sciendo

uniform distribution theory

DOI: 10.2478/udt-2020–0005
Unif. Distrib. Theory **15** (2020), no.1, 93–104

NOTES ON THE DISTRIBUTION OF ROOTS MODULO A PRIME OF A POLYNOMIAL III

Yoshiyuki Kitaoka

Author is retired, Asahi, JAPAN

ABSTRACT. Let $f(x)$ be a monic polynomial with integer coefficients and integers $r_1, \dots, r_n$ with $0 \le r_1 \le \cdots \le r_n < p$ the n roots of $f(x) \equiv 0 \bmod p$ for a prime p. We proposed conjectures on the distribution of the point $(r_1/p, \dots, r_n/p)$ in the previous papers. One aim of this paper is to revise them for a reducible polynomial $f(x)$, and the other is to show that they imply the one-dimensional equidistribution of $r_1/p, \dots, r_n/p$ for an irreducible polynomial $f(x)$ by a geometric way.

Communicated by Shigeki Akiyama

Throughout this paper, a polynomial means a monic one over the ring $\mathbb{Z}$ of integers and the letter p denotes a prime number. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

be a polynomial of degree n with complex roots $\alpha_1, \dots, \alpha_n$. We fix the numbering of roots once and for all, and define a vector space LR over the rational number field $\mathbb{Q}$ by

$$LR := \left\{ (l_1, \dots, l_{n+1}) \in \mathbb{Q}^{n+1} \,\middle|\, \sum_{i=1}^{n} l_i\alpha_i = l_{n+1} \right\},$$

which depends on the numbering of roots α_i. The projection defined by

$$(l_1, \dots, l_n, l_{n+1}) \mapsto (l_1, \dots, l_n)$$

from LR to

$$LR_0 := \left\{ (l_1, \dots, l_n) \in \mathbb{Q}^n \,\middle|\, \sum_{i=1}^{n} l_i\alpha_i \in \mathbb{Q} \right\}$$

2010 Mathematics Subject Classification: 11K.
Keywords: Equidistribution, polynomial, roots modulo a prime.

is an isomorphism, more strongly from $LR\cap\mathbb{Z}^{n+1}$ on $LR_0\cap\mathbb{Z}^n$, since numbers α_i are algebraic integers. Since there is a trivial linear relation $\sum\alpha_i = -a_{n-1}$, the non-zero vector $(1,\dots,1,-a_{n-1})$ is always in LR, hence $t := \dim_{\mathbb{Q}} LR = \dim_{\mathbb{Q}} LR_0 \geq 1$ is clear. The inequality $t \leq n$ is also clear and the condition $t = n$ holds if and only if $f(x)$ is a product of linear forms in $\mathbb{Q}[x]$. The vector $(1,\dots,1)$ is always in LR_0, and a polynomial $f(x)$ has a rational root if and only if a vector of the form $(0,\dots,0,1,0,\dots,0)$ is in LR_0, and $\alpha_i-\alpha_j\in\mathbb{Q}$ holds for distinct i,j if and only if a vector of the form $(0,\dots,0,1,0,\dots,0,-1,0,\dots,0)$ is in LR_0.

We say that a polynomial $f(x)$ has a non-trivial linear relation among roots if $t>1$.

We take a $\mathbb{Z}$-basis

$$\hat{\boldsymbol{m}}_j := (m_{j,1},\dots,m_{j,n},m_j)\ (j=1,\dots,t)$$

of $LR\cap\mathbb{Z}^{n+1}$, and put

$$\boldsymbol{m}_j := (m_{j,1},\dots,m_{j,n})\ (j=1,\dots,t).$$

By definition, the vector $\hat{\boldsymbol{m}}_j$ satisfies

$$\sum_{i=1}^{n} m_{j,i}\alpha_i = m_j\ (j=1,\dots,t)$$

and the vectors $\boldsymbol{m}_1,\dots,\boldsymbol{m}_t$ are a basis of $LR_0\cap\mathbb{Z}^n$. We fix the basis $\hat{\boldsymbol{m}}_j$ $(j=1,\dots,t)$ together with roots α_i once and for all.

We introduce two permutation groups associated with them:

$$\hat{\boldsymbol{G}} := \{\nu\in S_n \mid \langle\nu(\hat{\boldsymbol{m}}_1),\dots,\nu(\hat{\boldsymbol{m}}_t)\rangle_{\mathbb{Z}} = \langle\hat{\boldsymbol{m}}_1,\dots,\hat{\boldsymbol{m}}_t\rangle_{\mathbb{Z}}\},$$

$$\boldsymbol{G} := \{\nu\in S_n \mid \langle\nu(\boldsymbol{m}_1),\dots,\nu(\boldsymbol{m}_t)\rangle_{\mathbb{Z}} = \langle\boldsymbol{m}_1,\dots,\boldsymbol{m}_t\rangle_{\mathbb{Z}}\}.$$

Here,

$$\langle\boldsymbol{z}_1,\dots,\boldsymbol{z}_k\rangle_{\mathbb{Z}} := \{a_1\boldsymbol{z}_1+\cdots+a_k\boldsymbol{z}_k \mid a_1,\dots,a_k\in\mathbb{Z}\}$$

and we let, for $\boldsymbol{x}=(x_1,\dots,x_n)\in\mathbb{R}^n$, $x\in\mathbb{R}$ and a permutation $\nu\in S_n$

$$\nu(\boldsymbol{x}) := \big(x_{\nu^{-1}(1)},\dots,x_{\nu^{-1}(n)}\big),\ \nu\big((\boldsymbol{x},x)\big) := \big(\nu(\boldsymbol{x}),x\big).$$

Note that

$$\hat{\boldsymbol{G}} = \{\nu\in S_n \mid \nu(LR)=LR\},\ \boldsymbol{G} = \{\nu\in S_n \mid \nu(LR_0)=LR_0\},$$

hence, groups $\hat{\boldsymbol{G}},\boldsymbol{G}$ are independent of the choice of bases $\hat{\boldsymbol{m}}_i$ and $\hat{\boldsymbol{G}}$ is a subgroup of $\boldsymbol{G}$. If $f(x)$ is irreducible, then they are identical. However, they are not necessarily equal for a reducible polynomial.

We may take the vector $(1,\dots,1,-a_{n-1})$ as $\hat{\boldsymbol{m}}_1$, and if $f(x)$ has no non-trivial linear relation among roots, then it is a basis of $LR\cap\mathbb{Z}^{n+1}$, hence $\hat{\boldsymbol{G}}=\boldsymbol{G}=S_n$.

Next, we put

$$\mathrm{Spl}_X(f) := \{p \le X \mid f(x) \text{ is fully splitting modulo } p\}$$

for a positive number X and $\mathrm{Spl}(f) := \mathrm{Spl}_\infty(f)$.

We require the following conditions on the local roots $r_1, \dots, r_n\,(\in \mathbb{Z})$ of $f(x) \equiv 0 \bmod p$ for a prime $p \in \mathrm{Spl}(f)$:

$$f(x) \equiv \prod_{i=1}^{n}(x - r_i) \bmod p, \tag{1}$$

$$0 \le r_1 \le r_2 \le \cdots \le r_n < p. \tag{2}$$

The condition (1) is nothing but the definition of $p \in \mathrm{Spl}(f)$, and (2) determines local roots r_i uniquely. From now on, local roots r_i are supposed to satisfy two conditions (1) and (2). The global ordering (2) to local roots is a key.

We know that for a sufficiently large prime $p \in \mathrm{Spl}(f)$, there is at least one permutation $\sigma \in S_n$ dependent on p such that

$$\sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} \equiv m_j \bmod p \quad \left(1 \le {}^{\forall} j \le t\right). \tag{3}$$

To state conjectures, we introduce the following notation corresponding to the condition (3)

$$\mathrm{Spl}_X(f, \sigma) := \{p \in \mathrm{Spl}_X(f) \mid (3)\},$$

which is independent of the choice of the basis $\hat{\boldsymbol{m}}_i$, and we define the density by

$$Pr(f, \sigma) := \lim_{X \to \infty} \frac{\#\,\mathrm{Spl}_X(f, \sigma)}{\#\,\mathrm{Spl}_X(f)}.$$

We suppose that the limit exists. The existence of the limit is supported by computer experiment.

Next, we introduce geometric objects

$$\hat{\mathfrak{D}}_n := \left\{ (x_1 \dots, x_n) \in [0,1]^n \,\middle|\, 0 \le x_1 \le \cdots \le x_n \le 1, \sum_{i=1}^{n} x_i \in \mathbb{Z} \right\},$$

$$\mathfrak{D}(f, \sigma) := \left\{ (x_1 \dots, x_n) \in [0,1]^n \,\middle|\, \begin{array}{l} 0 \le x_1 \le \cdots \le x_n \le 1, \\ \sum\limits_{i=1}^{n} m_{j,i}\, x_{\sigma(i)} \in \mathbb{Z} \ \left(1 \le {}^{\forall} j \le t\right) \end{array} \right\}$$

$$= \left\{ \boldsymbol{x} \in \hat{\mathfrak{D}}_n \mid \left(\sigma(\boldsymbol{l}), \boldsymbol{x}\right) \in \mathbb{Z} \ \left({}^{\forall}\boldsymbol{l} \in LR_0 \cap \mathbb{Z}^n\right) \right\}.$$

The dimension of $\hat{\mathfrak{D}}_n$ is $n-1$ and that of $\mathfrak{D}(f,\sigma)$ is less than or equal to $n-t$. In the following, the volume $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)$ means that as an $(n-t)$-dimensional set, that is for a set S in $\boldsymbol{v}+\mathbb{R}[\boldsymbol{v}_1,\dots,\boldsymbol{v}_{n-t}](\subset\mathbb{R}^n)$ with orthonormal elements $\boldsymbol{v}_1,\dots,\boldsymbol{v}_{n-t}\in\mathbb{R}^n$, we identify $\boldsymbol{v}+\sum y_i\boldsymbol{v}_i\in S$ with a point $(y_1,\dots,y_{n-t})\in\mathbb{R}^{n-t}$. So, $\mathrm{vol}(\mathfrak{D}(f,\sigma))=0$ holds if $\dim\mathfrak{D}(f,\sigma)<n-t$.

In case that $f(x)$ is a product of linear forms, which is equivalent to $t=n$, $\dim\mathfrak{D}(f,\sigma)=0$ holds, hence the discussion about $\mathfrak{D}(f,\sigma)$ is almost meaningless.

If there is no non-trivial linear relation among roots, then $\mathfrak{D}(f,\sigma)$ is equal to $\hat{\mathfrak{D}}_n$ for every permutation σ.

The first conjecture is

Conjecture 1. *For a permutation σ with $Pr(f,\sigma)>0$, the ratio*

$$c=\frac{\mathrm{vol}(\mathfrak{D}(f,\sigma))}{Pr(f,\sigma)} \tag{4}$$

is independent of σ. If $\boldsymbol{G}=\hat{\boldsymbol{G}}$ holds, then two conditions $Pr(f,\sigma)>0$ and $\mathrm{vol}(\mathfrak{D}(f,\sigma))>0$ are equivalent.

If (i) $f(x)$ is not a product of linear forms, (ii) $\alpha_i-\alpha_j\notin\mathbb{Q}$ for any distinct i,j, that is, $f(x)\neq F(x)g(x)g(x+a)$ for any $F(x),g(x)\in\mathbb{Q}[x],a\in\mathbb{Q}$ and (iii) $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)=cPr(f,\sigma)$ holds for every $\sigma\in S_n$, then

$$c=\sqrt{\det((\boldsymbol{m}_i,\boldsymbol{m}_j))}/\#\hat{\boldsymbol{G}}$$

is known (cf. [K4]), although it is not necessary here.

There is an example of a reducible polynomial $f(x)$ such that $Pr(f,\sigma)=0$ but $\mathrm{vol}(\mathfrak{D}(f,\sigma))>0$ for some permutation σ as follows, and Expectation $1''$ in [K1], [K3] should be revised as above, not to exclude a reducible polynomial.

Example. Let us consider the polynomial $f(x)=(x^2-2)((x-1)^2-2)$ with roots $\alpha_1=\sqrt{2},\alpha_2=1+\sqrt{2},\alpha_3=-\sqrt{2},\alpha_4=1-\sqrt{2}$. Then $t=3$ and the matrix $(m_{j,i})$ and m_i are

$$\begin{pmatrix}1&0&0&1\\1&-1&0&0\\1&0&1&0\end{pmatrix},\quad\begin{pmatrix}1\\-1\\0\end{pmatrix},$$

and

$$\boldsymbol{G}=\{[1,2,3,4],[1,2,4,3],[2,1,3,4],[2,1,4,3],$$
$$[3,4,1,2],[3,4,2,1],[4,3,1,2],[4,3,2,1]\}$$

and

$$\hat{\boldsymbol{G}}=\{[1,2,3,4],[3,4,1,2]\},$$

where a permutation σ is identified with the vector $[\sigma(1),\dots,\sigma(4)]$ of images.

Then we see that

$$\mathfrak{D}(f,\sigma)=\begin{cases}\{(x,x,1-x,1-x)\mid 0\le x\le 1/2\} & \text{if } \sigma\in \boldsymbol{G},\\ \{(1/2,1/2,1/2,1/2)\} & \text{otherwise.}\end{cases}$$

Two conditions $\dim \mathfrak{D}(f,\sigma)=1\,(=n-t)$ and $\sigma\in G$ are equivalent. We find

$$Pr(f,\sigma)=\begin{cases}1 & \text{if } \sigma\in \hat{\boldsymbol{G}},\\ 0 & \text{otherwise,}\end{cases}$$

since $p\in \mathrm{Spl}(f,\sigma)$ means

$$r_{\sigma(1)}+r_{\sigma(4)}=p+1, r_{\sigma(1)}-r_{\sigma(2)}=-1, r_{\sigma(1)}+r_{\sigma(3)}=p$$

for a sufficiently large p, which implies $\sigma\in\hat{\boldsymbol{G}}$. This is an example such that $Pr(f,\sigma)=0$ but $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)>0$ for $\sigma\in \boldsymbol{G}\setminus\hat{\boldsymbol{G}}$ by $\#\boldsymbol{G}=8, \#\hat{\boldsymbol{G}}=2$, and this supports Conjecture 1.

The revision with respect to Expectation 1′ in [K4] for a reducible polynomial $f(x)$ is

Conjecture 2. *Suppose that* $Pr(f,\sigma)>0, \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)>0$ *for a permutation* σ*; then for a set* $D=\overline{D^\circ}\subset[0,1)^n$*, we have*

$$\begin{aligned}Pr_D(f,\sigma)&:=\lim_{X\to\infty}\frac{\#\{p\in \mathrm{Spl}_X(f,\sigma)\mid (r_1/p,\dots,r_n/p)\in D\}}{\#\mathrm{Spl}_X(f,\sigma)}\\ &=\frac{\mathrm{vol}(D\cap\mathfrak{D}(f,\sigma))}{\mathrm{vol}(\mathfrak{D}(f,\sigma))}.\end{aligned}$$

The suppositions $Pr(f,\sigma)>0, \mathrm{vol}(\mathfrak{D}(f,\sigma))>0$ are added.

Next, we discuss the one-dimensional equidistribution of r_i/p $\big(1\le i\le n, p\in \mathrm{Spl}(f)\big)$ for local roots r_i, that is, whether for $0\le a<1$,

$$\lim_{X\to\infty}\frac{\sum_{p\in\mathrm{Spl}_X(f)}\#\{i\mid r_i/p\le a, 1\le i\le n\}}{n\cdot\#\,\mathrm{Spl}_X(f)}=a$$

is true or not. We note that if $f(x)$ has a rational integral root r_0, then $r=r_0$ or $r=p+r_0$ is a local root according to $r_0\ge 0$ or $r_0<0$ for a large prime $p\in\mathrm{Spl}(f)$, hence r/p tends to 0 or 1, that is the one-dimensional equidistribution is false. So, we exclude a polynomial with a rational integral root. We showed that Conjectures above imply the one-dimensional equidistribution of roots r_i/p for a polynomial which has no non-trivial linear relation among roots by calculation (cf. [K2]). Here we show for a more general polynomial, e.g., an irreducible polynomial of degree larger than 1, that Conjectures 1, 2 imply the one-dimensional equidistribution of roots r_i/p not based on hard calculation.

Putting

$$D_{i,a} := \{(x_1, \dots, x_n) \in [0,1)^n \mid x_i \le a\},$$

it is easy to see

$$\begin{aligned}
&\sum_{p \in \mathrm{Spl}_X(f)} \#\{i \mid r_i/p \le a, 1 \le i \le n\} \\
&= \sum_{p \in \mathrm{Spl}_X(f)} \#\{i \mid (r_1/p, \dots, r_n/p) \in D_{i,a}\} \\
&= \sum_{i=1}^{n} \#\{p \in \mathrm{Spl}_X(f) \mid (r_1/p, \dots, r_n/p) \in D_{i,a}\} \\
&= \sum_{i=1}^{n} \sum_{\sigma \in S_n} \#\{p \in \mathrm{Spl}_X(f,\sigma) \mid (r_1/p, \dots, r_n/p) \in D_{i,a}\}/\#\hat{\boldsymbol{G}} + O(1),
\end{aligned}$$

since we know by Proposition 2 in [K3] that if a prime $p \in \mathrm{Spl}(f)$ is sufficiently large, then there are exactly $\#\hat{\boldsymbol{G}}$ permutations σ satisfying $p \in \mathrm{Spl}(f,\sigma)$. Therefore we have

$$\begin{aligned}
&\lim_{X\to\infty} \frac{\sum_{p \in \mathrm{Spl}_X(f)} \#\{i \mid r_i/p \le a, 1 \le i \le n\}}{n\#\,\mathrm{Spl}_X(f)} \\
&= \lim_{X\to\infty} \sum_{i=1}^{n} \frac{\sum_{\sigma \in S_n} \#\{p \in \mathrm{Spl}_X(f,\sigma) \mid (r_1/p, \dots, r_n/p) \in D_{i,a}\}}{n \cdot \#\hat{\boldsymbol{G}} \cdot \#\,\mathrm{Spl}_X(f)} \\
&= \lim_{X\to\infty} \sum_{i=1}^{n} \frac{\sum_{\sigma \in S'_n} \#\{p \in \mathrm{Spl}_X(f,\sigma) \mid (r_1/p, \dots, r_n/p) \in D_{i,a}\}}{\#\,\mathrm{Spl}_X(f,\sigma)} \\
&\quad \times \frac{\#\,\mathrm{Spl}_X(f,\sigma)}{n \cdot \#\hat{\boldsymbol{G}} \cdot \#\,\mathrm{Spl}_X(f)}
\end{aligned}$$

where S'_n is a subset of S_n consisting of permutations satisfying $Pr(f,\sigma) > 0$

$$\begin{aligned}
&= \frac{1}{n\#\hat{\boldsymbol{G}}} \sum_{i=1}^{n} \sum_{\sigma \in S'_n} Pr_{D_{i,a}}(f,\sigma) Pr(f,\sigma) \\
&= \frac{1}{nc\#\hat{\boldsymbol{G}}} \sum_{i=1}^{n} \sum_{\sigma \in S'_n} Pr_{D_{i,a}}(f,\sigma) \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big) \quad \text{(by Conjecture 1)} \\
&= \frac{1}{nc\#\hat{\boldsymbol{G}}} \sum_{i=1}^{n} \sum_{\sigma \in S'_n} \mathrm{vol}\big(D_{i,a} \cap \mathfrak{D}(f,\sigma)\big) \qquad \text{(by Conjecture 2).}
\end{aligned}$$

We note that the dimension of the set

$$D_{i,0} \cap \mathfrak{D}(f,\sigma) = \left\{ (x_1,\dots,x_n) \middle| 0 \le x_1 \le \cdots \le x_n < 1, x_i = 0, \sum_{k=1}^{n} m_{j,k} x_{\sigma(k)} \in \mathbb{Z}\ (^\forall j) \right\}$$

is less than $n-t$, since the condition $x_i = 0$ is independent of conditions $\sum_{k=1}^{n} m_{j,k} x_{\sigma(k)} \in \mathbb{Z}\ (^\forall j)$ by the assumption that $f(x)$ has no rational root. Therefore the above is equal to 0 at $a=0$, and to 1 at $a=1$ by

$$c = \frac{\sum_{Pr(f,\sigma)>0} \mathrm{vol}(\mathfrak{D}(f,\sigma))}{\sum Pr(f,\sigma)} = \sum_{Pr(f,\sigma)>0} \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)/\#\hat{\boldsymbol{G}},$$

using Corollary 2 in [K3]. Hence, once we have shown that it is a linear form in a, it is equal to a on $[0,1)$, that is the distribution of r_i/p is uniform. The difference between the above sum restricted on S'_n and the full sum

$$\sum_{i=1}^{n} \sum_{\sigma \in S_n} \mathrm{vol}\big(D_{i,a} \cap \mathfrak{D}(f,\sigma)\big) \tag{5}$$

is

$$\sum_{i=1}^{n} \sum_{Pr(f,\sigma)=0,\ \mathrm{vol}(\mathfrak{D}(f,\sigma))>0} \mathrm{vol}\big(D_{i,a} \cap \mathfrak{D}(f,\sigma)\big). \tag{6}$$

From now on, the aim is to show that (5) is a linear form in a. Under the assumption that the conditions $Pr(f,\sigma)>0$ and $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)>0$ are equivalent, it means that (6) vanishes and the distribution of r_i/p is uniform.

We assume still that a polynomial $f(x)$ has no rational roots, and put

$$\begin{aligned}
\mathbb{Q}(f) &:= \mathbb{Q}(\alpha_1,\dots,\alpha_n),\\
\beta_i &:= \alpha_i - tr_{\mathbb{Q}(f)/\mathbb{Q}}(\alpha_i)/[\mathbb{Q}(f):\mathbb{Q}] \quad (\neq 0),\\
LR_0 &:= \left\{ (l_1,\dots,l_n) \in \mathbb{Q}^n \middle| \sum_{i=1}^{n} l_i\alpha_i \in \mathbb{Q} \right\}\\
&= \left\{ (l_1,\dots,l_n) \in \mathbb{Q}^n \middle| \sum_{i=1}^{n} l_i\beta_i = 0 \right\},\\
\mathfrak{D}_f &:= \big\{ \boldsymbol{x} \in \mathbb{R}^n \big| (\boldsymbol{l},\boldsymbol{x}) \in \mathbb{Z} \quad for\ ^\forall \boldsymbol{l} \in LR_0 \cap \mathbb{Z}^n \big\}.
\end{aligned}$$

Lemma 0.1. *Suppose that $\alpha_i - \alpha_j \notin \mathbb{Q}$ for any distinct i, j. We have*

$$\sum_{i=1}^{n} \sum_{\sigma \in S_n} \mathrm{vol}\big(D_{i,a} \cap \mathfrak{D}(f,\sigma)\big) = \sum_{i=1}^{n} \mathrm{vol}\big(\{\boldsymbol{x} \in [0,1)^n \mid x_i \le a\} \cap \mathfrak{D}_f\big),$$

in particular,

$$\sum_{\sigma \in S_n} \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big) = \mathrm{vol}\big([0,1)^n \cap \mathfrak{D}_f\big).$$

P r o o f. The equations

$$\begin{aligned} &D_{i,a} \cap \mathfrak{D}(f,\sigma) \\ &= \big\{\boldsymbol{x} \in [0,1)^n \mid x_1 \le \cdots \le x_n, x_i \le a, \big(\boldsymbol{l}, \sigma^{-1}(\boldsymbol{x})\big) \in \mathbb{Z} \quad \text{for } {}^{\forall}\boldsymbol{l} \in LR_0 \cap \mathbb{Z}^n\big\} \\ &= \{\boldsymbol{x} \in [0,1)^n \mid x_1 \le \cdots \le x_n, x_i \le a, \sigma^{-1}(\boldsymbol{x}) \in \mathfrak{D}_f\} \\ &= \sigma\big(\{\boldsymbol{y} \in [0,1)^n \mid y_{\sigma^{-1}(1)} \le \cdots \le y_{\sigma^{-1}(n)}, y_{\sigma^{-1}(i)} \le a\} \cap \mathfrak{D}_f\big) \end{aligned}$$

imply

$$\begin{aligned} &\mathrm{vol}\big(D_{i,a} \cap \mathfrak{D}(f,\sigma)\big) \\ &= \mathrm{vol}\big(\{\boldsymbol{y} \in \mathbb{R}^n \mid 0 < y_{\sigma^{-1}(1)} < \cdots < y_{\sigma^{-1}(n)} < 1, y_{\sigma^{-1}(i)} \le a\} \cap \mathfrak{D}_f\big). \end{aligned}$$

Here, we note that by the assumption, LR_0 contains no vector of the form $(0,\ldots,0,1,0,\ldots,-1,0,\ldots,0)$ and $\mathfrak{D}_f$ is defined by t linearly independent vectors $\boldsymbol{m}_j$ and the volume vol is $(n-t)$-dimensional one, hence it is not necessary to care an additional equation $x_i = x_j$ for $i \ne j$. Let us define a mapping ϕ from

$$X(i) := \{(\boldsymbol{x}, i) \mid \boldsymbol{x} \in (0,1)^n, 1 \le i \le n, x_i \le a, x_j \ne x_l \quad \text{if } j \ne l\}$$

to the union of

$$Y(\sigma,k) := \{(\boldsymbol{y}, \sigma, k) \mid \boldsymbol{y} \in (0,1)^n, 0 < y_{\sigma(1)} < \cdots < y_{\sigma(n)} < 1, y_{\sigma(k)} \le a\}$$

by $\phi((\boldsymbol{x}, i)) = (\boldsymbol{x}, \sigma, k)$, where σ, k are defined by

$$x_{\sigma(1)} < \cdots < x_{\sigma(n)},\ k = \sigma^{-1}(i),$$

hence

$$\phi\big(X(i)\big) = \cup_{\sigma,k:\sigma(k)=i} Y(\sigma,k) \quad \text{for } i = 1,\ldots,n.$$

The mapping is clearly bijective for any fixed i, and if $(\boldsymbol{y},\sigma,k) \in Y(\sigma,k)$ and $(\boldsymbol{y},\sigma',k') \in Y(\sigma',k')$ occur with $\sigma(k) = \sigma'(k')$, then $\sigma = \sigma', k = k'$ hold. Hence, defining pr by $pr(\boldsymbol{y},\sigma,k) = \boldsymbol{y}$, we have

$$pr\big(Y(\sigma,k)\big) \cap pr\big(Y(\sigma',k')\big) = \emptyset$$

if $\sigma(k) = \sigma'(k')$ and either $\sigma \ne \sigma'$ or $k \ne k'$, and so

$$
\begin{aligned}
&\sum_{i=1}^{n}\sum_{\sigma}\mathrm{vol}\big(D_{i,a}\cap\mathfrak{D}(f,\sigma)\big)\\
&=\sum_{i=1}^{n}\sum_{\sigma}\mathrm{vol}\Big(pr\big(Y(\sigma^{-1},i)\big)\cap\mathfrak{D}_f\Big)\\
&=\sum_{k=1}^{n}\sum_{\sigma}\mathrm{vol}\Big(pr\big(Y(\sigma,k)\big)\cap\mathfrak{D}_f\Big)\\
&=\sum_{i}\sum_{k,\sigma:\sigma(k)=i}\mathrm{vol}\Big(pr\big(Y(\sigma,k)\big)\cap\mathfrak{D}_f\Big)\\
&=\sum_{i}\mathrm{vol}\Big(\cup_{k,\sigma:\sigma(k)=i}pr\big(Y(\sigma,k)\big)\cap\mathfrak{D}_f\Big)\\
&=\sum_{i}\mathrm{vol}\Big(pr\big(\cup_{k,\sigma:\sigma(k)=i}Y(\sigma,k)\big)\cap\mathfrak{D}_f\Big)\\
&=\sum_{i}\mathrm{vol}\Big(pr\big(X(i)\big)\cap\mathfrak{D}_f\Big)\\
&=\sum_{i}\mathrm{vol}\big(\{\boldsymbol{x}\in[0,1)^n\mid x_i\le a\}\cap\mathfrak{D}_f\big).
\end{aligned}
$$

□

Hence to show the equidistribution, we have only to see that each factor $\mathrm{vol}\big(\{\boldsymbol{x}\in[0,1)^n\mid x_i\le a\}\cap\mathfrak{D}_f\big)$ is a linear form in a.

Lemma 0.2. *Suppose that $\beta_1,\dots,\beta_r$ are linearly independent over $\mathbb{Q}$ and*

$$(\beta_{r+1},\dots,\beta_n)=(\beta_1,\dots,\beta_r)\,T\quad \textit{for } {}^{\exists}T\in M_{r,n-r}(\mathbb{Q}).$$

Then we have $r=n-t$,

$$LR_0=\left\{(l_1,\dots,l_n)\in\mathbb{Q}^n\,\middle|\,\begin{pmatrix}l_1\\ \vdots\\ l_r\end{pmatrix}=-T\begin{pmatrix}l_{r+1}\\ \vdots\\ l_n\end{pmatrix}\right\}$$

and

$$\begin{pmatrix}\boldsymbol{m}_1\\ \vdots\\ \boldsymbol{m}_t\end{pmatrix}=(S^tT,-S)\quad \textit{for } {}^{\exists}S\in GL_{n-r}(\mathbb{Q})\cap M_{n-r}(\mathbb{Z}).$$

P r o o f. By

$$\sum_{i=1}^{n} x_i\beta_i = (\beta_1,\dots,\beta_r)\left\{\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} + T\begin{pmatrix} x_{r+1} \\ \vdots \\ x_n \end{pmatrix}\right\} \quad (x_i \in \mathbb{R}),$$

we see

$$LR_0 = \left\{(l_1,\dots,l_n) \in \mathbb{Q}^n \middle| \sum_{i=1}^{n} l_i\beta_i = 0\right\}$$

$$= \left\{(l_1,\dots,l_n) \in \mathbb{Q}^n \middle| \begin{pmatrix} l_1 \\ \vdots \\ l_r \end{pmatrix} = -T\begin{pmatrix} l_{r+1} \\ \vdots \\ l_n \end{pmatrix}\right\},$$

which implies $t = \dim LR_0 = n - r$. On the other hand, the definition of T implies

$$({}^tT, -1_{n-r})\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = 0^{(n-r,1)},$$

hence row vectors of the matrix $({}^tT, -1_{n-r})$ spann LR_0 by $\mathrm{rank}({}^tT, -1_{n-r}) = \dim LR_0$ and so there is a matrix $S \in GL_{n-r}(\mathbb{Q})$ such that

$$\begin{pmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_t \end{pmatrix} = S({}^tT, -1_{n-r}) = (S{}^tT, -S),$$

which implies that S is integral. □

Lemma 0.3. *Supposing the assumption on β_i in Lemma 0.2, we have*

$$\mathfrak{D}_f = \left\{\boldsymbol{x} \in \mathbb{R}^n \mid (S{}^tT, -S)^t\boldsymbol{x} \in M_{t,1}(\mathbb{Z})\right\}$$

$$= \left\{\boldsymbol{x} \in \mathbb{R}^n \mid (x_{r+1},\dots,x_n) = (x_1,\dots,x_r)T + \boldsymbol{k}^tS^{-1}\left({}^{\exists}\boldsymbol{k} \in M_{1,t}(\mathbb{Z})\right)\right\}.$$

For $(x_1,\dots,x_r) \in [0,1)^r$, there are exactly $|\det(S)|$ vectors $(x_{r+1},\dots,x_n) \in [0,1)^{n-r}$ such that $(x_1,\dots,x_n) \in \mathfrak{D}_f$.

P r o o f. We see that

$$\mathfrak{D}_f = \left\{ \boldsymbol{x} \in \mathbb{R}^n \middle| \begin{pmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_t \end{pmatrix} {}^t\boldsymbol{x} \in M_{t,1}(\mathbb{Z}) \right\} = \left\{ \boldsymbol{x} \in \mathbb{R}^n \mid (S\,{}^tT, -S)^t\boldsymbol{x} \in M_{t,1}(\mathbb{Z}) \right\}$$

$$= \left\{ \boldsymbol{x} \in \mathbb{R}^n \mid ((x_{r+1}, \dots, x_n) - (x_1, \dots, x_r)T)^t S \in M_{1,t}(\mathbb{Z}) \right\}$$

$$= \left\{ \boldsymbol{x} \in \mathbb{R}^n \mid (x_{r+1}, \dots, x_n) = (x_1, \dots, x_r)T + \boldsymbol{k}^t S^{-1}\ ({}^\exists\boldsymbol{k} \in M_{1,t}(\mathbb{Z})) \right\}.$$

Since $S \in GL_{n-r}(\mathbb{Q})$ is an integral regular matrix, the inclusion $\mathbb{Z}^{n-r}\,{}^tS^{-1} \supset \mathbb{Z}^{n-r}$ is clear. Hence, for $(x_1, \dots, x_r) \in \mathbb{R}^r$, there is a vector $(x_{r+1}, \dots, x_n) := (x_1, \dots, x_r)T + \boldsymbol{k}^t S^{-1} \in [0,1)^{n-r}$ for some integral vector $\boldsymbol{k}$. The number of such integral vectors is $|\det(S)|$ since S is integral. □

Thus we see that, assuming that $\beta_1, \dots, \beta_r$ is linearly independent over $\mathbb{Q}$ and $1 \le i \le r$ as above

$$\{\boldsymbol{x} \in [0,1)^n \mid x_i \le a\} \cap \mathfrak{D}_f =$$

$$\left\{ \boldsymbol{x} \in [0,1)^n \,|\, x_i \le a, (x_{r+1}, \dots, x_n) = (x_1, \dots, x_r)T + \boldsymbol{k}^t S^{-1}\ \left({}^\exists\boldsymbol{k} \in M_{1,t}(\mathbb{Z})\right) \right\},$$

which is included in the union of sets parallel to the subspace

$$\{\boldsymbol{x} \in \mathbb{R}^n \mid (x_{r+1}, \dots, x_n) = (x_1, \dots, x_r)T\},$$

and the projection to $E_{i,a} := \{\boldsymbol{x} \in [0,1)^r \mid x_i \le a\}$ is exactly $|\det(S)|$-fold independently on $\boldsymbol{x}$ by the lemma above. Hence the volume of $\{\boldsymbol{x} \in [0,1)^n \mid x_i \le a\} \cap \mathfrak{D}_f$ as an $r\,(= n-t)$-dimensional set is proportional to $a = \mathrm{vol}(E_{i,a})$. In general, for given i, we have only to take a subset $j_1, \dots, j_r$ such that $\beta_{j_1}, \dots, \beta_{j_r}$ are linearly independent over $\mathbb{Q}$ and $j_k = i$ for some k. Thus, we have proved that

Theorem 0.1. *If a polynomial $f(x)$ has no rational root, $\alpha_i - \alpha_j \notin \mathbb{Q}$ for any distinct i, j, and the conditions $Pr(f, \sigma) > 0$ and $\mathrm{vol}\big(\mathfrak{D}(f, \sigma)\big) > 0$ are equivalent, then Conjectures 1, 2 imply the equidistribution of r_i/p for local roots r_i of the polynomial.*

So, the equidistribution of r_i/p for local roots r_i is likely for an irreducible polynomial $f(x)$ of $\deg f > 1$. Although the polynomial

$$f(x) = (x^2 - 2)\big((x-1)^2 - 2\big)$$

does not satisfy the assumption of the theorem, the equidistribution of local roots r_i/p is true by [DFI], [T].

Put, for an algebraic number field F containing $\mathbb{Q}(f)$

$$\mathrm{Spl}(f, F) := \{p \in \mathrm{Spl}(f) \mid p \text{ is fully splitting at } F\}.$$

If a subsequence of r_i/p for local roots r_i of f restricted on $p \in \mathrm{Spl}(f, F)$ distributes uniformly for every irreducible polynomial f of $\deg f > 1$ and every number field F, then the one-dimensional distribution of r_i/p for any reducible polynomial without rational root is true.

Remark. Foo proves in [F] that the set $\{r_i/p \mid 1 \leq i \leq n, p \in \mathrm{Spl}(f)\}$ is dense in the interval $(0, 1)$ for an irreducible polynomial $f(x)$ of degree > 1 under the Bouniakowsky conjecture.

REFERENCES

[DFI] DUKE, W.—FRIEDLANDER, J. B.—IWANIEC, H.: *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. Math. **141** (1995), 423–441.

[F] FOO, T.: *The Bouniakowsky conjecture and the density of polynomial roots to prime moduli*, Acta Arith. **144** (2010), 1–4.

[K1] KITAOKA, Y.: *Notes on the distribution of roots modulo a prime of a polynomial*, Unif. Distrib. Theory **12** (2017), no. 2, 91–116.

[K2] KITAOKA, Y.: *Statistical distribution of roots of a polynomial modulo primes III*, International Journal of Statistics and Probability **7** (2017), 115–124.

[K3] KITAOKA, Y.: *Notes on the distribution of roots modulo a prime of a polynomial II*, Unif. Distrib. Theory **14** (2019), no. 1, 87–104.

[K4] KITAOKA, Y.: *Conjectures on the distribution of roots modulo a prime of a polynomial*, arXiv : 1905.02364v7

[T] TÓTH, Á.: *Roots of quadratic congruences*, Internat. Math. Res. Notices, (2000), 719–739.

Received February 14, 2020
Accepted April 21, 2020

Yoshiyuki Kitaoka
(Author is retired)
Asahi
JAPAN
E-mail: kitaoka@meijo-u.ac.jp