Ihara zeta functions of abstract isogeny graphs and modular curves

Jun Bo Lau, Travis Morrison, **Eli Orvis**, Gabrielle Scullard, and Lukas Zobernig

University of Colorado Boulder

November 4, 2025

Cryptographic motivation

Expansion properties of isogeny graphs with level structure have appeared in cryptography, notably in *Supersingular Elliptic Curves You Can Trust* [1].

Cryptographic motivation

Expansion properties of isogeny graphs with level structure have appeared in cryptography, notably in *Supersingular Elliptic Curves You Can Trust* [1].

This paper uses

Cryptographic motivation

Expansion properties of isogeny graphs with level structure have appeared in cryptography, notably in *Supersingular Elliptic Curves You Can Trust* [1].

This paper uses

1. non-backtracking walks, in

Cryptographic motivation

Expansion properties of isogeny graphs with level structure have appeared in cryptography, notably in *Supersingular Elliptic Curves You Can Trust* [1].

This paper uses

1. non-backtracking walks, in
2. $G(p, \ell, B_0(N))$,

Cryptographic motivation

Expansion properties of isogeny graphs with level structure have appeared in cryptography, notably in *Supersingular Elliptic Curves You Can Trust* [1].

This paper uses

1. non-backtracking walks, in
2. $G(p, \ell, B_0(N))$,

to provide a zero-knowledge proof of knowledge of an isogeny.

Cryptographic motivation

Expansion properties of isogeny graphs with level structure have appeared in cryptography, notably in *Supersingular Elliptic Curves You Can Trust* [1].

This paper uses

1. non-backtracking walks, in
2. $G(p, \ell, B_0(N))$,

to provide a zero-knowledge proof of knowledge of an isogeny.

Our work gives a framework for studying expansion of non-backtracking walks in isogeny graphs with level structure through their *zeta functions*.

Zeta functions in general

Recall the Euler product description of the Riemann zeta function:

Zeta functions in general

Recall the Euler product description of the Riemann zeta function:

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

Zeta functions in general

Recall the Euler product description of the Riemann zeta function:

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

The Riemann zeta function encodes information about the distribution of prime numbers in the location of its zeros.

Zeta functions in general

There are other zeta functions, however, which capture the distribution of other objects.

Zeta functions in general

There are other zeta functions, however, which capture the distribution of other objects.

Definition

Let X be a smooth, irreducible, projective variety defined over $\mathbb{F}_\ell$. The **Hasse-Weil zeta function** for X is defined as:

$$Z(X,u) = \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{\ell^n})}{n} u^n\right) = \prod_{x\in[X]} \frac{1}{1-u^{\deg(x)}},$$

where the product is defined over the closed points of X.

Zeta functions in general

There are other zeta functions, however, which capture the distribution of other objects.

Definition

Let X be a smooth, irreducible, projective variety defined over $\mathbb{F}_\ell$. The **Hasse-Weil zeta function** for X is defined as:

$$Z(X,u) = \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{\ell^n})}{n} u^n\right) = \prod_{x\in[X]} \frac{1}{1-u^{\deg(x)}},$$

where the product is defined over the closed points of X.

Again, these zeta functions have a version of the Riemann hypothesis, now known by work of Deligne (and others).

Zeta functions in general

In this talk, we will be interested in zeta function *of graphs*.

Zeta functions in general

In this talk, we will be interested in zeta function *of graphs*.

This leads to the following question:

Zeta functions in general

In this talk, we will be interested in zeta function *of graphs*.

This leads to the following question: what is a “prime” in a graph?

Zeta functions in general

In this talk, we will be interested in zeta function *of graphs*.

This leads to the following question: what is a "prime" in a graph?

Definition

A *prime* in a graph G is a closed walk, containing no backtracking or tail, which is not a shorter walk repeated multiple times.

Zeta functions in general

In this talk, we will be interested in zeta function *of graphs*.

This leads to the following question: what is a “prime” in a graph?

Definition

A *prime* in a graph G is a closed walk, containing no backtracking or tail, which is not a shorter walk repeated multiple times.

But what does *no backtracking* mean?

Serre's definition of a graph

To interpret backtracking, we use Serre's definition of a graph:

Serre's definition of a graph

To interpret backtracking, we use Serre's definition of a graph:

Definition

A *graph* is a set of vertices X and a set of edges Y, such that each edge has a *source* and a *target*, together with a fixed-point free involution J, which swaps sources and targets.

Serre's definition of a graph

To interpret backtracking, we use Serre's definition of a graph:

Definition

A *graph* is a set of vertices X and a set of edges Y, such that each edge has a *source* and a *target*, together with a fixed-point free involution J, which swaps sources and targets.

A walk in G has *no backtracking* if the edge y is never followed by the edge $J(y)$.

Serre's definition of a graph

To interpret backtracking, we use Serre's definition of a graph:

Definition

A *graph* is a set of vertices X and a set of edges Y, such that each edge has a *source* and a *target*, together with a fixed-point free involution J, which swaps sources and targets.

A walk in G has *no backtracking* if the edge y is never followed by the edge $J(y)$.

Teaser: this definition is not appropriate for isogeny graphs, particularly isogeny graphs with level structure.

Ihara zeta functions

Ihara zeta functions encode non-backtracking cycle counts in a graph G in a meromorphic function:

Ihara zeta functions

Ihara zeta functions encode non-backtracking cycle counts in a graph G in a meromorphic function:

Definition

Let G be an (undirected) graph. The *Ihara zeta function* of G is the function

$$\zeta_G(u) = \prod_{\text{primes } P} (1 - u^{|P|})^{-1}$$

Ihara zeta functions

Facts about Ihara zeta functions:

Ihara zeta functions

Facts about Ihara zeta functions:

1. $u\frac{d}{du}\log\zeta_G(u) = \sum_{m\geq 1} N_m u^m$, where N_m is the number of non-backtracking cycles of length m.

Ihara zeta functions

Facts about Ihara zeta functions:

1. $u \frac{d}{du} \log \zeta_G(u) = \sum_{m \geq 1} N_m u^m$, where N_m is the number of non-backtracking cycles of length m.
2. (Bass-Ihara determinant formula): Suppose that G is a d-regular graph, and let A be the adjacency matrix of G. Then we have:

$$\zeta_G(u) = \frac{(1-u^2)^{1-\chi(G)}}{\det(I - Au + (d-1)u^2)},$$

where χ is the Euler characteristic of G.

Abstract isogeny graphs

We would like to study *non-backtracking* cycles in many types of isogeny graphs:

Abstract isogeny graphs

We would like to study *non-backtracking* cycles in many types of isogeny graphs:

1. The (usual) supersingular isogeny graph, $G(p, \ell)$

Abstract isogeny graphs

We would like to study *non-backtracking* cycles in many types of isogeny graphs:

1. The (usual) supersingular isogeny graph, $G(p, \ell)$
2. Level H-structure, $G(p, \ell, H)$

Abstract isogeny graphs

We would like to study *non-backtracking* cycles in many types of isogeny graphs:

1. The (usual) supersingular isogeny graph, $G(p, \ell)$
2. Level H-structure, $G(p, \ell, H)$
3. Higher dimensional $(\ell, \ldots, \ell)$-graphs

Abstract isogeny graphs

We would like to study *non-backtracking* cycles in many types of isogeny graphs:

1. The (usual) supersingular isogeny graph, $G(p, \ell)$
2. Level H-structure, $G(p, \ell, H)$
3. Higher dimensional $(\ell, \ldots, \ell)$-graphs

In these graphs, the natural notion of "backtracking" is given by the dual map on isogenies.

Abstract isogeny graphs

We would like to study *non-backtracking* cycles in many types of isogeny graphs:

1. The (usual) supersingular isogeny graph, $G(p, \ell)$
2. Level H-structure, $G(p, \ell, H)$
3. Higher dimensional $(\ell, \ldots, \ell)$-graphs

In these graphs, the natural notion of "backtracking" is given by the dual map on isogenies.

But recall that J needed to be a *fixed-point free involution*.

Issues with backtracking

In $G(p, \ell)$, the dual may have fixed points, and may not be an involution!

Issues with backtracking

In $G(p, \ell)$, the dual may have fixed points, and may not be an involution!

1. Let $p \equiv 3 \pmod 4$, and write $\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}i + \frac{1+k}{2}\mathbb{Z} + \frac{i+j}{2}\mathbb{Z}$, with $i^2 = -1$. Then

$$\widehat{1+i} = 1 - i = (-i)(1+i).$$

Issues with backtracking

In $G(p, \ell)$, the dual may have fixed points, and may not be an involution!

1. Let $p \equiv 3 \pmod 4$, and write $\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}i + \frac{1+k}{2}\mathbb{Z} + \frac{i+j}{2}\mathbb{Z}$, with $i^2 = -1$. Then

$$\widehat{1+i} = 1 - i = (-i)(1+i).$$

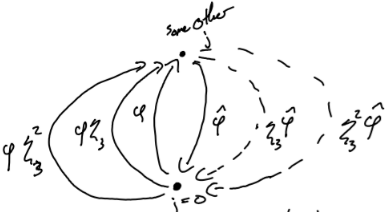
2. The dual may also fail to be an involution:

Cryptographic Motivation
Ihara zeta functions
Graphs
Abstract Isogeny Graphs
Orientable graphs
Modular Curves
Asymptotics
References

Issues with backtracking

In $G(p, \ell)$, the dual may have fixed points, and may not be an involution!

1. Let $p \equiv 3 \pmod 4$, and write $\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}i + \frac{1+k}{2}\mathbb{Z} + \frac{i+j}{2}\mathbb{Z}$, with $i^2 = -1$. Then
$$\widehat{1+i} = 1 - i = (-i)(1+i).$$
2. The dual may also fail to be an involution:



Credit: Orientations and Cycles in Supersingular ℓ-isogeny graphs

Abstract isogeny graphs

Abstract isogeny graphs provide a framework for addressing these issues:

Abstract isogeny graphs

Abstract isogeny graphs provide a framework for addressing these issues:

Definition

An *abstract isogeny graph* is the following collection of data:

- A set X of vertices;
- a set Y of edges;
- functions, $s, t : Y \to X \times X$;
- a function $J : Y \to Y$; and
- a function $L : X \to X$,

such that $s(J(e)) = t(e)$ and $t(J(e)) = L(s(e))$ for all $e \in Y$.

The L function

To motivate the function L, we need to dig in to an even worse failure of the dual map in isogeny graphs with level structure. Recall:

The L function

To motivate the function L, we need to dig in to an even worse failure of the dual map in isogeny graphs with level structure. Recall:

Definition

For $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, a *level H-structure* on an elliptic curve E is an isomorphism $\phi : \mathbb{Z}/N\mathbb{Z}^2 \to E[N]$, up to pre-composition by elements of H.

The L function

To motivate the function L, we need to dig in to an even worse failure of the dual map in isogeny graphs with level structure. Recall:

Definition

For $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, a *level H-structure* on an elliptic curve E is an isomorphism $\phi : \mathbb{Z}/N\mathbb{Z}^2 \to E[N]$, up to pre-composition by elements of H.

Isogenies must satisfy:

The L function

To motivate the function L, we need to dig in to an even worse failure of the dual map in isogeny graphs with level structure. Recall:

Definition

For $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, a *level H-structure* on an elliptic curve E is an isomorphism $\phi : \mathbb{Z}/N\mathbb{Z}^2 \to E[N]$, up to pre-composition by elements of H.

Isogenies must satisfy:

$$\begin{tikzcd} (\mathbb{Z}/N\mathbb{Z})^2 \arrow[r, "id"] \arrow[d, "\phi"'] & (\mathbb{Z}/N\mathbb{Z})^2 \arrow[d, "\phi'"] \\ E[N] \arrow[r, "\psi"] & E'[N] \end{tikzcd}$$

The L function

In $G(p, \ell, H)$, the dual might not swap sources and targets!

The L function

In $G(p, \ell, H)$, the dual might not swap sources and targets!

The L function

In $G(p, \ell, H)$, the dual might not swap sources and targets!

$$\begin{tikzcd}
(\mathbb{Z}/N\mathbb{Z})^2 \arrow[r, "id"] \arrow[d, "\phi"'] & (\mathbb{Z}/N\mathbb{Z})^2 \arrow[r, "id"] \arrow[d, "\phi'"] & (\mathbb{Z}/N\mathbb{Z})^2 \arrow[d, "\ell\phi"] \\
E[N] \arrow[r, "\psi"] & E'[N] \arrow[r, "\hat{\psi}"] & E[N]
\end{tikzcd}$$

Thus the target of the dual of $\psi : (E, [\phi]) \to (E', [\phi']])$ is $(E, [\ell\phi])$.

The L function

In $G(p, \ell, H)$, the dual might not swap sources and targets!

$$\begin{tikzcd}
(\mathbb{Z}/N\mathbb{Z})^2 \arrow[r, "id"] \arrow[d, "\phi"'] & (\mathbb{Z}/N\mathbb{Z})^2 \arrow[r, "id"] \arrow[d, "\phi'"] & (\mathbb{Z}/N\mathbb{Z})^2 \arrow[d, "\ell\phi"] \\
E[N] \arrow[r, "\psi"] & E'[N] \arrow[r, "\hat{\psi}"] & E[N]
\end{tikzcd}$$

Thus the target of the dual of $\psi : (E, [\phi]) \to (E', [\phi'])$ is $(E, [\ell\phi])$.

The operator L keeps track of how the target of J depends on the source of the edge.

The L function

In $G(p, \ell, H)$, the dual might not swap sources and targets!

$$\begin{tikzcd}
(\mathbb{Z}/N\mathbb{Z})^2 \arrow[r, "id"] \arrow[d, "\phi"'] & (\mathbb{Z}/N\mathbb{Z})^2 \arrow[r, "id"] \arrow[d, "\phi'"] & (\mathbb{Z}/N\mathbb{Z})^2 \arrow[d, "\ell\phi"] \\
E[N] \arrow[r, "\psi"] & E'[N] \arrow[r, "\hat{\psi}"] & E[N]
\end{tikzcd}$$

Thus the target of the dual of $\psi : (E, [\phi]) \to (E', [\phi'])$ is $(E, [\ell\phi])$.

The operator L keeps track of how the target of J depends on the source of the edge.

$$\begin{tikzcd}
s(e) \arrow[r, "e"] \arrow[rr, bend left, "L"] & \begin{array}{c} s(Je) \\ \shortparallel \\ t(e) \end{array} \arrow[r, "Je"] & \begin{array}{c} t(Je) \\ \shortparallel \\ Ls(e) \end{array}
\end{tikzcd}$$

Motivating abstract isogeny graphs

Theorem

Choosing appropriate representatives for edges in order to define J as the dual map, we can realize $G(p, \ell, H)$ as an abstract isogeny graph for any H. The same is true for $(\ell, \ldots, \ell)$-isogeny graphs.

Motivating abstract isogeny graphs

Theorem

Choosing appropriate representatives for edges in order to define J as the dual map, we can realize $G(p, \ell, H)$ as an abstract isogeny graph for any H. The same is true for $(\ell, \ldots, \ell)$-isogeny graphs.

Technical remark: The choice of representatives is designed to deal with the fact that the dual map is not well-defined on edges - this was already noted in [2], and our solution is equivalent to theirs.

Ihara zeta functions for abstract isogeny graphs

We can now define the Ihara zeta function of an abstract isogeny graph, which will capture the “correct” notion of backtracking:

Ihara zeta functions for abstract isogeny graphs

We can now define the Ihara zeta function of an abstract isogeny graph, which will capture the "correct" notion of backtracking:

$$\zeta_G(u) = \prod_{\text{prime cycles } P} (1 - u^{|P|})^{-1},$$

where the primes are non-backtracking with respect to the J function.

Ihara zeta functions for abstract isogeny graphs

We can now define the Ihara zeta function of an abstract isogeny graph, which will capture the "correct" notion of backtracking:

$$\zeta_G(u) = \prod_{\text{prime cycles } P} (1 - u^{|P|})^{-1},$$

where the primes are non-backtracking with respect to the J function.

Another teaser: note that primes in an abstract isogeny graph are exactly the *isogeny cycles* studied previously by [2] and [3].

Ihara zeta functions for abstract isogeny graphs

We will give the Ihara zeta function of an abstract isogeny graph in two ways:

Ihara zeta functions for abstract isogeny graphs

We will give the Ihara zeta function of an abstract isogeny graph in two ways:

1. by combinatorial data,

Ihara zeta functions for abstract isogeny graphs

We will give the Ihara zeta function of an abstract isogeny graph in two ways:

1. by combinatorial data,
2. by relation to zeta functions of modular curves.

Ihara zeta function - combinatorial formula

For a function $f : S \to S$ acting on a finite set S, we define $C_k(f)$ to be the number of k-cycles in the largest permutation induced by f.

Ihara zeta function - combinatorial formula

For a function $f : S \to S$ acting on a finite set S, we define $C_k(f)$ to be the number of k-cycles in the largest permutation induced by f.

Theorem

Let $\Gamma = (X, Y, J, L)$ be an abstract isogeny graph with regular out degree d and adjacency matrix A. Then $\zeta_\Gamma(u)$ is given by:

$$\frac{(1-u^2)^{C_1(L)}(1+u)^{-C_1(J)} \prod_{k>1}(1-(-1)^k u^{2k})^{C_k(L)}(1-u^k)^{-C_k(J)}}{\det(1 - Au + u^2(d-1)L)}$$

Orientable graphs associated to abstract isogeny graphs

For both simplification of the previous formula, and the statement of the next, we use the *orientable graphs* associated to an abstract isogeny graph Γ.

Orientable graphs associated to abstract isogeny graphs

For both simplification of the previous formula, and the statement of the next, we use the *orientable graphs* associated to an abstract isogeny graph Γ.

Definition

Let $\Gamma = (X, Y, J, L)$ be an abstract isogeny graph. We define $\sim_X$ to be the smallest equivalence relation on X such that $x \sim_X Lx$ for all $x \in X$, and $\sim_Y$ to be the smallest equivalence relation on Y such that $y \sim_Y J^2 y$ for all $y \in Y$. The *orientable graphs associated to* Γ are
$\Gamma^{+1} = (X/\sim_X, Y/\sim_Y - \{[y] : J[y] = [y]\})$ and
$\Gamma^{-1} = (X/\sim_X, Y/\sim_Y \sqcup \{[y] : J[y] = [y]\})$

Orientable graphs associated to abstract isogeny graphs

In many cases, we can simplify our formula for $\zeta_\Gamma(u)$ using these orientable graphs:

Orientable graphs associated to abstract isogeny graphs

In many cases, we can simplify our formula for $\zeta_\Gamma(u)$ using these orientable graphs:

Theorem

Let Γ be a d-regular abstract isogeny graph for $d \geq 1$, and suppose that the permutation induced by J is an involution and $s(J^2 y) = s(y)$ for every edge $y \in Y$. Then we have

$$\zeta_\Gamma(u) = \frac{(1+u)^{\chi(\Gamma^{-1})}(1-u)^{\chi(\Gamma^{+1})}}{\det(\mathrm{id}_{\mathbb{C}_X} - uA + u^2 Q)}.$$

Hasse-Weil Zeta functions

Our next goal is to relate Ihara zeta functions of abstract isogeny graphs to Hasse Weil zeta functions of modular curves. This will allow us to understand asymptotics of cycles in graphs with level structure.

Hasse-Weil Zeta functions

Our next goal is to relate Ihara zeta functions of abstract isogeny graphs to Hasse Weil zeta functions of modular curves. This will allow us to understand asymptotics of cycles in graphs with level structure.

Ihara zeta function - modular curves formula

Let $B_1(N) \leq H \leq B_0(N)$, and $H_p = H \times B_0(p)$.

Ihara zeta function - modular curves formula

Let $B_1(N) \leq H \leq B_0(N)$, and $H_p = H \times B_0(p)$.

Theorem

Let $G = G(p, \ell, H)$. Denote by $X_{H,\mathbb{F}_\ell}$, and $X_{H_p,\mathbb{F}_\ell}$ the associated modular curves over $\mathbb{F}_\ell$. Then

$$\frac{Z(X_{H_p,\mathbb{F}_\ell}, u)}{Z(X_{H,\mathbb{F}_\ell}, u)^2}\zeta_G(u) = \frac{(1-u^2)^{C_1(L)}}{(1+u)^{C_1(J)}} \prod_{k>1} \frac{(1-(-1)^k u^{2k})^{C_k(L)}}{(1-u^k)^{C_k(J)}}.$$

Ihara zeta function - modular curves formula

As with the previous description of $\zeta_G(u)$, in many cases, we can give a simpler formula involving the orientable graphs associated to G:

Ihara zeta function - modular curves formula

As with the previous description of $\zeta_G(u)$, in many cases, we can give a simpler formula involving the orientable graphs associated to G:

Corollary

Let $G = (p, \ell, B_0(N))$. Let $X_0(pN)_{\mathbb{F}_\ell}$ and $X_0(N)_{\mathbb{F}_\ell}$ denote the modular curves over $\mathbb{F}_\ell$. Then we have that

$$\frac{Z(X_0(pN)_{\mathbb{F}_\ell}, u)}{Z(X_0(N)_{\mathbb{F}_\ell}, u)^2}\zeta_G(u) = (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})}.$$

.

Asymptotics for graphs with level structure in arbitrary characteristic

Finally, we use this product to deduce asymptotics for the number of cycles of length r as $r \to \infty$, for arbitrary p, and in the presence of level structure.

Asymptotics for graphs with level structure in arbitrary characteristic

Finally, we use this product to deduce asymptotics for the number of cycles of length r as $r \to \infty$, for arbitrary p, and in the presence of level structure.

Theorem

Let G be the ℓ-isogeny graph with Borel level structure, and N_r be the number of non-backtracking tailless cycles of length r in G. Then we have that

$$N_r = 2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) - \chi(G^{+1}) + (-1)^{r-1}\chi(G^{-1}).$$

Asymptotics for graphs with level structure in arbitrary characteristic

The previous theorem gives the following asymptotic:

Asymptotics for graphs with level structure in arbitrary characteristic

The previous theorem gives the following asymptotic:

Theorem

Let G be the ℓ-isogeny graph with N-level structure for an arbitrary prime p. Let N_r be the number of non-backtracking cycles of length r in G. Then N_r asymptotically approaches ℓ^r as $r \to \infty$.

Point counts on modular curves

As a final application, we can "flip the script," and use isogeny graphs to study modular curves.

Point counts on modular curves

As a final application, we can "flip the script," and use isogeny graphs to study modular curves.

Theorem

Let p, ℓ be distinct primes and $r > 2$ such that $\ell^r < p$. Let $G := G(p, \ell)$. Then we have that

$$\begin{aligned}\#X_0(p)(\mathbb{F}_{\ell^r}) = & 2(1+\ell^r) - \chi(G^{+1}) + (-1)^{r-1}\chi(G^{-1}) \\ & - 2\sum_{n|r}\sum_{\mathcal{O}\in\mathcal{I}_n} h(\mathcal{O}),\end{aligned}$$

where $\mathcal{I}_n$ is an explicit set of imaginary quadratic orders.

The end :)

Thanks for listening!

References I

[1] Andrea Basso et al. "Supersingular curves you can trust". In: *Advances in cryptology—EUROCRYPT 2023. Part II.* Vol. 14005. Lecture Notes in Comput. Sci. Springer, Cham, [2023] ©2023, pp. 405–437. ISBN: 978-3-031-30616-7; 978-3-031-30617-4. DOI: 10.1007/978-3-031-30617-4_14. URL: https://doi.org/10.1007/978-3-031-30617-4_14.

[2] Sarah Arpin et al. *Orientations and cycles in supersingular isogeny graphs*. 2022. arXiv: 2205.03976 [math.NT].

[3] Sarah Arpin et al. *Cycles and Cuts in Supersingular L-Isogeny Graphs*. 2025. arXiv: 2502.00638 [math.NT]. URL: https://arxiv.org/abs/2502.00638.