THE ERDŐS-KAC THEOREM FOR POLYNOMIALS OF SEVERAL VARIABLES

MAOSHENG XIONG

ABSTRACT. We prove two versions of the Erdős-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 Erdős and Kac ([7]) asserts that, for any $\gamma \in \mathbb{R}$,

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

where

$$G(\gamma) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-\frac{t^2}{2}} \mathrm{d}t$$

is the Gaussian distribution function.

Erdős and Kac proved it by a probabilistic idea, building upon the work of Hardy and Ramanujan ([10]) and Turán ([21]) on the normal order of $\omega(n)$. Since then there has been a very rich literature on various aspects of the Erdős-Kac theorem (see for example [1, 9, 11, 13, 14, 15, 16, 17, 19, 20]). Interested readers can refer to Granville and Soundararajan's paper [8] for the most recent account and Elliot's monograph [6] for a comprehensive treatment of the subject. In particular, Halberstam in [9] proved that

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

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

$$A(n) = \sum_{p < n} \frac{r(p)}{p}, \quad B(n) = \sum_{p < n} \frac{r(p)^2}{p}$$

2000 Mathematics Subject Classification. 11N64, 11R09.

XIONG

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

In a recent paper ([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 $\Lambda = \mathbb{Z}\underline{e}_1 \bigoplus \cdots \bigoplus \mathbb{Z}\underline{e}_k$ for \mathbb{Q} -linearly independent vectors $\underline{e}_1, \ldots, \underline{e}_k \in \mathbb{Z}^n$, we denote by $V = Zcl(\Lambda)$ the Zariski closure of Λ in the affine space \mathbb{A}^n over \mathbb{Q} . For any $\underline{b} \in \mathbb{Z}^n$, denote $\mathcal{O}_{\underline{b}} = \Lambda + \underline{b}$ and for any L > 0, denote

$$\mathcal{O}_{\underline{b}}(L) = \{ y_1 \underline{e}_1 + \dots + y_k \underline{e}_k + \underline{b} \in \mathcal{O}_{\underline{b}} : |y_i| \le L, \ y_i \in \mathbb{Z}, \ 1 \le i \le k \}.$$

Theorem 1. Let Λ 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 $\overline{\mathbb{Q}}[V]$. Let $f = f_1 \cdots f_t$. Then for any $\underline{b} \in \mathbb{Z}^n$ and for any $\gamma \in \mathbb{R}$, we have

$$\lim_{L \to \infty} \frac{1}{\#\mathcal{O}_{\underline{b}}(L)} \#\left\{ \underline{x} \in \mathcal{O}_{\underline{b}}(L) : \frac{\omega(f(\underline{x})) - t \log \log L}{\sqrt{t \log \log L}} \le \gamma \right\} = G(\gamma) \,.$$

When k = n = 1, Theorem 1 coincides with (1) on 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 $1 \le i \le t$. One sees that this choice of Λ and f_i 's satisfies all the above conditions.

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

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

$$\mathcal{O}_{\underline{b}}(L) = \{ \underline{x} \in \mathcal{O}_{\underline{b}} : v(\underline{x}, \underline{b}) \le \log L \}.$$

ERDŐS-KAC THEOREM

Theorem 2. Let Λ, \underline{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 $\overline{\mathbb{Q}}[V]$, let $f = f_1 \cdots f_t$. Then for any $\gamma \in \mathbb{R}$, we have

$$\lim_{L \to \infty} \frac{1}{\#\mathcal{O}_{\underline{b}}(L)} \#\left\{ \underline{x} \in \mathcal{O}_{\underline{b}}(L) : \frac{\omega(f(\underline{x})) - t \log \log L}{\sqrt{t \log \log L}} \le \gamma \right\} = G(\gamma) .$$

As an example we may choose \underline{b} to be the 2 by 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 $\Lambda \subset$ $\mathbf{SL}(2, \mathbb{Z})$ to be generated by two elements

$$\Lambda = \left\langle \left[\begin{array}{cc} 1 & 2 \\ 0 & 1 \end{array} \right], \left[\begin{array}{cc} 1 & 0 \\ 2 & 1 \end{array} \right] \right\rangle.$$

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

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

2. Preliminaries

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

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 $f : \mathcal{O} \longrightarrow \mathbb{Z} \setminus \{0\}$ 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 major term $\lambda_l(X)$ and error term $e_l(X)$. For any *u* distinct primes l_1, l_2, \ldots, l_u , we write

$$\frac{1}{X} \# \{ n \in \mathcal{O}(L) : f(n) \text{ is divisible by } l_1 l_2 \cdots l_u \} = \prod_{i=1}^u \lambda_{l_i}(X) + e_{l_1 l_2 \cdots l_u}(X) + e_{l_i l_i \cdots l_u}(X$$

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

XIONG

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

Suppose there exist absolute constants β , 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) $\sum_{Y < l < X^{\beta}} \lambda_l = o((\log \log X)^{1/2}).$
- (iii) $\sum_{Y < l < X^{\beta}} |e_l| = o((\log \log X)^{1/2}).$
- (iv) $\sum_{l \leq Y} \overline{\lambda}_l = c \log \log X + o((\log \log X)^{1/2}).$
- (v) $\sum_{l \le Y} \lambda_l^2 = o((\log \log X)^{1/2}).$

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

$$\lim_{X \to \infty} \frac{\sum_{u=0}^{n''} |e_{l_1 \cdots l_u}|}{(\log \log X)^{-r/2}} = 0,$$

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

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

While the conditions of Theorem 3 may appear complicated, in our applications, the terms λ_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 \underline{e}_i , $1 \leq i \leq k$, of Λ by $\underline{e}_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{Z}^n$. Put

$$A = \left(\begin{array}{ccc} a_{11} & \cdots & a_{1n} \\ & \cdots & \\ a_{k1} & \cdots & a_{kn} \end{array}\right) ,$$

which is a matrix of rank k. For a row vector \underline{y} , let $|\underline{y}|$ be the maximum modulus of its components. Then for L large, denote

$$\mathcal{O}_{\underline{b}}(L) = \{ yA + \underline{b} : y \in \mathbb{Z}^k, |y| \le L \}.$$

4

ERDŐS-KAC THEOREM

We write X for $\#\mathcal{O}_{\underline{b}}(L) = (2[L]+1)^k$. To apply Theorem 3, one needs to estimate, for each square-free integer d, the sum

$$\sum_{\substack{\underline{x}\in\mathcal{O}_{\underline{b}}(L)\\f(\underline{x})\equiv 0\pmod{d}}} 1 = \sum_{\substack{\underline{y}\in\mathbb{Z}^k\\|\underline{y}|\leq L\\f(\underline{y}A+\underline{b})\equiv 0\pmod{d}}} 1 = \sum_{\substack{\underline{y}\in(\mathbb{Z}/d\mathbb{Z})^k\\f(\underline{y}A+\underline{b})\equiv 0\pmod{d}\\g(\underline{y}A+\underline{b})\equiv 0\pmod{d}}} \sum_{\substack{\underline{x}\in\mathbb{Z}^k\\f(\underline{y}A+\underline{b})\equiv 0\pmod{d}\\x_i\equiv y_i\pmod{d}}} 1$$

Suppose $d \leq L$. The inner sum can be estimated as

$$\frac{(2[L]+1)^k}{d^k} + O\left(\frac{(2[L]+1)^{k-1}}{d^{k-1}}\right) = \frac{X}{d^k} + O\left(\frac{X^{1-\frac{1}{k}}}{d^{k-1}}\right).$$

Since the affine variety $V' = V + \underline{b}$ is absolutely irreducible, and the polynomials f_1, \ldots, f_t generate distinct prime ideals in the coordinate ring $\overline{\mathbb{Q}}[V]$, one sees that all the varieties

$$W_i = V' \bigcap \{ f_i = 0 \}, \quad i = 1, 2, \dots, t$$

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 $V', W_i \pmod{p}$. 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 $p \notin S_1$,

$$#V'(\mathbb{Z}/p\mathbb{Z}) = p^k + O\left(p^{k-\frac{1}{2}}\right),$$

$$#W_i(\mathbb{Z}/p\mathbb{Z}) = p^{k-1} + O\left(p^{k-\frac{3}{2}}\right).$$

Since the map

$$\begin{array}{cccc} \mathbb{A}^k & \longrightarrow & V' \\ \underline{y} & \mapsto & \underline{y}A + \underline{b} \end{array}$$

is a bijection, one obtains

$$\sum_{\substack{\underline{y} \in (\mathbb{Z}/d\mathbb{Z})^k \\ f(A\underline{y}+\underline{b}) \equiv 0 \pmod{d}}} 1 = \sum_{\substack{\underline{y} \in V'(\mathbb{Z}/d\mathbb{Z}) \\ f(\underline{y}) \equiv 0 \pmod{d}}} 1 = \#W(\mathbb{Z}/d\mathbb{Z}),$$

where

$$W(\mathbb{Z}/d\mathbb{Z}) = \{ \underline{y} \in V'(\mathbb{Z}/d\mathbb{Z}) : f(\underline{y}) \equiv 0 \pmod{d} \}.$$

Let

$$\lambda_d = \frac{\#W(\mathbb{Z}/d\mathbb{Z})}{d^k}.$$

By Chinese Remainder Theorem, λ_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

$$#W(\mathbb{Z}/d\mathbb{Z}) \leq \sum_{i=1}^{t} #W_i(\mathbb{Z}/d\mathbb{Z}) = \sum_{i=1}^{t} \prod_{p|d} #W_i(\mathbb{Z}/p\mathbb{Z})$$
$$= \sum_{i=1}^{t} \prod_{p|d} \left(p^{k-1} + O(p^{k-3/2}) \right) \ll_{\epsilon} d^{k-1+\epsilon}.$$

Therefore for $d \leq L$ and $\gcd\left(d, \prod_{p \in S_1} p\right) = 1$, we obtain

(2)
$$\sum_{\substack{\underline{x}\in\mathcal{O}_{\underline{b}}(L)\\f(\underline{x})\equiv 0\pmod{d}}} 1 = X(\lambda_d + e_d), \text{ where } e_d \ll_{\epsilon} d^{\epsilon} X^{-\frac{1}{k}}.$$

It follows from Lemma 1 below that the estimate (2) still holds if on the left hand side the points $\underline{x} \in \mathcal{O}_{\underline{b}}(L)$ such that $f(\underline{x}) = 0$ are removed. Thus we may assume that $f(\underline{x}) \neq 0$ for all $\underline{x} \in \mathcal{O}_{\underline{b}}(L)$. Now we return to λ_d . For d = l a prime and $l \notin S_1$ 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 $W' = W_i(\mathbb{Z}/l\mathbb{Z}) \bigcap W_j(\mathbb{Z}/l\mathbb{Z})$ is defined over the finite field $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$ and has dimension at most k-2, it follows from Lemma 2.1 of [4] that

$$\#\left(W_i(\mathbb{Z}/l\mathbb{Z})\bigcap W_j(\mathbb{Z}/l\mathbb{Z})\right) \ll l^{k-2},$$

where the implied constant depends on f and V only. By the inclusionexclusion principle

$$\sum_{i=1}^{t} \#W_i(\mathbb{Z}/l\mathbb{Z}) - \sum_{1 \le i < j \le t} \#\left(W_i(\mathbb{Z}/l\mathbb{Z}) \bigcap W_j(\mathbb{Z}/l\mathbb{Z})\right)$$
$$\leq \#W(\mathbb{Z}/l\mathbb{Z}) \le \sum_{i=1}^{t} \#W_i(\mathbb{Z}/l\mathbb{Z}),$$

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)
$$\lambda_l = \frac{t}{l} + O\left(l^{-\frac{3}{2}}\right).$$

Using (2) and (3) 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 for f and $\mathcal{O}_{\underline{b}}$. For example, for (i), noticing that $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and $\underline{x} \in \mathcal{O}_{\underline{b}}(L)$, one has $f(\underline{x}) \ll L^{\deg f} \ll X^{\frac{\deg f}{k}}$, thus $\sum_{\substack{l > X^{\beta} \\ l \mid f(\underline{x})}} 1 \ll 1$, i.e., the number of distinct prime divisors l of $f(\underline{x})$ with $l > X^{\beta}$ is bounded uniformly. For (ii), noticing $\log \log Y = \log \log X - \log \log \log X$, one has

$$\sum_{\substack{Y < l \le X^{\beta} \\ l \notin S_{1}}} \lambda_{l} \le \sum_{Y < l \le X^{\beta}} \frac{t}{l} + O\left(l^{-\frac{3}{2}}\right) \ll t \log \log X^{\beta} - t \log \log Y + O(1),$$

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 $1 \leq u \leq r$,

$$\sum_{l_i \le Y}^{''} |e_{l_1 \cdots l_u}| \le_{\epsilon} \sum_{l_i \le Y} X^{-\frac{1}{k}} (l_1 \cdots l_u)^{\epsilon} \le X^{-\frac{1}{k}} Y^{r(1+\epsilon)} \le X^{-\frac{1}{k}} (\log X)^{2r},$$

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 $\mathcal{O}_{\underline{b}}$, the desired conclusion follows from Theorem 3. The proof of Theorem 1 will be completed once we prove Lemma 1 below.

Lemma 1. Let W be a proper closed subset of $V' = V + \underline{b}$ defined over \mathbb{Q} . Then as $L \to \infty$ one has

$$\#\left(\mathcal{O}_{\underline{b}}(L)\bigcap W\right)\ll X^{1-\frac{1}{\dim V}}.$$

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 $V' = V + \underline{b}$ 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 $W = \bigcup_{i=1}^r W_j$, where 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 $\mathcal{O}_K/\mathcal{P}$ ([18]). Hence

by [12] we have

$$#W_j(\mathcal{O}_K/\mathcal{P}) \ll N(\mathcal{P})^{\dim(W_j)} \le N(\mathcal{P})^{k-1}.$$

Here, as usual, $N(\mathcal{P}) = \#(\mathcal{O}_K/\mathcal{P})$. Choose p so that it splits completely in K and let $\mathcal{P}|(p)$. Then $\mathcal{O}_K/\mathcal{P} \cong \mathbb{F}_p$ and we have

(4)
$$\#W(\mathbb{Z}/p\mathbb{Z}) \le \sum_{j=1}^{r} \#W_j(\mathcal{O}_K/\mathcal{P}) \ll N(P)^{k-1} = p^{k-1}.$$

Now proceed as before. For $L \to \infty$ and any large p as above, we have

$$\#\left(\mathcal{O}_{\underline{b}}(L)\bigcap W\right) = \sum_{\underline{x}\in\mathcal{O}_{\underline{b}}(L)\atop\underline{x}\in\overline{W}} 1 \leq \sum_{\underline{x}\in W(\mathbb{Z}/p\mathbb{Z})} \sum_{\underline{y}\in\mathbb{Z}^{k}, |\underline{y}|\leq L\\\underline{y}A+\underline{b}\equiv\underline{x} \pmod{p}} 1.$$

Similarly the right hand side can be estimated as

$$\sum_{\underline{x}\in W(\mathbb{Z}/p\mathbb{Z})} \left(\frac{X}{p^k} + O\left(\frac{X^{1-1/k}}{p^{k-1}}\right)\right) \,.$$

Hence for large p as in (4),

$$\#\left(\mathcal{O}_{\underline{b}}(L)\bigcap W\right)\ll Xp^{-1}+X^{1-1/k}.$$

By the Chebotarev density theorem ([5]) we can choose p which splits completely in K and which satisfies

$$X^{1/k}/2 \le p \le 2X^{1/k}$$

With this choice we get the bound claimed in Lemma 1. \Box

4. Proof of Theorem 2

It is elementary that the number of points on a 2*d*-regular tree whose distance to a given vertex is at most $[\log L]$ is equal to $X = \#\mathcal{O}_{\underline{b}}(L) = \frac{d(2d-1)^{\lfloor \log L \rfloor}-1}{d-1}$. 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 $\overline{\mathbb{Q}}[V]$. Hence for $i = 1, \ldots, t$, the varieties

$$W_i = V \bigcap \{f_i = 0\}$$

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 [18] and the Lang-Weil Theorem [12], there is a finite set S_1 of primes such that if $p \notin S_1$, the varieties $V(\mathbb{Z}/p\mathbb{Z}), W_i(\mathbb{Z}/p\mathbb{Z})$

8

are absolutely irreducible and

$$#V(\mathbb{Z}/p\mathbb{Z}) = p^{\dim V} + O\left(p^{\dim V - \frac{1}{2}}\right),$$

$$#W_i(\mathbb{Z}/p\mathbb{Z}) = p^{\dim V - 1} + O\left(p^{\dim V - \frac{3}{2}}\right).$$

By using the uniform expansion property of 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

(5)
$$\frac{1}{X} \sum_{\substack{\underline{x} \in \mathcal{O}_{\underline{b}}(L) \\ v(\underline{x}, \underline{b}) \leq L \\ f(\underline{x}) \equiv 0 \pmod{d}}} 1 = \lambda_d + e_d,$$

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

$$\lambda_d = \frac{\#V_0(\mathbb{Z}/d\mathbb{Z})}{\#V(\mathbb{Z}/d\mathbb{Z})}, \quad e_d \ll_{\epsilon} d^{\dim V - 1 + \epsilon} X^{\gamma - 1},$$

where

$$V_0(\mathbb{Z}/d\mathbb{Z}) = \{ \underline{y} \in V(\mathbb{Z}/d\mathbb{Z}) : f(\underline{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 $\underline{x} \in \mathcal{O}_{\underline{b}}(L)$ with $f(\underline{x}) = 0$ can also be omitted without altering (5). Clearly λ_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 $l \notin S_2$ we have

(6)
$$\lambda_l = \frac{t}{l} + O\left(l^{-\frac{3}{2}}\right).$$

Now using (5), (6), 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 $\mathcal{O}_{\underline{b}}$ hold. This completes the proof of Theorem 2.

References

- K. Alladi, An Erdős-Kac theorem for integers without large prime factors, Acta Arith. 49(1987), no. 1, 81–105.
- [2] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of SL₂(F_p), Annals of Mathematics, to appear.
- [3] J. Bourgain, A. Gamburd, P. Sarnak, *Sieving, expanders, and sum-product*, preprint.

XIONG

- [4] A. Cafurea, G Materab, Improved explicit estimates on the number of solutions of equations over a finite field, Finite Fields and Their Applications 12(2006), 155–185
- [5] N.G. Chebotarev, Opredelenie plotnosti sovokupnosti prostykh chisel, prinadlezhashchikh zadannomu klassu podstanovok, Izv. Ross. Akad. Nauk. 17(1923), 205-250.
- [6] P.D.T.A Elliott, "Probabilistic Number Theory, I & II.", Grundlehren Math. Wiss. vol. 239 and 240, Springer, New York, 1979.
- [7] P. Erdős, M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions, Amer. J. Math. 62(1940), 738–742.
- [8] A. granville, K. Soundararajan, Sieving and the Erdős-Kac theorem, Equidistribution in number theory, an introduction, 15–27, NATO Sci. Ser. II Math. Phys. Chem. 237, Springer, Dordrecht, 2007.
- [9] H. Halberstam, On the distribution of additive number theoretic functions, II, J. London Math. Soc. 31(1956), 1–14.
- [10] G.H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, Quar. J. Pure Appl. Math. 48(1917), 76–97.
- [11] H. Hwang, On convergence rates in the central limit theorems for combinatorial structures, European J. Combin. 19(1998), no. 3, 329–343.
- [12] S. Lang, A. Weil, Number of points of varieties in finite fields, Amer. J. Math. 76, 1954, 819–827.
- [13] Y. Liu, Prime divisors of number of rational points on elliptic curves with complex multiplication, Bull. London Math. Soc. 37(2005), 658–664.
- [14] Y. Liu, A generalization of the Erdős-Kac theorem and its applications, Canad. Math. Bull. 47(2004), no. 4, 589–606.
- [15] Y. Liu, Prime analogues of the Erdős-Kac theorem for elliptic curves, J. Number Theory 119(2006), no. 2, 155–170.
- [16] R. Murty, K. Murty, An analogue of the Erdős-Kac theorem for Fourier coefficients of modular forms, Indian J. Pure Appl. Math. 15(1984), no. 10, 1090–1101.
- [17] R. Murty, F. Saidak, Non-abelian generalizations of the Erdős-Kac theorem, Canad. J. Math. 56(2004), no. 2, 356–372.
- [18] E. Noether, Ein algebraisches Kriterium f
 ür absolute Irreduzibilit
 ät, Mathematische Annalen 85(1922), 26–40.
- [19] F. Saidak, New Erdős-Kac type theorems, Arch. Math. (Basel) 85(2005), no. 4, 345–361.
- [20] J. Thuswaldner, R. Tichy, An Erdős-Kac theorem for systems of q-additive functions, Indag. Math. (N.S.) 11(2000), no. 2, 283–291.
- [21] P. Turán, On a theorem of Hardy and Ramanujan, J. London Math. Soc. 9(1934), 274–276.

MAOSHENG XIONG: DEPARTMENT OF MATHEMATICS, EBERLY COLLEGE OF SCIENCE, PENNSYLVANIA STATE UNIVERSITY, MCALLISTER BUILDING, UNIVER-SITY PARK, PA 16802 USA

E-mail address: xiong@math.psu.edu

10