mathematics

MDPI

Article

Notes on the Distribution of Roots Modulo a Prime of a Polynomial VI: Case of Polynomials with Local Roots

Yoshiyuki Kitaoka

Independent Researcher, Nagoya 4680073, Japan; y_kitaoka@tg.commufa.jp

Abstract

Let $f(x)$ be a monic integral polynomial of degree n and p a prime number for which $f(x)$ is the fully decomposable modulo p. Let integers $r_1, \dots, r_n$ be the roots of $f(x) \bmod p$ with $0 \le r_1 \le \cdots \le r_n < p$. In this series of papers, we have investigated the distribution of the points $(r_1, \dots, r_n)$. In the present paper, we present several conjectures concerning the distribution of polynomials in the roots r_i.

Keywords: polynomial; local root of a polynomial; uniform distribution

MSC: 11C08; 11N69

1. Introduction and Conjectures

For a monic polynomial $f(x) \in \mathbb{Z}[x]$, we proposed several conjectures about the distribution of the roots of $f(x) \equiv 0 \bmod p$ for a prime number p [1–6].We begin by briefly stating the relevant notation to state new observations. Let a polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad (a_0, \cdots, a_{n-1} \in \mathbb{Z})$$

be 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

$$LR := \{(l_1, \dots, l_{n+1}) \in \mathbb{Q}^{n+1} \mid \textstyle\sum_{i=1}^{n} l_i\alpha_i = l_{n+1}\}.$$

Since the non-zero vector $(1, \dots, 1, -a_{n-1})$ is in LR, we see clearly

$$1 \le t := \dim_{\mathbb{Q}} LR \le n, \ \dim_{\mathbb{Q}} \mathbb{Q}[1, \alpha_1, \dots, \alpha_n] = n + 1 - t.$$

We take and fix a $\mathbb{Z}$-basis of $LR \cap \mathbb{Z}^{n+1}$

$$(m_{j,1}, \dots, m_{j,n}, m_j) \ (j = 1, \dots, t),$$

where

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

Note that vectors $(m_{j,1}, \dots, m_{j,n})$ $(j = 1, \dots, t)$ are also linearly independent.

We write $\mathbb{Q}(f) := \mathbb{Q}(\alpha_1, \dots, \alpha_n)$, which is a finite Galois extension field generated by all roots of $f(x)$ over the rational number field $\mathbb{Q}$ and write

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

Check for updates

Academic Editor: Jay M. Jahangiri

Received: 4 August 2026
Revised: 27 August 2026
Accepted: 28 August 2026
Published: 3 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

where the letter p denotes a prime number. For a prime $p \in \mathrm{Spl}(f)$, we define the integers $r_1, \ldots, r_n$ by the following two conditions:

$$f(x) \equiv \prod_{i=1}^{n}(x - r_i) \bmod p,$$
$$0 \le r_1 \le \cdots \le r_n < p.$$

The first condition is equivalent to $p \in \mathrm{Spl}(f)$. The integers r_i are uniquely determined, and we call them local roots (of $f(x)$ at p). We define two subsets of $\mathrm{Spl}(f)$:

$$\mathrm{Spl}(f,\sigma) := \{p \in \mathrm{Spl}(f) \mid \sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} \equiv m_j \bmod p \ (1 \le {}^{\forall} j \le t)\},$$
$$M(f,\sigma) := \left\{p \in \mathrm{Spl}(f) \mid \alpha_i \equiv r_{\sigma(i)} \bmod \mathfrak{p} \ (1 \le {}^{\forall} i \le n) \text{ for } {}^{\exists}\mathfrak{p} \mid p\right\},$$

where $\sigma \in S_n$ is a permutation and $\mathfrak{p}$ is a prime ideal of $\mathbb{Q}(f)$ lying above p. Note that by setting $\beta_i = \alpha_{\sigma^{-1}(i)}$, $M(f,\sigma)$ can be identified with $M(f,\mathrm{id})$ under the ordering by the roots β_i of $f(x)$. Up to a finite set of prime numbers, the set $\mathrm{Spl}(f)$ is a disjoint union of several $\mathrm{Spl}(f,\sigma)$; furthermore, each $\mathrm{Spl}(f,\sigma)$ is a disjoint union of several $M(f,\mu)$. Whether this is an infinite set or not depends on the permutation. However, the number of distinct infinite sets $\mathrm{Spl}(f,\sigma)$ in $\mathrm{Spl}(f)$ is independent of the numbering of the roots of $f(x)$, and the same holds for the number of $M(f,\mu)$ in $\mathrm{Spl}(f,\sigma)$. It is known that $\mathrm{Spl}(f)$ is an infinite set; to be more precise, the density of the infinite set $\mathrm{Spl}(f)$ in the set of all prime numbers is equal to $[\mathbb{Q}(f):\mathbb{Q}]^{-1}$ due to Chebotarev.

For a real number x, $\{x\}$ denotes the decimal part of x, i.e., $0 \le \{x\} < 1$ and $x - \{x\} \in \mathbb{Z}$.

For a rational number $a = b/c$ $(b, c \in \mathbb{Z})$ and a prime p with $(c,p) = 1$, the symbol $\lfloor a \rfloor_p$ denotes an integer k such that $0 \le k < p$ and $a = k$ in $\mathbb{Z}/p\mathbb{Z}$, i.e., $b \equiv ck \bmod p$.

Last, we introduce geometric objects:

$$\Delta := \{(x_1, \ldots, x_n) \mid 0 \le x_1 \le \cdots \le x_n \le 1\},$$
$$\mathfrak{D}(f,\sigma) := \{\boldsymbol{x} \in \Delta \mid \sum_{i=1}^{n} m_{j,i}\, x_{\sigma(i)} \in \mathbb{Z} \ (1 \le {}^{\forall} j \le t)\}.$$

Now we can state the following conjectures.

Conjecture 1. *Let $f(x)$ be an irreducible polynomial of degree n (≥2). Then the sequence of points*

$$\left(\left\{\frac{r}{p}\right\}, \ldots, \left\{\frac{r^{n-1}}{p}\right\}\right) \in [0,1)^{n-1}$$

is uniformly distributed in $[0,1)^{n-1}$, where p runs over the set $\mathrm{Spl}(f)$ and r runs over the local roots of $f(x)$ at p.

When $n = 2$, this is true [7,8].

Next, write $m = [\mathbb{Q}(f):\mathbb{Q}]$ and let elements $\gamma_{(n+1-t)+1}, \ldots, \gamma_m \in \mathbb{Q}(f)$ satisfy

$$\mathbb{Q}(f) = \mathbb{Q}[1, \alpha_1, \ldots, \alpha_n] \oplus \mathbb{Q}[\gamma_{(n+1-t)+1}, \ldots, \gamma_m]$$

as vector spaces over $\mathbb{Q}$, and write $\gamma_i = g_i(\alpha_1, \ldots, \alpha_n)$ by some polynomial $g_i(x_1, \ldots, x_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$. Assume that $M(f,id)$ is an infinite set. For a prime $p \in M(f,id)$, we see $m_j = \sum_i m_{j,i}\alpha_i \equiv \sum_i m_{j,i} r_i \bmod \mathfrak{p}$; hence, $m_j = \sum_i m_{j,i} r_i - k_j p$ for an integer k_j. Therefore, for

$$D := \mathfrak{D}(f, id) \times [0,1]^{m-(n+1-t)},$$

every accumulation points of

$$v(p) := (\boldsymbol{r}/p, \{\lfloor g_{(n+1-t)+1}(\boldsymbol{r})\rfloor_p/p\}, \ldots, \{\lfloor g_m(\boldsymbol{r})\rfloor_p/p\})$$

is on D, where p runs over the set $M(f, id)$ such that p does not divide the denominator of any coefficient of $g_i(x_1, \ldots, x_n)$ for every i, and $\boldsymbol{r}$, $\boldsymbol{r}/p$ denote the vector $(r_1, \ldots, r_n)$ of local roots of $f(x)$ at p and $(r_1/p, \ldots, r_n/p)$, respectively. The second conjecture is as follows:

Conjecture 2. *The sequence of points $v(p)$ $(p \in M(f, id))$ is uniformly distributed on D.*

We note that $v(p)$ is not on D if $m_j \neq 0$; hence, we need to clarify the definition of "uniformly distributed". In the next section, we will do this and provide the background and data to support Conjectures.

In the third section, we will make a remark about the order of the local roots of polynomials $g(x)$ and $h(x)$, which is independent of the conjectures.

The computations in this paper were performed using the PARI/GP system [9].

2. Background and Numerical Data to Conjectures 1, 2

With respect to the distribution of local roots of an irreducible polynomial, it appears that the sequence $\{r_i/p\}$ $(1 \leq i \leq n, p \in \mathrm{Spl}(f))$ is uniformly distributed on $[0,1)$ as is commonly believed. However, this has only been proven for $n = 2$ [7,8]. Following another question in [10], we have become interested in the distribution of points

$$v_0(p) := \boldsymbol{r}/p\,(= (r_1/p, \ldots, r_n/p) \in \Delta) \quad (p \in \mathrm{Spl}(f)),$$

and we proposed the following conjecture in [1,3,6]:

Conjecture 2′. *Let $f(x)$ be a monic polynomial of degree n in $\mathbb{Z}[x]$. Then, the sequence of $v_0(p)$ $(p \in \mathrm{Spl}(f, \sigma))$ is uniformly distributed on $\mathfrak{D}(f, \sigma)$ if $\mathrm{Spl}(f, \sigma)$ is an infinite set.*

We expect that for $M(f, \mu)$ contained in $\mathrm{Spl}(f, \sigma)$, the density of $M(f, \mu)$ in $\mathrm{Spl}(f, \sigma)$ is independent of a permutation μ if $M(f, \mu)$ is an infinite set. Under this assumption, Conjecture 2 implies Conjecture 2′.

We must explain the uniformity of the sequence of $v_0(p)$ on $\mathfrak{D}(f, \sigma)$, because this uniformity is different from what is usual (cf. [11]). For a prime $p \in \mathrm{Spl}(f, \sigma)$, we have the identity

$$\sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} = m_j + k_j p \quad (j = 1, \ldots, t)$$

for integers k_j. Since the integers $m_{j,i}$ and m_j are fixed and the condition $0 \leq r_i < p$ is supposed, the number of possible values for k_j is finite. If $m_j = 0$ is true for $j = 1, \ldots, t$, then the point $v_0(p)$ is on $\mathfrak{D}(f, \sigma)$. Otherwise, it is not on $\mathfrak{D}(f, \sigma)$, but every accumulation point of $v_0(p)$ $(p \in \mathrm{Spl}(f, \sigma))$ is clearly on $\mathfrak{D}(f, \sigma)$. We define the sequence of $v_0(p)$ being uniformly distributed as follows: Since we see

$$\mathfrak{D}(f, \sigma) = \cup_{\{k_j\} \in \mathbb{Z}^t} \{\boldsymbol{x} \in \Delta \mid \sum_{i=1}^{n} m_{j,i} x_{\sigma(i)} = k_j\, (1 \leq {}^{\forall} j \leq t)\},$$

$\mathfrak{D}(f,\sigma)$ is contained in a finite union of $(n-t)$-dimensional planes, which are parallel to

$$P := \{\boldsymbol{x} \in \mathbb{R}^n \mid \sum_{i=1}^{n} m_{j,i} x_{\sigma(i)} = 0\,(1 \leq {}^{\forall} j \leq t)\}\,(\cong \mathbb{R}^{n-t}).$$

We define the volume for a subset S of $\mathfrak{D}(f,\sigma)$ as follows: By decomposing S as $S = \cup_i(\boldsymbol{v}_i + S_i)$ for some points $\boldsymbol{v}_i$ and subsets $S_i \subset P$, we define the volume $\mathrm{vol}(S)$ by the sum $\sum_i \mathrm{vol}(S_i)$, where $\mathrm{vol}(S_i)$ is the standard volume on the $(n-t)$-dimensional Euclidian space P. Hence, $\dim S < n-t$ implies $\mathrm{vol}(S) = 0$. For $0 \leq a_i < b_i < 1$ $(i = 1,\ldots,n)$, write $B(\{a_i,b_i\}) := \prod_{i=1}^{n}[a_i,b_i]$ (rectangular parallelepiped). Then, the above conjecture means that, for any a_i, b_i

$$\lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}(f,\sigma) \mid p < X, v_0(p) \in B(\{a_i,b_i\})\}}{\#\{p \in \mathrm{Spl}(f,\sigma) \mid p < X\}} = \frac{\mathrm{vol}(\mathfrak{D}(f,\sigma) \cap B(\{a_i,b_i\}))}{\mathrm{vol}(\mathfrak{D}(f,\sigma))}.$$

This implies that the sequence of r_i/p $(i = 1,\ldots,n, p \in \mathrm{Spl}(f))$ is uniformly distributed on $[0,1)$ for an irreducible polynomial [2,4]. The condition $v_0(p) \in B(\{a_i,b_i\})$ may be weakened [6].

This definition of the uniformity is naturally generalized in Conjecture 2, replacing $\mathrm{Spl}(f,\sigma)$ by $M(f,id)$.

Since the ratio of volumes is more important than the volumes themselves, it is often useful to compute the volume by projecting from the original plane P onto a suitably defined $(n-t)$-dimensional plane Q.

Before moving on to the set $M(f,\mu)$, we note the following facts from the theory of an algebraic number field:

1. Let K be an algebraic number field, i.e., a finite extension field of the rational number field $\mathbb{Q}$; write $K = \mathbb{Q}(\alpha)$ by an algebraic integer α; and denote the ring of all algebraic integers in K by $\mathcal{O}_K$. Let $F(x) \in \mathbb{Z}[x]$ be a monic minimal polynomial of α. Then, for a prime p that does not divide the discriminant of the polynomial $F(x)$, the following conditions (i), (ii) are equivalent: (i) $F(x) \equiv \prod(x - r_i) \bmod p$ holds for integers r_i; (ii) the ideal $p\mathcal{O}_K$ is the product of $[K:\mathbb{Q}]$ prime ideals of degree 1, in which case each prime ideal is of the form $(\alpha - r_i, p) := (\alpha - r_i)\mathcal{O}_K + p\mathcal{O}_K$.
2. Let K_1, K_2 be algebraic number fields and K the composite field of K_1 and K_2. For a prime p, the ideal $p\mathcal{O}_K$ is the product of prime ideals of degree 1 in K if and only if the same holds in K_i (i = 1,2).

Let us come back to $M(f,\mu)$. Write $\mathbb{Q}(f) = \mathbb{Q}(\alpha)$ for an algebraic integer α, and denote the monic minimal polynomial of α by $F(x)$. Using the above, we see $\mathrm{Spl}(f) = \mathrm{Spl}(F)$ except finitely many primes as follows: Write $f(x) = \prod f_i(x)$ for monic irreducible polynomials $f_i(x)$. Then, using the above facts, we have, except finitely many primes: $p \in \mathrm{Spl}(F) \Leftrightarrow p$ decomposes into the product of prime ideals of degree 1 in $\mathbb{Q}(f) \Leftrightarrow p$ decomposes into the product of prime ideals of degree 1 in $\mathbb{Q}(f_i)$ by virtue of $\mathbb{Q}(f) = \prod \mathbb{Q}(f_i) \Leftrightarrow p \in \mathrm{Spl}(f_i)$ for all $i \Leftrightarrow p \in \mathrm{Spl}(f)$.

Write $\alpha_i = c_i(\alpha)$ $(i = 1,\ldots,n)$ for a polynomial $c_i(x) \in \mathbb{Q}[x]$. Then we see that, except for finitely many primes p that divide the denominator of some coefficient of polynomials $c_i(x)$

$$
\begin{aligned}
&M(f,\mu)\\
&=\{p\in \mathrm{Spl}(f)\mid c_i(\alpha)\equiv r_{\mu(i)} \bmod \mathfrak{p}\ \ (1\le {}^{\forall}i\le n) \text{ for } {}^{\exists}\mathfrak{p}\mid p\}\\
&=\left\{p\in \mathrm{Spl}(f)\ \middle|\ \begin{array}{l}\text{there is an integer } R \text{ such that } F(R)\equiv 0 \bmod p\\ \text{and } \lfloor c_i(R)\rfloor_p \equiv r_{\mu(i)} \bmod p\ \ (1\le {}^{\forall}i\le n)\end{array}\right\}\\
&=\left\{p\in \mathrm{Spl}(f)\ \middle|\ \begin{array}{l}\text{there is an integer } R \text{ such that } F(R)\equiv 0 \bmod p\\ \text{and } \{\lfloor c_{\mu^{-1}(1)}(R)\rfloor_p/p\}\le\cdots\le\{\lfloor c_{\mu^{-1}(n)}(R)\rfloor_p/p\}\end{array}\right\}.
\end{aligned}
\tag{1}
$$

To verify the second equality, it is enough to note $\mathrm{Spl}(f)=\mathrm{Spl}(F)$, and the prime ideal $\mathfrak{p}$ of $\mathbb{Q}(f)$ is of the form $(\alpha-R)\mathcal{O}_{\mathbb{Q}(f)}+p\mathcal{O}_{\mathbb{Q}(f)}$. For the third equality, the following is helpful.

Proposition 1. *We keep the above notation. Let a prime $p\in\mathrm{Spl}(f)$ be sufficiently large and R a root of $F(x)\equiv 0 \bmod p$. Then all the roots of $f(x)\equiv 0 \bmod p$ are given by $\lfloor c_i(R)\rfloor_p \bmod p$ $(i=1,\dots,n)$.*

Proof. Suppose that a prime $p\in\mathrm{Spl}(f)$ is sufficiently large; then it does not divide the denominator of any coefficient of the polynomials $c_i(x)$, and we consider $c_i(x)\in(\mathbb{Z}/p\mathbb{Z})[x]$. Moreover, $\mathfrak{p}:=(\alpha-R,p)$ is a prime ideal of $\mathbb{Q}(f)=\mathbb{Q}(\alpha)$ lying over p; hence, we see that $f(\lfloor c_i(R)\rfloor_p)\equiv f(c_i(\alpha)) \bmod \mathfrak{p}=f(\alpha_i)=0$, i.e., $f(\lfloor c_i(R)\rfloor_p)\equiv 0 \bmod p$. If $\lfloor c_i(R)\rfloor_p\equiv\lfloor c_j(R)\rfloor_p \bmod p$ holds, then we have $\alpha_i=c_i(\alpha)\equiv\lfloor c_i(R)\rfloor_p \bmod\mathfrak{p}\equiv\lfloor c_j(R)\rfloor_p\equiv\alpha_j$; therefore, the prime ideal $\mathfrak{p}$ divides $\alpha_i-\alpha_j$. The number of such prime ideals is finite. □

The inequality in (1) prompts us to investigate the density of primes $p\in\mathrm{Spl}(f)$ satisfying

$$
\left\{\frac{\lfloor g_1(r)\rfloor_p}{p}\right\}<\left\{\frac{\lfloor g_2(r)\rfloor_p}{p}\right\} \text{ for some root } r \text{ of } f(x)\equiv 0 \bmod p \tag{2}
$$

for polynomials $g_1(x),g_2(x)\in\mathbb{Q}[x]$.

In case of $\deg g_1=\deg g_2=1$, by writing $g_i(x)=a_ix$ with $a_i\in\mathbb{Z}$ $(i=1,2)$, the above condition is equivalent to

$$
(r_1/p,\dots,r_n/p)\in\{\boldsymbol{x}\in[0,1)^n\mid\{a_1x_i\}<\{a_2x_i\}(1\le{}^{\exists}i\le n)\}.
$$

Since the set $\{x\in[0,1)\mid\{a_1x\}<\{a_2x\}\}$ is a union of intervals, Conjecture 2′ is applicable. However, in the case of $\deg g_1>1$ or $\deg g_2>1$, it is helpless. As above, let the monic polynomial $F(x)$ be the minimal polynomial of an algebraic integer α satisfying $\mathbb{Q}(f)=\mathbb{Q}(F)=\mathbb{Q}(\alpha)$ and put $m=[\mathbb{Q}(f):\mathbb{Q}]$. Write

$$
\alpha_i=c_i(\alpha)\quad (c_i(x)\in\mathbb{Q}[x],\deg c_i<m),
$$

where $\alpha_1,\dots,\alpha_n$ are the roots of $f(x)$ as usual. Polynomials $c_i(x)$ are not necessarily either monic or integral. Let us consider the density of the complement set to (2), i.e., the problem studying the density of primes $p\in\mathrm{Spl}(f)$ that satisfy

$$
\left\{\frac{\lfloor g_1(r)\rfloor_p}{p}\right\}>\left\{\frac{\lfloor g_2(r)\rfloor_p}{p}\right\} \text{ for every root } r \text{ of } f(x)\equiv 0 \bmod p \tag{3}
$$

for polynomials $g_1(x),g_2(x)\in\mathbb{Q}[x]$. By Proposition 1, the above inequality is equivalent to

$$
\left\{\frac{\lfloor g_1(c_i(R))\rfloor_p}{p}\right\}>\left\{\frac{\lfloor g_2(c_i(R))\rfloor_p}{p}\right\}\quad (i=1,\dots n) \tag{4}
$$

for a root R of $F(x) \equiv 0 \bmod p$ except for a finite number of primes. By defining rational numbers $g_{l,i,k}$ by

$$g_l(c_i(\alpha)) = \sum_{k=0}^{m-1} g_{l,i,k}\alpha^k \quad (l = 1, 2),$$

data from computer experiments suggest that under the assumption that $g_{l,i,k} \in \mathbb{Z}$ for all l, i, k, the density of primes $p \in \mathrm{Spl}(f)$ satisfying (3) is equal to the volume of the set

$$\mathcal{D} := \left\{ \boldsymbol{x} \in [0,1)^{m-1} \middle| \left\{ \sum_{k=1}^{m-1} g_{1,i,k}x_k \right\} > \left\{ \sum_{k=1}^{m-1} g_{2,i,k}x_k \right\} (1 \le {}^{\forall} i \le n) \right\}.$$

This leads to Conjecture 1. For example, when $f(x)$ is a Galois polynomial $x^3 - 3x + 1$ with roots $c_1(\alpha) := \alpha, c_2(\alpha) := -\alpha^2 - \alpha + 2, c_3(\alpha) := \alpha^2 - 2$, all coefficients $g_{l,i,k}$ are integral. Here is an example such that some coefficient $g_{l,i,k}$ is not integral. For $f(x) = x^3 - 4x^2 - 9x + 4$, which gives the subfield of degree 3 in $\mathbb{Q}(\sqrt[43]{1})$, the roots of $f(x)$ are $c_1(\alpha) := \alpha, c_2(\alpha) := -\alpha^2/2 + 3\alpha/2 + 5, c_3(\alpha) := \alpha^2 - 5\alpha/2 - 1$. Hence, polynomials $g(c_i(x))$ are not necessarily integral. The density is not equal to the volume of $\mathcal{D}$ experimentally. There is no algebraic integer $\beta \in \mathbb{Q}(f)$ such that $\mathbb{Z}[\beta]$ contains all roots $c_i(\alpha)$ of $f(x)$.

Conjecture 1 implies, applying to the set $\{\boldsymbol{x} \in [0,1)^{n-1} \mid a \le x_k \le b\}$, the uniform distribution of the sequence $\left\{\frac{r^k}{p}\right\}$ $(p \in \mathrm{Spl}(f))$ where r runs over local roots of $f(x)$ at p and k is a fixed integer with $1 \le k \le n-1$. We cannot replace $\mathrm{Spl}(f)$ with smaller sets $M(f, \sigma)$.

As we shall see later, the formulation in (4) may not be particularly suitable for investigating the density of prime numbers satisfying (3).

Here are the data : Let $f(x)$ be an irreducible polynomial of degree n and d a positive integer, and write

$$B(\{k_i\}, d) := \prod_{i=1}^{n-1} [k_i/d, (k_i+1)/d) \subset [0,1)^{n-1}$$

for integers $0 \le k_i < d$ whose volume is $1/d^{n-1}$ and

$$Dens(X, \{k_i\}) := \frac{\#\{p \in \mathrm{Spl}_X(f), 1 \le j \le n \mid (\{r_j/p\}, \ldots, \{r_j^{n-1}/p\}) \in B(\{k_i\}, d)\}}{n\#\mathrm{Spl}_X(f)}.$$

For example, for polynomials $f(x) = x^3 - 2, x^4 + 1$ and $x^6 + \cdots + 1 = (x^7 - 1)/(x - 1)$, the value er that is the maximum in the set of $|Dens(X, \{k_i\}) - 1/d^{n-1}|$ $(0 \le k_i < d)$ is as follows:

For $f(x) = x^3 - 2$ and $d = 100$, er is

$$\begin{array}{ll} 4.56/d^2 & (X = 10^6) \\ 1.01/d^2 & (X = 10^7) \\ 6.07/(10d^2) & (X = 10^8) \\ 2.47/(10d^2) & (X = 10^9) \\ 1.15/(10d^2) & (X = 10^{10}) \\ 3.92/(10^2d^2) & (X = 10^{11}). \end{array}$$

For $f(x) = x^4 + 1$ and $d = 10$, er is

$$\begin{array}{ll} 3.93/(10d^3) & (X = 10^6) \\ 1.29/(10d^3) & (X = 10^7) \\ 3.96/(10^2d^3) & (X = 10^8) \\ 1.35/(10^2d^3) & (X = 10^9) \\ 5.27/(10^3d^3) & (X = 10^{10}) \\ 1.62/(10^3d^3) & (X = 10^{11}). \end{array}$$

For $f(x) = x^6 + x^5 + \cdots + x + 1$ and $d = 4$, er is

$$\begin{array}{ll} 4.25/(10d^5) & (X = 10^6) \\ 1.21/(10d^5) & (X = 10^7) \\ 5.75/(10^2d^5) & (X = 10^8) \\ 1.56/(10^2d^5) & (X = 10^9) \\ 6.05/(10^3d^5) & (X = 10^{10}) \\ 1.72/(10^3d^5) & (X = 10^{11}). \end{array}$$

Thus, we can expect that as X increases, the error er decreases towards zero.

Next, let us consider polynomials in many variables: Write

$$\begin{aligned} &M_X(f,\mu) := \{p \in M(f,\mu) \mid p < X\} \\ &= \{p \in \mathrm{Spl}(f) \mid p < X, \alpha_i \equiv r_{\mu(i)} \bmod {}^{\exists}\mathfrak{p} \ \ (1 \leq {}^{\forall} i \leq n)\}, \end{aligned}$$

where $\mathfrak{p}$ is a prime ideal of $\mathbb{Q}(f)$ lying above p and is independent of i. In view of (1), we are concerned with the following density for polynomials $g(\boldsymbol{x}), h(\boldsymbol{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ and $\mu \in S_n$:

$$\begin{aligned} &D_f(g,h;\mu) \\ &:= \lim_{X\to\infty} \frac{\#\left\{p \in M_X(f,\mu) \middle| \left\{\frac{g(\mu^{-1}(\boldsymbol{r}))}{p}\right\} < \left\{\frac{h(\mu^{-1}(\boldsymbol{r}))}{p}\right\}\right\}}{\#M_X(f,\mu)}, \end{aligned}$$

where $\mu^{-1}(\boldsymbol{r}) := (r_{\mu(1)}, \ldots, r_{\mu(n)})$. By

$$g(\alpha_1, \ldots, \alpha_n) \equiv g(\mu^{-1}(\boldsymbol{r})) \bmod \mathfrak{p}$$

for $p \in M(f,\mu)$, we see for $\beta := g(\alpha_1, \ldots, \alpha_n)$ and $\gamma := h(\alpha_1, \ldots, \alpha_n)$

$$D_f(g,h;\mu) = \lim_{X\to\infty} \frac{\#\left\{p \in M_X(f,\mu) \mid \left\{\frac{\beta_p}{p}\right\} < \left\{\frac{\gamma_p}{p}\right\}\right\}}{\#M_X(f,\mu)},$$

where β_p is an integer such that $\beta \equiv \beta_p \bmod \mathfrak{p}$; the same holds for γ_p. If we prioritize local roots over global roots, then writing

$$\tilde{D}_f(g,h;\mu) := \lim_{X\to\infty} \frac{\#\left\{p \in M_X(f,\mu) \middle| \left\{\frac{g(\boldsymbol{r})}{p}\right\} < \left\{\frac{h(\boldsymbol{r})}{p}\right\}\right\}}{\#M_X(f,\mu)},$$

we see

$$\tilde{D}_f(g_\mu, h_\mu; \mu) = D_f(g,h;\mu)$$

for $g_\mu(\boldsymbol{x}) := g(\mu^{-1}(\boldsymbol{x})), h_\mu(\boldsymbol{x}) := h(\mu^{-1}(\boldsymbol{x}))$.

For simplicity, assume that μ is the identity, since we do not deal with densities for distinct permutations at the same time in the following. If polynomials $g_1(\boldsymbol{x}), h_1(\boldsymbol{x})$ satisfy $g_1(\alpha_1,\dots,\alpha_n) = g(\alpha_1,\dots,\alpha_n)$, $h_1(\alpha_1,\dots,\alpha_n) = h(\alpha_1,\dots,\alpha_n)$, respectively, then we see $g(r_1,\dots,r_n) \equiv g_1(r_1,\dots,r_n) \bmod p$ for a prime $p \in M(f,id)$. Suppose that g_1, h_1 are linear and let $g_1(\boldsymbol{x}) = \sum_{i=1}^n a_i x_i$ and $h_1(\boldsymbol{x}) = \sum_{i=1}^n b_i x_i$. Then, it is clear that $\{g(\boldsymbol{r})/p\} < \{h(\boldsymbol{r})/p\}$ is equivalent to $\boldsymbol{r}/p \in D$, where

$$D := \left\{ \boldsymbol{x} \in [0,1)^n \middle| \left\{ \sum_{i=1}^n a_i x_i \right\} < \left\{ \sum_{i=1}^n b_i x_i \right\} \right\}.$$

Therefore, Conjecture 2′ is applicable to evaluate the density $D_f(h,g)$ under the assumption $\mathrm{Spl}(f,id) = M(f,id)$ (cf. the remark after Conjecture 2′).

Assume that $t = 1$ and $\mathbb{Q}(f)/\mathbb{Q}$ is a Galois extension with $\deg f = n$. Then we have $[\mathbb{Q}(f) : \mathbb{Q}] = n$ and $\dim \mathbb{Q}[\alpha_1,\dots,\alpha_n,1] = n+1-t = n$; thus, $\mathbb{Q}(f)$ is spanned by 1 and the roots $\alpha_1,\dots,\alpha_n$ of $f(x)$ as a vector space over $\mathbb{Q}$. Thus, for a polynomial $g(x_1,\dots,x_n) \in \mathbb{Q}[x_1,\dots,x_n]$, we see that there exists a linear polynomial $g_1(\boldsymbol{x})$ such that $g_1(\alpha_1,\dots,\alpha_n) = g(\alpha_1,\dots,\alpha_n)$, neglecting a constant term. Hence, we may assume that polynomials g, h are linear to study the density $D_f(g,h;id)$.

Unless $\mathbb{Q}(f)/\mathbb{Q}$ is a Galois extension and $t = 1$, what happens? Below are four examples: $f(x) = x^4+1$ in the case of $t = 2 > 1$ and $f(x) = x^3+2, x^4-2$, which are non-Galois, and $f(x) = (x^2-2)(x^2-3)$, which is reducible.

Example 1. *Set* $f(x) = x^4+1$ *with roots* $\alpha_1 := \frac{1+\sqrt{-1}}{\sqrt{2}}, \alpha_2 := \frac{1-\sqrt{-1}}{\sqrt{2}} = -\alpha_1^3, \alpha_3 := -\frac{1-\sqrt{-1}}{\sqrt{2}} = \alpha_1^3, \alpha_4 := -\frac{1+\sqrt{-1}}{\sqrt{2}} = -\alpha_1$, *where linear relations among roots over rationals are spanned by* $\alpha_1+\alpha_4 = \alpha_2+\alpha_3 = 0$. *It is easy to see that* $\mathfrak{D}(f,\sigma)$ *is not a finite set if and only if* σ *is contained in the group* $\hat{\boldsymbol{G}}$ *that consists of* σ *such that* $\{\sigma(1),\sigma(4)\} = \{1,4\}$ *or* $\{2,3\}$ *holds and*

$$\mathfrak{D}(f,\sigma) = \left\{ (x_1,\dots,x_4) \middle| \begin{array}{l} 0 \le x_1 \le \cdots \le x_4 \le 1, \\ x_1+x_4 = x_2+x_3 = 1 \end{array} \right\},$$

which is identified to

$$\mathfrak{D}_{pr}(f,id) := \{(x_1,x_2) \mid 0 \le x_1 \le x_2 \le 1/2\}, \tag{5}$$

by the projection $(x_1,\dots,x_4) \mapsto (x_1,x_2)$.

We remark that for a permutation $\sigma \in \hat{\boldsymbol{G}}$, $M(f,\sigma)$ *is equal to* $M(f,id)$ *or* $M(f,(2,3))$. *Denote by* $\boldsymbol{G}_0$ *the group that consists of permutations* μ *such that there is an automorphism* $\tilde{\mu} \in \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ *satisfying* $\alpha_{\mu(i)} = \tilde{\mu}(\alpha_i)$. *Then* $\hat{\boldsymbol{G}} = \boldsymbol{G}_0 \cup (2,3)\boldsymbol{G}_0$ *holds.*

We know by (1) *the following:*

$$M(f,\sigma) = \begin{cases} \{p \in \mathrm{Spl}(f) \mid r_3 \equiv r_1^3 \bmod p\} & \text{if } \sigma = id, \\ \{p \in \mathrm{Spl}(f) \mid r_2 \equiv r_1^3 \bmod p\} & \text{if } \sigma = (2,3). \end{cases}$$

Noting that $\mathbb{Q}(f) = \mathbb{Q}[1,\alpha_1,\alpha_2,\alpha_1^2]$ *with* $\alpha_1^2 = \sqrt{-1}$, *we see that for a polynomial* $g(\boldsymbol{x})$ *in* $\mathbb{Q}[x_1,\dots,x_4]$, *there are rational numbers* c_i *so that* $g(\alpha_1,\dots,\alpha_4) = c_0+c_1\alpha_1+c_2\alpha_2+c_3\alpha_1^2$. *So, we may assume that* $g(\boldsymbol{x}) = c_0+c_1x_1+c_2x_2+c_3x_1^2$.

The computer experiments suggest the following:

1. *The densities of* $M(f,id)$ *and* $M(f,(2,3))$ *in* $\mathrm{Spl}(f)$ *are equal to* $\frac{1}{2}$,
2. *Densities* $\tilde{D}_f(g,h;id.), \tilde{D}_f(g,h;(2,3))$ *are equal.*

Then we see that for every permutation σ such that $\{\sigma(1), \sigma(4)\} = \{1,4\}$ or $\{2,3\}$, the density $D_f(g,h;\sigma) = \frac{1}{2}(\tilde{D}_f(g,h;id.) + \tilde{D}_f(g,h;(2,3)))$ is equal to

$$\lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f) \mid \{\frac{g(\boldsymbol{r})}{p}\} < \{\frac{h(\boldsymbol{r})}{p}\}\}}{\#\mathrm{Spl}_X(f)}.$$

Thus, in case $g(\boldsymbol{x}), h(\boldsymbol{x})$ are linear, the density $\tilde{D}_f(g,h;\mu)$ is evaluated by Conjecture 2′. For example, let $g_1(\boldsymbol{x}) = 2x_1 - x_2, g_2(\boldsymbol{x}) = x_2$; then, the computer experiment suggests $\tilde{D}_f(g_1,g_2;\mu) = \frac{1}{2}$, which matches $\mathrm{vol}(\{(x_1,x_2) \mid 0 < x_1 < x_2 < \frac{1}{2}, \{2x_1 - x_2\} < \{x_2\}\}) = \mathrm{vol}(\{(x_1,x_2) \mid 0 < x_1 < x_2 < \frac{1}{2}, x_1 < x_2 < 2x_1\}) = \frac{1}{16}$ *and* $\mathrm{vol}(\{(x_1,x_2) \mid 0 < x_1 < x_2 < \frac{1}{2}\}) = \frac{1}{8}$.

We restrict polynomials to the following "reduced" type without constant term:

$$g(\boldsymbol{x}) = g_1x_1 + g_2x_2 + g_3x_1^2 \quad (g_1,g_2,g_3 \in \mathbb{Z}),$$
$$h(\boldsymbol{x}) = h_1x_1 + h_2x_2 + h_3x_1^2 \quad (h_1,h_2,h_3 \in \mathbb{Z}).$$

Suppose that $g(\boldsymbol{x}) \neq 0, h(\boldsymbol{x}) \neq 0, g(\boldsymbol{x}) \neq h(\boldsymbol{x})$ and either g_3 or h_3 is not zero. Writing $k_i := g_i - h_i$, condition $g(\boldsymbol{x}) \neq h(\boldsymbol{x})$ is equivalent to $k_i \neq 0$ for some i. Then the density $D_f(g,h) := \tilde{D}_f(g,h;\mu)$ ($\mu = id.$ or $(2,3)$) seems to be as follows, independently of μ.

1. $D_f(g,h) + D_f(h,g) = 1$.
2. *The case of $g_3h_3 \neq 0$. Then $D_f(g,h)$ is*

$$\frac{1}{2} + \begin{cases} \frac{1}{3k_2} & \text{if } k_1 = 0, k_3 = 0, k_2 \equiv 0 \bmod 2, \\ \frac{-1}{6k_2} & \text{if } k_1 = 0, k_3 = 0, k_2 \equiv 1 \bmod 2, \\ \frac{-1}{3k_1} & \text{if } k_2 = 0, k_3 = 0, \\ \frac{1}{3k_1} & \text{if } k_3 = 0, k_1 + k_2 = 0, \\ 0 & \text{otherwise, i.e., if } k_3 \neq 0 \text{ or } k_1k_2(k_1+k_2) \neq 0, \end{cases}$$

   which depends only on $g(\boldsymbol{x}) - h(\boldsymbol{x})$.
3. *The case of $g_3 = 0$ and $h_3 \neq 0$. Then $D_f(g,h)$ is*

$$\frac{1}{2} + \begin{cases} \frac{-1}{3g_2} & \text{if } g_1 = 0, g_2 \equiv 0 \bmod 2, \\ \frac{1}{6g_2} & \text{if } g_1 = 0, g_2 \equiv 1 \bmod 2, \\ \frac{1}{3g_1} & \text{if } g_2 = 0, \\ \frac{-1}{3g_1} & \text{if } g_1 + g_2 = 0, \\ 0 & \text{otherwise, i.e., if } g_1g_2(g_1+g_2) \neq 0, \end{cases}$$

   which depends only on $g(\boldsymbol{x})$.

We note that if the ordered pair g,h of polynomials does not satisfy the third condition, then the ordered pair h,g satisfies it.

To shed light on the background of these formulas, we will carry out the following experiment: For real numbers a,b,c with $0 \leq a,b,c < 1$, write

$$D(a,b,c) := \mathfrak{D}_{pr}(f,id) \times [0,1) \cap [0,a) \times [0,b) \times [0,c).$$

From the figure, it is easy to see

$$\begin{aligned}&\mathrm{vol}(\mathrm{D}(\mathrm{a},\mathrm{b},\mathrm{c}))\\&= c\cdot(\min(1/2,b)\cdot\min(1/2,a,b)-1/2\cdot\min(1/2,a,b)^2)\end{aligned}$$

and $\mathrm{vol}(\mathrm{D}(1/2,1/2,1)) = 1/8$. *For local roots* r_i, *the inclusion* $(\{r_1/p\},\{r_2/p\},\{r_1^2/p\}) \in D(1/2,1/2,1)$ *is clear by* $0<r_1<r_2<r_3<r_4<p$ *and* $r_1+r_4=r_2+r_3=p$. *Our observation suggests that*

$$\begin{aligned}&\lim_{X\to\infty}\frac{\#\{p\in \mathrm{Spl}_X(f)\mid(\{r_1/p\},\{r_2/p\},\{r_1^2/p\})\in D(a,b,c)\}}{\#\mathrm{Spl}_X(f)}\\&=\lim_{X\to\infty}\frac{\#\{p\in M_X(f,\mu)\mid(\{r_1/p\},\{r_2/p\},\{r_1^2/p\})\in D(a,b,c)\}}{\#M_X(f,\mu)}\\&=\mathrm{vol}(\mathrm{D}(\mathrm{a},\mathrm{b},\mathrm{c}))/\mathrm{vol}(\mathrm{D}(1/2,1/2,1))\end{aligned}$$

for $0\le a,b\le 1/2, 0\le c\le 1$ *independently of a permutation* μ. *This means that the sequence of the vectors* $(\{r_1/p\},\{r_2/p\},\{r_1^2/p\})\in D(1/2,1/2,1)$ *is uniformly distributed in* $D(1/2,1/2,1)$. *Although this uniformity should allow us to prove that the above equation for* $D_f(g,h)$ *is true, the calculation is not straightforward.*

This uniformity may hold not only for $(\{r_1/p\},\{r_2/p\},\{r_1^2/p\})$ *but also, more generally, for* $(\{r_1/p\},\{r_2/p\},\{\lfloor c_1r_1+c_2r_2+c_3r_1^2\rfloor_p/p\})$ $(c_1,c_2,c_3\in\mathbb{Q}$ *with* $c_3\neq 0)$, *which is equivalent to the fact that* $1,\alpha_1,\alpha_2,c_1\alpha_1+c_2\alpha_2+c_3\alpha_1^2$ *are linearly independent in the four dimensional vector space* $\mathbb{Q}(f)$ *over* $\mathbb{Q}$. *Here, we neglect a finite number of primes that divide a denominator of* c_1,c_2,c_3. *The computational data for the case* $c_1=1/2,c_2=1/7,c_3=2/3$ *support this. This observation naturally leads to Conjecture* 2.

Example 2. *Let* $f(x)=x^3+a_2x^2+a_1x+a_0\in\mathbb{Q}[x]$ *be an irreducible polynomial with roots* $\alpha_1,\alpha_2,\alpha_3$, *and suppose that the extension* $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ *is not a Galois extension; hence,* $[\mathbb{Q}(f):\mathbb{Q}]=6$. *The vector space* $\mathbb{Q}(f)$ *is spanned by* $1,\alpha_1,\alpha_2,\alpha_1^2,\alpha_2^2,\alpha_1^2\alpha_2$ *over* $\mathbb{Q}$ *because the identity* $\alpha_3=-\alpha_1-\alpha_2-a_2$ *implies that every polynomial in* $\alpha_1,\alpha_2,\alpha_3$ *is a polynomial in* α_1,α_2. *By denoting the vector space spanned by* $1,\alpha_1,\alpha_2,\alpha_1^2,\alpha_2^2,\alpha_1^2\alpha_2$ *by* V, *the identity* $0=f(\alpha_1)-f(\alpha_2)=(\alpha_1-\alpha_2)(\alpha_1^2+\alpha_1\alpha_2+\alpha_2^2+a_2(\alpha_1+\alpha_2)+a_1)$ *implies* $\alpha_1\alpha_2\in V$. *Hence,* $\alpha_1\alpha_2^2=(\alpha_1\alpha_2)\alpha_2=-\alpha_1^2\alpha_2-\alpha_2^3-a_2(\alpha_1\alpha_2+\alpha_2^2)-a_1\alpha_2\in V$ *follows. Finally,* $\alpha_1^2\alpha_2^2=\alpha_1(\alpha_1\alpha_2^2)=-\alpha_1^3\alpha_2-\alpha_1\alpha_2^3-a_2(\alpha_1^2\alpha_2+\alpha_1\alpha_2^2)-a_1\alpha_1\alpha_2\in V$ *is easily confirmed. Thus, every polynomial in* $\alpha_1,\alpha_2,\alpha_3$ *is contained in* V.

We can easily see $M(f,\mu)=\mathrm{Spl}(f)$ *for every permutation* μ, *in particular* $\mathrm{Spl}(f)=M(f,id)$, *since* $t=1$.

We specialize $f(x)$ *to* x^3+2, *and we suppose that polynomials* $g(\boldsymbol{x}),h(\boldsymbol{x})$ *are of the following "reduced" type*

$$\begin{aligned}g(\boldsymbol{x})&=g_1x_1+g_2x_2+g_3x_1^2+g_4x_2^2+g_5x_1^2x_2,\\h(\boldsymbol{x})&=h_1x_1+h_2x_2+h_3x_1^2+h_4x_2^2+h_5x_1^2x_2\end{aligned}$$

with rational integer coefficients g_i,h_i *without a constant term. Denote its homogeneous part of degree i by* $g_i(\boldsymbol{x})$, $h_i(\boldsymbol{x})$. *If both of* g,h *are linear, i.e.,* $g(\boldsymbol{x})=g_1(\boldsymbol{x}),h(\boldsymbol{x})=h_1(\boldsymbol{x})$, *then it is sufficient for us to refer to Conjecture* $2'$, *and so we suppose that* $g(\boldsymbol{x})$ *or* $h(\boldsymbol{x})$ *is not linear. Furthermore, suppose that they satisfy* $g(\boldsymbol{x})\neq 0$, $h(\boldsymbol{x})\neq 0$, *and* $g(\boldsymbol{x})\neq h(\boldsymbol{x})$. *Then, computer experiments suggest the following:*

1. $D_f(g,h;id)+D_f(h,g;id)=1$.
2. *The case of* $g_5\neq 0$ *or* $h_5\neq 0$. *Write* $k_i:=g_i-h_i$.

(a) *The case of* $k_3 = k_4 = k_5 = 0$. *The density* $D_f(g, h; id)$ *is*

$$\frac{1}{2} + \begin{cases} -\frac{1}{4k_1} & \text{if } k_2 = 0 \text{ or } k_1 = k_2, \\ \frac{1}{4k_1} & \text{if } k_2 = 2k_1 \text{ or } k_1 + k_2 = 0, \\ 0 & \text{otherwise.} \end{cases}$$

(b) *In the case of* ($k_3 \neq 0$ *or* $k_4 \neq 0$) *and* $k_5 = 0$, $D_f(g, h; id) = \frac{1}{2}$.

(c) *The case of* $k_5 \neq 0$ *and* $g_5 \neq 0$. *The density* $D_f(g, h; id)$ *is*

$$\frac{1}{2} + \begin{cases} -\frac{1}{4h_1} & \text{if } h_1 \neq 0, h_3 = h_4 = h_5 = 0 \text{ and} \\ & \quad (h_2 = 0 \text{ or } h_1 = h_2), \\ \frac{1}{4h_1} & \text{if } h_1 \neq 0, h_3 = h_4 = h_5 = 0 \text{ and} \\ & \quad (h_2 = 2h_1 \text{ or } h_1 + h_2 = 0), \\ 0 & \text{otherwise.} \end{cases}$$

3. *The case of* $g_5 = h_5 = 0$ *and* $g_2(\boldsymbol{x})h_2(\boldsymbol{x}) \neq 0$. *The density* $D_f(g, h; id)$ *is, writing* $k_i := g_i - h_i$

$$\frac{1}{2} + \begin{cases} -\frac{1}{4k_1} & \text{if } k_3 = k_4 = 0 \text{ and } (k_2 = 0 \text{ or } k_1 = k_2), \\ \frac{1}{4k_1} & \text{if } k_3 = k_4 = 0 \text{ and } (k_2 = 2k_1 \text{ or } k_1 + k_2 = 0), \\ 0 & \text{otherwise,} \end{cases}$$

which depends only on $g(\boldsymbol{x}) - h(\boldsymbol{x})$.

4. *The case of* $g_5 = h_5 = 0$ *and* $g(\boldsymbol{x}) = g_1(\boldsymbol{x})$, $h_2(\boldsymbol{x}) \neq 0$.

$$D_f(g, h; id) = \frac{1}{2} + \begin{cases} \frac{1}{4g_1} & \text{if } g_2 = 0 \text{ or } g_1 = g_2, \\ -\frac{1}{4g_1} & \text{if } g_2 = 2g_1 \text{ or } g_1 + g_2 = 0, \\ 0 & \text{otherwise,} \end{cases}$$

which depends only on $g(\boldsymbol{x})$.

Similarly to the case of $f(x) = x^4 + 1$, *let us consider the sequence of points*

$$v(p) := (\{r_1/p\}, \{r_2/p\}, \{r_1^2/p\}, \{r_2^2/p\}, \{r_1^2 r_2/p\})$$

for the local roots r_1, r_2, r_3 *of* $f(x) = x^3 + 2$. *This seems to be uniformly distributed on* $\mathfrak{D}_{pr}(f, id) \times [0, 1)^3$, *where*

$$\begin{aligned} \mathfrak{D}_{pr}(f, id) &= \{(x_1, x_2) \mid (x_1, x_2, x_3) \in \mathfrak{D}(f, id) \text{ for } {}^{\exists}x_3\} \\ &= \{(x_1, x_2) \mid 0 \leq x_1 \leq x_2 \leq x_3 \leq 1, \sum_{i=1}^{3} x_i \in \mathbb{Z} \text{ for } {}^{\exists}x_3\}. \end{aligned}$$

Let us present data. For $0 \leq g_1, g_2 \leq 1$, *write* $D(g_1, g_2) := \mathfrak{D}_{pr}(f, id) \cap [0, g_1) \times [0, g_2)$. *From the figure, we can see that the volume of* $D(g_1, g_2)$ *is as follows:*

in the case of $0 \leq g_1 \leq 1/3$,

$$\begin{cases} g_1(1 - g_1)/2 - (1 - g_2)^2/2 & \text{if } 1 - g_1/2 \leq g_2 \leq 1, \\ (1 - g_1)/2 - g_2 - g_1^2/4 + g_2^2/2 + g_1 g_2 & \text{if } 1 - g_1 \leq g_2 \leq 1 - g_1/2, \\ (2g_1 - 3g_1^2)/4 & \text{if } 1/2 \leq g_2 \leq 1 - g_1, \\ (2g_1 - 3g_1^2)/4 - (1 - 2g_2)^2/4 & \text{if } (1 - g_1)/2 \leq g_2 \leq 1/2, \\ (g_2 - g_1/2)g_1 & \text{if } g_1 \leq g_2 \leq (1 - g_1)/2, \\ g_2^2/2 & \text{if } 0 \leq g_2 \leq g_1, \end{cases}$$

in the case of $1/3 \leq g_1 \leq 1/2$,

$$\begin{cases} 1/12 + g_1^2/4 - (1-g_2)^2/2 & \text{if } 1 - g_1/2 \leq g_2 \leq 1, \\ 1/12 + (g_1 + g_2 - 1)^2/2 & \text{if } 1 - g_1 \leq g_2 \leq 1 - g_1/2, \\ 1/12 & \text{if } 1/2 \leq g_2 \leq 1 - g_1, \\ 1/12 - (1-2g_2)^2/4 & \text{if } 1/3 \leq g_2 \leq 1/2, \\ g_2^2/2 & \text{if } 0 \leq g_2 \leq 1/3, \end{cases}$$

in the case of $1/2 \leq g_1 \leq 2/3$,

$$\begin{cases} 1/6 - (1-3g_1/2)^2/3 - (1-g_2)^2/2 & \text{if } 1 - g_1/2 \leq g_2 \leq 1, \\ 1/12 + (g_1 + g_2 - 1)^2/2 - (2g_1 - 1)^2/4 & \text{if } g_1 \leq g_2 \leq 1 - g_1/2, \\ 1/12 + (2g_2 - 1)^2/4 & \text{if } 1/2 \leq g_2 \leq g_1, \\ 1/12 - (2g_2 - 1)^2/4 & \text{if } 1/3 \leq g_2 \leq 1/2, \\ g_2^2/2 & \text{if } 0 \leq g_2 \leq 1/3, \end{cases}$$

in the case of $g_1 \geq 2/3$, $\mathrm{vol}(D(g_1, g_2)) = \mathrm{vol}(D(2/3, g_2))$, *and* $\mathrm{vol}(D(1,1)) = 1/6$. *For a positive integer* d *and integers* $k_i = 0, \ldots, d-1$ $(1 \leq i \leq 5)$, *define a box* $B(\{k_i\}, d)$ *by*

$$B(\{k_i\}, d) := \prod_{i=1}^{5} [k_i/d, (k_i + 1)/d).$$

For a positive number X, *let* $diff(\{k_i\})$ *denote the absolute value of the difference between*

$$\frac{\#\{p \in \mathrm{Spl}_X(f) \mid v(p) \in B(\{k_i\}, d)\}}{\#\mathrm{Spl}_X(f)}$$

and

$$d(\{k_i\}) := \frac{\mathrm{vol}(\mathfrak{D}_{pr}(f, id) \times [0,1)^3 \cap B(\{k_i\}, d))}{\mathrm{vol}(\mathfrak{D}_{pr}(f, id) \times [0,1)^3)},$$

and let er *be the maximum in the set of* $diff(\{k_i\})$ *where* $\{k_i\}$ *runs over the set of* $(k_1, \ldots, k_5)$ *with* $0 \leq k_i \leq d-1$. *The denominator* $\mathrm{vol}(\mathfrak{D}_{pr}(f, id) \times [0,1)^3)$ *is equal to* $1/6$. *The data are as follows: for* $d = 6$, er *decreases as*

$$\begin{array}{ll} 2.53 \cdot 10^{-5} & (X = 10^8), \\ 1.10 \cdot 10^{-5} & (X = 10^9), \\ 7.75 \cdot 10^{-6} & (X = 10^{10}), \\ 3.39 \cdot 10^{-6} & (X = 10^{11}). \end{array}$$

The least value of non-zero $d(\{k_i\})$ *is* $1/5184 = 1.9 \cdots \times 10^{-4}$ *for* $(k_1, k_2) = (0,5), (1,2), (1,5), (3,4)$.

For another polynomial such as $x^3 + x^2 + 1$, *where* $[\mathbb{Q}(f) : \mathbb{Q}] = 6$, *and for other polynomials, the situation is similar.*

Example 3. *Let* $f(x) = x^4 - 2$ *with roots* $\alpha_1 := \sqrt[4]{2}, \alpha_2 := \alpha_1 \cdot i, \alpha_3 := -\alpha_2, \alpha_4 := -\alpha_1$, *and* $F(x) = x^8 + 4x^6 + 2x^4 + 28x^2 + 1$, *which has a root* $\alpha := \sqrt[4]{2} + i$. *It is easy to see that* $\mathbb{Q}(f) = \mathbb{Q}(\alpha)$, *which is a Galois extension over* $\mathbb{Q}$, *and* $g_i(\alpha) = \alpha_i$ $(i = 1, 2)$ *for polynomials* $g_i(x)$:

$$\begin{aligned} g_1(x) &= 5/24x^7 + 19/24x^5 + 5/24x^3 + 151/24x, \\ g_2(x) &= 1/24x^6 + 5/24x^4 + 13/24x^2 + 29/24. \end{aligned}$$

We have

$$\begin{aligned}\mathbb{Q}(f) &= \mathbb{Q}[1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{2}^3, i, \sqrt[4]{2} \cdot i, \sqrt{2} \cdot i, \sqrt[4]{2}^3 \cdot i] \\ &= \mathbb{Q}[1, \alpha_1, \alpha_2] \oplus \mathbb{Q}[\alpha_1^2, \alpha_1^3, \alpha_1^3\alpha_2, \alpha_1\alpha_2, \alpha_1^2\alpha_2]\end{aligned}$$

and we write, for a prime $p \in \mathrm{Spl}(f)$ *and local vectors* $\mathbf{r}$ *of* $f(x)$*,*

$$\begin{aligned}&v(p) \\ &:= \left(\left\{ \frac{r_1}{p} \right\}, \left\{ \frac{r_2}{p} \right\}, \left\{ \frac{r_1^2}{p} \right\}, \left\{ \frac{r_1^3}{p} \right\}, \left\{ \frac{r_1^3 r_2}{p} \right\}, \left\{ \frac{r_1 r_2}{p} \right\}, \left\{ \frac{r_1^2 r_2}{p} \right\} \right) \\ &\in \mathfrak{D}_{pr}(f, id) \times [0,1)^5,\end{aligned}$$

where $\mathfrak{D}_{pr}(f, id)$ *is the same as* (5)*. For a positive integer* d *and integers* $k_i = 0, \ldots, d-1$ $(1 \le i \le 7)$*, define a box* $B(\{k_i\}, d)$ *by*

$$B(\{k_i\}, d) := \prod_{i=1}^{7} [k_i/d, (k_i+1)/d).$$

By (1)*, we know*

$$M(f, id) = \left\{ p \in \mathrm{Spl}(f) \;\middle|\; \begin{array}{l} \text{there is an integer } R \text{ such that } F(R) \equiv 0 \bmod p \\ \text{and } g_i(R) \equiv r_i \bmod p \;\; (1 \le {}^{\forall} i \le 4) \end{array} \right\}.$$

The sequence of points $v(p)$ *for* $p \in M(f, id)$ *is uniformly distributed on* $\mathfrak{D}_{pr}(f, id) \times [0,1)^5$ *if and only if for every positive integer* d *and every box* $B(\{k_i\}, d)$

$$T(X) := \frac{\#\{p \in M_X(f, id) \mid v(p) \in \mathfrak{D}_{pr}(f, id) \times [0,1)^5 \cap B(\{k_i\}, d)\}}{\#M_X(f, id)}$$

converges to

$$Y(B(\{k_i\}, d)) := \frac{\mathrm{vol}(\mathfrak{D}_{pr}(f, id) \times [0,1)^5 \cap B(\{k_i\}, d))}{\mathrm{vol}(\mathfrak{D}_{pr}(f, id) \times [0,1)^5)},$$

where the volume in the denominator is $1/8$*. The data are as follows: for* $d = 3$*, the maximum of the set of errors* $|T(X) - Y(B(\{k_i\}, 3))|$ $(0 \le k_i < d)$ *decreases as*

$$\begin{aligned} &7.68 \cdot 10^{-5} \quad (X = 10^9), \\ &1.80 \cdot 10^{-5} \quad (X = 10^{10}), \\ &6.12 \cdot 10^{-6} \quad (X = 10^{11}). \end{aligned}$$

For

$$\begin{aligned}u(p) :=& \left(\left\{ \frac{r_1}{p} \right\}, \left\{ \frac{r_2}{p} \right\}, \left\{ \frac{\lfloor r_1^2/2 \rfloor_p}{p} \right\}, \left\{ \frac{\lfloor r_1^3/3 \rfloor_p}{p} \right\}, \left\{ \frac{\lfloor r_1^3 r_2/5 \rfloor_p}{p} \right\}, \right. \\ &\left. \left\{ \frac{\lfloor r_1 r_2/7 \rfloor_p}{p} \right\}, \left\{ \frac{\lfloor r_1^2 r_2/11 \rfloor_p}{p} \right\} \right) \in \mathfrak{D}_{pr}(f, id) \times [0,1)^5\end{aligned}$$

https://doi.org/10.3390/math14173175

instead of $v(p)$, we have a similar estimate:

$$\begin{aligned} &6.84 \cdot 10^{-5} \quad (X = 10^9),\\ &1.54 \cdot 10^{-5} \quad (X = 10^{10}),\\ &6.45 \cdot 10^{-6} \quad (X = 10^{11}). \end{aligned}$$

Here we note that $\alpha_1^2/2, \alpha_1^3/3, \alpha_1^3\alpha_2/5, \alpha_1\alpha_2/7, \alpha_1^2\alpha_2/11$ are not algebraic integers.

Here are supplementary data: For integers c_i with $|c_i| \leq 2$ except $c_1 = \cdots = c_5 = 0$, the sequence of the points

$$w(p) := \{(c_1 r_1^2 + c_2 r_1^3 + c_3 r_1^3 r_2 + c_4 r_1 r_2 + c_5 r_1^2 r_2)/p\} \in [0,1)$$

seems to be uniformly distributed on $[0,1)$. This is because for $d = 100$, there exists $X < 10^{10}$ such that the absolute value of the difference between

$$\frac{\#\{p \in M_X(f,id) \mid k/d \leq w(p) < (k+1)/d\}}{\#M_X(f,id)}$$

and $1/d$ is less than $1/(100d)$ for every $0 \leq k < d$ and c_i.

Example 4. *Let $f(x) = (x^2-2)(x^2-3)$, which is reducible. Write $\alpha_1 := \sqrt{2}, \alpha_2 := \sqrt{3}, \alpha_3 := -\alpha_2, \alpha_4 := -\alpha_1$ and $\alpha := \sqrt{2}+\sqrt{3}$. Writing $g_1(x) = (x^3-9x)/2, g_2(x) = (-x^3+11x)/2$ and $F(x) = x^4 - 10x^2 + 1$, we have $g_i(\alpha) = \alpha_i$ $(i = 1,2)$ and $F(\alpha) = 0$. Since $\mathbb{Q}(f) = \mathbb{Q}[1,\alpha_1,\alpha_2] \oplus \mathbb{Q}[\alpha_1\alpha_2]$, we consider the distribution of points $v(p) := (\{r_1/p\}, \{r_2/p\}, \{r_1r_2/p\})$. We write*

$$T(X) := \frac{\#\{p \in M_X(f,id) \mid v(p) \in \mathfrak{D}_{pr}(f,id) \times [0,1) \cap B(\{k_i\},d)\}}{\#M_X(f,id)},$$

where $\mathfrak{D}_{pr}(f,id)$ is the same as (5), $B(\{k_i\},d)$ is defined in the same way before, and

$$Y(B(\{k_i\},d)) := \frac{\mathrm{vol}(\mathfrak{D}_{pr}(f,id) \times [0,1) \cap B(\{k_i\},d))}{\mathrm{vol}(\mathfrak{D}_{pr}(f,id) \times [0,1))}.$$

As before, let us see the maximum value er in the set of $|T(X) - Y(B(\{k_i\},d)|$ where $0 \leq k_i < d$. For $d = 10$, er decreases as follows:

$$\begin{aligned} &8.48 \cdot 10^{-4} \quad (X = 10^7),\\ &3.57 \cdot 10^{-4} \quad (X = 10^8),\\ &8.11 \cdot 10^{-5} \quad (X = 10^9),\\ &2.87 \cdot 10^{-5} \quad (X = 10^{10}),\\ &9.08 \cdot 10^{-6} \quad (X = 10^{11}). \end{aligned}$$

This supports that the sequence of $v(p)$ $(p \in M(f,id))$ is uniformly distributed on $\mathfrak{D}_{pr}(f,id) \times [0,1) \cap B(\{k_i\},d)$.

The formula for $D_f(g,h)$ is the same as in Example 1.

These data appear to suggest that the set $M(f,\sigma)$ is more essential than $\mathrm{Spl}(f,\sigma)$.

The congruence conditions for local roots should be included in Conjectures 1, 2 (cf. Conjecture 3 in [6]).

3. Arrangement of Local Roots of Two Polynomials

What is the relation between the positions of the local roots of two polynomials $g(x)$ and $h(x)$? For example, let $g(x) = x^2 + x + 1, h(x) = x^2 + 2x + 2$ and $f(x) = g(x)h(x)$. Denote the local roots of $g(x), h(x)$ by s_i, t_i, respectively. The density of $p \in \mathrm{Spl}(f)$ satisfying either $s_1 < t_1 < t_2 < s_2$ or $t_1 < s_1 < s_2 < t_2$ appears to be $1/2$ in each case.

Another example: Let $g(x) = x^2 + x + 1, h(x) = x^3 + 3$ and $f(x) = g(x)h(x)$, and denote the local roots of $g(x)$ by s_i and those of $h(x)$ by t_i. Denoting the accumulation points of $s_i/p, t_i/p$ by x_i, y_i, we have $0 \le x_1 \le x_2 \le 1, 0 \le y_1 \le y_2 \le y_3 \le 1$; furthermore, $x_1 + x_2 = 1, y_1 + y_2 + y_3 = k\,(= 1, 2)$, which follow from the trivial linear relation among the roots. Therefore, we have

$$0 \le x_1 \le \frac{1}{2} \text{ and } x_2 = 1 - x_1, \tag{6}$$

$$\begin{aligned} 0 \le y_1 \le y_2,\ k - y_1 - 1 \le y_2 \le \frac{k - y_1}{2}, \\ \text{and } y_3 = k - y_1 - y_2 \text{ for } {}^{\exists}k(= 1, 2). \end{aligned} \tag{7}$$

The volume of the set $\mathfrak{D}$ of points (x_1, y_1, y_2) that satisfy (6) and (7) is $1/12$. We divide the cases as follows:

$$\begin{array}{rcll} 1 & : & s_1 < t_1, s_2 < t_1 & (\leftrightarrow 0 \le x_1 \le x_2 \le y_1 \le y_2 \le y_3 \le 1), \\ 2 & : & s_1 < t_1, t_1 < s_2 < t_2 & (\leftrightarrow 0 \le x_1 \le y_1 \le x_2 \le y_2 \le y_3 \le 1), \\ 3 & : & s_1 < t_1, t_2 < s_2 < t_3 & (\leftrightarrow 0 \le x_1 \le y_1 \le y_2 \le x_2 \le y_3 \le 1), \\ 4 & : & s_1 < t_1, t_3 < s_2 & (\leftrightarrow 0 \le x_1 \le y_1 \le y_2 \le y_3 \le x_2 \le 1), \\ 5 & : & t_1 < s_1 < t_2, s_2 < t_2 & (\leftrightarrow 0 \le y_1 \le x_1 \le x_2 \le y_2 \le y_3 \le 1), \\ 6 & : & t_1 < s_1 < t_2, t_2 < s_2 < t_3 & (\leftrightarrow 0 \le y_1 \le x_1 \le y_2 \le x_2 \le y_3 \le 1), \\ 7 & : & t_1 < s_1 < t_2, t_3 < s_2 & (\leftrightarrow 0 \le y_1 \le x_1 \le y_2 \le y_3 \le x_2 \le 1), \\ 8 & : & t_2 < s_1 < t_3, s_2 < t_3 & (\leftrightarrow 0 \le y_1 \le y_2 \le x_1 \le x_2 \le y_3 \le 1), \\ 9 & : & t_2 < s_1 < t_3, t_3 < s_2 & (\leftrightarrow 0 \le y_1 \le y_2 \le x_1 \le y_3 \le x_2 \le 1), \\ 10 & : & t_3 < s_1 & (\leftrightarrow 0 \le y_1 \le y_2 \le y_3 \le x_1 \le x_2 \le 1). \end{array}$$

The density d_i of prime numbers $p \in \mathrm{Spl}(f)$ satisfying the ith condition appears to be as follows:

i	1	2	3	4	5	6	7	8	9	10
$72 \times d_i$	1	6	12	16	9	0	12	9	6	1

We will see that the density is $2^5 3^3/72\,(= 1/\mathrm{vol}(\mathfrak{D}))$ times the volume of the three dimensional figure D defined by the inequalities in each case.

Let us consider the first case. The inequalities are $x_2 < y_1$, (6) and (7). Denote by D_k the figure defined by (6) and (7) and the inequalities in this case, i.e.,

$$\begin{aligned} D_k : 0 \le x_1 \le \frac{1}{2}, 0 \le y_1 \le y_2,\ k - y_1 - 1 \le y_2 \le \frac{k - y_1}{2}, \\ 1 - x_1 \le y_1. \end{aligned}$$

If $k = 1$, then the conditions $y_1 \le (1 - y_1)/2$ and $1/2 \le 1 - x_1 \le y_1$ imply the contradiction $1/2 \le y_1 \le 1/3$. Thus, the set D_1 is empty. The figure D_2 is defined by

$$\frac{1}{3} \le x_1 \le \frac{1}{2}\, 1 - x_1 \le y_1 \le \frac{2}{3},\ y_1 \le y_2 \le 1 - y_1/2.$$

The volume is calculated using the iterated integration $\int_{x_1} \int_{y_1} \int_{y_2} dy_2 dy_1 dx_1$, which is $1/(2^5 3^3)$. Thus, the density $d_1 = 1/72 = \mathrm{vol}(D)/\mathrm{vol}(\mathfrak{D})$. The other cases are similarly verified.

https://doi.org/10.3390/math14173175

For a general reducible polynomial $f(x) = g(x)h(x)$, there is no doubt that the density is the volume of a union of convex bodies defined by inequalities as above for any arrangement of the local roots s_i and t_j of $g(x)$ and $h(x)$.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Kitaoka, Y. Notes on the distribution of roots modulo a prime of a polynomial. *Unif. Distrib. Theory* **2017**, *12*, 91–116. [CrossRef]
2. Kitaoka, Y. Statistical distribution of roots of a polynomial modulo primes III. *Int. J. Stat. Probab.* **2018**, *7*, 115–124. [CrossRef]
3. Kitaoka, Y. Notes on the distribution of roots modulo a prime of a polynomial II. *Unif. Distrib. Theory* **2019**, *14*, 87–104. [CrossRef]
4. Kitaoka, Y. Notes on the distribution of roots modulo a prime of a polynomial III. *Unif. Distrib. Theory* **2020**, *15*, 93–104. [CrossRef]
5. Kitaoka, Y. Notes on the distribution of roots modulo a prime of a polynomial IV. *Unif. Distrib. Theory* **2023**, *18*, 9–30. [CrossRef]
6. Kitaoka, Y. Notes on the Distribution of Roots Modulo a Prime of a Polynomial V: Weyl's Criterion. *Mathematics* **2025**, *13*, 3401. [CrossRef]
7. Duke, W.; Friedlander, J.B.; Iwaniec, H. Equidistribution of roots of a quadratic congruence to prime moduli. *Ann. Math.* **1995**, *141*, 423–441. [CrossRef]
8. Tóth, Á. Roots of Quadratic congruences. *Internat. Math. Res. Not.* **2000**, *2000*, 719–739.
9. The PARI Group. *PARI/GP*, version 2.17.3; Université Bordeaux: Bordeaux, France, 2025. Available online: http://pari.math.u-bordeaux.fr/ (accessed on 27 August 2026).
10. Hadano, T.; Kitaoka, Y.; Kubota, T.; Nozaki, M. Densities of sets of primes related to decimal expansion of rational numbers. In *Number Theory, Tradition and Modernization*; Zhang, W., Tanigawa, Y., Eds.; Springer Science + Business Media, Inc.: Berlin/Heidelberg, Germany, 2006; Volume 15.
11. Kuipers, L.; Niederreiter, H. *Uniform Distribution of Sequences*; John Wiley & Sons: Hoboken, NJ, USA, 1974.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.