Embedding Quadratic Fields into Quaternion Algebras

Rose Mintzer-Sweeney, Alexander Schlesinger, Katherine Xiu

August 4, 2016

Overview

Quadratic Fields

Definition

A quadratic field is the set

$$\mathbb{Q}(\sqrt{k}) = \{a + b\sqrt{k} : a, b \in \mathbb{Q}\}$$

with the usual addition and multiplication. Here k is a squarefree integer other than 0 or 1.

Rational Quaternion Algebras

Definition

A quaternion algebra is the set of all elements

$$\left(\frac{m, n}{\mathbb{Q}}\right) = \{a + bi + cj + dij : a, b, c, d \in \mathbb{Q}\}$$

with component-wise addition and multiplication defined by

Rational Quaternion Algebras

Definition

A quaternion algebra is the set of all elements

$$\left(\frac{m, n}{\mathbb{Q}}\right) = \{a + bi + cj + dij : a, b, c, d \in \mathbb{Q}\}$$

with component-wise addition and multiplication defined by

- $i^2 = m$,

Rational Quaternion Algebras

Definition

A quaternion algebra is the set of all elements

$$\left(\frac{m, n}{\mathbb{Q}}\right) = \{a + bi + cj + dij : a, b, c, d \in \mathbb{Q}\}$$

with component-wise addition and multiplication defined by

- $i^2 = m$,
- $j^2 = n$,

Rational Quaternion Algebras

Definition

A quaternion algebra is the set of all elements

$$\left(\frac{m, n}{\mathbb{Q}}\right) = \{a + bi + cj + dij : a, b, c, d \in \mathbb{Q}\}$$

with component-wise addition and multiplication defined by

- $i^2 = m$,
- $j^2 = n$,
- $ij = -ji$.

Rational Quaternion Algebras

Definition

A quaternion algebra is the set of all elements

$$\left(\frac{m,n}{\mathbb{Q}}\right) = \{a + bi + cj + dij : a, b, c, d \in \mathbb{Q}\}$$

with component-wise addition and multiplication defined by

- $i^2 = m$,
- $j^2 = n$,
- $ij = -ji$.

Here m, n are again squarefree integers other than 0 or 1.

Rational Quaternion Algebras

Definition

A quaternion algebra is the set of all elements

$$\left(\frac{m,n}{\mathbb{Q}}\right) = \{a + bi + cj + dij : a, b, c, d \in \mathbb{Q}\}$$

with component-wise addition and multiplication defined by

- $i^2 = m$,
- $j^2 = n$,
- $ij = -ji$.

Here m, n are again squarefree integers other than 0 or 1.

ij is often written as k.

Examples of Rational Quaternion Algebras

Example

The classic example is $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, the Hamiltonian quaternions. Here $i^2 = j^2 = (ij)^2 = -1$.

Examples of Rational Quaternion Algebras

Example

The classic example is $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, the Hamiltonian quaternions. Here $i^2 = j^2 = (ij)^2 = -1$.

Example

A more unusual example is $\left(\frac{2,-3}{\mathbb{Q}}\right)$. Here $i^2 = 2$, $j^2 = -3$, and $(ij)^2 = 6$.

Embeddings

Definition

We say $\mathbb{Q}(\sqrt{k})$ **embeds** into a quaternion algebra $\left(\frac{m,n}{\mathbb{Q}}\right)$ if there exists an injective ring homomorphism $\phi : \mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$.

Embeddings

Definition

We say $\mathbb{Q}(\sqrt{k})$ **embeds** into a quaternion algebra $\left(\frac{m,n}{\mathbb{Q}}\right)$ if there exists an injective ring homomorphism $\phi : \mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$.

For fixed k, we are interested in knowing for which (m, n) there is such an embedding.

Examples of Embeddings

Let $k = -1$.

Examples of Embeddings

Let $k = -1$.

Example

$$\mathbb{Q}(\sqrt{-1}) \to \left(\frac{-1,-1}{\mathbb{Q}}\right)$$

$$a + b\sqrt{-1} \mapsto a + bi$$

Examples of Embeddings

Let $k = -1$.

Example

$$\mathbb{Q}(\sqrt{-1}) \to \left(\frac{-1,-1}{\mathbb{Q}}\right)$$

$$a + b\sqrt{-1} \mapsto a + bi$$

Example

$$\mathbb{Q}(\sqrt{-1}) \to \left(\frac{2,-3}{\mathbb{Q}}\right)$$

$$a + b\sqrt{-1} \mapsto a + b(i + j)$$

An Equivalent Condition

- There is an equivalent, easier to check condition for the existence of ϕ.

An Equivalent Condition

- There is an equivalent, easier to check condition for the existence of ϕ.
- The embedding exists iff $\exists \omega \in \left(\frac{m,n}{\mathbb{Q}}\right)$ such that $\omega^2 = k$.

An Equivalent Condition

- There is an equivalent, easier to check condition for the existence of ϕ.
- The embedding exists iff $\exists \omega \in \left(\frac{m,n}{\mathbb{Q}}\right)$ such that $\omega^2 = k$.
- Given ω, the corresponding map is $\phi : a + b\sqrt{k} \to a + b\omega$.

An Equivalent Condition

- There is an equivalent, easier to check condition for the existence of ϕ.
- The embedding exists iff $\exists \omega \in \left(\frac{m,n}{\mathbb{Q}}\right)$ such that $\omega^2 = k$.
- Given ω, the corresponding map is $\phi : a + b\sqrt{k} \to a + b\omega$.
- The other direction is similar.

Reduction to Quadratic Forms

- One can check that for any ω such that $\omega^2 = k$, $Re(\omega) = 0$.

Reduction to Quadratic Forms

- One can check that for any ω such that $\omega^2 = k$, $Re(\omega) = 0$.
- Write $\omega = xi + yj + zij$. We can check that

Reduction to Quadratic Forms

- One can check that for any ω such that $\omega^2 = k$, $Re(\omega) = 0$.
- Write $\omega = xi + yj + zij$. We can check that

$$\begin{aligned} -k &= -\omega^2 \\ &= mx^2 + ny^2 + mnz^2 \end{aligned}$$

Reduction to Quadratic Forms

- One can check that for any ω such that $\omega^2 = k$, $Re(\omega) = 0$.
- Write $\omega = xi + yj + zij$. We can check that

$$\begin{aligned} -k &= -\omega^2 \\ &= mx^2 + ny^2 + mnz^2 \end{aligned}$$

- Clearing denominators, we see that there exists ω such that $\omega^2 = k$ iff

Reduction to Quadratic Forms

- One can check that for any ω such that $\omega^2 = k$, $Re(\omega) = 0$.
- Write $\omega = xi + yj + zij$. We can check that

$$\begin{aligned} -k &= -\omega^2 \\ &= mx^2 + ny^2 + mnz^2 \end{aligned}$$

- Clearing denominators, we see that there exists ω such that $\omega^2 = k$ iff

$$kW^2 - mX^2 - nY^2 + mnZ^2 = 0$$

for some $W, X, Y, Z \in \mathbb{Z}$ not all zero.

Hasse-Minkowski

There are well-developed tools for handling a problem like this. We depend on two main theorems.

Hasse-Minkowski

There are well-developed tools for handling a problem like this. We depend on two main theorems.

Theorem (Hasse-Minkowski)

Given an integer quadratic form $Q(x)$, $Q(x) = 0$ has non-zero integer solutions if and only if

Hasse-Minkowski

There are well-developed tools for handling a problem like this. We depend on two main theorems.

Theorem (Hasse-Minkowski)

Given an integer quadratic form $Q(x)$, $Q(x) = 0$ has non-zero integer solutions if and only if

- *$Q(x) = 0$ has non-zero real solutions, and*

Hasse-Minkowski

There are well-developed tools for handling a problem like this. We depend on two main theorems.

Theorem (Hasse-Minkowski)

Given an integer quadratic form $Q(x)$, $Q(x) = 0$ has non-zero integer solutions if and only if

- $Q(x) = 0$ *has non-zero real solutions, and*
- $Q(x) = 0$ *has non-zero solutions in* $\mathbb{Z}_p$ *for every prime* p.

Hasse-Minkowski

There are well-developed tools for handling a problem like this. We depend on two main theorems.

Theorem (Hasse-Minkowski)

Given an integer quadratic form $Q(x)$, $Q(x) = 0$ has non-zero integer solutions if and only if

- $Q(x) = 0$ *has non-zero real solutions, and*
- $Q(x) = 0$ *has non-zero solutions in* $\mathbb{Z}_p$ *for every prime* p.

Checking whether there are real solutions is easy.

Hensel's Lemma

Checking whether there are p-adic solutions is also tractable.

Hensel's Lemma

Checking whether there are p-adic solutions is also tractable.

Theorem (Hensel's Lemma)

Let $P(x)$ be an integer polynomial. Suppose $P(x_0) = 0 \mod p^n$ and $P'(x_0) \neq 0 \mod p$. Then $\exists \tilde{x_0} \in \mathbb{Z}_p$ such that $P(\tilde{x_0}) = 0$.

Hensel's Lemma

Checking whether there are p-adic solutions is also tractable.

Theorem (Hensel's Lemma)

Let $P(x)$ be an integer polynomial. Suppose $P(x_0) = 0 \mod p^n$ and $P'(x_0) \neq 0 \mod p$. Then $\exists \tilde{x_0} \in \mathbb{Z}_p$ such that $P(\tilde{x_0}) = 0$.

So, we can lift solutions modulo p into solutions in $\mathbb{Z}_p$.

Legendre Symbol

Recall that:

Definition

For an odd prime p and an integer x, the Legendre symbol is defined by

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } p \mid x \\ 1 & \text{if } \exists y \text{ s.t. } x \equiv y^2 \mod p \\ -1 & \text{otherwise} \end{cases}.$$

Conditions

Theorem (Ehrman, Mintzer-Sweeney, Schlesinger, Sheydvasser, Xiu 2016)

There exists an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ *iff the following conditions are met*

Conditions

Theorem (Ehrman, Mintzer-Sweeney, Schlesinger, Sheydvasser, Xiu 2016)

There exists an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ *iff the following conditions are met*

1. *(Conditions from* $\mathbb{R}$*-analysis) If* $m < 0$ *and* $n < 0$*, then* $k < 0$*.*

Conditions

Theorem (Ehrman, Mintzer-Sweeney, Schlesinger, Sheydvasser, Xiu 2016)

There exists an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ *iff the following conditions are met*

1. *(Conditions from* $\mathbb{R}$*-analysis) If* $m < 0$ *and* $n < 0$*, then* $k < 0$*.*
2. *(Conditions from* $\mathbb{Z}_p$*,* $p \neq 2$*) If* $p \nmid k$ *is an odd prime and* $\left(\frac{k}{p}\right) = 1$*, then*

Conditions

Theorem (Ehrman, Mintzer-Sweeney, Schlesinger, Sheydvasser, Xiu 2016)

There exists an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ *iff the following conditions are met*

1. *(Conditions from* $\mathbb{R}$*-analysis) If* $m < 0$ *and* $n < 0$*, then* $k < 0$*.*
2. *(Conditions from* $\mathbb{Z}_p$*,* $p \neq 2$*) If* $p \nmid k$ *is an odd prime and* $\left(\frac{k}{p}\right) = 1$*, then*
   - *If* $p \mid m$*,* $p \mid n$*, then* $\left(\frac{\frac{-m}{p} \cdot \frac{n}{p}}{p}\right) = 1$*.*

Conditions

Theorem (Ehrman, Mintzer-Sweeney, Schlesinger, Sheydvasser, Xiu 2016)

There exists an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ *iff the following conditions are met*

1. *(Conditions from* $\mathbb{R}$*-analysis) If* $m < 0$ *and* $n < 0$*, then* $k < 0$*.*
2. *(Conditions from* $\mathbb{Z}_p$*,* $p \neq 2$*) If* $p \nmid k$ *is an odd prime and* $\left(\frac{k}{p}\right) = 1$*, then*
   - *If* $p \mid m$*,* $p \mid n$*, then* $\left(\frac{\frac{-m}{p} \cdot \frac{n}{p}}{p}\right) = 1$*.*
   - *If* $p \mid m$*,* $p \nmid n$*, then* $\left(\frac{n}{p}\right) = 1$*.*

Conditions

Theorem (Ehrman, Mintzer-Sweeney, Schlesinger, Sheydvasser, Xiu 2016)

There exists an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ *iff the following conditions are met*

1. *(Conditions from* $\mathbb{R}$*-analysis) If* $m < 0$ *and* $n < 0$*, then* $k < 0$*.*
2. *(Conditions from* $\mathbb{Z}_p$*,* $p \neq 2$*) If* $p \nmid k$ *is an odd prime and* $\left(\frac{k}{p}\right) = 1$*, then*
   - *If* $p \mid m$*,* $p \mid n$*, then* $\left(\frac{\frac{-m}{p} \cdot \frac{n}{p}}{p}\right) = 1$*.*
   - *If* $p \mid m$*,* $p \nmid n$*, then* $\left(\frac{n}{p}\right) = 1$*.*
   - *If* $p \nmid m$*,* $p \mid n$*, then* $\left(\frac{m}{p}\right) = 1$*.*

Conditions

Theorem (Ehrman, Mintzer-Sweeney, Schlesinger, Sheydvasser, Xiu 2016)

There exists an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ *iff the following conditions are met*

1. *(Conditions from* $\mathbb{R}$*-analysis) If* $m < 0$ *and* $n < 0$*, then* $k < 0$*.*
2. *(Conditions from* $\mathbb{Z}_p$*,* $p \neq 2$*) If* $p \nmid k$ *is an odd prime and* $\left(\frac{k}{p}\right) = 1$*, then*
   - *If* $p \mid m$*,* $p \mid n$*, then* $\left(\frac{\frac{-m}{p} \cdot \frac{n}{p}}{p}\right) = 1$*.*
   - *If* $p \mid m$*,* $p \nmid n$*, then* $\left(\frac{n}{p}\right) = 1$*.*
   - *If* $p \nmid m$*,* $p \mid n$*, then* $\left(\frac{m}{p}\right) = 1$*.*
3. *(Conditions from* $\mathbb{Z}_2$*) Omitted for the sake of brevity.*

Long-Term Behavior

The next logical question is to determine how often these conditions are met. Define

$$S_N = \left\{(m, n) \in \mathbb{Z}^2 : 1 < m, n < N, \ \ m, n \text{ squarefree}\right\}$$

Long-Term Behavior

The next logical question is to determine how often these conditions are met. Define

$$S_N = \left\{(m,n) \in \mathbb{Z}^2 : 1 < m,n < N,\ \ m,n \text{ squarefree}\right\}$$

Conjecture

For any fixed k,

$$\lim_{N\to\infty} \frac{\#\left(S_N \cap \left\{(m,n) : \mathbb{Q}\left(\sqrt{k}\right) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)\right\}\right)}{\#S_N} = 0.$$

Our Theorem

Theorem (EMSSSX 2016)

For any fixed k,

$$\lim_{N\to\infty} \frac{\#\left(S'_N \cap \left\{(m,n) : \mathbb{Q}\left(\sqrt{k}\right) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)\right\}\right)}{\#S'_N} = 0,$$

where

$$S'_N = \left\{(m,n) \in \mathbb{Z}^2 : 1 < m,n < N,\ m,n \text{ squarefree and coprime}\right\}.$$

Our Theorem

Theorem (EMSSSX 2016)

For any fixed k,

$$\lim_{N\to\infty} \frac{\#\left(S'_N \cap \left\{(m,n) : \mathbb{Q}\left(\sqrt{k}\right) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)\right\}\right)}{\#S'_N} = 0,$$

where

$$S'_N = \left\{(m,n) \in \mathbb{Z}^2 : 1 < m,n < N,\ m,n \text{ squarefree and coprime}\right\}.$$

Note: we are using $1 < m, n < N$ for simplicity, but the same proof applies to $-1 > m, n > -N$.

Our Approach

- How can one prove a result like this?

Our Approach

- How can one prove a result like this?
- One can check that $\#S'_N \approx \left(\frac{6}{\pi^2}\right)^3 N^2$ for large N.

Our Approach

- How can one prove a result like this?
- One can check that $\#S'_N \approx \left(\frac{6}{\pi^2}\right)^3 N^2$ for large N.
- To show that the limit is 0, we find an upper bound for the numerator that is $o(N^2)$.

Our Approach

- How can one prove a result like this?
- One can check that $\#S'_N \approx \left(\frac{6}{\pi^2}\right)^3 N^2$ for large N.
- To show that the limit is 0, we find an upper bound for the numerator that is $o(N^2)$.
- We do this by focusing exclusively on the p-adic conditions on n coming from m.

Definitions for a Sieve Approach

Recall that there is an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ only if

$$\text{If } p \mid m,\ p \nmid n, \text{ and } \left(\frac{k}{p}\right) = 1, \text{ then } \left(\frac{n}{p}\right) = 1$$

Definitions for a Sieve Approach

Recall that there is an embedding $\mathbb{Q}(\sqrt{k}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right)$ only if

$$\text{If } p \mid m,\ p \nmid n, \text{ and } \left(\frac{k}{p}\right) = 1, \text{ then } \left(\frac{n}{p}\right) = 1$$

Let

$$\tilde{m} = \prod_{\substack{\left(\frac{k}{p}\right)=1 \\ p \mid m}} p.$$

Definitions for a Sieve Approach

Definition

The admissible class is the set

$$\mathcal{A}(\tilde{m}) := \{x \in \mathbb{Z}/\tilde{m}\mathbb{Z} : \left(\frac{x}{p}\right) = 1, \forall p \mid \tilde{m}\}$$

Definitions for a Sieve Approach

Definition

The admissible class is the set

$$\mathcal{A}(\tilde{m}) := \{x \in \mathbb{Z}/\tilde{m}\mathbb{Z} : \left(\frac{x}{p}\right) = 1, \forall p \mid \tilde{m}\}$$

Note that n satisfies the conditions for an embedding if and only if

$$n \mod \tilde{m} \in \mathcal{A}(\tilde{m})$$

Definitions for a Sieve Approach

Definition

The admissible class is the set

$$\mathcal{A}(\tilde{m}) := \{x \in \mathbb{Z}/\tilde{m}\mathbb{Z} : \left(\frac{x}{p}\right) = 1, \forall p \mid \tilde{m}\}$$

Note that n satisfies the conditions for an embedding if and only if

$$n \mod \tilde{m} \in \mathcal{A}(\tilde{m})$$

Thus an upper bound for the numerator of our limit is given by

$$\sum_{(m,n)\in S'_N} 1_{\{n \mod \tilde{m} \in \mathcal{A}(\tilde{m})\}}$$

Approximating the Size of the Admissible Class

This upper bound is useful because we have a good approximation of the size of the admissible class $\mathcal{A}(\tilde{m})$.

Approximating the Size of the Admissible Class

This upper bound is useful because we have a good approximation of the size of the admissible class $\mathcal{A}(\tilde{m})$. Specifically,

$$\#\mathcal{A}(\tilde{m}) \approx \frac{\tilde{m}}{2^{\omega(\tilde{m})}},$$

where $\omega(x)$ is the number of distinct prime factors of x.

An Upper Bound

Thus,

$$\sum_{(m,n)\in S'_N} 1_{\{n \mod \tilde{m}\in\mathcal{A}(\tilde{m})\}} \approx \sum_{m<N} \frac{N}{\tilde{m}} \left(\#\mathcal{A}(\tilde{m})\right)$$

$$\approx N \sum_{m<N} \frac{1}{2^{\omega(\tilde{m})}}$$

An Upper Bound

Thus,

$$\sum_{(m,n)\in S'_N} 1_{\{n \mod \tilde{m}\in\mathcal{A}(\tilde{m})\}} \approx \sum_{m<N} \frac{N}{\tilde{m}} \left(\#\mathcal{A}(\tilde{m})\right)$$
$$\approx N \sum_{m<N} \frac{1}{2^{\omega(\tilde{m})}}$$

Therefore, if we show that

$$\sum_{m<N} \frac{1}{2^{\omega(\tilde{m})}} = o(N),$$

then we are done.

Splitting the Sum

- Note that, on average, $\omega(x) \approx \log\log(x)$.

Splitting the Sum

- Note that, on average, $\omega(x) \approx \log\log(x)$.
- So, we split our sum into two pieces: one where ω is close to the average, and one where it is not.

Splitting the Sum

- Note that, on average, $\omega(x) \approx \log\log(x)$.
- So, we split our sum into two pieces: one where ω is close to the average, and one where it is not.

Definition

$$B(N) = \left\{ m < N : \left| \omega(\tilde{m}) - \frac{1}{2} loglog(N) \right| < \frac{loglog(N)}{4} \right\}$$

$$B(N)^c = \{ m < N : m \notin B(N) \}$$

Splitting the Sum

- Note that, on average, $\omega(x) \approx \log\log(x)$.
- So, we split our sum into two pieces: one where ω is close to the average, and one where it is not.

Definition

$$B(N) = \left\{ m < N : \left| \omega(\tilde{m}) - \frac{1}{2} loglog(N) \right| < \frac{loglog(N)}{4} \right\}$$

$$B(N)^c = \{ m < N : m \notin B(N) \}$$

So,

$$\sum_{m<N} \frac{1}{2^{\omega(\tilde{m})}} = \sum_{m \in B(N)} \frac{1}{2^{\omega(\tilde{m})}} + \sum_{m \in B(N)^c} \frac{1}{2^{\omega(\tilde{m})}}.$$

An Outline of How to Control the Sums

- Why is this splitting useful?

[1] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac Theorem*

An Outline of How to Control the Sums

- Why is this splitting useful?
- $B(N)$ is tightly controlled, so it is easy to show that the sum over $B(N)$ is $o(N)$.

[1] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac Theorem*

An Outline of How to Control the Sums

- Why is this splitting useful?
- $B(N)$ is tightly controlled, so it is easy to show that the sum over $B(N)$ is $o(N)$.
- We can use a result of Granville and Soundararajan (2006)[1] to show that $\#B(N)^c$ is small.

[1] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac Theorem*

An Outline of How to Control the Sums

- Why is this splitting useful?
- $B(N)$ is tightly controlled, so it is easy to show that the sum over $B(N)$ is $o(N)$.
- We can use a result of Granville and Soundararajan (2006)[1] to show that $\#B(N)^c$ is small.
- It follows that the sum over $B(N)^c$ is also $o(N)$.

[1] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac Theorem*

An Outline of How to Control the Sums

- Why is this splitting useful?
- $B(N)$ is tightly controlled, so it is easy to show that the sum over $B(N)$ is $o(N)$.
- We can use a result of Granville and Soundararajan (2006)[1] to show that $\#B(N)^c$ is small.
- It follows that the sum over $B(N)^c$ is also $o(N)$.
- We are done!

□

[1] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac Theorem*

Further Research

- How fast does this limit goes to 0?

Further Research

- How fast does this limit goes to 0?
  - How small of an upper bound on the number of embeddings can we obtain using sieve methods?

Further Research

- How fast does this limit goes to 0?
  - How small of an upper bound on the number of embeddings can we obtain using sieve methods?
  - Can we find a lower bound on the number of embeddings?

Acknowledgements

We would like to thank Max Ehrman and Senia Sheydvasser for their wonderful mentorship and expert guidance.
We would like to thank Sam Payne, José González, and Michael Magee for organizing the SUMRY program.
Finally, we would like to thank MathFest for having us!