ON A SPECIAL METRIC IN CYCLOTOMIC FIELDS

Katerina Saettone
Department of Mathematics, University of Illinois Urbana-Champaign, Urbana, Illinois
kas18@illinois.edu

Alexandru Zaharescu
Department of Mathematics, University of Illinois Urbana-Champaign, Urbana, Illinois
zaharesc@illinois.edu

Zhuo Zhang
Department of Mathematics, University of Illinois Urbana-Champaign, Urbana, Illinois
zhuoz4@illinois.edu

Received: 8/3/24, Accepted: 1/27/25, Published: 2/21/25

Abstract

Let p be an odd prime and ω be a primitive pth root of unity. In this paper, we introduce a metric on the cyclotomic field $K = \mathbb{Q}(\omega)$. We prove that this metric has several remarkable properties, such as invariance under the action of the Galois group. Furthermore, we show that points in the ring of integers $\mathcal{O}_K$ behave in a highly uniform way under this metric. More specifically, we prove that for a certain hypercube in $\mathcal{O}_K$ centered at the origin, almost all pairs of points in the cube are almost equi-distanced from each other when p and N are large enough. When suitably normalized, this distance is exactly $1/\sqrt{6}$.

1. Introduction

Cyclotomic fields play an essential role in algebra and number theory, particularly in understanding the behavior of prime numbers and the solutions to Diophantine equations. In this paper, we uncover properties of cyclotomic fields equipped with a special metric, which we study from both algebraic and probabilistic standpoints.

Let p be an odd prime and ω be a primitive p-th root of unity. The extension of $\mathbb{Q}$ generated by ω in the field of complex numbers is the p-th cyclotomic field

DOI: 10.5281/zenodo.14907262

$K = \mathbb{Q}(\omega)$. We shall denote by $\mathrm{Tr}_{K/\mathbb{Q}}$ the *trace map* of the number field K (the precise definition of $\mathrm{Tr}_{K/\mathbb{Q}}$ will be reviewed in Section 2).

For $\alpha \in K$, we denote by v_α the vector in $\mathbb{Q}^{p-1}$ whose jth component is $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega^j)$, for $1 \leq j \leq p-1$. In this paper, we define $d(\alpha, \beta)$, the *distance* between α and β in K, as the Euclidean distance between the vectors v_α and v_β in $\mathbb{Q}^{p-1}$. We shall show that d is a metric on K, where positive-definiteness is the only nontrivial property. Note that d is canonically defined and is independent of the choice of ω.

We aim to investigate this metric d from several perspectives. In Section 3, we show that d has certain nice properties that are related to the algebraic and number-theoretic structure of $\mathbb{Q}(\omega)$. For instance, the metric d is invariant under the action of the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. In turn, this gives us an analogy of *Krasner's lemma* within the context of cyclotomic fields equipped with the metric d.

In Section 4, we derive an explicit formula for the metric in terms of the coordinates under the canonical basis $\{\omega, \ldots, \omega^{p-1}\}$ of K.

In the rest of the paper, we build on the ideas of [1] and [2] to study the metric d from a statistical point of view. More specifically, for a positive integer N, we denote by $B(p, N)$ the symmetric *box of cyclotomic lattice points*:

$$B(p,N) := \left\{a_1\omega + \ldots + a_{p-1}\omega^{p-1} : a_1, \ldots, a_{p-1} \in [-N, N] \cap \mathbb{Z}\right\},$$

which lies in the ring of integers $\mathcal{O}_K$. In Section 5, we normalize the metric d so that the diameter of $B(p, N)$ is exactly 1 in the sense of metric spaces, i.e., the points furthest apart in $B(p, N)$ are at a distance of exactly 1 from each other. This gives us a scaled distance, denoted by $\mathfrak{d}_{p,N}(\alpha, \beta)$, which serves as a unitary means of comparing the spacing of points in different hypercubes $B(p, N)$, as p and N vary. Our main theorem states that points in $B(p, N)$ are almost equi-distanced from each other in the following sense.

Theorem 1. *For any $\varepsilon > 0$, there exists an absolute and effectively computable constant $A(\varepsilon)$ such that if $N, p > A(\varepsilon)$, then*

$$\frac{1}{\#B(p,N)^2} \# \left\{(\alpha, \beta) \in B(p,N) \times B(p,N) : \left|\mathfrak{d}_{p,N}(\alpha,\beta) - \frac{1}{\sqrt{6}}\right| > \varepsilon\right\} < \varepsilon.$$

Theorem 1 reveals a surprising uniformity in the spacing of points among the high-dimensional lattice points in K. It provides insight into a certain "statistical regularity" in the geometric properties of cyclotomic fields when viewed through the lens of this particular metric. Theorem 1 will follow from Theorem 5, which is an explicit quantitative version that we shall prove in Section 6. Our methods rely on calculating the various *moments* of distances between points in $B(p, N)$.

2. Notations and Definition of the Metric

2.1. Notations and Setup

In this subsection, we set up some notations and recall some preliminary facts from algebraic number theory that will be needed in the later discussions. More details can be found in [5], [6], and [11].

Throughout this paper, let p be an odd prime, and let ω be a primitive pth root of unity, say $\omega = e^{2\pi i/p}$. Let $K = \mathbb{Q}(\omega)$ be the pth cyclotomic field. It is well known that the Galois group $G := \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the group $(\mathbb{Z}/p\mathbb{Z})^\times$, which is cyclic of order $p-1$.

We denote by $\mathcal{O}_K$ the ring of integers of K, that is, the integral closure of $\mathbb{Z}$ in K. It is well known that rings of integers have integral bases, and in this case, an integral basis of $\mathcal{O}_K$ is given by $\{\omega, \ldots, \omega^{p-1}\}$. Therefore,

$$\mathcal{O}_K = \{a_1\omega + \ldots + a_{p-1}\omega^{p-1} : a_1, \ldots, a_{p-1} \in \mathbb{Z}\}.$$

Many key properties of number fields can be studied via the *trace map*. Since cyclotomic fields are always Galois over $\mathbb{Q}$, the trace map $\mathrm{Tr}_{K/\mathbb{Q}}$ has a simple definition in this case, which is

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha), \quad \alpha \in K. \tag{1}$$

It can be proved that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ for all $\alpha \in K$. Furthermore, if $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Finally, for complex-valued functions f and g, we write $f \ll g$ or $f = O(g)$ to indicate that there exists an absolute and effectively computable constant C such that $|f| \leq C|g|$ for all inputs.

2.2. Definition of the Metric

We now formally define the metric d mentioned in the introduction. The metric is, in fact, induced by a norm on K as a $\mathbb{Q}$-vector space. The norm is defined as follows.

Definition 1. For any $\alpha \in K$, we define

$$\|\alpha\| = \sqrt{\sum_{j=1}^{p-1} \Big(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega^j)\Big)^2} = \|v_\alpha\|_E,$$

where $v_\alpha \in \mathbb{Q}^{p-1}$ is the vector whose jth component is $\mathrm{Tr}(\alpha\omega^j)$ and $\|\cdot\|_E$ denotes the usual Euclidean norm on $\mathbb{Q}^{p-1}$.

Definition 2. For $\alpha, \beta \in K$, we define their distance $d(\alpha, \beta)$ to be $\|\alpha - \beta\|$.

Theorem 2. *The function $\|\cdot\|$ defined as in Definition 1 is a norm on K.*

Proof. We verify the three conditions of a norm. The triangle inequality follows immediately from the usual triangle inequality in Euclidean spaces $\mathbb{Q}^{p-1} \subseteq \mathbb{R}^{p-1}$.

For any $\alpha \in K$ and $\lambda \in \mathbb{Q}$, we need to prove that $\|\lambda\alpha\| = |\lambda|\|\alpha\|$. This follows from the $\mathbb{Q}$-linearity of trace, since it implies that $v_{\lambda\alpha} = \lambda v_\alpha$.

It remains to prove positive-definiteness. Clearly $\|\alpha\| \geq 0$. Suppose $\|\alpha\| = 0$. Then $v_\alpha \in \mathbb{Q}^{p-1}$ is the zero vector. Hence,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega^j) = 0,$$

for all $j = 1, \ldots, p-1$. Suppose $\alpha \neq 0$. Then, we may write

$$\frac{1}{\alpha} = c_1\omega + \ldots + c_{p-1}\omega^{p-1}, \quad \text{where } c_i \in \mathbb{Q}.$$

Therefore,

$$1 = c_1\alpha\omega + \ldots + c_{p-1}\alpha\omega^{p-1}.$$

Taking the trace of both sides and using the fact that trace is $\mathbb{Q}$-linear, we have

$$p - 1 = \sum_{j=1}^{p-1} c_j \,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega^j) = 0,$$

which is a contradiction. Hence, $\alpha = 0$. □

It follows that the function d is indeed a metric on K. The distance defined in this manner closely resembles the Euclidean distance in vector spaces but also has properties that are well-suited to the study of cyclotomic fields. This will be further explored in Section 3.

We remark that the norm in Definition 1 must be distinguished from the usual norm of an algebraic number (say, over a Galois extension), which is defined to be the product of all its Galois conjugates. There also exist several other notions of norms over number fields. For example, one can define the *Siegel norm* of algebraic numbers (see [4] and [10] for its construction and some interesting properties; for some questions related to Siegel's trace problem, see [8] and [9]). In this paper, the word "norm" always refers to the norm we just defined unless stated otherwise.

3. Properties of the Metric

The metric d on $K = \mathbb{Q}(\omega)$ defined above is the main object we investigate in this paper. To convince the readers that the metric is a natural object worth studying, we shall first prove a number of remarkable facts about this metric, the most important one of which is the invariance under the action of the Galois group. This is the content of the following proposition.

3.1. Invariance Under the Galois Group Action

Proposition 1. *The metric d is invariant under the action of the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. In other words, for any $\sigma \in G$ and $\alpha, \beta \in K$, we have*

$$d(\alpha, \beta) = d(\sigma(\alpha), \sigma(\beta)).$$

Proof. It suffices to show that the norm in Definition 1 is invariant under G, i.e., $\|\sigma(\alpha)\| = \|\alpha\|$ for all $\alpha \in K$ and $\sigma \in G$. Suppose $\sigma^{-1}(\omega) = \omega^k$, where $1 \leq k \leq p-1$. Then we have

$$\begin{aligned}
\|\sigma(\alpha)\| &= \sqrt{\sum_{j=1}^{p-1} \left(\mathrm{Tr}_{K/\mathbb{Q}}(\sigma(\alpha)\omega^j) \right)^2} \\
&= \sqrt{\sum_{j=1}^{p-1} \left(\mathrm{Tr}_{K/\mathbb{Q}} \left(\sigma\left(\alpha \cdot \sigma^{-1}(\omega)^j \right) \right) \right)^2} \\
&= \sqrt{\sum_{j=1}^{p-1} \left(\mathrm{Tr}_{K/\mathbb{Q}} \left(\alpha \cdot \sigma^{-1}(\omega)^j \right) \right)^2} \\
&= \sqrt{\sum_{j=1}^{p-1} \left(\mathrm{Tr}_{K/\mathbb{Q}} \left(\alpha\omega^{kj} \right) \right)^2},
\end{aligned}$$

where the third equality follows from the fact that $\mathrm{Tr}_{K/\mathbb{Q}}$ is invariant under G. Since k must be coprime to p, it follows that $\{kj : 1 \leq j \leq p-1\}$ is a permutation of $\{j : 1 \leq j \leq p-1\}$. Hence, $\|\sigma(\alpha)\| = \|\alpha\|$, as required. □

3.2. An Analogue of Krasner's Lemma

As a consequence of Proposition 1, we now prove that the metric d has another surprising property, with which we will draw an analogy between the following version of Krasner's lemma.

Theorem 3 ([7, Lemma 8.1.6])**.** *Let κ be a complete field with respect to a non-Archimedean valuation, and let Ω be an algebraic closure of κ. Let $\alpha \in \Omega$ be separable over κ and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over κ. Suppose that for $\beta \in \Omega$ we have*

$$|\alpha - \beta| < |\alpha - \alpha_i| \quad \text{for } i = 2, \ldots, n,$$

where $|\cdot|$ denotes the unique extension of the valuation to Ω. Then $\kappa(\alpha) \subseteq \kappa(\beta)$.

We now prove the following analogous result.

Theorem 4. *Let $K = \mathbb{Q}(\omega)$, where ω is a primitive pth root of unity. Let α be an element of K and let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α over K, with $\alpha_1 = \alpha$. Suppose that for $\beta \in K$ we have*

$$d(\alpha, \beta) < \frac{1}{2}\, d(\alpha, \alpha_i) \quad \text{for } i = 2, \ldots, n,$$

where d is the metric in Definition 2. Then $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$.

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. From Galois theory, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$ if and only if $\mathrm{Gal}(K/\mathbb{Q}(\beta)) \subseteq \mathrm{Gal}(K/\mathbb{Q}(\alpha))$. Since G is a cyclic group of order $p-1$, the preceding condition is equivalent to $|\mathrm{Gal}(K/\mathbb{Q}(\beta))|$ dividing $|\mathrm{Gal}(K/\mathbb{Q}(\alpha))|$, which is then equivalent to $[K : \mathbb{Q}(\beta)]$ dividing $[K : \mathbb{Q}(\alpha)]$. By the tower law, this is equivalent to $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ dividing $[\mathbb{Q}(\beta) : \mathbb{Q}]$.

As in the statement, let $\alpha_1, \ldots, \alpha_n$ be the Galois conjugates of α over K, with $\alpha_1 = \alpha$. Similarly, let $\beta_1, \ldots, \beta_m$ be the Galois conjugates of β over K, with $\beta_1 = \beta$. Since $K/\mathbb{Q}$ is Galois, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = m$. Therefore, we need to prove that n divides m under the hypothesis that $d(\alpha, \beta) < \frac{1}{2} d(\alpha, \alpha_i)$ for all $i = 2, \ldots, n$.

Let

$$r = \frac{1}{2} \min_{2 \le i \le n} d(\alpha, \alpha_i).$$

Then $d(\alpha, \beta) < r$. For any element $x \in K$, denote by $B(x, r)$ the open ball centered at x with radius r under the metric d. Observe that if α_i, α_j are two *distinct* Galois conjugates of α, say $\alpha_i = \sigma(\alpha)$ and $\alpha_j = \tau(\alpha)$, where $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q}(\alpha))$, then

$$d(\alpha_i, \alpha_j) = d(\sigma(\alpha), \tau(\alpha)) = d(\alpha, \sigma^{-1}\tau(\alpha)) \ge 2r.$$

It follows that any two distinct conjugates α_i and α_j are at a distance of at least $2r$ from each other. In particular, the open balls $\{B(\alpha_i, r) : 1 \le i \le n\}$ are pairwise disjoint.

We claim that for every β_j there exists an α_i such that $\beta_j \in B(\alpha_i, r)$. In other words, the balls contain *all* conjugates of β. Indeed, if $\beta_j = \sigma(\beta)$, then

$$d(\sigma(\alpha), \beta_j) = d(\sigma(\alpha), \sigma(\beta)) = d(\alpha, \beta) < r,$$

by Proposition 1. Hence, $\beta_j \in B(\sigma(\alpha), r)$.

Furthermore, we claim that for $1 \le i \le n$, each ball $B(\alpha_i, r)$ contains the same number of conjugates of β. Indeed, suppose $\alpha_i = \sigma(\alpha)$. Then by Proposition 1 again, we have

$$d(\alpha_i, \beta_j) = d(\sigma(\alpha), \beta_j) = d(\alpha, \sigma^{-1}(\beta_j)).$$

Therefore, $\beta_j \in B(\alpha_i, r)$ if and only if $\sigma^{-1}(\beta_j) \in B(\alpha, r)$. Since σ is a bijection, this proves that $B(\alpha, r)$ and $B(\alpha_i, r)$ contain the same number of Galois conjugates of β. This number is nonzero because $\beta \in B(\alpha, r)$. Since the balls are disjoint, we conclude that n divides m, as desired. □

Remark 1. The following example illustrates that the constant $\frac{1}{2}$ in the statement of Theorem 4 is optimal, in the sense that any larger constant would make the statement false. Consider $p = 3$, $\alpha = \omega$, and $\beta = -\frac{1}{2}$. Then α only has one Galois conjugate other than itself, namely ω^2. A straightforward computation shows that

$$d(\alpha, \beta) = \frac{3}{\sqrt{2}} \quad \text{and} \quad d(\alpha, \omega^2) = 3\sqrt{2}.$$

Therefore,

$$d(\alpha, \beta) = \frac{1}{2} d(\alpha, \omega^2),$$

but $\mathbb{Q}(\alpha)$ is not contained in $\mathbb{Q}(\beta)$.

As a simple consequence, we deduce the following corollary, which is reminiscent of the primitive element theorem in field theory.

Corollary 1. *Let $\alpha, \beta \in K = \mathbb{Q}(\omega)$. Define $\gamma_n = \alpha + \frac{\beta}{n}$. Then $\mathbb{Q}(\gamma_n) = \mathbb{Q}(\alpha, \beta)$ for all sufficiently large n.*

Proof. Clearly, $\mathbb{Q}(\gamma_n) \subseteq \mathbb{Q}(\alpha, \beta)$, so it suffices to prove the reverse inclusion. Note that

$$d(\alpha, \gamma_n) = \|\alpha - \gamma_n\| = \left\| \frac{\beta}{n} \right\| = \frac{\|\beta\|}{n}.$$

Thus, when n is sufficiently large, we would have $d(\alpha, \gamma_n) < \frac{1}{2} d(\alpha, \sigma(\alpha))$ for all $\sigma \in G$. Theorem 4 implies that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma_n)$. In particular, $\alpha \in \mathbb{Q}(\gamma_n)$, and so $\beta \in \mathbb{Q}(\gamma_n)$, as desired. □

Not only does Corollary 1 prove a special case of the primitive element theorem, but it also provides a simple algorithm to find generators of subextensions of K.

4. Computing the Metric in Coordinates

In this section, we aim to derive an explicit formula of the metric d in terms of the coordinates of $\alpha \in K$ under the integral basis $\{\omega, \ldots, \omega^{p-1}\}$. We first note that $\mathrm{Tr}_{K/\mathbb{Q}}(1) = p - 1$, and $\mathrm{Tr}_{K/\mathbb{Q}}(\omega) = \ldots = \mathrm{Tr}_{K/\mathbb{Q}}(\omega^{p-1}) = -1$. Therefore, if

$$\alpha = a_1 \omega + \ldots + a_{p-1} \omega^{p-1},$$

then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -(a_1 + \ldots + a_{p-1}), \tag{2}$$

and for $j = 1, \ldots, p-1$, we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha \omega^j) = -\sum_{\substack{i=1 \\ i \neq p-j}}^{p-1} a_i + (p-1) a_{p-j} = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + p a_{p-j}.$$

Therefore,

$$\begin{aligned}
\|\alpha\|^2 &= \sum_{j=1}^{p-1} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega^j)^2 \\
&= \sum_{j=1}^{p-1} \Big(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + pa_{p-j} \Big)^2 \\
&= \sum_{j=1}^{p-1} \Big(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + pa_j \Big)^2 \\
&= \sum_{j=1}^{p-1} \Big(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2 + 2pa_j \,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + p^2 a_j^2 \Big) \\
&= (p-1)\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2 + 2p\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \sum_{j=1}^{p-1} a_j + p^2 \sum_{j=1}^{p-1} a_j^2.
\end{aligned}$$

From Equation (2) we see that

$$\begin{aligned}
\|\alpha\|^2 &= (p-1)\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2 - 2p\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2 + p^2 \sum_{j=1}^{p-1} a_j^2 \\
&= p^2 \sum_{j=1}^{p-1} a_j^2 - (p+1)\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2.
\end{aligned}$$

Hence, we have arrived at the following convenient formula, which we shall frequently use in the later sections.

Lemma 1. *Suppose $\alpha = a_1\omega + \ldots + a_{p-1}\omega^{p-1} \in K$. Then*

$$\|\alpha\|^2 = p^2\|\alpha\|_E^2 - (p+1)\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2, \tag{3}$$

where $\|\alpha\|_E$ is the Euclidean norm of α, i.e., $\|\alpha\|_E^2 = \sum_{i=1}^{p-1} a_i^2$.

Also, note that by the Cauchy-Schwarz inequality,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2 = \Big(\sum_{j=1}^{p-1} a_j \Big)^2 \le (p-1) \sum_{j=1}^{p-1} a_j^2 = (p-1)\|\alpha\|_E^2,$$

so we conclude that

$$\|\alpha\|^2 \ge \Big(p^2 - (p+1)(p-1) \Big) \|\alpha\|_E^2 = \|\alpha\|_E^2.$$

In other words, the norm of α is always larger than or equal to the Euclidean norm of α.

5. The Normalized Distance

Let $B(p, N)$ be the hypercube

$$B(p, N) := \left\{a_1\omega + \ldots + a_{p-1}\omega^{p-1} : a_i \in \mathbb{Z} \cap [-N, N]\right\} \subset \mathcal{O}_K.$$

Then $B(p, N)$ contains $(2N + 1)^{p-1}$ points in total. In this section, we introduce a normalized distance on $B(p, N)$. To do so, we shall need to compute the diameter of the hypercube $B(p, N)$. This is done in the following lemma.

Lemma 2. *The diameter of $B(p, N)$, i.e., the maximum distance between two points in $B(p, N)$, is exactly*

$$\operatorname{diam} B(p, N) = 2Np\sqrt{p-1},$$

which is achieved by the following pairs of points

$$\alpha = \sum_{i=1}^{p-1} N(-\omega)^{i-1} = N\omega - N\omega^2 + \ldots + N\omega^{p-2} - N\omega^{p-1} \quad \textit{and} \quad \beta = -\alpha.$$

Proof. It suffices to maximize Equation (3) for $\alpha - \beta$, where $\alpha, \beta \in B(p, N)$. Note that

$$\alpha - \beta = 2\alpha = 2N\omega - 2N\omega^2 - \ldots + 2N\omega^{p-2} - 2N\omega^{p-1}.$$

It is easy to see that choosing such α and β would simultaneously maximize the Euclidean norm $\|\alpha - \beta\|_E^2$ and minimize the trace term $(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha - \beta))^2$, because in this case $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha - \beta) = 0$. Therefore, this pair must achieve the maximum distance. It follows from Lemma 1 that

$$(\operatorname{diam} B(p, N))^2 = \|\alpha - \beta\|^2 = p^2(p-1)(2N)^2,$$

as required. □

Definition 3. For $\alpha, \beta \in B(p, N)$, we define the *normalized distance* of α and β in the cube by

$$\mathfrak{d}_{p,N}(\alpha, \beta) = \frac{d(\alpha, \beta)}{2Np\sqrt{p-1}}.$$

If we normalize the metric in this way, then the diameter of the hypercube $B(p, N)$ is exactly 1. This normalized distance is not only more aesthetically appealing but also very useful in comparing the distribution of points in different hypercubes $B(p, N)$, as p and N vary.

6. Almost All Points in $B(p, N)$ are Almost Equi-distanced

In this section, we show that, in an appropriate sense, almost all points in $B(p, N)$ are "equi-distanced" from each other in the sense of Theorem 1. Our proof relies on

the explicit calculations of the second and fourth moments of the distances, which we define below.

Definition 4. Fix p, N, and let k be a positive integer. We define the *kth moment of distances between points in $B(p,N)$* to be the following averaged sum:

$$M_k(p,N) := \frac{1}{\#B(p,N)^2} \sum_{\alpha \in B(p,N)} \sum_{\beta \in B(p,N)} d(\alpha,\beta)^k.$$

6.1. Computation of the Second Moment

Now, we evaluate the second moment of the distances in the following lemmas.

Lemma 3. *For integers $r \geq 0$ and $N \geq 1$, consider the sum of powers*

$$S_r(N) := \sum_{-N \leq a \leq N} a^r.$$

Then we have:

$$\begin{aligned} S_r(N) &= 0, \quad \text{if } r \text{ is odd,} \\ S_2(N) &= \frac{1}{3}N(N+1)(2N+1), \\ S_4(N) &= \frac{1}{15}N(N+1)(2N+1)(3N^2+3N-1). \end{aligned}$$

Proof. When r is odd, the sum is zero because $a^r + (-a)^r = 0$. When r is even, this follows from the well-known Faulhaber's formula of sums of powers (see [3] for example). □

Lemma 4. *The second moment of distances between points in $B(p,N)$ is given by*

$$\begin{aligned} M_2(p,N) &= \frac{2}{3}(p^3 - 2p^2 + 1)N(N+1) \\ &= \frac{2}{3}p^3N^2 + O(p^2N^2 + p^3N). \end{aligned}$$

Proof. By Lemma 1, we have

$$\begin{aligned} \sum_{\alpha \in B(p,N)} \sum_{\beta \in B(p,N)} d(\alpha,\beta)^2 = \sum_{-N \leq a_1, b_1 \leq N} \cdots \sum_{-N \leq a_{p-1}, b_{p-1} \leq N} \Big(& p^2 \sum_{i=1}^{p-1} (a_i - b_i)^2 \\ & - (p+1) \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} (a_i - b_i)(a_j - b_j) \Big). \end{aligned}$$

We break this sum into two pieces by linearity. The first piece equals

$$p^2 \sum_{i=1}^{p-1} \sum_{-N \leq a_1, b_1 \leq N} \cdots \sum_{-N \leq a_{p-1}, b_{p-1} \leq N} (a_i - b_i)^2. \tag{4}$$

The second piece equals

$$(p+1)\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}(a_i-b_i)(a_j-b_j).$$

We now simplify the second piece. If $i\neq j$, then the terms a_i-b_i and a_j-b_j are independent, in which case the sum is zero because

$$\sum_{-N\le a_i,b_i\le N}(a_i-b_i)=0. \tag{5}$$

If $i=j$, then $(a_i-b_i)(a_j-b_j)=(a_i-b_i)^2$, in which case the sum becomes

$$(p+1)\sum_{i=1}^{p-1}\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}(a_i-b_i)^2,$$

which is exactly the same as Equation (4), up to a difference in the coefficient. It follows that

$$\begin{aligned}&\sum_{\alpha\in B(p,N)}\sum_{\beta\in B(p,N)}d(\alpha,\beta)^2\\&=(p^2-p-1)\sum_{i=1}^{p-1}\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}(a_i-b_i)^2\\&=(p^2-p-1)(p-1)(2N+1)^{2p-4}\sum_{-N\le a_1,\le b_1\le N}(a_1^2-2a_1b_1+b_1^2).\end{aligned}$$

Again, we break the above sum by linearity and note that

$$\sum_{-N\le a_1,b_1\le N}a_1b_1=\Big(\sum_{-N\le a_1\le N}a_1\Big)\Big(\sum_{-N\le b_1\le N}b_1\Big)=0, \tag{6}$$

and

$$\sum_{-N\le a_1,b_1\le N}(a_1^2+b_1^2)=2(2N+1)\sum_{-N\le a_i\le N}a_i^2=2(2N+1)S_2(N), \tag{7}$$

where the value of $S_2(N)$ is computed in Lemma 3. Therefore, we obtain

$$\begin{aligned}\sum_{\alpha\in B(p,N)}\sum_{\beta\in B(p,N)}d(\alpha,\beta)^2&=\frac{2}{3}(p^2-p-1)(p-1)(2N+1)^{2p-3}\cdot N(N+1)(2N+1)\\&=\frac{2}{3}(p^3-2p^2+1)N(N+1)(2N+1)^{2p-2},\end{aligned}$$

and the result follows from dividing the above quantity by $\#B(p,N)^2=(2N+1)^{2p-2}$. □

We will argue that almost all pairs of points $(\alpha, \beta) \in B(p,N)^2$ are almost $\sqrt{\mu}$ away from each other, where

$$\mu = \mu(p,N) = \frac{2}{3}p^3N^2 \tag{8}$$

is exactly the main term appearing in the expression in Lemma 4. To this end, we shall need to compute the fourth moment $M_4(p,N)$.

6.2. Computation of the Fourth Moment

The following lemma will be used several times in the evaluation of $M_4(p,N)$, so we prove it here explicitly.

Lemma 5. *We have*

$$\begin{aligned}\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}(a_i-b_i)^2(a_j-b_j)^2 \qquad (9)\\ = \frac{2}{45}N(N+1)(p-1)(10N^2p+4N^2+10Np+4N-3).\end{aligned}$$

Proof. We break Equation (9) into two pieces according to whether i equals j. The $i=j$ piece equals:

$$(2N+1)^{2p-4}(p-1)\sum_{-N\le a_1,b_1\le N}(a_1-b_1)^4. \tag{10}$$

Since $(a_1-b_1)^4 = (a_1^4+b_1^4)+4(a_1^3b+a_1b_1^3)+6a_1^2b_1^2$, we can further rewrite the sum in Equation (10) as

$$2(2N+1)\sum_{-N\le a_1\le N}a_1^4+6\Big(\sum_{-N\le a_1\le N}a_1^2\Big)^2,$$

since all terms with odd powers vanish. The above quantity can be computed directly using Lemma 3.

On the other hand, the $i\neq j$ piece of Equation (9) equals

$$(2N+1)^{2p-6}(p-1)(p-2)\Big(\sum_{-N\le a_1,b_1\le N}\Big(a_1-b_1\Big)^2\Big)^2. \tag{11}$$

The innermost sum inside the square has been previously calculated in Equations (6) and (7). The result now follows from combining the $i=j$ piece and the $i\neq j$ piece. We omit the details of the tedious calculation. □

Lemma 6. *The fourth moment of distances between points in $B(p,N)$ is given by*

$$\begin{aligned}M_4(p,N) =& \frac{2}{45}N(N+1)(p-1)((2N^2+2N)(5p^5-8p^4+p^3+8p^2-21p-18)\\ &-3(p^2-p-1)^2)\\ =& \frac{4}{9}p^6N^4+O(p^5N^4+p^6N^3).\end{aligned}$$

Proof. By Lemma 1, we need to compute

$$\begin{aligned}&\sum_{\alpha\in B(p,N)}\sum_{\beta\in B(p,N)} d(\alpha,\beta)^4\\ &= \sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}\Big(p^4\Big(\sum_{j=1}^{p-1}(a_j-b_j)^2\Big)^2\\ &\quad -2p^2(p+1)\Big(\sum_{i=1}^{p-1}\Big(a_i-b_i\Big)^2\Big)\Big(\sum_{j=1}^{p-1}\Big(a_j-b_j\Big)\Big)^2+(p+1)^2\Big(\sum_{j=1}^{p-1}(a_j-b_j)\Big)^4\Big).\end{aligned}$$

By linearity, similar to the proof of Lemma 4, we break up the sum above into three pieces.

The first piece of the sum equals

$$p^4\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}(a_i-b_i)^2(a_j-b_j)^2. \tag{12}$$

Observe that this has been calculated in Lemma 5

We now evaluate the second piece of the sum, which is

$$2p^2(p+1)\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}\sum_{i=1}^{p-1}(a_i-b_i)^2\Big(\sum_{i=1}^{p-1}(a_i-b_i)\Big)^2. \tag{13}$$

Omitting the coefficient $2p^2(p+1)$, Equation (13) equals

$$\begin{aligned}&\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\sum_{k=1}^{p-1}\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}(a_i-b_i)^2(a_j-b_j)(a_k-b_k)\\ &=\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\sum_{-N\le a_1,b_1\le N}\cdots\sum_{-N\le a_{p-1},b_{p-1}\le N}(a_i-b_i)^2(a_j-b_j)^2,\end{aligned}$$

because when $j\neq k$, the sum vanishes as in Equation (5). Hence, Equation (13) is the same as Equation (12), up to a constant multiple, so it can also be calculated using Lemma 5.

The third piece of the sum is

$$(p+1)^2 \sum_{-N\le a_1,b_1\le N} \cdots \sum_{-N\le a_{p-1},b_{p-1}\le N} \Big(\sum_{j=1}^{p-1}(a_j-b_j)\Big)^4. \tag{14}$$

Omitting the coefficient $(p+1)^2$, we may rewrite Equation (14) as

$$\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\sum_{k=1}^{p-1}\sum_{l=1}^{p-1} \sum_{-N\le a_1,b_1\le N} \cdots \sum_{-N\le a_{p-1},b_{p-1}\le N} (a_i-b_i)(a_j-b_j)(a_k-b_k)(a_l-b_l). \tag{15}$$

Depending on the relations between i, j, k, and l, the above sum can be split into pieces that correspond to the set of all integer partitions of 4. For example, if $i=j=k\neq l$, then the partition is $4=3+1$; if $i=j\neq k=l$, then the partition is $4=2+2$. Now, observe that if the partition has an odd number in it (which is either 1 or 3 in this case), then the sum must vanish because

$$\sum_{-N\le a_i,b_i\le N}(a_i-b_i) = \sum_{-N\le a_i,b_i\le N}(a_i-b_i)^3 = 0.$$

Hence, only the partitions $4=4$ and $4=2+2$ result in nonzero summands. Therefore, Equation (15) equals (omitting the coefficient $(p+1)^2$)

$$\begin{aligned}&\sum_{i=1}^{p-1} \sum_{-N\le a_1,b_1\le N} \cdots \sum_{-N\le a_{p-1},b_{p-1}\le N} (a_i-b_i)^4 \\ &+\frac{\binom{4}{2}}{2}\sum_{i=1}^{p-1}\sum_{\substack{j=1\\ j\neq i}}^{p-1} \sum_{-N\le a_1,b_1\le N} \cdots \sum_{-N\le a_{p-1},b_{p-1}\le N} (a_i-b_i)^2(a_j-b_j)^2,\end{aligned}$$

which can be further simplified to

$$\begin{aligned}&(p-1)(2N+1)^{2p-4} \sum_{-N\le a_1,b_1\le N}(a_1-b_1)^4 \\ &+3(p-1)(p-2)(2N+1)^{2p-6}\Big(\sum_{-N\le a_1,b_1\le N}(a_1-b_1)^2\Big)^2.\end{aligned}$$

We recognize that these two smaller sums have been previously calculated in the two subcases of Lemma 5 (see Equations (10) and (11), respectively). Again, we omit some details of the tedious calculation.

Now, combining these three pieces gives the total sum in the lemma, and dividing the quantity by $\#B(p,N)^2=(2N+1)^{2p-2}$ yields the result. □

Remark 2. We shall never appeal to the first explicit formula of $M_4(p,N)$ in Lemma 6. Rather, the second asymptotic estimate of $M_4(p,N)$ will be much more useful in the following analyses.

6.3. Computation of the Second Moment about the Mean

In this subsection, we apply Lemmas 4 and 6 to obtain an estimate of the *second moment of distances about the mean* between points in $B(p,N)$, which is formally defined by

$$R(p,N) := \frac{1}{\#B(p,N)^2} \sum_{\alpha\in B(p,N)} \sum_{\beta\in B(p,N)} (d(\alpha,\beta)^2-\mu)^2,$$

where μ is defined by Equation (8). $R(p,N)$ will play a crucial role in the proof of our main theorem, and the following lemma establishes an upper bound of this quantity.

Lemma 7. *We have*

$$R(p,N) \ll p^5N^4 + p^6N^3.$$

Proof. Indeed, we have

$$\sum_{\alpha,\beta}(d(\alpha,\beta)^2-\mu)^2 = \sum_{\alpha,\beta} d(\alpha,\beta)^4 - 2\mu\sum_{\alpha,\beta} d(\alpha,\beta)^2 + \mu^2(2N+1)^{2p-2}.$$

By Lemmas 4 and 6, we have

$$\begin{aligned} R(p,N) =& \frac{4}{9}p^6N^4 + O(p^5N^4+p^6N^3) - 2\cdot\left(\frac{2}{3}p^3N^2\right)\cdot\left(\frac{2}{3}p^3N^2 + O(p^2N^2+p^3N)\right) \\ &+ \left(\frac{2}{3}p^3N^2\right)^2 \\ \ll& p^5N^4 + p^6N^3, \end{aligned}$$

where the main terms cancel nicely, leaving us with only the big-O term. □

6.4. Proof of Theorem 1

Our main result Theorem 1 now follows immediately from the following quantitative estimate in Theorem 5. Note that, instead of normalizing the distance by a factor of $2Np\sqrt{p-1}$, we chose to normalize it by $2Np^{3/2}$ in Theorem 5. This choice makes the computations much cleaner, and it will not at all affect the end result since $2Np\sqrt{p-1}$ and $2Np^{3/2}$ are asymptotic as $p\to\infty$.

Theorem 5. *For any $\varepsilon>0$ and any positive positive integer N,*

$$\frac{1}{\#B(p,N)^2}\#\left\{(\alpha,\beta)\in B(p,N)^2 : \left|\frac{d(\alpha,\beta)}{2Np^{3/2}} - \frac{1}{\sqrt{6}}\right| > \varepsilon\right\} \ll \frac{1}{\varepsilon^2}\left(\frac{1}{p}+\frac{1}{N}\right). \quad (16)$$

Proof. Multiplying both sides of the required inequality in Equation (16) by $2Np^{3/2}$ gives us

$$\left|d(\alpha,\beta) - \sqrt{\frac{2}{3}}Np^{3/2}\right| > \varepsilon\cdot 2Np^{3/2},$$

which may be rewritten as

$$|d(\alpha,\beta)-\sqrt{\mu}|>\varepsilon\sqrt{6\mu}.$$

Also, note that

$$\left|d(\alpha,\beta)^2-\mu\right|=|d(\alpha,\beta)+\sqrt{\mu}|\,|d(\alpha,\beta)-\sqrt{\mu}|\geq\sqrt{\mu}\,|d(\alpha,\beta)-\sqrt{\mu}|\,.$$

Therefore, by Lemma 7,

$$\begin{aligned}
p^5N^4+p^6N^3 &\gg \frac{1}{\#B(p,N)^2}\sum_{\alpha,\beta}(d(\alpha,\beta)^2-\mu)^2\\
&\gg \frac{1}{\#B(p,N)^2}\sum_{\substack{\alpha,\beta\\ \left|d(\alpha,\beta)-\sqrt{\mu}\right|>\varepsilon\sqrt{6\mu}}}(d(\alpha,\beta)^2-\mu)^2\\
&\gg \frac{\#\left\{(\alpha,\beta)\in B(p,N)^2:\left|d(\alpha,\beta)-\sqrt{\mu}\right|>\varepsilon\sqrt{6\mu}\right\}}{\#B(p,N)^2}(\varepsilon\sqrt{6\mu}\cdot\sqrt{\mu})^2\\
&= \frac{\#\left\{(\alpha,\beta)\in B(p,N)^2:\left|d(\alpha,\beta)/(2Np^{3/2})-1/\sqrt{6}\right|\right\}}{\#B(p,N)^2}6\varepsilon^2\mu^2.
\end{aligned}$$

Therefore, dividing both sides by $6\varepsilon^2\mu^2$, we have

$$\begin{aligned}
\frac{1}{\#B(p,N)^2}\#\left\{(\alpha,\beta)\in B(p,N)^2:\left|\frac{d(\alpha,\beta)}{2Np^{3/2}}-\frac{1}{\sqrt{6}}\right|>\varepsilon\right\} &\ll \frac{1}{6\varepsilon^2}\frac{p^5N^4+p^6N^3}{\mu^2}\\
&\ll \frac{1}{\varepsilon^2}\Big(\frac{1}{p}+\frac{1}{N}\Big).
\end{aligned}$$

□

Acknowledgement. The authors are grateful to the referee for their comments and suggestions.

References

[1] J. Anderson, C. Cobeli, and A. Zaharescu, Counterintuitive patterns on angles and distances between lattice points in high dimensional hypercubes, *Results Math.* **79 (2)** (2024), #A94.

[2] J. S. Athreya, C. Cobeli, and A. Zaharescu, Visibility phenomena in hypercubes, *Chaos Solitons Fractals* **175 (1)** (2023), #A114024.

[3] D. E. Knuth, Johann Faulhaber and sums of powers, *Math. Comp.* **61** (1993), 277-294.

[4] A. Malik, F. Stan, and A. Zaharescu, The Siegel norm, the length function and character values of finite groups, *Indag. Math.* **25 (3)** (2014), 475-486.

[5] D. A. Marcus, *Number Fields*, Springer, New York, 2018.

[6] J. Neukirch and N. Schappacher, *Algebraic Number Theory*, Springer Berlin, Heidelberg, 1999.

[7] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, Springer Berlin, Heidelberg, 2008.

[8] C. L. Siegel, The trace of totally positive and real algebraic integers, *Ann. of Math.* **46 (2)** (1945), 302-312.

[9] F. Stan and A. Zaharescu, Siegel's trace problem and character values of finite groups, *J. Reine Angew. Math.* **637** (2009), 217-234.

[10] F. Stan and A. Zaharescu, The Siegel norm of algebraic numbers, *Bull. Math. Soc. Sci. Math. Roumanie* **55 (103)** (2012), 69-77.

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.