THE ERD\H OŠ-KAC THEOREM FOR POLYNOMIALS
OF SEVERAL VARIABLES

MAOSHENG XIONG

(Communicated by Wen-Ching Winnie Li)

Abstract. We prove two versions of the Erd\H os-Kac type theorem for polynomials of several variables on some varieties arising from translation and affine linear transformation.

1. Introduction

For a positive integer \( n \), let \( \omega(n) \) be the number of distinct prime divisors of \( n \). The remarkable theorem of Erd\H os and Kac (\cite{7}) asserts that, for any \( \gamma \in \mathbb{R} \),

\[
\lim_{X \to \infty} \frac{1}{X} \# \left\{ 1 \leq n \leq X : \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \leq \gamma \right\} = G(\gamma),
\]

where

\[
G(\gamma) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2} dt
\]

is the Gaussian distribution function.

Erd\H os and Kac proved this theorem by a probabilistic idea, building upon the work of Hardy and Ramanujan (\cite{10}) and Tur\H an (\cite{21}) on the normal order of \( \omega(n) \).

Since then there has been a very rich literature on various aspects of the Erd\H os-Kac theorem (see, for example, \cite{1, 9, 11, 13, 14, 15, 16, 17, 19, 20}). Interested readers can refer to Granville and Soundararajan’s paper \cite{8} for the most recent account and Elliot’s monograph \cite{6} for a comprehensive treatment of the subject.

In particular, Halberstam in \cite{9} proved that

\[
\lim_{X \to \infty} \frac{1}{X} \# \left\{ n : 1 \leq n \leq X, \frac{\omega(g(n)) - A(n)}{\sqrt{B(n)}} \leq \gamma \right\} = G(\gamma),
\]

where \( g(x) \in \mathbb{Z}[x] \) is an irreducible polynomial,

\[
A(n) = \sum_{p \leq n} \frac{r(p)}{p}, \quad B(n) = \sum_{p \leq n} \frac{r(p)^2}{p},
\]

and \( r(p) \) is the number of solutions of \( g(m) \equiv 0 \pmod{p} \), \( 0 \leq m < p \).

In a recent paper (\cite{3}) Bourgain, Gamburd and Sarnak showed among other things that a large family of polynomials is “factor finite”; that is, the subset at which the polynomial has a bounded number of prime factors is Zariski dense in the orbit obtained by translation and affine linear transformation. By adapting their
proofs and applying a criterion of Liu ([15]), in this paper we obtain two versions of the Erdős-Kac type theorem for polynomials of several variables.

To state the first result, we need some notation.

For an additive subgroup $\Lambda \subset \mathbb{Z}^n$ of rank $k$ ($1 \leq k \leq n$), explicitly given by $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_k$ for $\mathbb{Q}$-linearly independent vectors $e_1, \ldots, e_k \in \mathbb{Z}^n$, we denote by $V = Zcl(\Lambda)$ the Zariski closure of $\Lambda$ in the affine space $\Lambda^n$ over $\mathbb{Q}$. For any $b \in \mathbb{Z}^n$, denote $O_b = \Lambda + b$ and for any $L > 0$, denote

$$O_b(L) = \{ y_1e_1 + \cdots + y_ke_k + b \in O_b : |y_i| \leq L, \ y_i \in \mathbb{Z}, \ 1 \leq i \leq k \}.$$ 

**Theorem 1.** Let $\Lambda$ be as above. Suppose each of the polynomials $f_1, \ldots, f_t \in \mathbb{Z}[x_1, \ldots, x_n]$ generates a distinct prime ideal in the coordinate ring $\mathbb{Q}[V]$. Let $f = f_1 \cdots f_t$. Then for any $b \in \mathbb{Z}^n$ and for any $\gamma \in \mathbb{R}$, we have

$$\lim_{L \to \infty} \frac{1}{\#O_b(L)} \# \left\{ x \in O_b(L) : \frac{\omega(f(x)) - t \log \log L}{\sqrt{t \log \log L}} \leq \gamma \right\} = G(\gamma).$$

When $k = n = 1$, Theorem 1 coincides with ([11]) in the special case that $g(x) \in \mathbb{Z}[x]$ is absolutely irreducible. As another example we may choose $\Lambda = \mathbb{Z}^2$ and $f_i(x, y) = x^i - y$ for $1 \leq i \leq t$. One sees that this choice of $\Lambda$ and $f_i$'s satisfies all the above conditions.

To state the second result, we use the following notation.

Let $\Lambda \subset \text{GL}(n, \mathbb{Z})$ be a free subgroup generated by the $d$ elements $A_1, \ldots, A_d$. Suppose the Zariski closure $G = Zcl(\Lambda)$ is isomorphic to $\text{SL}_2$ over $\mathbb{Q}$. Given a matrix $b \in \text{Mat}_{m \times n}(\mathbb{Z})$, $\Lambda$ acts on $b$ by right multiplication. Suppose $\text{Stab}_\Lambda(b)$ is trivial and the $G$ orbit $V = b \cdot G$ is Zariski closed and hence defines a variety over $\mathbb{Q}$. Assume $\text{dim} \ V > 0$. Denote $O_b = b \cdot \Lambda$. We turn $O_b$ into a $2d$-regular tree by joining the vertex $x \in O_b$ with the vertices $x \cdot A_1, x \cdot A_1^{-1}, \ldots, x \cdot A_d, x \cdot A^{-1}_d$. (This is indeed a tree because $\Lambda$ is free on the generators and $\text{Stab}_\Lambda(b)$ is trivial.) For $x, y \in O_b$, let $v(x, y)$ denote the distance in the tree from $x$ to $y$. For any $L > 0$, we denote

$$O_b(L) = \{ x \in O_b : v(x, b) \leq \log L \}.$$ 

**Theorem 2.** Let $\Lambda, b$ be as above. Suppose each of the polynomials $f_1, \ldots, f_t \in \mathbb{Z}[x_1, \ldots, x_{mn}]$ generates a distinct prime ideal in the coordinate ring $\mathbb{Q}[V]$, and let $f = f_1 \cdots f_t$. Then for any $\gamma \in \mathbb{R}$, we have

$$\lim_{L \to \infty} \frac{1}{\#O_b(L)} \# \left\{ x \in O_b(L) : \frac{\omega(f(x)) - t \log \log L}{\sqrt{t \log \log L}} \leq \gamma \right\} = G(\gamma).$$

As an example we may choose $b$ to be the $2 \times 2$ identity matrix, $f_i(x_1, x_2, x_3, x_4) = x_1^i - x_4$ for each $1 \leq i \leq t$ and the subgroup $\Lambda \subset \text{SL}(2, \mathbb{Z})$ to be generated by two elements:

$$\Lambda = \left\langle \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \right\rangle.$$ 

Since $\Lambda$ is a non-elementary subgroup of $\text{SL}(2, \mathbb{Z})$ and $\Lambda \subset \Gamma(2)$, it is known that $Zcl(\Lambda) = \text{SL}_2$ and $\Lambda$ is a free group ([2]). One can check that the $f_i$'s generate distinct prime ideals in $\mathbb{Q}[V]$ and $\Lambda$, and the $f_i$'s and $b$ satisfy the conditions of Theorem 2.

This paper is organized as follows. Liu’s criterion is briefly reviewed in Section 2. In Section 3, we use it to prove Theorem 1 by adapting the sieving process of the proof of Theorem 1.6 in [3]. Since the proof of Theorem 2 is similar, it is sketched in Section 4.
2. Preliminaries

We shall need the following criterion obtained by Liu ([15]). For completeness and for later applications we reproduce the statement with some adjustments.

Let \( \mathcal{O} \) be an infinite set. For any \( L > 1 \), assign a finite subset \( \mathcal{O}(L) \subset \mathcal{O} \) such that \( \# \mathcal{O}(L) \to \infty \) as \( L \to \infty \) and \( \# \mathcal{O}(L^{1/2}) = o(\# \mathcal{O}(L)) \). Let \( f : \mathcal{O} \to \mathbb{Z} \setminus \{0\} \) be a map. Put \( X = X(L) = \# \mathcal{O}(L) \) and write, for each prime \( l \),

\[
\frac{1}{X} \# \{ n \in \mathcal{O}(L) : f(n) \text{ is divisible by } l \} = \lambda_l(X) + e_l(X)
\]

as a sum of the major term \( \lambda_l(X) \) and the error term \( e_l(X) \). For any \( u \) distinct primes \( l_1, l_2, \ldots, l_u \), we write

\[
\frac{1}{X} \# \{ n \in \mathcal{O}(L) : f(n) \text{ is divisible by } l_1l_2 \cdots l_u \} = \prod_{i=1}^{u} \lambda_{l_i}(X) + e_{l_1l_2 \cdots l_u}(X).
\]

To ease our notation, the dependence on \( X \) will be dropped when there is no ambiguity.

In order to gain information on the distribution of \( \omega(f(n)) \), some control on \( \lambda_l \) and \( e_l \) is needed. Liu’s criterion uses the conditions below.

Suppose there exist absolute constants \( \beta, c \), where \( 0 < \beta \leq 1 \) and \( c > 0 \), and a function \( Y = Y(X) \leq X^\beta \) such that the following hold:

(i) For each \( n \in \mathcal{O}(L) \), the number of distinct prime divisors \( l \) of \( f(n) \) with \( l > X^\beta \) is bounded uniformly.

(ii) \( \sum_{Y < t \leq X^\beta} \lambda_t = o((\log \log X)^{1/2}) \).

(iii) \( \sum_{Y < t \leq X^\beta} |e_t| = o((\log \log X)^{1/2}) \).

(iv) \( \sum_{t \leq Y} \lambda_t = c \log \log X + o((\log \log X)^{1/2}) \).

(v) \( \sum_{t \leq Y} \lambda_t^2 = o((\log \log X)^{1/2}) \).

The sums in (ii)–(v) are over primes \( l \) in the given range.

(vi) For any \( r \in \mathbb{N} \) and any integer \( u \) with \( 1 \leq u \leq r \), we have

\[
\lim_{X \to \infty} \frac{1}{(\log \log X)^{r/2}} \sum_{l_1 \cdots l_u} |e_{l_1 \cdots l_u}| = 0,
\]

where for each \( u \), the sum \( \sum'' \) extends over all \( u \) distinct primes \( l_1, l_2, \ldots, l_u \) with \( l_i \leq Y \).

**Theorem 3** (Liu [15, Theorem 3]). If \( \mathcal{O} \) and \( f : \mathcal{O} \to \mathbb{Z} \setminus \{0\} \) satisfy all the above conditions, then for \( \gamma \in \mathbb{R} \), we have

\[
\lim_{L \to \infty} \frac{1}{X(L)} \# \left\{ n \in \mathcal{O}(L) : \frac{\omega(f(n)) - c \log \log X(L)}{\sqrt{c \log \log X(L)}} \leq \gamma \right\} = G(\gamma).
\]

While the conditions of Theorem 3 may appear complicated, in our applications, the terms \( \lambda_l \) and \( e_l \) can be easily identified and the conditions easily verified, as we shall see in the proofs of Theorems 1 and 2 below.

3. Proof of Theorem [1]

We denote the basis \( e_i, 1 \leq i \leq k, \) of \( \Lambda \) by \( e_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{Z}^n \). Put

\[
A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kn} \end{pmatrix},
\]
which is a matrix of rank $k$. For a row vector $y$, let $|y|$ be the maximum modulus of its components. Then for $L$ large, denote
\[ \mathcal{O}_b(L) = \{ yA + b : y \in \mathbb{Z}^k, |y| \leq L \}. \]
We write $X$ for $\# \mathcal{O}_b(L) = (2|L| + 1)^k$. To apply Theorem 3 one needs to estimate, for each square-free integer $d$, the sum
\[
\sum_{\substack{x \in \mathcal{O}_b(L) \in f(x) \equiv 0 \pmod{d} \leq L}} 1 = \sum_{\substack{y \in \mathbb{Z}^k \in f(yA + b) \equiv 0 \pmod{d} \leq L}} 1 = \sum_{\substack{y \in (\mathbb{Z}/d\mathbb{Z})^k \in f(yA + b) \equiv 0 \pmod{d} \leq L}} 1.
\]
Suppose $d \leq L$. The inner sum can be estimated as
\[
\frac{(2|L| + 1)^k}{d^k} + O \left( \frac{(2|L| + 1)^{k-1}}{d^{k-1}} \right) = X + O \left( \frac{X^{1-\frac{1}{k}}}{d^{k-1}} \right).
\]
Since the affine variety $V' = V + b$ is absolutely irreducible, and the polynomials $f_1, \ldots, f_t$ generate distinct prime ideals in the coordinate ring $\mathbb{Q}[V]$, one sees that all the varieties
\[ W_i = V' \cap \{ f_i = 0 \}, \quad i = 1, 2, \ldots, t, \]
are defined over $\mathbb{Q}$, absolutely irreducible, and of dimension equal to $\dim V' - 1 = k + 1 \geq 0$. Consider the reduction of the varieties $V', W_i$ (mod $p$). According to Noether’s theorem [18], for $p$ outside a finite set $S_1$ of primes, the reductions of $V'$ and $W_i$, $i = 1, \ldots, t$, yield absolutely irreducible affine varieties over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Denote by $V'(\mathbb{F}_p), V'(\mathbb{Z}/d\mathbb{Z})$, etc., the reduction of the varieties in the corresponding ring. By the Lang-Weil Theorem [12] we have that for $p \not\in S_1$,
\[
\# V'(\mathbb{Z}/p\mathbb{Z}) = p^k + O \left( p^{k-\frac{1}{2}} \right),
\]
\[
\# W_i(\mathbb{Z}/p\mathbb{Z}) = p^{k-1} + O \left( p^{k-\frac{1}{2}} \right).
\]
Since the map
\[
\mathbb{A}_d^k \rightarrow V', \quad y \mapsto yA + b
\]
is a bijection, one obtains
\[
\sum_{\substack{y \in (\mathbb{Z}/d\mathbb{Z})^k \in f(yA + b) \equiv 0 \pmod{d} \leq L}} 1 = \sum_{\substack{y \in V'(\mathbb{Z}/d\mathbb{Z}) \in f(y) \equiv 0 \pmod{d} \leq L}} 1 = \# W(\mathbb{Z}/d\mathbb{Z}),
\]
where
\[
W(\mathbb{Z}/d\mathbb{Z}) = \{ y \in V'(\mathbb{Z}/d\mathbb{Z}) : f(y) \equiv 0 \pmod{d} \}.
\]
Let
\[
\lambda_d = \frac{\# W(\mathbb{Z}/d\mathbb{Z})}{d^k}.
\]
By the Chinese Remainder Theorem, $\lambda_d$ is multiplicative for $d$ coprime to $\prod_{p \in S_1} p$.
Since
\[
W(\mathbb{Z}/d\mathbb{Z}) = \bigcup_{i=1}^t W_i(\mathbb{Z}/d\mathbb{Z}),
\]

for such square-free $d$ one has
\[
\# W(\mathbb{Z}/d \mathbb{Z}) \leq \sum_{i=1}^{t} \# W_i(\mathbb{Z}/d \mathbb{Z}) = \sum_{i=1}^{t} \prod_{p \mid d} \# W_i(\mathbb{Z}/p \mathbb{Z}) = \sum_{i=1}^{t} \prod_{p \mid d} \left( p^{k-1} + O(p^{k-3/2}) \right) \ll d^{k-1+\epsilon}.
\]

Therefore for $d \leq L$ and $\gcd \left( d, \prod_{p \in S_1} p \right) = 1$, we obtain
\[
(3.1) \quad \sum_{f(x) \equiv 0 \pmod{d}} 1 = X(\lambda_d + e_d), \text{ where } e_d \ll d^k X^{-\frac{1}{2}}.
\]

It follows from Lemma 3.1 below that the estimate (3.1) still holds if on the left-hand side the points $x \in \mathcal{O}_L(L)$ such that $f(x) = 0$ are removed. Thus we may assume that $f(x) \neq 0$ for all $x \in \mathcal{O}_L(L)$. Now we return to $\lambda_d$. For $d = l$ a prime and $l \not\in S_1$ we have
\[
W(\mathbb{Z}/l \mathbb{Z}) = \bigcup_{i=1}^{t} W_i(\mathbb{Z}/l \mathbb{Z}).
\]

For fixed $i \neq j$, the algebraic subset $W_i = W_i(\mathbb{Z}/l \mathbb{Z}) \cap W_j(\mathbb{Z}/l \mathbb{Z})$ is defined over the finite field $\mathbb{F}_l = \mathbb{Z}/l \mathbb{Z}$ and has dimension at most $k - 2$. Then it follows from Lemma 2.1 of [4] that
\[
\# (W_i(\mathbb{Z}/l \mathbb{Z}) \cap W_j(\mathbb{Z}/l \mathbb{Z})) \ll l^{k-2},
\]

where the implied constant depends on $f$ and $V$ only. By the inclusion-exclusion principle,
\[
\sum_{i=1}^{t} \# W_i(\mathbb{Z}/l \mathbb{Z}) - \sum_{1 \leq i < j \leq t} \# (W_i(\mathbb{Z}/l \mathbb{Z}) \cap W_j(\mathbb{Z}/l \mathbb{Z})) \leq \# W(\mathbb{Z}/l \mathbb{Z}) \leq \sum_{i=1}^{t} \# W_i(\mathbb{Z}/l \mathbb{Z}),
\]

from which one obtains
\[
\# W(\mathbb{Z}/l \mathbb{Z}) = tl^{k-1} + O \left( l^{k-\frac{3}{2}} \right).
\]

This implies that
\[
(3.2) \quad \lambda_l = \frac{t}{l} + O \left( l^{-\frac{3}{2}} \right).
\]

Using (3.1) and (3.2) and choosing
\[
Y' = \exp \left( \frac{\log X}{\log \log X} \right), \quad \beta = \frac{1}{2k},
\]

one can verify the conditions (i)–(vi) of Theorem 3.3 for $f$ and $\mathcal{O}_L$. For example, for (i), noticing that $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and $x \in \mathcal{O}_L(L)$, one has $f(x) \ll L^{\deg f} \ll X^{\frac{\deg f}{2k}}$. Thus $\sum_{l \mid f(x)} 1 \ll X^{\beta}$; i.e., the number of distinct prime divisors $l$ of $f(x)$ with $l > X^{\beta}$.
is bounded uniformly. For (ii), noticing \( \log \log Y = \log \log X - \log \log \log X \), one has
\[
\sum_{Y < t \leq X^a} \lambda_t \leq \sum_{Y < t \leq X^a} \frac{t}{\rho} + O \left( t^{\frac{-2}{3}} \right) \ll t \log \log X^a - t \log \log Y + O(1),
\]
which is \( o((\log \log X)^{1/2}) \) as \( X \) goes to infinity. The conditions (iii)–(v) can be verified similarly.

Finally, for (vi), for any fixed \( r \in \mathbb{N} \) and \( 1 \leq u \leq r \),
\[
\sum_{l_i \leq Y} |\epsilon_{l_1 \cdots l_u}| \leq \epsilon \sum_{l_i \leq Y} X^{-\frac{2}{3}}(l_1 \cdots l_u)^r \ll X^{-\frac{2}{3}}Y^{r(1+\epsilon)} \ll X^{-\frac{2}{3}}(\log X)^{2r},
\]
which is \( o((\log \log X)^{-r/2}) \) as \( X \) goes to infinity.

Since the conditions (i)–(vi) of Theorem 3 are satisfied for \( f \) and \( O_{\mathbb{R}} \), the desired conclusion follows from Theorem 3. The proof of Theorem 1 will be completed once we prove Lemma 3.1 below.

**Lemma 3.1.** Let \( W \) be a proper closed subset of \( V' = V + \mathbb{A} \) defined over \( \mathbb{Q} \). Then as \( L \to \infty \) one has
\[
\#(O_{\mathbb{R}}(L) \cap W) \ll X^{1 - \frac{1}{k}}.
\]

**Proof.** The proof is very similar to that of Proposition 3.2 in [3]. For the sake of completeness we give a detailed proof here.

Since \( V' = V + \mathbb{A} \) is irreducible, \( W \) is defined over \( \mathbb{Q} \) and has dimension at most \( \dim V - 1 = k - 1 \). Let \( W_1, \ldots, W_r \) be the irreducible components of \( W \). Then we have \( W = \bigcup_{j=1}^r W_j \), where the \( W_j \)'s are defined over a finite extension \( K \) of \( \mathbb{Q} \) and \( \dim W_j \leq k - 1 \) for each \( j \). For \( \mathcal{P} \) outside a finite set of prime ideals of the ring of integers \( \mathcal{O}_K \), \( W_j \) is an absolutely irreducible variety over the finite field \( \mathcal{O}_K / \mathcal{P} \) ([13]). Hence by [12] we have
\[
\#W_j(\mathcal{O}_K / \mathcal{P}) \ll N(\mathcal{P})^{\dim(W_j)} \leq N(\mathcal{P})^{k-1}.
\]
Here, as usual, \( N(\mathcal{P}) = \#(\mathcal{O}_K / \mathcal{P}) \). Choose \( p \) so that it splits completely in \( K \) and let \( \mathcal{P} \cap (p) \). Then \( \mathcal{O}_K / \mathcal{P} \cong \mathbb{F}_p \) and we have
\[
(3.3) \quad \#W(\mathbb{Z}/p\mathbb{Z}) \leq \sum_{j=1}^r \#W_j(\mathcal{O}_K / \mathcal{P}) \ll N(\mathcal{P})^{k-1} = p^{k-1}.
\]
Now proceed as before. For \( L \to \infty \) and any large \( p \) as above, we have
\[
\#(O_{\mathbb{R}}(L) \cap W) = \sum_{x \in O_{\mathbb{R}}(L)} 1 \leq \sum_{x \in W(\mathbb{Z}/p\mathbb{Z})} \sum_{y \in \mathbb{Z}_L^k, |y| \leq L} \sum_{y \equiv \xi (\text{mod } p)} 1.
\]
Similarly the right-hand side can be estimated as
\[
\sum_{x \in W(\mathbb{Z}/p\mathbb{Z})} \left( \frac{X}{p^{1/k}} + O \left( \frac{X^{1-1/k}}{p^{1/k}} \right) \right).
\]
Hence for large \( p \) as in (3.3),
\[
\#(O_{\mathbb{R}}(L) \cap W) \ll Xp^{-1} + X^{1-1/k}.
\]
By the Chebotarev density theorem \([3]\) we can choose a \(p\) which splits completely in \(K\) and which satisfies
\[
X^{1/k}/2 \leq p \leq 2X^{1/k}.
\]
With this choice we get the bound claimed in Lemma 3.1. \(\square\)

4. Proof of Theorem \([2]\)

It is elementary that the number of points on a \(2d\)-regular tree whose distance to a given vertex is at most \([\log L]\) is equal to \(X = \#O_2(L) = \frac{d(2d-1)^{[\log L]}-1}{d-1}\). By the assumptions of Theorem \([2]\) \(V\) is an absolutely irreducible affine variety defined over \(\mathbb{Q}\) with \(\dim V > 0\) and \(f_1, \ldots, f_t\) generate distinct prime ideals in \(\mathbb{Q}[V]\). Hence for \(i = 1, \ldots, t\), the varieties
\[
W_i = V \cap \{f_i = 0\}
\]
are defined over \(\mathbb{Q}\), absolutely irreducible, and of dimension equal to \(\dim V - 1\). We consider the reduction of the varieties (mod \(p\)). By Noether’s theorem \([13]\) and the Lang-Weil Theorem \([12]\), there is a finite set \(S_1\) of primes such that if \(p \not\in S_1\), the varieties \(V(\mathbb{Z}/p\mathbb{Z}), W_i(\mathbb{Z}/p\mathbb{Z})\) are absolutely irreducible and
\[
\begin{align*}
\#V(\mathbb{Z}/p\mathbb{Z}) &= p^{\dim V} + O\left(p^{\dim V - \frac{1}{2}}\right), \\
\#W_i(\mathbb{Z}/p\mathbb{Z}) &= p^\dim V - 1 + O\left(p^{\dim V - \frac{3}{2}}\right).
\end{align*}
\]
By using the uniform expansion property of \(\text{SL}_2\) established in \([2]\) (or assuming a conjecture of Lubotzy for a more general setting), Bourgain, Gamburd and Sarnak proved (Proposition 3.1, \([3]\)) that
\[
\mathbb{E}_X \sum_{\substack{y \in O_2(L) \\ f(y) \equiv 0 \mod d}} 1 = \lambda_d + e_d,
\]
for square-free integers \(d \leq X\) coprime to \(\prod_{p \in S_2} p\). Here \(S_2\) is a finite set of primes containing \(S_1\) and
\[
\lambda_d = \frac{\#V_0(\mathbb{Z}/d\mathbb{Z})}{\#V(\mathbb{Z}/d\mathbb{Z})}, \quad e_d \ll d^{\dim V - 1 + \epsilon}X^{\gamma - 1},
\]
where
\[
V_0(\mathbb{Z}/d\mathbb{Z}) = \{y \in V(\mathbb{Z}/d\mathbb{Z}) : f(y) \equiv 0 \pmod{d}\},
\]
and the absolute constant \(\gamma < 1\) is bounded below by some \(\delta > 0\). Also by Proposition 3.2 in \([3]\), in the sum the terms \(x \in O_2(L)\) with \(f(x) = 0\) can also be omitted without altering (4.1). Clearly \(\lambda_d\) is a multiplicative function of \(d\) coprime to \(\prod_{p \in S_2} p\). With similar arguments as in the proof of Theorem \([1]\) for \(d = l\) a prime and \(l \not\in S_2\) we have
\[
\lambda_l = \frac{t}{l} + O\left(l^{-\frac{3}{2}}\right)
\]
Now using (4.1), (4.2), choosing \(Y = \exp(\log X/\log \log X)\) and \(\beta > 0\) to be sufficiently small, we can similarly verify that the conditions (i)–(vi) of Theorem 3 for \(f\) and \(O_2\) hold. This completes the proof of Theorem \([2]\).

Acknowledgment

The author is grateful to the referee for many valuable suggestions.
References


