

参赛学生姓名： 覃子瑄

中学： 上海民办包玉刚实验学校

省份： 上海

国家/地区： 中国

指导老师姓名： 汤继尧

指导老师单位： Northwestern University

论文题目： On the simultaneous divisibility
of multiplicative orders

ON THE SIMULTANEOUS DIVISIBILITY OF MULTIPLICATIVE ORDERS

ZIXUAN QIN

ABSTRACT. We present an alternative proof of the proposition that, for any finite collection of elements of $\mathbb{Z} \setminus \{0, \pm 1\}$ and integer $m \geq 1$, the set of primes p modulo which their multiplicative orders are divisible by m has a positive density. The proof combines existing methods from algebraic and analytic number theory with a novel mechanism for extracting suitable automorphisms. In particular, we capitalize on a fixed-point counting argument that enables this construction.

CONTENTS

1. Introduction	2
2. Preliminaries	3
3. A counting argument	5
4. Character extraction and Galois realization	7
5. Proof of the main theorem	11
References	14
Acknowledgments	15

1. INTRODUCTION

Let $a \in \mathbb{Z} \setminus \{0, \pm 1\}$, and let $m \geq 1$ be an integer. For an integer $n \geq 2$ coprime to a , let $\text{ord}_n(a)$ denote the order of a in $(\mathbb{Z}/n\mathbb{Z})^\times$. For a set $\mathcal{P}$ of rational primes, let

$$\delta(\mathcal{P}) = \lim_{x \rightarrow \infty} \frac{\#\{p \in \mathcal{P} : p \leq x\}}{\pi(x)}$$

be its density when the limit exists. In 1978, Wiertelak [9] proved that the set of primes p with

$$m \mid \text{ord}_p(a)$$

has a positive density; in 2005, Moree [5] refined this result by deriving a compact expression for the density. More recently in 2023, Sgobba [7] extended this line of work by providing unconditional asymptotics for such primes in general number fields.

In related work, Perucca [6] established that, given a prime ℓ , prescribing the ℓ -valuations of the orders of finitely many points on products of abelian varieties and tori modulo $\mathfrak{p}$ yields a set of primes that is either finite or of positive density. In addition, she proved a criterion for the infinitude of the set of admissible primes. Her proof encodes the required order valuations using an appropriate torsion point and then proceeds with Kummer theory to establish the result.

The purpose of this paper is to give an alternative proof of a multivariable analogue of Wiertelak's theorem.

Theorem 1.1. *Let $a_1, a_2, \dots, a_k \in \mathbb{Z} \setminus \{0, \pm 1\}$, and let $m \geq 1$ be an integer. Then there are infinitely many primes p such that*

$$m \mid \text{ord}_p(a_j)$$

for every $1 \leq j \leq k$. Moreover, the density of such primes exists and is positive.

Exploiting the Kummer-theoretic approach he developed in a previous paper [3], Järvinen [4] established Theorem 1.1 by a different method in 2022 as a corollary of more general results on the insolubility of exponential congruences.

Our approach is similar to Järvinen's [4] in that the positivity of the density is established by extracting a subset of positive density; the existence of the density, however, requires a separate argument.

The main new ingredient of the present proof is a fixed-point argument that allows us to produce squarefree composite moduli satisfying the divisibility conditions. In Section 3, we prove the following result.

Theorem 1.2. *Let $a_1, \dots, a_k, m$ be as in Theorem 1.1, and let S be a finite set of primes containing the prime factors of $a_1, \dots, a_k, m$. Then there is a squarefree integer n supported outside S such that*

$$m \mid \text{ord}_n(a_j)$$

for every $1 \leq j \leq k$. Recall that the support of an integer is the set of its prime factors.

To show why Theorem 1.2 holds, we first introduce a mechanism that allows us to count the number of fixed points of a prescribed multiplication map on a subgroup of the 1-dimensional torus. Subsequently, assuming the contrary of Theorem 1.2 imposes a relation between the fixed-point counts of two distinct maps that is inconsistent with established estimates, leading to a contradiction.

In Section 4, we then draw on the integer furnished by Theorem 1.2, and, using character counting and power residue symbols, we extract an appropriate Galois automorphism of a Kummer extension. In Section 5, we apply the Chebotarev density theorem to obtain a positive-density set of primes satisfying the divisibility conditions prescribed by Theorem 1.1. This demonstrates that if the density of the full admissible set exists, it is positive. Finally, we complete the proof with a truncation argument, which establishes the existence of the density of the full admissible set.

2. PRELIMINARIES

In this section, we introduce a few concepts and results that are used later in this paper.

Let L/K be a Galois extension of number fields, and let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the integer rings of K and L , respectively. Consider a nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. Then it yields a unique factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \dots \mathfrak{P}_k^{e_k}$$

in $\mathcal{O}_L$. We say that $\mathfrak{p}$ is unramified in L if $e_j = 1$ for every $1 \leq j \leq k$.

We now cite a discriminant-based criterion for unramifiedness from Borevich and Shafarevich [1, p. 203], which is utilized later in Section 4. Let $\text{disc}(f)$ be the discriminant of f .

Lemma 2.1. *Let $\mathfrak{q}$ be a prime of K , let $A = (\mathcal{O}_K \setminus \mathfrak{q})^{-1} \mathcal{O}_K$, and let f be the minimal polynomial of α over K , where α is integral over A (in other words, α satisfies some monic polynomial in $A[X]$), and $L = K(\alpha)$. Then $\mathfrak{q}$ is unramified in L if $\text{disc}(f) \in A^\times$.*

Let $\mathfrak{q} \neq 0$ be a prime above a rational prime q . The residue field at $\mathfrak{q}$ is

$$k_{\mathfrak{q}} = \mathcal{O}_K / \mathfrak{q}.$$

Since $\mathfrak{q}$ is maximal, $k_{\mathfrak{q}}$ is a finite field. The residue degree of $\mathfrak{q}$ over q is

$$f(\mathfrak{q}/q) = [k_{\mathfrak{q}} : \mathbb{F}_q].$$

Consequently, $\#k_{\mathfrak{q}} = q^{f(\mathfrak{q}/q)}$. The quantity $N\mathfrak{q} = \#k_{\mathfrak{q}}$ denotes the absolute norm of $\mathfrak{q}$.

Let μ_m denote the m -th roots of unity, and let $K = \mathbb{Q}(\mu_m)$.

Lemma 2.2. *If $q \nmid m$, then reduction modulo $\mathfrak{q}$ induces an isomorphism*

$$\mu_m \cong \{x \in k_{\mathfrak{q}}^{\times} : x^m = 1\}.$$

Proof. Reduction clearly gives a homomorphism. Its image lies in the subgroup of m -th roots of unity. We first show that it is injective. If $\zeta \in \mu_m$ reduces to 1, but $\zeta \neq 1$, then

$$1 + \zeta + \cdots + \zeta^{m-1} = 0.$$

Reducing modulo $\mathfrak{q}$ gives $m \equiv 0 \pmod{\mathfrak{q}}$, a contradiction. Hence, $\zeta = 1$. Thus, the image contains m distinct roots of $x^m - 1$ in $k_{\mathfrak{q}}$. Since a polynomial of degree m over a field has at most m roots, the reduction map is an isomorphism. $\square$

We cite another result from Washington [8, p. 14].

Lemma 2.3. *Let $m \geq 2$ be an integer, and let $q \nmid m$. Then*

$$f(\mathfrak{q}/q) = \text{ord}_m(q).$$

Let $q \nmid m$, and let $a \in K^{\times}$ satisfy $v_{\mathfrak{q}}(a) = 0$. The m -th power residue symbol of a at $\mathfrak{q}$ is the unique element $(a/q)_m \in \mu_m$ such that

$$\left(\frac{a}{\mathfrak{q}}\right)_m \equiv a^{(N\mathfrak{q}-1)/m} \pmod{\mathfrak{q}}.$$

Let $\mathfrak{Q} \subset \mathcal{O}_L$ be a prime above $\mathfrak{q}$. If $\mathfrak{q}$ is unramified, then the Frobenius element associated to $\mathfrak{Q}$ over $\mathfrak{q}$ is the unique element $\text{Frob}_{\mathfrak{Q}/\mathfrak{q}} \in \text{Gal}(L/K)$ such that

$$\text{Frob}_{\mathfrak{Q}/\mathfrak{q}}(x) \equiv x^{N\mathfrak{q}} \pmod{\mathfrak{Q}}$$

for all $x \in \mathcal{O}_L$.

If L/K is abelian, the element does not depend on the choice of $\mathfrak{Q}$. Hence, we may write $\text{Frob}_{\mathfrak{q}}$ for $\text{Frob}_{\mathfrak{Q}/\mathfrak{q}}$. Under this assumption, we verify that, if $\beta \in L$, and $\beta^m = a$,

$$\frac{\text{Frob}_{\mathfrak{q}}(\beta)}{\beta} = \left(\frac{a}{\mathfrak{q}}\right)_m.$$

Since $v_{\mathfrak{Q}}(\beta) = 0$, the left-hand side is congruent to $\beta^{N\mathfrak{q}-1}$. Now

$$\beta^{N\mathfrak{q}-1} = (\beta^m)^{(N\mathfrak{q}-1)/m} = a^{(N\mathfrak{q}-1)/m}.$$

Since $a \in K$, $\text{Frob}_{\mathfrak{q}}$ fixes a . Therefore,

$$\left(\frac{\text{Frob}_{\mathfrak{q}}(\beta)}{\beta}\right)^m = \frac{\text{Frob}_{\mathfrak{q}}(\beta^m)}{\beta^m} = \frac{\text{Frob}_{\mathfrak{q}}(a)}{a} = 1.$$

Thus, $\text{Frob}_{\mathfrak{q}}(\beta)/\beta \in \mu_m$. By Lemma 2.2, reduction on μ_m is injective, so $\text{Frob}_{\mathfrak{q}}(\beta)/\beta$ and $(a/q)_m$ are the same element. This proves the claim.

Let $G = \text{Gal}(L/K)$. For an automorphism $\sigma \in G$, define its conjugacy class

$$C = \{g\sigma g^{-1} : g \in G\}.$$

We cite Zaman [10] for the following version of the Chebotarev density theorem.

Theorem 2.4 (Chebotarev). *Write $\mathfrak{p} \cap \mathbb{Z} = (p)$. Then*

$$\#\{\mathfrak{p} : f(\mathfrak{p}/p) = 1, N\mathfrak{p} \leq x, \text{Frob}_{\mathfrak{p}/\mathfrak{p}}(L/K) = C\} \sim \frac{\#C}{\#G} \frac{x}{\log x}.$$

Here $\text{Frob}_{\mathfrak{p}}(L/K)$ refers to the conjugacy class of $\text{Frob}_{\mathfrak{p}}$.

This follows from the standard Chebotarev density theorem, which yields the same asymptotic without the condition $f(\mathfrak{p}/p) = 1$. Indeed, if $f(\mathfrak{p}/p) \geq 2$, then $N\mathfrak{p} \leq x$ implies $p \leq x^{1/2}$. For each rational prime p , there are at most $[K : \mathbb{Q}]$ primes of K above it. Therefore, the number of excluded primes is

$$O([K : \mathbb{Q}]\pi(\sqrt{x})) = o\left(\frac{x}{\log x}\right).$$

Hence, imposing $f(\mathfrak{p}/p) = 1$ does not change the asymptotic.

Finally, we record two results in finite group theory. First, we observe that, if $n = \text{lcm}(d_1, d_2, \dots, d_k)$, and a is a unit modulo n , then

$$\text{ord}_n(a) = \text{lcm}_{1 \leq j \leq k} \text{ord}_{d_j}(a).$$

Indeed, $a^r \equiv 1 \pmod{n}$ holds exactly when $a^r \equiv 1 \pmod{d_j}$ for every j , so the permissible exponents are the common multiples of the individual orders. The second result is the following lifting fact.

Lemma 2.5. *Let $p \nmid a$ be prime, and let $e \geq 1$. Then there is an integer f such that*

$$\text{ord}_{p^e}(a) = p^f \text{ord}_p(a).$$

Proof. Let

$$m = \text{ord}_{p^e}(a), \quad n = \text{ord}_p(a).$$

It is clear that $n \mid m$. Therefore, $\text{ord}_{p^e}(a^n) = m/n$. However, $a^n \equiv 1 \pmod{p}$, so a^n lies in the kernel of the reduction map $(\mathbb{Z}/p^e\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$, which has order p^{e-1} . Thus, m/n is a power of p . This completes the proof. $\square$

3. A COUNTING ARGUMENT

In this section, we prove Theorem 1.2. First, we reduce it to the following theorem.

Theorem 3.1. *Let $a \geq 2$ and $m \geq 1$ be integers, and let S be a finite set of primes containing the prime factors of a and m . Then there is a squarefree integer n supported outside S such that*

$$m \mid \text{ord}_n(a).$$

Indeed, Theorem 1.2 follows from this result.

Proof of Theorem 1.2. By Theorem 3.1, choose a squarefree integer n_1 supported outside $S^{(1)} = S$ such that $m \mid \text{ord}_{n_1}(a_1^2)$. Let $S^{(2)}$ be the union of $S^{(1)}$ and the prime factors of n_1 , and choose another squarefree integer n_2 supported outside $S^{(2)}$ such that $m \mid \text{ord}_{n_2}(a_2^2)$. Repeating this process gives a squarefree integer $n = n_1 n_2 \cdots n_k$ supported outside S such that

$$m \mid \text{ord}_{n_j}(a_j^2) \mid \text{ord}_n(a_j^2) \mid \text{ord}_n(a_j)$$

for every $1 \leq j \leq k$. $\square$

Throughout this section, let a , m , and S be as in Theorem 3.1. Let X_S denote the subgroup of the 1-dimensional torus

$$X_S = \{x \in \mathbb{R}/\mathbb{Z} : \text{the denominator of } x \text{ is supported outside } S\}.$$

Let T be the automorphism defined by

$$T : X_S \longrightarrow X_S, \quad T(x) = ax,$$

and let $\text{Fix}(T, X_S)$ be the fixed-point set of T on X_S .

Let $N_S(x)$ denote the S -free part of x , that is, the greatest divisor of x supported outside S .

Lemma 3.2.

$$\#\text{Fix}(T^n, X_S) = N_S(a^n - 1).$$

Proof. By definition,

$$x \in \text{Fix}(T^n, X_S) \iff (a^n - 1)x \equiv 0 \pmod{1}.$$

Thus,

$$(3.1) \quad \text{Fix}(T^n, X_S) = \left\{ \frac{j}{a^n - 1} \in X_S : j = 0, 1, \dots, a^n - 2 \right\}.$$

Among all indices j , those that provide a point in X_S are exactly those for which

$$\frac{a^n - 1}{\gcd(j, a^n - 1)}$$

has no prime factors in S . Let

$$N = \frac{a^n - 1}{N_S(a^n - 1)}.$$

This means that $N \mid j$. Hence, the admissible indices are exactly $0, N, \dots, (N_S(a^n - 1) - 1)N$. This completes the proof. $\square$

Lemma 3.3. *Let p be a prime. Then, there is a constant C_p such that*

$$v_p(a^n - 1) \leq C_p + v_p(n).$$

Proof. If $p \mid a$, then $v_p(a^n - 1) = 0$.

If $p \nmid a$, then let $d = \text{ord}_p(a)$. If $d \nmid n$, then $v_p(a^n - 1) = 0$; otherwise, let $n = kd$. If p is odd, then

$$v_p(a^n - 1) = v_p(a^d - 1) + v_p(k) \leq v_p(a^d - 1) + v_p(n)$$

by the lifting-the-exponent lemma. Similarly, if both p and k are even, then

$$\begin{aligned} v_2(a^n - 1) &= v_2(a^d - 1) + v_2(a^d + 1) + v_2(k) - 1 \\ &\leq v_2(a^d - 1) + v_2(a^d + 1) - 1 + v_2(n). \end{aligned}$$

If p is even while k is odd, then

$$v_2(a^n - 1) = v_2(a^d - 1) \leq v_2(a^d - 1) + v_2(n).$$

This completes the proof. $\square$

Lemma 3.4. *Let ℓ be prime, and let $e \geq 1$ be an integer. As $s \rightarrow \infty$,*

$$\frac{\#\text{Fix}(T^{\ell^e s}, X_S)}{\#\text{Fix}(T^{\ell^{e-1} s}, X_S)} \longrightarrow \infty.$$

Proof. By Lemma 3.3,

$$\prod_{r \in S} r^{v_r(a^{\ell^e s} - 1)} \leq \prod_{r \in S} r^{C_r + v_r(\ell^e s)} \leq A_S \prod_{r \in S} r^{e + v_r(s)} \leq B_{S,e} s.$$

Therefore,

$$N_S(a^{\ell^e s} - 1) = (a^{\ell^e s} - 1) \left(\prod_{r \in S} r^{v_r(a^{\ell^e s} - 1)} \right)^{-1} \geq (a^{\ell^e s} - 1) (B_{S,e} s)^{-1}.$$

On the other hand,

$$N_S(a^{\ell^{e-1} s} - 1) \leq a^{\ell^{e-1} s} - 1.$$

Then $a^{\ell^e s}$ outgrows $a^{\ell^{e-1} s}$, and $B_{S,e} s$ grows linearly with s . By Lemma 3.2, this completes the proof. $\square$

Proof of Theorem 3.1. The case where $m = 1$ is trivial, so we assume that $m \geq 2$. Fix a prime $\ell \mid m$, and let $e = v_\ell(m)$. Suppose for contradiction that there is not a point $x \in X_S$ with period d under T such that $\ell^e \mid d$. Let

$$U = T^{\ell^e}, \quad V = T^{\ell^{e-1}}.$$

Then U^s fixes x if and only if $d \mid \ell^e s$; V^s fixes x if and only if $d \mid \ell^{e-1} s$. Since $v_\ell(d) < e$, these two conditions are equivalent. Thus,

$$\text{Fix}(U^s, X_S) = \text{Fix}(V^s, X_S).$$

However, as $s \rightarrow \infty$, $\#\text{Fix}(U^s, X_S)$ outgrows $\#\text{Fix}(V^s, X_S)$ by Lemma 3.4, a contradiction. Therefore, there is a point x with period divisible by ℓ^e . Let $x = u/v$ be in lowest terms. Then $\ell^e \mid \text{ord}_v(a)$. Since ℓ is arbitrary, we can choose such a v_ℓ for every ℓ . Let N be their least common multiple. Then $m \mid \text{ord}_N(a)$. Let

$$N = \prod_{q \mid N} q^{r_q}, \quad n = \prod_{q \mid N} q.$$

We claim that $m \mid \text{ord}_n(a)$. Indeed, since $q \nmid m$ for every $q \mid N$, $\text{ord}_{q^{r_q}}(a)/\text{ord}_q(a)$ is a power of q by Lemma 2.5. Therefore, the quotient

$$\frac{\text{ord}_N(a)}{\text{ord}_n(a)} = \frac{\text{lcm}_{q \mid N} \text{ord}_{q^{r_q}}(a)}{\text{lcm}_{q \mid N} \text{ord}_q(a)}$$

is supported outside S . Consequently, $m \mid \text{ord}_N(a)$ implies $m \mid \text{ord}_n(a)$. Since n is squarefree, this completes the proof. $\square$

4. CHARACTER EXTRACTION AND GALOIS REALIZATION

Throughout this section, let $a_1, a_2, \dots, a_k, m, S$ be as in Theorem 1.2, and let $K = \mathbb{Q}(\mu_M)$, where M is an integer with the same support as m to be chosen. Thus define a Galois extension L/K with

$$L = K(a_1^{1/M}, a_2^{1/M}, \dots, a_k^{1/M}).$$

Proposition 4.1. *There is a Galois extension L/K and an element $\sigma \in \text{Gal}(L/K)$ such that for any choice of $\beta_j \in L$ with $\beta_j^M = a_j$,*

$$m \mid \text{ord} \left(\frac{\sigma(\beta_j)}{\beta_j} \right)$$

for every $1 \leq j \leq k$.

Let ℓ be prime, and let $j \geq 1$ be an integer. Consider a finite abelian ℓ -group G with exponent dividing ℓ^j . Fix $h \in G$ with $\text{ord}(h) = \ell^r$, and let $1 \leq s \leq r$ be an integer.

Lemma 4.2. *Among all characters $\chi : G \rightarrow \mu_{\ell^j}$, the proportion satisfying*

$$\text{ord}(\chi(h)) \mid \ell^{s-1}$$

is ℓ^{s-r-1} .

Proof. Let $H = \langle h \rangle$, and let $\text{Hom}(X, Y)$ denote the set of homomorphisms $X \rightarrow Y$.

We claim that the restriction map

$$\rho : \text{Hom}(G, \mu_{\ell^j}) \longrightarrow \text{Hom}(H, \mu_{\ell^j})$$

is surjective. Indeed, if $H = G$, then the statement is trivial. Assume that $H < G$. Fix a homomorphism $\varphi \in \text{Hom}(H, \mu_{\ell^j})$ and an element $x \in G \setminus H$. Treat the groups additively, and identify

$$\mu_{\ell^j} \cong \frac{1}{\ell^j} \mathbb{Z} / \mathbb{Z} \subseteq \mathbb{Q} / \mathbb{Z}.$$

Since $\mathbb{Q}/\mathbb{Z}$ is divisible, there is a point y such that $\varphi(dx) = dy$, where d is the order of $x + H$ in G/H . Let $H^{(1)} = H + \mathbb{Z}x$, and let $\varphi^{(1)} : H^{(1)} \rightarrow \mathbb{Q}/\mathbb{Z}$ be given by

$$\varphi^{(1)}(h + nx) = \varphi(h) + ny.$$

It is routine to verify that $\varphi^{(1)}$ is well-defined. Iterating this process yields a character $\varphi^{(t)} : G \rightarrow \mathbb{Q}/\mathbb{Z}$. Then

$$\ell^j \varphi^{(t)}(g) = \varphi^{(t)}(\ell^j g) = 0$$

for every $g \in G$. Thus, the image of $\varphi^{(t)}$ lies in μ_{ℓ^j} , and $\varphi^{(t)} \in \text{Hom}(G, \mu_{\ell^j})$. This proves the claim.

Let $\rho^{-1}(x)$ denote the fiber of $\rho(x)$. For every element $x \in \text{Hom}(H, \mu_{\ell^j})$, there is a homomorphism $\varphi_0 \in \rho^{-1}(x)$. Let $\ker \rho$ denote the kernel of ρ . Then $\varphi \in \rho^{-1}(x)$ if and only if $\varphi_0 - \varphi \in \ker \rho$. Therefore, $\#\rho^{-1}(x) = \#\ker \rho$. Fix $\varphi \in \text{Hom}(H, \mu_{\ell^j})$. Since $\text{ord}(h) = \ell^r$,

$$\varphi(h)^{\ell^r} = \varphi(h^{\ell^r}) = 1.$$

Therefore, $\varphi(h) \in \mu_{\ell^r}$. Since H is cyclic, φ is uniquely determined by $\varphi(h)$. Consequently, $\#\text{Hom}(H, \mu_{\ell^j}) = \ell^r$. Since $\text{ord}(\varphi(h))$ is a power of ℓ , the characters satisfying $\text{ord}(\varphi(h)) \mid \ell^{s-1}$ are exactly those with $\varphi(h) \in \mu_{\ell^{s-1}}$. Hence, the number of such characters is ℓ^{s-1} , and the desired proportion is

$$\frac{\ell^{s-1} \#\ker \rho}{\ell^r \#\ker \rho} = \ell^{s-r-1}.$$

□

Lemma 4.3. *There is an integer M with the same support as m , a squarefree integer n supported outside S , and a character $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \mu_M$ such that*

$$m \mid \text{ord}(\chi(a_j))$$

for every j .

Proof. Write $m = \prod \ell^{s_\ell}$. For every prime $\ell \mid m$, pick N_ℓ sufficiently large such that $k\ell^{s_\ell - N_\ell - 1} < 1$. By Theorem 1.2, there is a squarefree integer n supported outside S such that

$$\prod_{\ell \mid m} \ell^{N_\ell} \mid \text{ord}_n(a_j)$$

for every $1 \leq j \leq k$.

Let $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Since G is finite abelian, we may write

$$G = \prod_{\ell \mid \#G} \text{Syl}_\ell(G), \quad a_j = \prod_{\ell \mid \#G} h_{j,\ell},$$

where $\text{Syl}_\ell(G)$ denotes the Sylow ℓ -subgroup of G , and $\text{ord}(h_{j,\ell}) = \ell^{r_{j,\ell}}$. Let the exponent of $\text{Syl}_\ell(G)$ be ℓ^{e_ℓ} , and let $t_\ell \geq e_\ell$. For each prime $\ell \mid m$, choose a character

$$\chi_\ell : \text{Syl}_\ell(G) \longrightarrow \mu_{\ell^{t_\ell}}$$

such that $\ell^{s_\ell} \mid \text{ord}(\chi_\ell(h_{j,\ell}))$ for every j . We show that such a character exists. Since $\ell \mid \text{ord}_n(a_j)$, $\ell \mid \#G$. This implies that $\text{Syl}_\ell(G)$ is nontrivial. Since the orders of distinct components $h_{j,\ell}$ are powers of different primes, $r_{j,\ell} \geq N_\ell$. By Lemma 4.2, the characters $\chi_\ell : \text{Syl}_\ell(G) \rightarrow \mu_{\ell^{t_\ell}}$ satisfying $\text{ord}(\chi_\ell(h_{j,\ell})) \mid \ell^{s_\ell - 1}$ have proportion $\ell^{s_\ell - r_{j,\ell} - 1} \leq \ell^{s_\ell - N_\ell - 1}$. By the union bound, the proportion of characters that are bad for at least one j is at most

$$\sum_{j=1}^k \ell^{s_\ell - r_{j,\ell} - 1} \leq k\ell^{s_\ell - N_\ell - 1} < 1.$$

Hence, a character that is good for every j exists.

Let $M = \prod \ell^{t_\ell}$. For every $g \in G$, let g_ℓ denote its projection to $\text{Syl}_\ell(G)$. Let

$$\chi(g) = \prod_{\ell|m} \chi_\ell(g_\ell).$$

Since each factor lies in $\mu_{\ell^{t_\ell}} \subseteq \mu_M$, this gives a homomorphism $G \rightarrow \mu_M$. The factors have pairwise coprime orders. Therefore,

$$\text{ord}(\chi(a_j)) = \prod_{\ell|m} \text{ord}(\chi_\ell(h_{j,\ell})).$$

Since each factor on the right is divisible by ℓ^{s_ℓ} , $m \mid \text{ord}(\chi(a_j))$ for every j . This completes the proof. $\square$

Lemma 4.4. *Let m and n be coprime. Then there is an integer M with the same support as m such that*

$$v_\ell(q^{f_q} - 1) = v_\ell(M)$$

for every $\ell \mid m$ and $q \mid n$ with $\ell \mid q - 1$, where $f_q = \text{ord}_M(q)$.

Proof. Fix $\ell \mid m$ and $q \mid n$ such that $\ell \mid q - 1$. Let b_ℓ be the maximum ℓ -valuation $r - 1$ attains as r iterates over the prime factors of m other than ℓ . When there are no other prime factors, let $b_\ell = 0$. If ℓ is odd, then write $s_{\ell,q} = v_\ell(q - 1) > 0$. Let $t_\ell > s_{\ell,q}$. Then

$$v_\ell(q^{\ell^{t_\ell - s_{\ell,q}}} - 1) = s_{\ell,q} + (t_\ell - s_{\ell,q}) = t_\ell.$$

However,

$$v_\ell(q^{\ell^{t_\ell - s_{\ell,q} - 1}} - 1) = s_{\ell,q} + (t_\ell - s_{\ell,q} - 1) = t_\ell - 1.$$

Therefore, $\text{ord}_{\ell^{t_\ell}}(q) = \ell^{t_\ell - s_{\ell,q}}$.

For another prime $r \neq \ell$ with $r \mid m$ and an integer $d \geq 1$, $v_\ell(\text{ord}_{r^d}(q)) = v_\ell(\text{ord}_r(q)) \leq v_\ell(r - 1)$ by Lemma 2.5. Note that since the right side is independent of t_r , increasing the exponent of r does not increase the ℓ -part of this order. Since $f_q = \text{lcm}_{r|m} \text{ord}_{r^{t_r}}(q)$,

$$v_\ell(f_q) = \max_{r|m} v_\ell(\text{ord}_{r^{t_r}}(q)).$$

If $t_\ell - s_{\ell,q} > b_\ell$, then the factor ℓ^{t_ℓ} controls this maximum. Hence, $v_\ell(f_q) = t_\ell - s_{\ell,q}$, and

$$v_\ell(q^{f_q} - 1) = s_{\ell,q} + v_\ell(f_q) = t_\ell = v_\ell(M).$$

Now we turn to the cases where $\ell = 2$. If $q \equiv 1 \pmod{4}$, then let $s_{\ell,q} = v_\ell(q - 1)$; otherwise, let $s_{\ell,q} = v_\ell(q + 1)$. As such, $s_{\ell,q} > 0$. By the same argument, $\text{ord}_{\ell^{t_\ell}}(q) = \ell^{t_\ell - s_{\ell,q}}$ for $t_\ell > s_{\ell,q}$ in the former case. In the latter case, let $e = \ell^{t_\ell - s_{\ell,q}}$ if $t_\ell > s_{\ell,q}$. Then

$$\begin{aligned} v_\ell(q^e - 1) &= v_\ell(q - 1) + v_\ell(q + 1) + v_\ell(e) - 1 \\ &= 1 + s_{\ell,q} + (t_\ell - s_{\ell,q}) - 1 \\ &= t_\ell. \end{aligned}$$

For $t_\ell > s_{\ell,q} + 1$, $v_\ell(q^{e/\ell} - 1) = t_\ell - 1$, whereas for $t_\ell = s_{\ell,q} + 1$, $v_\ell(q^{e/\ell} - 1) = v_\ell(q - 1) < t_\ell$. Therefore, $\text{ord}_{\ell^{t_\ell}}(q) = \ell^{t_\ell - s_{\ell,q}}$ for $t_\ell > s_{\ell,q}$. Choose t_ℓ such that $t_\ell - s_{\ell,q} > b_\ell$. Then $v_\ell(f_q) = t_\ell - s_{\ell,q}$. Since $t_\ell > s_{\ell,q}$, $\text{ord}_{\ell^{t_\ell}}(q)$ is even. Hence, f_q is even, and $v_\ell(q^{f_q} - 1) = t_\ell$. Let c_ℓ be the largest value $s_{\ell,q}$ attains as q iterates over all primes factors of n with $\ell \mid q - 1$. When no prime $q \mid n$ satisfies $\ell \mid q - 1$, let $c_\ell = 0$. Finally, choose $t_\ell > b_\ell + c_\ell$, and let $M = \prod \ell^{t_\ell}$. This completes the proof. $\square$

Remark 4.5. The exponents of the integers M produced by Lemma 4.3 and Lemma 4.4 can be arbitrarily enlarged. Indeed, the proofs require only $t_\ell \geq e_\ell$ and $t_\ell > b_\ell + c_\ell$, respectively.

Lemma 4.6. *Let*

$$G = \prod_{\ell \mid M} \text{Syl}_\ell((\mathbb{Z}/q\mathbb{Z})^\times).$$

Let $Nq = q^f$, where $\mathfrak{q}$ is a prime of $K = \mathbb{Q}(\mu_M)$ above a rational prime $q \nmid m$, and let $N = (q^f - 1)/M$. If $\gcd(N, \#G) = 1$, then the map

$$\rho : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mu_M, \quad \rho(x) = \left(\frac{x}{\mathfrak{q}}\right)_M \equiv x^N \pmod{\mathfrak{q}}$$

generates $\text{Hom}((\mathbb{Z}/q\mathbb{Z})^\times, \mu_M)$.

Proof. By Lemma 2.2, the reduction map gives an embedding $\mu_M \hookrightarrow k_{\mathfrak{q}}^\times$. Therefore, $M \mid q^f - 1$, and N is an integer. Consider an element $x \in G$ such that $\rho(x) = 1$. Since $\rho(x) \equiv x^N \pmod{\mathfrak{q}}$, $x^N = 1$ in $(\mathbb{Z}/q\mathbb{Z})^\times$. Let its order be d . Then d divides N and $\#G$ simultaneously. Hence, $d = 1$, and $x = 1$. Let the restriction of ρ to G be ρ' . Then its kernel is trivial. Therefore, ρ' is injective. As a result, after writing

$$(\mathbb{Z}/q\mathbb{Z})^\times \cong G \times H,$$

it is clear that $\gcd(\#H, M) = 1$. For every character $\varphi \in \text{Hom}((\mathbb{Z}/q\mathbb{Z})^\times, \mu_M)$ and $h \in H$, the order of $\varphi(h)$ divides both $\#H$ and M . Consequently, $\varphi(h) = 1$. This implies φ is determined by its restriction to G . Thus, the restriction map induces an isomorphism

$$\text{Hom}((\mathbb{Z}/q\mathbb{Z})^\times, \mu_M) \cong \text{Hom}(G, \mu_M).$$

Indeed, every character of G extends to $G \times H$ by being trivial on H . In addition, G is cyclic because $G \leq (\mathbb{Z}/q\mathbb{Z})^\times$. Injectivity gives $\#\rho'(G) = \#G$, so ρ' has order $e = \#G$. Let g generate G . Then $\rho'(g)$ has order e , so

$$\langle \rho'(g) \rangle = \mu_e \subseteq \mu_M.$$

For any $\pi : G \rightarrow \mu_M$, $\pi(g)^e = 1$. Hence, $\pi(g) = \rho'(g)^c$ for some integer c . Since g generates G , $\pi = (\rho')^c$. Thus, ρ' generates $\text{Hom}(G, \mu_M)$. By the isomorphism established previously, this completes the proof. $\square$

Lemma 4.7. *Let $q \nmid M$, and let $\mathfrak{q}$ be a prime of K above q , where $L = K(\beta)$, and $\beta^M = a$. If $v_{\mathfrak{q}}(a) = 0$, then $\mathfrak{q}$ is unramified in L/K .*

Proof. Let A be as in Lemma 2.1. Since $v_{\mathfrak{q}}(a) = 0$, $a \in A^\times$. Since $q \nmid M$, $M \in A^\times$. Let $f(X) = X^M - a$. Then its discriminant is given by

$$\text{disc}(f) = \pm M^M a^{M-1}.$$

Therefore, $\text{disc}(f) \in A^\times$. Let g be the minimal polynomial of β over K . Since $f(\beta) = 0$, and f is monic, β is integral over A . It follows from A being a discrete valuation ring that A is integrally closed. Thus, $g \in A[X]$, and $f = gh$ for some monic $h \in A[X]$. Let $\text{Res}(g, h)$ denote the resultant of g and h . Then the discriminant-resultant identity [2, p. 285] gives

$$\text{disc}(f) = \text{disc}(g) \text{disc}(h) \text{Res}(g, h)^2.$$

Since $\text{disc}(f) \in A^\times$, $\text{disc}(g) \in A^\times$. By Lemma 2.1, $\mathfrak{q}$ is unramified in L/K . This completes the proof. $\square$

Proof of Proposition 4.1. First, we apply Lemma 4.3 to obtain an integer M_1 , a squarefree integer n supported outside S , and a character $\chi \in \text{Hom}((\mathbb{Z}/n\mathbb{Z})^\times, \mu_{M_1})$ such that $m \mid \text{ord}(\chi(a_j))$ for every j . Then, by Lemma 4.4, choose an integer M_2 such that $v_\ell(q^{f_q} - 1) = v_\ell(M_2)$ for every $\ell \mid m$ and $q \mid n$ with $\ell \mid q - 1$, where $f_q = \text{ord}_{M_2}(q)$. Let $M = \text{lcm}(M_1, M_2)$, and let $f'_q = \text{ord}_M(q)$. Since $\mu_{M_1} \subseteq \mu_M$, we may identify χ as an element of $\text{Hom}((\mathbb{Z}/n\mathbb{Z})^\times, \mu_M)$.

Let $K = \mathbb{Q}(\mu_M)$, and choose a prime $\mathfrak{q} \subset \mathcal{O}_K$ above q for every $q \mid n$. Thus, by Lemma 2.3, $f(\mathfrak{q}/q) = f'_q$. Let G_q and N_q be as in Lemma 4.6. If $\ell \mid \#G_q$, then $\ell \mid m$, and $\ell \mid q - 1$. Thus,

$$v_\ell(N_q) = v_\ell(q^{f'_q} - 1) - v_\ell(M) = 0$$

(see Remark 4.5 for justification). Consequently, $\gcd(N, \#G) = 1$. Since n is squarefree,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{q|n} (\mathbb{Z}/q\mathbb{Z})^\times$$

by the Chinese Remainder Theorem. Thus, χ decomposes into local characters χ_q . By Lemma 4.6, the power residue symbol $(x/\mathfrak{q})_M$ generates $\text{Hom}((\mathbb{Z}/q\mathbb{Z})^\times, \mu_M)$ for each $q | n$. Let $\chi_q(x) = (x/\mathfrak{q})_M^{c_q}$. Hence, we can write

$$\chi(a_j) = \prod_{q|n} \left(\frac{a_j}{\mathfrak{q}} \right)_M^{c_q}.$$

Choose β_j with $\beta_j^M = a_j$, and let $L = K(\beta_1, \beta_2, \dots, \beta_k)$. Since $\mu_M \subseteq K$, L/K is abelian. Moreover, L is the splitting field of

$$\prod_{j=1}^k (X^M - a_j)$$

over K . Therefore, L/K is Galois. Since $q \nmid M$, we can apply Lemma 4.7 to each $K(\beta_j)/K$. A prime $\mathfrak{q}$ that is unramified in each $K(\beta_j)/K$ is also unramified in their compositum. Hence, every chosen $\mathfrak{q}$ is unramified in L/K . Consequently, $\text{Frob}_{\mathfrak{q}} \in \text{Gal}(L/K)$ is well-defined, and

$$\frac{\text{Frob}_{\mathfrak{q}}(\beta_j)}{\beta_j} = \left(\frac{a_j}{\mathfrak{q}} \right)_M.$$

Let

$$\sigma = \prod_{q|n} \text{Frob}_{\mathfrak{q}}^{c_q} \in \text{Gal}(L/K).$$

Since $\mu_M \subseteq K$, σ fixes every point of μ_M . Moreover, since L/K is abelian,

$$\frac{\sigma(\beta_j)}{\beta_j} = \prod_{q|n} \left(\frac{\text{Frob}_{\mathfrak{q}}(\beta_j)}{\beta_j} \right)^{c_q} = \prod_{q|n} \left(\frac{a_j}{\mathfrak{q}} \right)_M^{c_q} = \chi(a_j).$$

Thus,

$$m \mid \text{ord} \left(\frac{\sigma(\beta_j)}{\beta_j} \right)$$

for every $1 \leq j \leq k$. Changing β_j multiplies it by an element of $\mu_M \subseteq K$, so the ratios above do not change. $\square$

5. PROOF OF THE MAIN THEOREM

In this section, we prove Theorem 1.1. We begin by establishing the positivity of the density.

If $m = 1$, every prime $p \nmid a_j$ is admissible. Hence, we assume that $m \geq 2$. By Proposition 4.1, there is a Galois extension L/K , with $K = \mathbb{Q}(\mu_M)$ and $L = K(a_1^{1/M}, \dots, a_k^{1/M})$, and an element $\sigma \in G = \text{Gal}(L/K)$ such that for any $\beta_j \in L$ satisfying $\beta_j^M = a_j$,

$$m \mid \text{ord} \left(\frac{\sigma(\beta_j)}{\beta_j} \right)$$

for every $1 \leq j \leq k$. Let C be the conjugacy class of σ in G . Since G is abelian, $C = \{\sigma\}$. Let $\mathcal{P}$ be the set of unramified, degree-1 primes $\mathfrak{p} \subset \mathcal{O}_K$ satisfying $\text{Frob}_{\mathfrak{p}} = \sigma$. Then

$$\#\{\mathfrak{p} \in \mathcal{P} : N\mathfrak{p} \leq x\} \sim \frac{1}{\#G} \frac{x}{\log x}.$$

Fix an element $\mathfrak{p}$ of the set, and write $(p) = \mathfrak{p} \cap \mathbb{Z}$. After excluding finitely many primes from $\mathcal{P}$, we may assume that p divides neither M nor any a_j . We claim that $m \mid \text{ord}_p(a_j)$ for every j . For a remaining $\mathfrak{p}$ above p , $k_{\mathfrak{p}} \cong \mathbb{F}_p$. Since $p \nmid M$, Lemma 2.2 gives an injection

$$\mu_M \hookrightarrow k_{\mathfrak{p}}^{\times} \cong \mathbb{F}_p^{\times}.$$

Consequently, $M \mid p-1$. Let $\zeta_j = \sigma(\beta_j)/\beta_j$. Since $v_{\mathfrak{p}}(a_j) = 0$ for every j , $\zeta_j = (a_j/\mathfrak{p})_M$. Let $\bar{\zeta}_j$ and $\bar{a}_j$ denote the reductions of ζ_j and a_j modulo $\mathfrak{p}$, respectively. Then

$$\bar{\zeta}_j = \bar{a}_j^{(N\mathfrak{p}-1)/M} = \bar{a}_j^{(p-1)/M}.$$

Since reduction preserves the order of ζ_j ,

$$m \mid \text{ord}(\zeta_j) = \text{ord}(\bar{\zeta}_j) \mid \text{ord}_p(a_j).$$

Let A denote the full admissible set of primes, and let

$$A(x) = \#\{p \in A : p \leq x\}.$$

Each prime p has at most $[K : \mathbb{Q}]$ primes of K above it. Moreover, since $f(\mathfrak{p}/p) = 1$, $N\mathfrak{p} = p$. Therefore,

$$[K : \mathbb{Q}]A(x) \geq \#\{\mathfrak{p} \in \mathcal{P} : N\mathfrak{p} \leq x\}.$$

Hence,

$$\liminf_{x \rightarrow \infty} \frac{A(x)}{\pi(x)} \geq \frac{1}{[L : K][K : \mathbb{Q}]} = \frac{1}{[L : \mathbb{Q}]} > 0.$$

Now we prove that the density of A exists. Let $e_{\ell} = v_{\ell}(m)$ for every $\ell \mid m$. Since $\text{ord}_p(a_j) \mid p-1$, $v_{\ell}(p-1) \geq e_{\ell}$ for every $p \in A$. For $N \geq \max_{\ell \mid m} e_{\ell}$, let

$$A_N = \{p \in A : e_{\ell} \leq v_{\ell}(p-1) \leq N \text{ for every } \ell\}.$$

We demonstrate that A_N has a natural density.

After letting $v_{\ell}(p-1) = r_{\ell}$ and $d_{\ell} = \ell^{r_{\ell}-e_{\ell}+1}$, we claim that $\ell^{e_{\ell}} \mid \text{ord}_p(a)$ if and only if a is not a d_{ℓ} -th power modulo p . Assume that $r_{\ell} \geq e_{\ell}$, choose a generator g of $\mathbb{F}_p^{\times}$, and write $a = g^s$ in this group. Indeed,

$$\text{ord}_p(a) = \frac{\text{ord}_p(g)}{\gcd(\text{ord}_p(g), s)} = \frac{p-1}{\gcd(p-1, s)}.$$

Consequently, $\ell^{e_{\ell}} \mid \text{ord}_p(a)$ if and only if $v_{\ell}(\gcd(p-1, s)) \leq r_{\ell} - e_{\ell}$, which is equivalent to $d_{\ell} \nmid s$. Since $d_{\ell} \mid p-1$, the subgroup of d_{ℓ} -th powers is $(\mathbb{F}_p^{\times})^{d_{\ell}} = \langle g^{d_{\ell}} \rangle$. Thus, $a = g^s$ belongs to this subgroup exactly when $d_{\ell} \mid s$. This proves the claim.

For a fixed integer N , let

$$C_N = \prod_{\ell \mid m} \ell^{N+1}, \quad F_N = \mathbb{Q} \left(\mu_{C_N}, a_j^{1/\ell^N} : 1 \leq j \leq k, \ell \mid m \right),$$

and fix a vector (r_{ℓ}) with $e_{\ell} \leq r_{\ell} \leq N$. Then F_N is Galois. It contains all roots of the polynomial $X^{d_{\ell}} - a_j$ for every j and $\ell \mid m$. Discard the finitely many primes ramified in $F_N/\mathbb{Q}$ or dividing C_N or some a_j . Then the condition $v_{\ell}(p-1) = r_{\ell}$ is equivalent to $p \equiv 1 \pmod{\ell^{r_{\ell}}}$ and $p \not\equiv 1 \pmod{\ell^{r_{\ell}+1}}$ holding simultaneously. Choose a prime $\mathfrak{P}$ of F_N above p . These conditions are determined by the Frobenius element $\text{Frob}_{\mathfrak{P}/p}$ on the cyclotomic subfields of F_N . Moreover, a_j is not an d_{ℓ} -th power modulo p if and only if no root of the reduction of $X^{d_{\ell}} - a_j$ lies in $\mathbb{F}_p$. This is equivalent to $\text{Frob}_{\mathfrak{P}/p}$ fixing no root of $X^{d_{\ell}} - a_j$.

Both conditions are invariant under conjugation. Let Frob_p denote the conjugacy class of $\text{Frob}_{\mathfrak{P}/p}$. Thus, the membership of a prime p in that layer of A_N is determined by whether Frob_p belongs to a specific collection of conjugacy classes in $\text{Gal}(F_N/\mathbb{Q})$. Then the Chebotarev density theorem shows that the primes in each layer have a natural density. Since there are only finitely many disjoint layers, A_N has a natural density.

Let that density be δ_N . Since the sets A_N expand as N grows, δ_N converges to some $\delta \leq 1$. In addition, if $p \in A \setminus A_N$, then $v_\ell(p-1) > N$ for some $\ell \mid m$. As a result,

$$A \setminus A_N \subseteq \bigcup_{\ell} \{p : p \equiv 1 \pmod{\ell^{N+1}}\}.$$

The set on the right has upper density bounded by

$$\varepsilon_N = \sum_{\ell} \frac{1}{\varphi(\ell^{N+1})} \longrightarrow 0.$$

Let $\bar{\delta}(A)$ and $\underline{\delta}(A)$ denote the upper and lower densities of A , respectively. Then,

$$\delta_N \leq \underline{\delta}(A) \leq \bar{\delta}(A) \leq \delta_N + \varepsilon_N.$$

Consequently, $\delta(A) = \delta$. This proves the existence of the natural density.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics, vol. 20, Academic Press, 1986.
2. Lindsay Childs, *A concrete introduction to higher algebra*, Undergraduate Texts in Mathematics, Springer, New York, 1984.
3. Olli Järvinen, *Equality of orders of a set of integers modulo a prime*, Proceedings of the American Mathematical Society **149** (2021), no. 9, 3651–3668.
4. ———, *Simultaneous insolvability of exponential congruences*, Journal of Number Theory **239** (2022), 335–351.
5. Pieter Moree, *On primes p for which d divides $\text{ord}_p(g)$* , Functiones et Approximatio Commentarii Mathematici **33** (2005), 85–95.
6. Antonella Perucca, *On the reduction of points on abelian varieties and tori*, International Mathematics Research Notices **2011** (2011), no. 2, 293–308.
7. Pietro Sgobba, *Divisibility conditions on the order of the reductions of algebraic numbers*, Mathematics of Computation **92** (2023), no. 343, 2281–2305.
8. Lawrence C. Washington, *Introduction to cyclotomic fields*, 1 ed., Graduate Texts in Mathematics, vol. 83, Springer, New York, 2012, Electronic reprint of the 1982 first edition.
9. K. Wiertelak, *On the density of some sets of primes, II*, Acta Arithmetica **34** (1978), no. 3, 197–210.
10. Asif Zaman, *Bounding the least prime ideal in the chebotarev density theorem*, Functiones et Approximatio Commentarii Mathematici **57** (2017), no. 1, 115–142.

ACKNOWLEDGMENTS

I wish to express my sincere gratitude to Jiyao Tang. Tang has been my mentor since I was in middle school. It was he who taught me the fundamentals of analysis and algebra, setting me on the road to serious mathematical research. He received no financial benefit from supporting me throughout the project. I would like to thank Tang for the helpful discussions that have been key to the development of this research.

The problem was inspired by a simple lemma from Tang's own research, which illustrates the use of a fixed-point technique in a narrow setting. The order problem discussed in the paper, however, is much broader. It arose from a long-standing line of work in algebraic number theory. After locating the problem in the literature, I began to seek an alternative proof of a theorem first established in 2022.

Tang brought the lemma to my attention. He also offered suggestions on the exposition during the process of writing the paper. I carried out the remainder of the research.

I first proved a weaker form of the single-variable theorem, establishing infinitude rather than positive density, which is significantly easier to establish using the fixed-point technique that I developed. In the multivariable setting, the main technical difficulty lies in controlling several congruences simultaneously. I resolved this by constructing a Kummer extension, in which the divisibility conditions are encoded Galois-theoretically, and applying the Chebotarev density theorem to produce a set of admissible primes. This establishes the positivity part of the main theorem.

The remaining obstruction is the extraction of a suitable Galois automorphism that allows the Chebotarev density theorem to be applied. For this purpose, I first demonstrated the infinitude of integer moduli for which the order conditions are satisfied. Then, from these composite moduli, I applied techniques in elementary group theory to extract a character encoding the prescribed conditions and realized the desired automorphism via power residue symbols. The last part of my work was a truncation argument used to establish the existence part of the main theorem.

Finally, I would like to express my deepest gratitude to my parents for bringing me into this wonderful world. Their unwavering support and encouragement have made it possible for me to pursue mathematics with determination and confidence. I am profoundly grateful for all that they have done for me.

Email address: s25516@stu.ykpaoschool.cn

YK PAO SCHOOL, HIGH SCHOOL DIVISION, 1800 LANE 900 NORTH SANXIN ROAD, SONGJIANG DISTRICT, SHANGHAI 201620, CHINA