solution** to $p_1, \ldots, p_m$ is
$\le 2500 m^6 b^{m/6}$.

PART ONE: Intervals

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.
If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B}$) then:

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.

If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:

1) $p_1(a,d)$ mod q is in int that COL' colors $\mathbf{B}$. Prob b.

$\vdots \qquad \vdots \qquad \vdots$

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.

If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:

1) $p_1(a,d)$ mod q is in int that COL' colors $\mathbf{B}$. Prob b.

$\vdots \qquad \vdots \qquad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors $\mathbf{B}$. Prob b.

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.
If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:
1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.
$\vdots \quad \vdots \quad \vdots$
m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m.

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.
If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:
1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.

$\vdots \qquad \vdots \qquad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small!

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.
If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:
1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.

$\vdots \qquad \vdots \qquad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small! Good!

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \textbf{B})$.
If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \textbf{B})$ then:
1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.
$\vdots \quad \vdots \quad \vdots$
m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small! Good! Alas No.

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.

If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B}$) then:

1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.

$\vdots \quad \vdots \quad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small! Good! Alas No.

If all of the $p_i(a,d)$ mod q in same int then Prob just b.

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.

If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:

1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.

$\vdots \quad \vdots \quad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small! Good! Alas No.

If all of the $p_i(a,d)$ mod q in same int then Prob just b.

How many distinct intervals do we get?

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.

If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:

1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.

$\vdots \qquad \vdots \qquad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small! Good! Alas No.

If all of the $p_i(a,d)$ mod q in same int then Prob just b.

How many distinct intervals do we get?

By earlier Int theorem intersect $\geq q/6$ ints.

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$.
If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B})$ then:
1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.

$\vdots \quad \vdots \quad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small! Good! Alas No.

If all of the $p_i(a,d)$ mod q in same int then Prob just b.

How many distinct intervals do we get?

By earlier Int theorem intersect $\geq q/6$ ints.

$\{p_1(a,d) \bmod q, \ldots, p_m(a,d) \bmod q\}$ will int $\geq q/6$ intervals.

PART ONE: Intervals

We want to bound
$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \textbf{B})$.

If $\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \textbf{B})$ then:

1) $p_1(a,d)$ mod q is in int that COL' colors **B**. Prob b.

$\vdots \quad \vdots \quad \vdots$

m) $p_m(a,d)$ mod q is in an int that COL' colors **B**. Prob b.
Might think prob is b^m. Small! Good! Alas No.

If all of the $p_i(a,d)$ mod q in same int then Prob just b.

How many distinct intervals do we get?

By earlier Int theorem intersect $\ge q/6$ ints.

$\{p_1(a,d) \bmod q, \ldots, p_m(a,d) \bmod q\}$ will int $\ge q/6$ intervals.

$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \textbf{B}) \le b^{q/6}$.

PART TWO: How Many Sets of Intervals?

$$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B}) \le b^{q/6}.$$

is not about a, d: its about interval patterns.

PART TWO: How Many Sets of Intervals?

$$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B}) \le b^{q/6}.$$

is not about a, d: its about interval patterns.

We map a, d to the set of intervals mod q that

PART TWO: How Many Sets of Intervals?

$$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B}) \le b^{q/6}.$$

is not about a, d: its about interval patterns.

We map a, d to the set of intervals mod q that

$p_1(a,d)$ mod $q, \ldots, p_m(a,d)$ mod q are in.

PART TWO: How Many Sets of Intervals?

$$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B}) \le b^{q/6}.$$

is not about a, d: its about interval patterns.

We map a, d to the set of intervals mod q that

$p_1(a,d)$ mod $q, \ldots, p_m(a,d)$ mod q are in.

Prob that ANY of those sets of ints are BLUE is

$\le$ (Number of sets of intervals) $\times b^{q/6}$

PART TWO: How Many Sets of Intervals?

$$\Pr(\mathrm{COL}(p_1(a,d)) = \cdots = \mathrm{COL}(p_m(a,d)) = \mathbf{B}) \le b^{q/6}.$$

is not about a, d: its about interval patterns.

We map a, d to the set of intervals mod q that

$p_1(a,d)$ mod $q, \ldots, p_m(a,d)$ mod q are in.

Prob that ANY of those sets of ints are BLUE is

$\le$ (Number of sets of intervals) $\times b^{q/6}$

Need number of intervals

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \leq p_i(a, d) \leq 2m^2$.

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \leq p_i(a, d) \leq 2m^2$.

We now ask about the intervals (not mod q).

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \leq p_i(a, d) \leq 2m^2$.

We now ask about the intervals (not mod q).

1) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_1(a, d)$? There are $2m^2$ possibilities.

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \le p_i(a, d) \le 2m^2$.

We now ask about the intervals (not mod q).

1) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_1(a, d)$? There are $2m^2$ possibilities.

Which ints can be determined from the sign changes of:

$$p_1(a, d) - 1, p_1(a, d) - 2, \ldots, p_1(a, d) - 2m^2.$$

$\vdots \quad \vdots \quad \vdots$

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \le p_i(a, d) \le 2m^2$.

We now ask about the intervals (not mod q).

1) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_1(a, d)$? There are $2m^2$ possibilities.

Which ints can be determined from the sign changes of:

$$p_1(a, d) - 1, p_1(a, d) - 2, \ldots, p_1(a, d) - 2m^2.$$

$\vdots \quad \vdots \quad \vdots$

m) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_m(a, d)$? There are $2m^2$ possibilities.
Which ints can be determined from the sign changes of:

$$p_m(a, d) - 1, p_m(a, d) - 2, \ldots, p_m(a, d) - 2m^2.$$

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \le p_i(a, d) \le 2m^2$.

We now ask about the intervals (not mod q).

1) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_1(a, d)$? There are $2m^2$ possibilities.

Which ints can be determined from the sign changes of:

$$p_1(a, d) - 1, p_1(a, d) - 2, \ldots, p_1(a, d) - 2m^2.$$

$\vdots \quad \vdots \quad \vdots$

m) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_m(a, d)$? There are $2m^2$ possibilities.
Which ints can be determined from the sign changes of:

$$p_m(a, d) - 1, p_m(a, d) - 2, \ldots, p_m(a, d) - 2m^2.$$

Seems like there are $(2m^2)^m$ possibilities.

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \le p_i(a, d) \le 2m^2$.

We now ask about the intervals (not mod q).

1) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_1(a, d)$? There are $2m^2$ possibilities.

Which ints can be determined from the sign changes of:

$$p_1(a, d) - 1, p_1(a, d) - 2, \ldots, p_1(a, d) - 2m^2.$$

$\vdots \qquad \vdots \qquad \vdots$

m) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_m(a, d)$? There are $2m^2$ possibilities.
Which ints can be determined from the sign changes of:

$$p_m(a, d) - 1, p_m(a, d) - 2, \ldots, p_m(a, d) - 2m^2.$$

Seems like there are $(2m^2)^m$ possibilities. Big.

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \le p_i(a, d) \le 2m^2$.

We now ask about the intervals (not mod q).

1) Of the ints $[0, 1)$, $[1, 2)$, …, $[2m^2 - 1, 2m^2)$ which one has $p_1(a, d)$? There are $2m^2$ possibilities.

Which ints can be determined from the sign changes of:

$$p_1(a, d) - 1, p_1(a, d) - 2, \ldots, p_1(a, d) - 2m^2.$$

$\vdots \qquad \vdots \qquad \vdots$

m) Of the ints $[0, 1)$, $[1, 2)$, …, $[2m^2 - 1, 2m^2)$ which one has $p_m(a, d)$? There are $2m^2$ possibilities.
Which ints can be determined from the sign changes of:

$$p_m(a, d) - 1, p_m(a, d) - 2, \ldots, p_m(a, d) - 2m^2.$$

Seems like there are $(2m^2)^m$ possibilities. Big. Bad for us.

PART TWO: Counting the Number of Intervals

Since the coloring is mod q we can assume $a, d \in [0, q)$.

By premise, $0 \le p_i(a, d) \le 2m^2$.

We now ask about the intervals (not mod q).

1) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_1(a, d)$? There are $2m^2$ possibilities.

Which ints can be determined from the sign changes of:

$$p_1(a, d) - 1, p_1(a, d) - 2, \ldots, p_1(a, d) - 2m^2.$$

$\vdots \qquad \vdots \qquad \vdots$

m) Of the ints $[0, 1)$, $[1, 2)$, ..., $[2m^2 - 1, 2m^2)$ which one has $p_m(a, d)$? There are $2m^2$ possibilities.
Which ints can be determined from the sign changes of:

$$p_m(a, d) - 1, p_m(a, d) - 2, \ldots, p_m(a, d) - 2m^2.$$

Seems like there are $(2m^2)^m$ possibilities. Big. Bad for us. Boo!

PART TWO: Counting the Number of Intervals (cont)

Consider the sequence of polynomials

PART TWO: Counting the Number of Intervals (cont)

Consider the sequence of polynomials

$$p_1(z_1, z_2) - 1, \ldots, p_1(z_1, z_2) - 2m^2,$$

PART TWO: Counting the Number of Intervals (cont)

Consider the sequence of polynomials

$$p_1(z_1, z_2) - 1, \ldots, p_1(z_1, z_2) - 2m^2,$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots$$

$$p_m(z_1, z_2) - 1, \ldots, p_m(z_1, z_2) - 2m^2.$$

PART TWO: Counting the Number of Intervals (cont)

Consider the sequence of polynomials

$$p_1(z_1, z_2) - 1, \ldots, p_1(z_1, z_2) - 2m^2,$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$p_m(z_1, z_2) - 1, \ldots, p_m(z_1, z_2) - 2m^2.$$

Max numb of sign changes in this sequence is upper bound on numb of ways $p_1(a, d)$, ..., $p_m(a, d)$ can be in the intervals.

PART TWO: Counting the Number of Intervals (cont)

Consider the sequence of polynomials

$$p_1(z_1, z_2) - 1, \ldots, p_1(z_1, z_2) - 2m^2,$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$p_m(z_1, z_2) - 1, \ldots, p_m(z_1, z_2) - 2m^2.$$

Max numb of sign changes in this sequence is upper bound on numb of ways $p_1(a, d)$, ..., $p_m(a, d)$ can be in the intervals.

By Sign Pattern Lemma, this is $\leq 625(2m^3)^2 = 2500m^6$.

PART TWO: Counting the Number of Intervals (cont)

Consider the sequence of polynomials

$$p_1(z_1, z_2) - 1, \ldots, p_1(z_1, z_2) - 2m^2,$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$p_m(z_1, z_2) - 1, \ldots, p_m(z_1, z_2) - 2m^2.$$

Max numb of sign changes in this sequence is upper bound on numb of ways $p_1(a, d)$, ..., $p_m(a, d)$ can be in the intervals.

By Sign Pattern Lemma, this is $\le 625(2m^3)^2 = 2500m^6$.

Number of ways $p_1(a, d), \ldots, p_m(a, d)$ are in the ints is $\le 2500m^6$.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\leq 2500 m^6 b^{q/6}$.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\le 2500 m^6 b^{q/6}$.

Take $m = q^3$ and $b = 1 - q^{-1/2} \sim e^{q^{-1/2}}$.
$b^{q/6} \sim (e^{q^{-1/2}})^{q/6} = e^{q^{-3q}}$.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\le 2500m^6 b^{q/6}$.

Take $m = q^3$ and $b = 1 - q^{-1/2} \sim e^{q^{-1/2}}$.
$b^{q/6} \sim (e^{q^{-1/2}})^{q/6} = e^{q^{-3q}}$.

Prob is $\le 2500m^6 b^{q/6} = 2500(q^3)^6 e^{q^{-3q}} \sim 2500\frac{q^{18}}{e^{q^{3q}}}$.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\le 2500 m^6 b^{q/6}$.

Take $m = q^3$ and $b = 1 - q^{-1/2} \sim e^{q^{-1/2}}$.
$b^{q/6} \sim (e^{q^{-1/2}})^{q/6} = e^{q^{-3q}}$.

Prob is $\le 2500 m^6 b^{q/6} = 2500(q^3)^6 e^{q^{-3q}} \sim 2500 \frac{q^{18}}{e^{q^{3q}}}$.

For q large enough this Prob is $< \frac{1}{2}$.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\leq 2500m^6 b^{q/6}$.

Take $m = q^3$ and $b = 1 - q^{-1/2} \sim e^{q^{-1/2}}$.
$b^{q/6} \sim (e^{q^{-1/2}})^{q/6} = e^{q^{-3q}}$.

Prob is $\leq 2500m^6 b^{q/6} = 2500(q^3)^6 e^{q^{-3q}} \sim 2500\frac{q^{18}}{e^{q^{3q}}}$.

For q large enough this Prob is $< \frac{1}{2}$.

Prob of **R**is $q^{-1/2}$. Implies Prob of **R**sol to $y_1 + y_3 = 2y_2 + 2$ is $< \frac{1}{2}$.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\le 2500m^6b^{q/6}$.

Take $m = q^3$ and $b = 1 - q^{-1/2} \sim e^{q^{-1/2}}$.
$b^{q/6} \sim (e^{q^{-1/2}})^{q/6} = e^{q^{-3q}}$.

Prob is $\le 2500m^6b^{q/6} = 2500(q^3)^6e^{q^{-3q}} \sim 2500\frac{q^{18}}{e^{q^{3q}}}$.

For q large enough this Prob is $< \frac{1}{2}$.

Prob of **R**is $q^{-1/2}$. Implies Prob of **R**sol to $y_1 + y_3 = 2y_2 + 2$ is $< \frac{1}{2}$.

Prob of **B**is $1 - q^{1/2}$. Implies Prob of **B**image-Sol is $< \frac{1}{2}$.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\le 2500m^6 b^{q/6}$.

Take $m = q^3$ and $b = 1 - q^{-1/2} \sim e^{q^{-1/2}}$.
$b^{q/6} \sim (e^{q^{-1/2}})^{q/6} = e^{q^{-3q}}$.

Prob is $\le 2500m^6 b^{q/6} = 2500(q^3)^6 e^{q^{-3q}} \sim 2500\frac{q^{18}}{e^{q^{3q}}}$.

For q large enough this Prob is $< \frac{1}{2}$.

Prob of **R**is $q^{-1/2}$. Implies Prob of **R**sol to $y_1 + y_3 = 2y_2 + 2$ is $< \frac{1}{2}$.

Prob of **B**is $1 - q^{1/2}$. Implies Prob of **B**image-Sol is $< \frac{1}{2}$.

Last line implies Prob of **B** solution to
$(\forall 2 \le lem - 2)[y_{i-1} + y_{i+2} = 2y_i + 2]$ is $\le \frac{1}{2}$ for large enough m.

COMBINE PARTS ONE AND TWO

Prob there is a **blue image-sol** is $\le 2500 m^6 b^{q/6}$.

Take $m = q^3$ and $b = 1 - q^{-1/2} \sim e^{q^{-1/2}}$.
$b^{q/6} \sim (e^{q^{-1/2}})^{q/6} = e^{q^{-3q}}$.

Prob is $\le 2500 m^6 b^{q/6} = 2500 (q^3)^6 e^{q^{-3q}} \sim 2500 \frac{q^{18}}{e^{q^{3q}}}$.

For q large enough this Prob is $< \frac{1}{2}$.

Prob of **R**is $q^{-1/2}$. Implies Prob of **R**sol to $y_1 + y_3 = 2y_2 + 2$ is $< \frac{1}{2}$.

Prob of **B**is $1 - q^{1/2}$. Implies Prob of **B**image-Sol is $< \frac{1}{2}$.

Last line implies Prob of **B** solution to
$(\forall 2 \le lem - 2)[y_{i-1} + y_{i+2} = 2y_i + 2]$ is $\le \frac{1}{2}$ for large enough m.

Hence there exists a 2-coloring with no **R**ℓ_3 or **B**ℓ_m for large enough m.