ON THE MINIMUM NORM OF REPRESENTATIVES OF RESIDUE CLASSES IN NUMBER FIELDS

Jean Bourgain Mei-Chu Chang

ABSTRACT

In this paper we consider the problem of finding upperbounds on the minimum norm of representatives in residue classes in quotient O/I, where I is an integral ideal in the maximal order O of a number field K. In particular, we answer affirmatively a question of Konyagin and Shparlinski, stating that an upperbound $o(N(I))$ holds for most ideals I, denoting $N(I)$ the norm of I. More precise statements are obtained, especially when I is prime. We use the method of exponential sums over multiplicative groups, exploiting essentially the new bounds obtained by the methods in [BC1] and [BC2].

Introduction.

Let I be an integral ideal in an algebraic number field K. For a residue class $\alpha \in O/I$, denote by $N_I(\alpha)$ the minimal norm of all elements of α. Thus

$$N_I(\alpha) = \min_{x \in \alpha} |N(x)|. \tag{0.1}$$

Following [KS] (Chapter 9), we define further

$$L(K, I) = \max_{\alpha \in (O/I)^*} N_I(\alpha). \tag{0.2}$$

The inequality

$$L(K, I) < N(I) = |O/I| \tag{0.3}$$

for all integral ideals (even for principal ideal only) means that K is Euclidean with respect to its norm. Only few examples of Euclidean number fields are known. However, one may hope to establish estimates of the form

$$L(K, I) = o(N(I)), \tag{0.4}$$

or even

$$L(K, I) \ll N(I)^{1-\varepsilon}, \text{ for some } \varepsilon > 0, \tag{0.5}$$

for 'most' integral ideals, which would mean that K is 'roughly' Euclidean.

The purpose of this paper is to pursue a line of research exposed in [KS]. (See [KS], Chapter 9 for related references.) Let us be more precise. In [KS], inequalities of the form (0.5) were obtained, assuming O has an infinite group of units, for a sequence of prime ideals of asymptotic density 1. (See [KS], Theorem 9.10.). In this statement, it suffices to consider only prime ideals of first degree. The key ingredients then in [KS] to obtain estimates in this case are bounds on exponential sums over prime fields. Our first set of results (see Sections 3 and 4) provide further refinements for the prime case $I = \mathcal{P}$. We are able to treat as well the situation where $\mathcal{P}$ is not of first degree and moreover obtain a much smaller exceptional set of prime ideals. In Corollary 4.1 below, we show that for all $\delta > 0$, there is $\varepsilon > 0$ such that (0.5) is valid for all but at most T^{δ} prime ideals $\mathcal{P}$ of norm $N(\mathcal{P}) \leq T$. The method exploited here is roughly the same as in [KS] and the key issues are uniform distribution properties of the group U of the units in the quotient O/I. These are expressed by exponential sum bounds. At this point, we are able to rely on the recent theory developed in [BGK], [B], [BC2], [BC1], which qualitatively does better than estimates so far available. First in [BGK], non-trivial exponential sum bounds over multiplicative subgroups G of prime fields $\mathbb{F}_p$ were obtained, under the very weak assumption $|G| > p^{\varepsilon}$, with $\varepsilon > 0$ arbitrary (earlier

results based on variants of Stepanov's method requiring $\varepsilon > \frac{1}{4}$). Then, in [BC1], similar results were shown for subgroups G of $\mathbb{F}_{p^f}^*$, with $f > 1$ (where prior to this little was known if $|G| < p^{\frac{f}{2}}$). Following the method in [KS], the relevant group G is $\phi(U)$, with $\phi : O \to O/\mathcal{P}$ the quotient map. Therefore, we are concerned with $\phi(U)$ being sufficiently large, say

$$|\phi(U)| > N(\mathcal{P})^{\varepsilon}, \text{ for some } \varepsilon > 0$$

so that our exponential sum bounds become applicable. (See Theorem 3.1 below.) This property obviously depends on the given prime ideal $\mathcal{P}$. Let us next consider the case of general integral ideals I. The quotient O/I is not necessarily a field and the method of [KS] needs to be modified appropriately. The main analytical ingredient now becomes an exponential sum estimate from [BC2] (Theorem 3.1). Roughly speaking it is applied in the situation where O/I essentially factors as a product of a few prime fields. This requires some restrictions on the ideals I under consideration, but the excluded sets are still of zero density. The main result is formulated in Theorem 5.1 below and states that (0.4) holds (actually in the form (0.5)) for almost all integral ideals I in O. This answers Question 9.14 from [KS] affirmatively. (In [KS] (see p.5), the problem is attributed to Egami.) Paraphrasing [KS], the meaning of this result for principal ideals is that the Euclidean algorithm may be applied and moreover runs in a sub-logarithmic number of steps (which is of course not the case in $\mathbb{Z}$) for the majority of the inputs.

We conclude with the following comment. It is possible to carry out an approach in a similar spirit but relying on ergodic methods rather than exponential sums. But for this, we need to make the stronger assumption that the group U contains at least two independent units. In this situation, we may appeal to Furstenberg's disjointness theory (See [F]) and its higher dimensional version due to Berend (See [Be]), characterizing invariant sets. The ergodic techniques perform very well qualitatively speaking

but are essentially non-effective. (So far estimates derived from 'effective' versions are extremely weak.) Along these lines, E. Lindenstrauss observed that (0.4) holds for $N(I) \to \infty$ with no exceptional subset, provided there are two independent units that do not belong to a proper subfield.

§1. Preliminaries.

Let K be a finite extension of $\mathbb{Q}$, $[K : \mathbb{Q}] = n = r_1 + 2r_2$ with r_1 (respectively r_2) the number of real (resp. complex) embeddings f_i of K in $\mathbb{C}$.

Let $O = O(K)$ be the ring of algebraic integers in K.

Denote $U = U(K)$ the group of units of K. Thus U is the direct product of the group $E = E(K)$ of roots of unity and a free Abelian group with $r_1 + r_2 - 1$ generators.

Fix an integral basis $z_1, \dots, z_n$. If $x \in O$ and $x = \sum x_i z_i, x_i \in \mathbb{Z}$, we have for the norm

$$N(x) = \prod_{j=1}^{n} f_j(x).$$

Hence

$$|N(x)| < \max_{i,j} f_j(x_i) \Big(\sum |x_i| \Big)^n = C \Big(\sum |x_i| \Big)^n \tag{1.1}$$

where $C = C(z_1, \dots, z_n)$ is a constant depending on K.

Let I be an ideal in O and $x \in I \backslash \{0\}$. Then $N(I) = |O/I|$ divides $N(x)$ and by (1.1)

$$\max |x_i| > cN(I)^{1/n} \text{ for } x \in I \backslash \{0\}. \tag{1.2}$$

Consider the lattice $\mathcal{L}$ associated to I

$$\mathcal{L} = \{(x_i)_{1 \le i \le n} \in \mathbb{Z}^n : \sum x_i z_i \in I\}$$

of determinant $d(\mathcal{L}) = N(I)$.

Denoting $\lambda_1, \dots, \lambda_n$ the consecutive minima of $\mathcal{L}$ with respect to the unit box, it follows from Minkowski's theorem that

$$\lambda_1 \dots \lambda_n \leq 2^n d(\mathcal{L}) \sim N(I). \tag{1.3}$$

Since by (1.2)

$$cN(I)^{1/n} < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$$

necessarily

$$\lambda_1 \sim \cdots \sim \lambda_n \sim N(I)^{1/n}. \tag{1.4}$$

Therefore $\mathcal{L}$ has a set of generators $v_1, \dots, v_n \in \mathbb{Z}^n$ satisfying the properties

$$C_1^{-1} N(I)^{1/n} < |v_i| < C_1 N(I)^{1/n} \tag{1.5}$$

and

$$\Big\{ \sum x_i e_i : |x_i| < N(I)^{1/n} \Big\} \subset \Big\{ \sum t_i v_i : |t_i| < C_2 \Big\} \tag{1.6}$$

where C_1, C_2 depend only on K (not on the ideal I).

In other words, $\mathcal{L} = \mathcal{L}_I$ is a lattice of determinant $d(\mathcal{L}) = N(I)$ and does not degenerate for $N(I) \to \infty$.

Denoting $\varphi : O \to O/I$ the quotient map, (1.2) implies that the restriction of φ to the set $\{\sum x_i z_i : |x_i| < \frac{c}{2} N(I)^{1/n}\}$ is one-to-one.

A useful notion is the height of an integral element. Let $z_1, \cdots, z_n$ be an integral basis, and let $x = \sum x_i z_i$. Then the *height* of x is

$$h(x) = \max_i |x_i|$$

The following properties are easy to check.

(1.7) $h(xy) \leq C(K)\, h(x)h(y)$.

(1.8) $h(x+y) \le h(x) + h(y);\ h(x-1) \le h(x) + C(K)$.

(1.9) $|N(x)| < C(K)\ h(x)^n$.

Here (and through out the paper) $C(K)$ denotes various constant depending on K.

§2 Exponential sum bounds on finite fields.

We will use the exponential sum bound for subgroups $G < \mathbb{F}_{p^f}^*$ obtained in [BC1].

Theorem 2.1. $[BC1]$.

Let $G < \mathbb{F}_{p^f}^*$ where $f \in \mathbb{Z}_+$ is arbitrary fixed and p large.

For all $\varepsilon > 0$ there is $\delta = \delta(f, \varepsilon)$ such that if

$$|G \cap F| < p^{-\varepsilon}|G| \tag{2.2}$$

for all proper subfields F of $\mathbb{F}_{p^f}$, then

$$\max_{\mathcal{X} \neq \mathcal{X}_0} \Big| \sum_{x \in G} \mathcal{X}(x) \Big| < p^{-\delta}|G| \tag{2.3}$$

where $\mathcal{X}$ runs over all non-trivial additive characters of $\mathbb{F}_{p^f}$.

Remark Let $G < \mathbb{F}_{p^f}^*$ and

$$|G| > p^{\varepsilon_o}. \tag{2.4}$$

Then there is $G' < G$,

$$|G'| > p^{\frac{\varepsilon_0}{2}} \tag{2.5}$$

such that for any additive character $\mathcal{X}$ of $\mathbb{F}_{p^f}$, either

$$\sum_{x \in G'} \mathcal{X}(x) = |G'|, \tag{2.6}$$

or

$$\Big| \sum_{x \in G'} \mathcal{X}(x) \Big| < p^{-\delta}|G'|. \tag{2.7}$$

In fact, take $\varepsilon = \frac{\varepsilon_0}{10f}$. If the assumption (2.2) is not satisfied, there is a proper subfield F_1 of $\mathbb{F}_{p^f}, |F_1| = p^{f_1}, f_1 < f$, such that

$$|G_1| > p^{\varepsilon_0 - \varepsilon} \text{ where } G_1 = G \cap F_1^*.$$

Either $|G_1 \cap F| < p^{-\varepsilon}|G_1|$ for any proper subfield F of F_1 or we may reduce G_1 further to $G_2 = G_1 \cap F_2^*$ where F_2 is a proper subfield of F_1, $|F_2| = p^{f_2}, f_2 < f_1$ and

$$|G_2| > p^{-\varepsilon}|G_1| > p^{\varepsilon_0 - 2\varepsilon}.$$

Continuing, we obtain a subfield F of $\mathbb{F}_{p^f}$ such that $G' = G \cap F^*$ satisfies

$$|G' \cap F_0| < p^{-\varepsilon}|G'| \text{ for any proper subfield } F_0 \text{ of } F$$

and

$$|G'| > p^{\varepsilon_0 - f\varepsilon} > p^{\frac{\varepsilon_0}{2}}.$$

At this point, we may apply Theorem 2.1 to the subgroup G' of F^*. It follows that if $\mathcal{X}$ is an additive character of $\mathbb{F}_{p^f}$, then either

$$\sum_{x \in G'} \mathcal{X}(x) = |G'|$$

or

$$\Big| \sum_{x \in G'} \mathcal{X}(x) \Big| < p^{-\delta}|G'|$$

depending on whether the restriction of $\mathcal{X}$ to the subfield F of $\mathbb{F}_{p^f}$ is trivial or not.

§3. The estimates for a prime ideal.

Theorem 3.1. *Let $\mathcal{P}$ be a prime ideal in O, $N(\mathcal{P}) = p^f$ where $f \leq n$ is the degree of $\mathcal{P}$. Denote $\varphi : O \to O/\mathcal{P} \approx \mathbb{F}_{p^f}$ the quotient map and assume*

$$|\varphi(U)| > p^{\varepsilon_0} \tag{3.2}$$

with $\varepsilon_0 > 0$ arbitrary and fixed.

Then there is $\delta_0 = \delta(\varepsilon_0, K) > 0$ such that

$$L(K, \mathcal{P}) := \max_{\alpha \in (O/\mathcal{P})^*} \min_{x \in \alpha} |N(x)| < N(\mathcal{P})^{1-\delta_0} \tag{3.3}$$

(assuming p sufficiently large).

Proof.

It is a variant of the argument in [KS], Ch. 9.

Define

$$\mathcal{B} = \Big\{ \sum x_i z_i : x_i \in \mathbb{Z}, 0 \le x_i \le h \Big\}$$

where we take

$$h = p^{-\delta_0} N(\mathcal{P})^{\frac{1}{n}} \tag{3.4}$$

(δ_0 to be specified in (3.11)).

Let $\alpha \in O/\mathcal{P}$ and $a \in \alpha$. Assume we showed that for some $y \in U$

$$\varphi(ay) \in \varphi(\mathcal{B} - \mathcal{B}). \tag{3.5}$$

Hence there are $x_i \in \mathbb{Z}, |x_i| \le h$ such that $x = y^{-1}(\sum x_i z_i) \in \alpha$ and

$$N(x) = N\Big(\sum x_i z_i \Big) < Ch^n < Cp^{-n\delta_0} N(\mathcal{P}) < N(\mathcal{P})^{1-\delta_0}. \tag{3.6}$$

It remains to establish (3.5) and we will proceed with the usual circle method. First, we consider the multiplicative group $G = \varphi(U)$ of $(O/\mathcal{P})^* \cong \mathbb{F}_{p^f}^*$, and apply the reduction process described in the Remark in §2. Therefore, we obtain $G' = G \cap F^*$, $|G'| > p^{\varepsilon_0/2}$, where F is a subfield of $O/\mathcal{P}$ and either (2.6) or (2.7) hold, for any additive character $\mathcal{X}$ of $O/\mathcal{P}$.

If we show that

$$\sum_{\mathcal{X}} \Big[\sum_{y \in G'} \mathcal{X}(\alpha y) \Big] \Big| \sum_{z \in \varphi(\mathcal{B})} \mathcal{X}(z) \Big|^2 \neq 0 \tag{3.7}$$

where $\mathcal{X}$ is taken in the system of additive characters $\{\mathcal{X}\}$ of $O/\mathcal{P}$, it will follow that

$$\alpha G' \cap \varphi(\mathcal{B} - \mathcal{B}) \neq \phi.$$

Thus (3.5) holds for some $y \in U$. Hence (3.6) is proved.

Assuming $\alpha \neq 0$, rewrite (3.7) as

$$\sum_{\mathcal{X}} \Big[\sum_{y \in G'} \mathcal{X}(y) \Big] \Big| \sum_{z \in \varphi(\mathcal{B})} \mathcal{X}(\alpha^{-1} z) \Big|^2. \tag{3.8}$$

We will use the circle method and write $\sum_{\mathcal{X}}$ in (3.8) as two summations. If $\mathcal{X}$ has trivial restriction to F, in particular if $\mathcal{X} = \mathcal{X}_0$, the trivial character of $\mathbb{F}_{p^f}$, then $\sum_{y \in G'} \mathcal{X}(y) = |G'|$.

Hence, since $|\varphi(\mathcal{B})| = |\mathcal{B}|$

$$\begin{aligned}
&\sum_{\mathcal{X}|_F \text{ trivial}} \Big| \sum_{y \in G'} \mathcal{X}(y) \Big| \Big| \sum_{z \in \varphi(\mathcal{B})} \mathcal{X}(\alpha^{-1} z) \Big|^2 \\
&= |G'| \Big(|\mathcal{B}|^2 + \sum_{\substack{\mathcal{X} \neq \mathcal{X}_0 \\ \mathcal{X}|_F \text{ trivial}}} \Big| \sum_{z \in \varphi(\mathcal{B})} \mathcal{X}(\alpha^{-1} z) \Big|^2 \Big) \\
&\geq |G'| \, |B|^2.
\end{aligned} \tag{3.9}$$

If $\mathcal{X}|_F$ is non-trivial, then (2.7) holds and by Parseval

$$\begin{aligned}
&\sum_{\mathcal{X}|_F \text{ nontrivial}} \Big| \sum_{y \in G'} \mathcal{X}(y) \Big| \Big| \sum_{z \in \varphi(\mathcal{B})} \mathcal{X}(\alpha^{-1} z) \Big|^2 \\
&< p^{-\delta} \, |G'| \sum_{\mathcal{X}} \Big| \sum_{z \in \varphi(\mathcal{B})} \mathcal{X}(\alpha^{-1} z) \Big|^2 \\
&= p^{-\delta} \, |G'| \, p^f \, |\varphi(\mathcal{B})|.
\end{aligned} \tag{3.10}$$

To insure (3.7), we let $\sum_{\chi|_F \text{ trivial}} > \sum_{\chi|_F \text{ nontrivial}}$ by taking $|\mathcal{B}| = h^n > p^{f-\delta}$ or $h > N(\mathcal{P})^{\frac{1}{n}} p^{-\frac{\delta}{n}}$ and

$$\delta_0 < \frac{\delta}{n} \tag{3.11}$$

in (3.4). This completes the proof.

§4. The prime ideal case.

Corollary 4.1. *Assume $U(K)$ infinite, i.e. $r_1 + r_2 - 1 > 0$.*

For all $\varepsilon > 0$, there is $\delta > 0$, $\delta = \delta(\varepsilon, K)$, such that for $T \to \infty$

$$\left|\{\mathcal{P} : \mathcal{P} \text{ is a prime ideal with } N(\mathcal{P}) \le T,\ \ L(K, \mathcal{P}) > N(\mathcal{P})^{1-\delta}\}\right| < T^{\varepsilon} \tag{4.2}$$

Recall that if $\pi_K(T)$ denotes the number of prime ideals of norm at most T, then

$$\pi_K(T) = \big(1 + o(1)\big)\frac{T}{\log T} \tag{4.3}$$

(see [N], p. 326, Cor. 1).

Proof of Corollary 4.1

Take $\xi \in U(K)\backslash E(K)$. In order to apply Theorem 3.1, we rule out those prime ideals $\mathcal{P}$ of norm at most T for which

$$|\varphi(\langle \xi \rangle)| \le |\varphi(U)| < T^{\varepsilon_0} \tag{4.4}$$

where $\varphi : O \to O/\mathcal{P}$ is the quotient map and $\varepsilon_0 > 0$ is arbitrary.

If (4.4) fails, then (3.3) holds with $\delta_0 = \delta_0(\varepsilon_0) > 0$.

Assuming (4.4), there is a positive integer $k < T^{\varepsilon_0}$ such that $\varphi(\xi^k) = 1$, hence $\mathcal{P}$ divides $\xi^k - 1 \in O\backslash\{0\}$. Therefore $N(\mathcal{P}) = p^f$ divides the integer

$$B = \prod_{k < T^{\varepsilon_0}} N(\xi^k - 1) \tag{4.5}$$

which is clearly bounded by $\prod_{k<T^{\varepsilon_0}} C(K)^k < C(K)^{T^{2\varepsilon_0}}$.

Therefore B has at most $C\frac{T^{2\varepsilon_0}}{\log T}$ prime divisors p. Since there are at most n prime ideals $\mathcal{P}$ above a given p, the number of exceptional prime ideals is at most $T^{3\varepsilon_0}$.

The others will satisfy

$$L(K,\mathcal{P}) < N(\mathcal{P})^{1-\delta_0}$$

for some $\delta_0 = \delta_0(\varepsilon_0, K)$.

Remark.

A result in the same spirit as Corollary 4.1 is obtained in Theorem 9.10 of [KS]. In [KS], only an exceptional sequence of prime ideals of asymptotic density 0 is excluded. Since the number $\pi'_K(T)$ of prime ideals of first degree over $\mathbb{Q}$ with norm at most T satisfies the same asymptotic (4.3), thus

$$\pi'_K(T) = \big(1+o(1)\big)\frac{T}{\log T} \tag{4.6}$$

(cf. [N], Cor. 2, p. 326), the problem reduces then to first degree prime ideals and exponential sum estimates in prime fields $\mathbb{F}_p$.

§5. The case of general integral ideals.

Let us now consider the case of a general ideal I in O_K. Our aim is to give a positive answer to Question 9.14 in [KS] in the following form:

Theorem 5.1. *Assume $U(K)$ infinite (the number field K is fixed).*

Then there is $\delta' = \delta'(\delta)$, $\delta' \to 0$ as $\delta \to 0$ such that

$$L(K,I) := \max_{\alpha \in (O/I)^*} \min_{x\in\alpha} N(x) < N(I)^{1-\delta} \tag{5.2}$$

holds for all ideals I in O outside a sequence of asymptotic density at most δ'. Hence

$$L(K,I) = o\big(N(I)\big) \tag{5.3}$$

for almost all ideals I in O.

Following [N], denote $M(T)$ the number of ideals I in O of norm $N(I) \leq T$. By the 'ideal theorem' (see [N], p. 327)

$$M(T) = \big(h(K)\kappa + o(1)\big)T \tag{5.4}$$

where $h(K)$ is the class number of K and

$$\kappa = \kappa(K) = 2^{r_1}(2\pi)^{r_2} R(K)\ |d(K)|^{-1/2} w(K)^{-1} \tag{5.5}$$

with $R(K)$ the regulator, $d(K)$ the discriminant and $w(K) = |E(K)|$ (see [N], p. 282).

We will first make several reductions (outside sequences of small density) of the ideals under consideration. Let

$$I = \prod_{i=1}^{m} \mathcal{P}_i^{a_i} = \prod_{\mathcal{P}} \mathcal{P}^{a(\mathcal{P})}$$

be the factorization of I in prime ideals. Then

$$T \geq N(I) = \prod_i N(\mathcal{P}_i)^{a_i} = \prod_i p_i^{f_i a_i} \tag{5.6}$$

where f_i is the degree of $\mathcal{P}_i$. Rewrite (5.6) as

$$N(I) = \prod_{p \text{ prime}} p^{\sum\limits_{p|N(\mathcal{P})} a(\mathcal{P}) f(\mathcal{P})}. \tag{5.7}$$

For any fixed prime number p, by (5.4) we get

$$\begin{aligned}
&\Big|\Big\{I : N(I) \leq T \text{ and } \sum_{p|N(\mathcal{P})} a(\mathcal{P}) f(\mathcal{P}) \geq 2\Big\}\Big| \\
&\leq \sum_{s\geq 2} s^n \left|\left\{I' : N(I') \leq \frac{T}{p^s}\right\}\right| \\
&< C_K T \sum_{s\geq 2} s^n p^{-s} \\
&< C'_K p^{-2} T.
\end{aligned} \tag{5.8}$$

Therefore, the number of ideals I with $N(I) \leq T$, and in expression (5.7), for some $p > C_1$, $\sum_{p|N(\mathcal{P})} a(\mathcal{P})f(\mathcal{P}) \geq 2$ is bounded by

$$\sum_{p>C_1} C'_K p^{-2} T < \frac{C'_K T}{C_1},$$

where $C_1 = C_1(\delta')$. Taking again (5.4) into account, we may therefore restrict ourselves to ideals

$$I = \prod \mathcal{P}^{\,a(\mathcal{P})}$$

with

$$\sum_{p|N(\mathcal{P})} a(\mathcal{P})f(\mathcal{P}) \leq 1 \text{ if } p > C_1 = C_1(\delta'). \tag{5.9}$$

In particular, if $N(\mathcal{P})$ is large enough and $a(\mathcal{P}) > 0$, then $a(\mathcal{P}) = 1$ and $\mathcal{P}$ is of first degree.

It follows that the ring

$$O/I \simeq \prod O/\mathcal{P}^{\,a(\mathcal{P})}$$

has the form

$$O/I = O/I_0 \times \prod \mathbb{F}_p \tag{5.10}$$

where

$$I_0 = \prod_{p \leq C_1} \mathcal{P}^{\,a(\mathcal{P})}$$

and the second product in (5.10) extends over primes $p > C_1$ to which $\sum_{p|N(\mathcal{P})} a(\mathcal{P}) = 1$.

Let $\xi \in U(K)\backslash E(K)$.

Denoting $\varphi_{\mathcal{P}} : O \to O/\mathcal{P}$ the quotient map, we already showed in the proof of Corollary 4.1 that for $\gamma < \frac{1}{2}$

$$\left|\left\{\mathcal{P} : \mathcal{P} \text{ is a prime ideal, } N(\mathcal{P}) \leq T \text{ and } |\varphi_{\mathcal{P}}(\langle\xi\rangle)| < T^{\gamma}\right\}\right| < T^{3\gamma}. \tag{5.11}$$

Let $\mathcal{I}$ be the collection of ideals I with the following properties

(a). I satisfies (5.9).

(b). $N(I) \le T$.

(c). There is a prime ideal $\mathcal{P}|I$ with $N(\mathcal{P}) > T^{\varepsilon_1}$ and $|\varphi_{\mathcal{P}}(U)| < N(\mathcal{P})^{1/4}$.

Hence by (5.4) and (5.11) (with $T = 2^{k+1}$ and $\gamma = \frac{1}{4}$), we have

$$\begin{aligned}
|\mathcal{I}| &< \sum_{\substack{N(\mathcal{P})=p>T^{\varepsilon_1} \\ |\varphi_{\mathcal{P}}(U)|<p^{1/4}}} \frac{T}{p} \\
&< \sum_{\substack{k\in\mathbb{Z}_+ \\ 2^k>T^{\varepsilon_1}}} \sum_{\substack{2^{k+1}>p>2^k \\ N(\mathcal{P})=p>T^{\varepsilon_1} \\ |\varphi_{\mathcal{P}}(U)|<p^{1/4}}} \frac{T}{2^k} \\
&< \sum_{\substack{k\in\mathbb{Z}_+ \\ 2^k>T^{\varepsilon_1}}} \frac{T}{2^k} \ |\{\mathcal{P} : \mathcal{P} \text{ is prime, } N(\mathcal{P}) < 2^{k+1} \text{ and } |\varphi_{\mathcal{P}}(U)| < 2^{\frac{k+1}{4}}\}| \\
&< \sum_{\substack{k\in\mathbb{Z}_+ \\ 2^k>T^{\varepsilon_1}}} \frac{T}{2^k} \ 2^{\frac{3(k+1)}{4}} \\
&< T^{1-\frac{\varepsilon_1}{5}}. \qquad (5.12)
\end{aligned}$$

We may therefore further assume that I satisfies

$$|\varphi_{\mathcal{P}}(U)| > N(\mathcal{P})^{1/4} \qquad (5.13)$$

for any prime ideal $\mathcal{P}$ dividing I with $N(\mathcal{P}) > N(I)^{\varepsilon_1}$ ($\varepsilon_1 > 0$ an arbitrary small fixed constant).

Finally we will restrict I as to ensure that, roughly speaking, $N(I)$ is a product of a few large prime factors and an integer of size at most $N(I)^{\varepsilon}$. This may be ensured again by excluding a sequence of small density.

One can use the following property (see Lemma 7, p. 264 in [HR]).

Lemma 5.14. $[HR]$.

Fix $\varepsilon > 0$ a small number and decompose every integer $0 < m \leq T$ as product $m = n^{(1)}.n^{(2)}$ where $n^{(1)}$ (respectively, $n^{(2)}$) is composed only of prime factors $p \leq T^{\varepsilon^2}$ (resp. $p > T^{\varepsilon^2}$). Then

$$k = |\{0 < m \leq T : n^{(1)} > T^{\varepsilon}\}| < C\varepsilon T. \tag{5.15}$$

We recall the elegant proof from [HR].

Proof of Lemma 5.14.

The exponent of the prime p in $T!$ is at most $\frac{T}{p} + \frac{T}{p^2} + \frac{T}{p^3} + \cdots < 2\frac{T}{p}$. Estimate

$$\begin{aligned} k \log T^{\varepsilon} &\leq \sum_{m<T} \log n^{(1)} \\ &< 2 \sum_{p<T^{\varepsilon^2}} \frac{T}{p} \log p \\ &< \sum_{2^{k+1}<T^{\varepsilon^2}} \sum_{2^k \leq p < 2^{k+1}} 2\,\frac{T}{2^k} \log p \\ &\lesssim \sum_{2^{k+1}<T^{\varepsilon^2}} \frac{2T}{2^k} \log 2^{k+1} \frac{2^{k+1}}{\log 2^{k+1}} = 4T \log T^{\varepsilon^2} \sim \varepsilon T \log T^{\varepsilon} \end{aligned}$$

and (5.15) follows.

Take

$$\varepsilon_2 = \frac{\varepsilon_1}{20} \ll \delta'. \tag{5.16}$$

Returning to (5.10), we can restrict ourselves to ideals $I, N(I) \sim T$ for which O/I has the form

$$O/I \simeq O/I_0 \times \prod_{p|n^{(1)}} \mathbb{F}_p \times \prod_{p|n^{(2)}} \mathbb{F}_p \tag{5.17}$$

where $n^{(1)}, n^{(2)}$ are integers depending on I such that $n^{(1)} < T^{\varepsilon_2}$ and $n^{(2)}$ has only prime factors $p > T^{\varepsilon_2^2}$ (hence at most ε_2^{-2} of them). Moreover we assume that $N(I)$, hence $n^{(2)}$ has a prime divisor $p > T^{\varepsilon_1}$.

Denote $G = \varphi_I(U)$ which is a multiplicative subgroup of (5.17).

Taking $p|n^{(2)}$ a prime of size at least T^{ε_1} and $\mathcal{P}$ the corresponding prime ideal dividing I of norm $N(\mathcal{P}) = p$, we have from the preceding

$$|G| \geq |\varphi_{\mathcal{P}}(U)| > N(\mathcal{P})^{\frac{1}{4}} > T^{\frac{\varepsilon_1}{4}}. \tag{5.18}$$

We now make the following construction.

Define

$$G_0 = \{x \in G : \pi_0(x) = 1 \text{ and } \pi_p(x) = 1 \text{ for all } p\big|n^{(1)}\} \tag{5.19}$$

(we define here π_0, π_p the obvious projections in (5.17)).

If for all $p|n^{(2)}$ we have

$$|\pi_p(G_0)| > T^{\varepsilon_2^3}, \tag{5.20}$$

then we let $G' = G_0$.

If not, let $p_1|n^{(2)}$ such that $|\pi_{p_1}(G_0)| \leq T^{\varepsilon_2^3}$ and reduce G_0 to

$$G_1 = \{x \in G_0 : \pi_{p_1}(x) = 1\}. \tag{5.21}$$

If G_1 satisfies (5.20) for all $p|\frac{n^{(2)}}{p_1}$, let $G' = G_1$. Otherwise repeat the construction. In this way, a sequence of prime divisors $p_1, \ldots, p_s$ ($s < \varepsilon_2^{-2}$) of $n^{(2)}$ is obtained such that if

$$G' = G_s = \{x \in G_0 : \pi_{p_1}(x) = \cdots = \pi_{p_s}(x) = 1\} \tag{5.22}$$

then

$$|\pi_p(G')| > T^{\varepsilon_2^3} \text{ for all } p|m = \frac{n^{(2)}}{p_1 \cdots p_s}. \tag{5.23}$$

Observe that

$$|G| \le |O/I_0|\ n^{(1)}\ |G_0| < CT^{\varepsilon_2}|G_0|$$

and from the construction

$$|G_0| < T^{\varepsilon_2^3}|G_1|$$

$$\vdots$$

$$|G_{s-1}| < T^{\varepsilon_2^3}|G'|.$$

Therefore by (5.16) and (5.18),

$$|G'| \gtrsim |G|\ T^{-\varepsilon_2}T^{-s\varepsilon_2^3} > T^{-3\varepsilon_2}|G| > T^{\varepsilon_1/10}. \tag{5.24}$$

Denote

$$I = I_1.I'$$

where

$$I_1 = I_0. \prod_{\mathcal{P}|I,\ N(\mathcal{P})|n^{(1)}p_1\dots p_s} \mathcal{P} \qquad \text{and } I' = \prod_{N(\mathcal{P})|m} \mathcal{P}. \tag{5.25}$$

Thus $G' = \{1\} \times \varphi_{I'}(G')$ in $O/I_1 \times O/I'$.

Consider the multiplicative group $\varphi_{I'}(G')$ of the ring $O/I' \simeq \prod_{p|m} \mathbb{F}_p$ satisfying (5.23) for all $p|m$. The exponential sum estimate from [BC2] applies and we obtain

Proposition 5.26. *If $\mathcal{X}$ is a nontrivial additive character of O/I', then*

$$\Big|\sum_{x\in\varphi_{I'}(G')} \mathcal{X}(x)\Big| < T^{-\gamma}|G'| \tag{5.27}$$

where $\gamma = \gamma(\varepsilon_2)$.

This is indeed a particular case of Theorem 3.1 in [BC2].

We now return to Theorem 5.1 and the norm estimate, using a similar approach as in the prime case.

Let

$$U' = \{u \in U : \varphi_{I_1}(u) = 1\}$$

hence

$$\varphi_I(U') = G'.$$

Fix $\alpha \in (O/I)^*$ and an element $a \in \alpha$.

Take $\xi_0, \xi_1 \in O$ satisfying

$$\xi_0 \in I_1 \tag{5.28}$$

$$\xi_1 - a \in I_1 \tag{5.29}$$

and with representations in the integral basis $z_1, \dots, z_n$

$$\xi_0 = \sum \xi_{0,i} z_i \qquad \xi_1 = \sum \xi_{1,i} z_i$$

such that

$$|\xi_{0,i}|, |\xi_{1,i}| < CN(I_1)^{1/n} \qquad (1 \le i \le n). \tag{5.30}$$

Let

$$\mathcal{B} = \Big\{ \sum x_i z_i : 0 \le x_i < H \Big\}$$

where

$$H = p^{-\kappa} N(I')^{1/n} \tag{5.31}$$

and κ appropriately chosen $\big($see (5.42)$\big)$.

Assume we established that for some $u \in U'$

$$\varphi_{I'}(au) \in \varphi_{I'}\big(\xi_1 + \xi_0(\mathcal{B} - \mathcal{B})\big) \tag{5.32}$$

hence for some $z \in \mathcal{B} - \mathcal{B}$

$$au - (\xi_1 + \xi_0 z) \in I'. \tag{5.33}$$

From (5.28), (5.29) and definition of U', also we have $au - \xi_1 \in I_1$ and

$$au - (\xi_1 + \xi_0 z) \in I_1. \tag{5.34}$$

Since I_1 and I' are relative prime ideals, it follows from (5.33), (5.34)

$$\begin{aligned} \varphi_I(au) &= \varphi_I(\xi_1 + \xi_0 z) \\ \varphi_I(a) &= \varphi_I\big(u^{-1}(\xi_1 + \xi_0 z)\big). \end{aligned} \tag{5.35}$$

We have by (5.30), (5.31), and (1.7)-(1.9),

$$\begin{aligned} N\big(u^{-1}(\xi_1 + \xi_0 z)\big) = N(\xi_1 + \xi_0 z) &\lesssim \big(h(\xi_1) + h(\xi_0 z)\big)^n \\ &\lesssim N(I_1) + CN(I_1)H^n \\ &\lesssim p^{-n\kappa} N(I_1)N(I') = p^{-n\kappa} N(I) \end{aligned} \tag{5.36}$$

as desired.

It remains to establish (5.32). Proceeding again by the circle method, we need to show that

$$0 \neq \sum_{\mathcal{X}} \Big[\sum_{x \in \varphi_{I'}(G')} \mathcal{X}\big(\varphi_{I'}(a)x\big) \Big] \, \mathcal{X}\big(\varphi_{I'}(\xi_1)\big) \, \Big| \sum_{y \in \varphi_{I'}(\mathcal{B})} \mathcal{X}\big(\varphi_{I'}(\xi_0)y\big) \Big|^2, \tag{5.37}$$

where in (5.37) $\mathcal{X}$ runs over the additive characters of O/I'.

Since $a \in \alpha$ and $\alpha \in (O/I)^*$, $\varphi_{I'}(a)$ is invertible in O/I'.

Also $\varphi_{I'}(\xi_0)$ is invertible in O/I'. Otherwise, there would be a prime ideal $\mathcal{P}$ dividing I' with $\xi_0 \in \mathcal{P}$. Hence, recalling (5.28), also $\xi_0 \in \mathcal{P} \cap I_1 = \mathcal{P}.I_1$ and by (5.30)

$$CN(I_1) > N(\xi_0) \geq N(I_1)N(\mathcal{P})$$

and

$$N(\mathcal{P}) < C. \tag{5.38}$$

Recalling also that $N(\mathcal{P}) = p|n^{(2)}$, necessarily $p > T^{\varepsilon_2^2}$, contradicting (5.38).

Returning to (5.37), the trivial character $\mathcal{X}_0$ of O/I' contributes for

$$|G'|\ |\varphi_{I'}(\mathcal{B})|^2 = |G'|\ |\mathcal{B}|^2. \tag{5.39}$$

By (5.27) and Parseval, the contribution of the remaining characters is bounded by

$$\begin{aligned} &T^{-\gamma}\ |G'|\ \sum_{\mathcal{X}} \left| \sum_{y \in \varphi_{I'}(\mathcal{B})} \mathcal{X}(y) \right|^2 \\ &< T^{-\gamma}\ |G'|\ N(I')\ |\mathcal{B}|. \end{aligned} \tag{5.40}$$

We need to ensure that

$$H^n = |\mathcal{B}| > T^{-\gamma} N(I') \tag{5.41}$$

and this will be satisfied if we take

$$\kappa < \gamma/n \tag{5.42}$$

in (5.31). This completes the proof of Theorem 5.1.

References

[Be]. D. Berend, *Multi invariant sets on tori*, TAMS 280 (283),no2,509-532.

[BC1]. J. Bourgain, M. Chang, *A Gauss sum estimate in arbitrary finite fields*, CRASC 2005.

[BC2]. J. Bourgain, M. Chang, *Exponential sum estimates on subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few factors*, GAFA (to appear).

[BGK]. J. Bourgain, A. Glibichuk, S. Konyagin, *Estimate for the number of sums and products and for exponential sums in fields of prime order*, London MS (to appear).

[B]. J. Bourgain, *Mordell's exponential sum estimate revisited, JAMS (to appear).*

[F]. H. Furstenberg, *Disjointness in ergodic theory,minimal sets and a problem of diophantine approximations*, Math.Systems Th 1 (1967),1-49.

[HR]. H. Halberstam, K. Roth, Sequences, Vol. I, Oxford Press 1966.

[KS]. S. Konyagin, I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge UP, 1999.

[N]. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PAN 1974.

Institute for Advanced Study, Olden Lane, Princeton, N.J. 08540, U.S.A.

E-mail address: bourgain@math.ias.edu

Mathematics Department, University of California, Riverside, CA 92521

E-mail address: mcc@math.ucr.edu