DE GRUYTER
OPEN

uniform distribution theory

DOI: 10.1515/udt-2017–0007
Unif. Distrib. Theory **12** (2017), no.1, 109–122

STATISTICAL DISTRIBUTION OF ROOTS OF A POLYNOMIAL MODULO PRIMES II

Yoshiyuki Kitaoka

ABSTRACT. Continuing the previous paper, we give several data on the distribution of roots modulo primes of an irreducible polynomial, and based on them, we propose problems on the distribution.

Communicated by Shigeki Akiyama

Throughout this paper, unless otherwise specified, a polynomial means a monic *irreducible* one of degree > 1 with integer coefficients, and the letter p denotes a prime number. For a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ of degree n and a prime number p, we say that $f(x)$ is fully splitting modulo p if there are integers $r_1, r_2, \ldots, r_n$ satisfying $f(x) \equiv \prod(x - r_i) \bmod p$. Throughout this paper except the final Subsection 3.2, we assume inequalities

$$0 \le r_1 \le \cdots \le r_n < p. \tag{1}$$

We note that if p is sufficiently large, (1) is equivalent to

$$0 < r_1 < \cdots < r_n < p.$$

Putting

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

for a positive number X and $\mathrm{Spl}(f) := \mathrm{Spl}(f, \infty)$, we know that $\mathrm{Spl}(f)$ is an infinite set and the density theorem due to Chebotarev

$$\lim_{X\to\infty} \frac{\#\mathrm{Spl}(f, X)}{\#\{p \le X\}} = \frac{1}{[\mathbb{Q}(f) : \mathbb{Q}]}$$

holds, where $\mathbb{Q}$ means the rational number field and $\mathbb{Q}(f)$ is a finite Galois extension field of $\mathbb{Q}$ generated by all roots of $f(x)$ ([3]). The author studied statistical distribution of local roots r_i for $p \in \mathrm{Spl}(f)$ in previous papers, and

2010 Mathematics Subject Classification: 11K.
Keywords: distribution, polynomial.

proposed the following problem : For a real function $t = t(x_1, \dots, x_n)$, study a density vector $\mathrm{Pr}(f, t, X) := [\dots, F_0, F_1, \dots]$ defined by

$$F_k := \frac{\#\{p \in \mathrm{Spl}(f, X) \mid \lceil t(r_1/p, \dots, r_n/p) \rceil = k\}}{\#\mathrm{Spl}(f, X)},$$

where $\lceil x \rceil$ is an integer defined by $x \leq \lceil x \rceil < x + 1$.
Here, we take up a function $t_j(x_1, \dots, x_n) = 2x_j$ $(1 \leq j \leq n)$ with the condition $k = 1$. The condition $\lceil t_j(r_1/p, \dots, r_n/p) \rceil = 1$ is obviously equivalent to $0 < r_j \leq p/2$. Let us define the following frequency $\mathrm{Pr}_D(f, X)$ for a domain $D \subset [0, 1)^n$,

$$\begin{aligned} \mathrm{Pr}_D(f, X) \quad &:= \frac{\#\{p \in \mathrm{Spl}(f, X) \mid (r_1/p, \dots, r_n/p) \in D\}}{\#\mathrm{Spl}(f, X)}, \\ \mathrm{Pr}_D(f) \quad &:= \lim_{X \to \infty} \mathrm{Pr}_D(f, X). \end{aligned} \tag{2}$$

Although the existence of the limit is not proved, the author has no data to deny it[1], and assume the existence hereafter.

In this paper, we are mainly concerned with making data on the special domain

$$D_j := \{(x_1, \dots, x_n) \in [0, 1]^n \mid x_j < 1/2\},$$

and we put

$$\mathrm{Pr}^*(f, X) := [\mathrm{Pr}_{D_1}(f, X), \dots, \mathrm{Pr}_{D_n}(f, X)],$$
$$\mathrm{Pr}^*(f) := \lim_{X \to \infty} \mathrm{Pr}^*(f, X) = [\mathrm{Pr}_{D_1}(f), \dots, \mathrm{Pr}_{D_n}(f)].$$

Based on data, we give questions in the last section.

1. Propositions

The followings are a few proved small results.

Theorem 1. For a domain $D \subset [0, 1]^n$, we put

$$D^\vee := \{(1 - x_n, \dots, 1 - x_1) \mid (x_1, \dots, x_n) \in D\}.$$

Then we have

$$\mathrm{Pr}_D\bigl(f(x)\bigr) = \mathrm{Pr}_{D^\vee}\bigl((-1)^n f(-x)\bigr).$$

[1]The data were obtained using pari/gp. The PARI Group, PARI/GP version `2.8.0`, Bordeaux, 2014, http://pari.math.u-bordeaux.fr/.

Proof. It is obvious that $\mathrm{Spl}\big(f(x)\big) = \mathrm{Spl}\big((-1)^n f(-x)\big)$. Assume that $f(x) \equiv \prod(x - r_i) \bmod p$ with the order (1) for a prime $p \in \mathrm{Spl}(f)$; then we have $(-1)^n f(-x) \equiv \prod(x+r_i) \equiv \prod(x-R_i) \bmod p$ for $0 < R_1 := p-r_n < \cdots < R_n := p-r_1 < p$ for a sufficiently large prime $p \in \mathrm{Spl}(f)$, hence $(r_1/p, \ldots, r_n/p) \in D$ is equivalent to $(R_1/p, \ldots, R_n/p) = (1 - r_n/p, \ldots, 1 - r_1/p) \in D^{\vee}$, which implies the statement. □

Theorem 2. Let a domain D_j be as before. We have, for $1 \le j \le n$

$$\mathrm{Pr}_{D_j}\big((-1)^n f\big(-x\big)\big) + \mathrm{Pr}_{D_{n+1-j}}\big(f(x)\big) = 1.$$

If $\mathrm{Pr}_{D_j}\big((-1)^n f(-x)\big) = \mathrm{Pr}_{D_j}\big(f(x)\big)$ holds, then $\mathrm{Pr}_{D_j}(f) + \mathrm{Pr}_{D_{n+1-j}}(f) = 1$.

Proof. Using notations r_j, R_j in the previous proof, we see easily that

$$\begin{aligned} &\#\big\{p \in \mathrm{Spl}\big((-1)^n f(-x), X\big) \mid R_j < p/2\big\} \\ &= \#\left\{p \in \mathrm{Spl}(f, X) \mid r_{n+1-j} > p/2\right\} \\ &= \#\mathrm{Spl}(f, X) - \#\left\{p \in \mathrm{Spl}(f, X) \mid r_{n+1-j} < p/2\right\}, \end{aligned}$$

which implies $\mathrm{Pr}_{D_j}\big((-1)^n f(-x)\big) = 1 - \mathrm{Pr}_{D_{n+1-j}}\big(f(x)\big)$. □

The case of $f(x) = g\big(h(x)\big)$ for a quadratic polynomial h is easy:

Theorem 3. Let a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be of form $g\big(h(x)\big)$ for a quadratic polynomial h. Then the limit $\mathrm{Pr}_{D_j}(f)$ exists and we have

$$\mathrm{Pr}_{D_j}(f) = \begin{cases} 1 & \text{if} \quad j \le n/2, \\ 0 & \text{if} \quad j > n/2. \end{cases}$$

Proof. We note that n is an even integer. As is shown in the proof of Proposition 2 of [1], we have $r_j + r_{n+1-j} = p - 2a_{n-1}/n$ under the assumption (1) if p is sufficiently large. Suppose $j \le n/2$; then $j < n + 1 - j$ implies

$$2r_j < r_j + r_{n+1-j} = p - 2a_{n-1}/n.$$

Assume that there are infinitely many primes p such that $2r_j > p$; then for such infinitely many primes p, we have $0 < 2r_j - p < -2a_{n-1}/n$. Hence for an integer R with $0 < R < -2a_{n-1}/n$, there are infinitely many primes p such that $2r_j - p = R$. Put $F(x) := 2^n f(x/2)$, which is a monic irreducible polynomial with integer coefficients. It is easy to see that $F(R) \equiv F(2r_j) = 2^n f(r_j) \equiv 0 \bmod p$ for infinitely many primes, which implies a contradiction $F(R) = 0$. Thus, $2r_j \le p$ holds if p is sufficiently large, hence $\mathrm{Pr}_{D_j}(f) = 1$.

Next, suppose that there are infinitely many primes p satisfying $r_j < p/2$ for $j \ge n/2 + 1$; then applying the above inequality to $n + 1 - j\,(\le n/2)$ instead of j, we have $2r_{n+1-j} < p - 2a_{n-1}/n$, hence $-2a_{n-1}/n > 2r_{n+1-j} - p$.

On the other hand, $r_{n+1-j} = p - 2a_{n-1}/n - r_j$ implies $2r_{n+1-j} - p = p - 2r_j - 4a_{n-1}/n > -4a_{n-1}/n$. They imply that there is an integer R satisfying that $-2a_{n-1}/n > R = 2r_{n+1-j} - p > -4a_{n-1}/n$ for infinitely many primes p. Similarly to the former, it implies a contradiction, which implies that the number of primes p satisfying $r_j < p/2$ is finite, i.e., $\mathrm{Pr}_{D_j}(f) = 0$. □

2. Numerical data

First, let us explain how to guess conjectural densities $\mathrm{Pr}_{D_j}(f)$ from an approximation $\mathrm{Pr}_{D_j}(f, 10^{10})$. We adopt the following double checking method. Let $\alpha = a/b$ be a rational number and suppose that a sequence of rational numbers c_n tends to α. We note that both $|c_n b - r(c_n b)|$ and $|c_n - r(c_n b)/b|$ tend to 0 as $n \to \infty$, where $r(x)$ is the nearest integer to x. For an approximate value $c = \mathrm{Pr}_{D_j}(f, 10^{10})$ to α, we take integers b_i such that b_1 (resp. b_2) gives the minimal value of $|cb_1 - r(cb_1)|$ (resp. $|c - r(cb_2)/b_2|$) to the extent of $1 \le b_i \le 1000$. If $b_1 = b_2$, we may suppose $\alpha = r(cb_1)/b_1$. In the following data, $\mathrm{Pr}_{D_j}\big((-1)^n f(-x)\big) = \mathrm{Pr}_{D_j}(f)$ seems to hold.

(1) The case of $n = 3$. For $f_3 := x^3 + 2$, a conjecture is

$$\mathrm{Pr}_3 := \mathrm{Pr}^*(f_3) = [7/8, 1/2, 1/8] = [7, 4, 1]/8. \tag{3}$$

The original data are

$$\mathrm{Pr}^*(f_3, 10^{10}) = [66357392/75839979, 12639203/25279993, 9478153/75839979]$$

and

$$\mathrm{Pr}_3 - \mathrm{Pr}^*(f_3, 10^{10}) = [3.4146, 3.1388, 2.4319]/10^5.$$

We checked the following : For any irreducible polynomial $f(x) = x^3 + a_2x^2 + a_1x + a_0$ with $|a_i| \le 5$, there is a large number X such that, putting $\mathrm{Pr}_3[j] = a/b\ \big((a,b) = 1\big)$,

$$r\big(mb \cdot \mathrm{Pr}_{D_j}\big(f, X\big)\big) = ma \text{ with } m = 10 \tag{4}$$

for $j = 1, \ldots, n$. The larger m is, the more precise the approximation is. The density $\mathrm{Pr}^*(f)$ is independent of each polynomial f in the case of $\deg(f) = 3$, which implies $\sum_i \mathrm{Pr}_{D_i}(f) = n/2 = 3/2$ by Theorem 2.

Let us give remarks. Since $r_1 + r_2 + r_3 + a_2 = C_p(f)p$ holds for an integer $C_p(f) = 1, 2$, the condition $r_2 < r_3 < p$ implies $r_2 < r_3 = C_p(f)p - r_1 - r_2 - a_2 < p$. It is not difficult to see that we have $C_p(f) = \lceil r_1/p + r_2/p \rceil$ and a stronger inequality $r_2 < C_p(f)p - r_1 - r_2 < p$ if p is sufficiently large. Taking account of it and neglecting a term a_2 by $a_2/p \to 0$ $(p \to \infty)$, we suppose that for $x_i := r_i/p$, $x_1 + x_2 + x_3 = k$ is an integer 1 or 2, and consider the region defined by

$$\begin{aligned}\mathfrak{D} &:= \bigcup_{k=1,2} \{(x_1, x_2) \mid 0 < x_1 < x_2 < x_3 := k - (x_1 + x_2) < 1\} \\ &= \{(x_1, x_2) \mid 0 < x_1 < x_2 < x_3 := \lceil x_1 + x_2 \rceil - (x_1 + x_2)\}.\end{aligned}$$

Then the area of $\mathfrak{D}$ is $1/6$, and the area of the intersection of $\mathfrak{D}$ and $x_j < 1/2$ is $1/6$ times

$$7/8, 4/8, 1/8 \text{ according to } j = 1, 2, 3 \text{ (cf. (3))}.$$

More generally, for a region D given by

$$\left\{(x_1, x_2) \mid 0 < x_1 < x_2 < x_3 := \lceil x_1 + x_2 \rceil - (x_1 + x_2), A_i \le x_i \le B_i\ ({}^\forall i)\right\},$$

the area of D is likely to be $1/6$ (= the area of $\mathfrak{D}$) times the density of p satisfying $A_i \le r_i/p \le B_i$ $(i = 1, 2, 3)$. For example, for $A_1 = A_2 = A_3 = 0$, $B_1 = 1/3, B_2 = 1, B_3 = 1$ $(area = 1/9)$, or $B_1 = 1/4, B_2 = 1/3, B_3 = 1/2$ $(area = 1/288)$, numerical data match with it. These suggest that the sequence of points $(r_1/p, r_2/p)$ is uniformly distributed on $\mathfrak{D}$ in some sense (cf. (9)).

Hereafter we omit the original data.

(2) The case of $n = 4$.

For $f_4 := x^4 + x^3 + x^2 + x + 1$, a conjecture is

$$\mathrm{Pr}_4 := \mathrm{Pr}^*(f_4) = [11, 9, 3, 1]/12. \tag{5}$$

$$\mathrm{Pr}_4 - \mathrm{Pr}^*(f_4, 10^{10}) = [2.3298, -1.8589, 2.2668, 3.1439]/10^5.$$

We checked the following : For any irreducible and indecomposable[2] polynomial $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ with $|a_i| \le 5$, there is a large number X such that an equation similar to (4) for Pr_4 instead of Pr_3 holds for $j = 1, \ldots, n$.

(3) The case of $n = 5$.

For $f_5 := x^5 - 10x^3 + 5x^2 + 10x + 1$, which defines a subfield of degree 5 in a cyclotomic field $\mathbb{Q}\big(\exp(2\pi i/25)\big)$, we conjecture

$$\mathrm{Pr}_5 := \mathrm{Pr}^*(f_5) = [31, 26, 16, 6, 1]/32. \tag{6}$$

$$\mathrm{Pr}_5 - \mathrm{Pr}^*(f_5, 10^{10}) = [-2.6026, -5.9824, -1.7630, -2.7167, -0.65312]/10^5.$$

[2]A polynomial $f(x)$ is called indecomposable unless $f(x)$ is of the form $g\big(h(x)\big)$ with $\deg h \ne 1, \deg f$.

We checked the following : For any irreducible polynomial $f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ with $|a_i| \le 3$, there is a large number X such that an equation similar to (4) holds for $j = 1, \dots, n$ for Pr_5 instead of Pr_3.

(4) The case of $n = 6$. Putting

$$\begin{cases} f_{6.1}(x) := x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & \text{(Ex.1 in [1])}, \\ f_{6.2n}(x) := x^6 - 2x^5 + 11x^4 + 6x^3 + 16x^2 + 122x + 127 & \text{(Ex.2 ibid.)}, \\ f_{6.2z}(x) := x^6 - 2x^3 + 9x^2 + 6x + 2 & \text{(Ex.3 ibid.)}, \\ f_{6.2p}(x) := f_{6.2n}(-x), & \\ f_{6.3}(x) := x^6 - 9x^5 - 3x^4 + 139x^3 + 93x^2 - 627x + 1289 & \text{(Ex.4 ibid.)}, \end{cases}$$

we conjecture

$$\mathrm{Pr}^*(f) = \begin{cases} [947, 845, 650, 310, 115, 13]/960 & \text{for } f = f_{6.1}, \\ [63, 57, 42, 22, 7, 1]/64 & \text{for } f = f_{6.2c}\ (c = n, z, p), \\ [35, 32, 26, 10, 4, 1]/36 & \text{for } f = f_{6.3}, \end{cases} \tag{7}$$

and

$$\mathrm{Pr}^*(f) - \mathrm{Pr}^*(f, X) =$$

$$\begin{cases} [-0.33, -1.37, -0.54, 1.03, -1.06, -0.29]/10^6 & \text{for } f = f_{6.1},\ X = 10^{13}, \\ [1.71, 2.38, -4.32, -8.71, 1.78, 3.29]/10^5 & \text{for } f = f_{6.2n}, X = 10^{10}, \\ [0.81, 0.13, 3.73, -4.08, -6.66, -1.91]/10^5 & \text{for } f = f_{6.2z}, X = 10^{10}, \\ [-0.74, -0.83, 0.02, 0.88, 6.34, 1.91]/10^5 & \text{for } f = f_{6.3},\ X = 10^{10}. \end{cases}$$

Although polynomials $f_{6.1}, f_{6.2n}, f_{6.3}$ define the same field $\mathbb{Q}\big(\exp(2\pi i/7)\big)$, that is their $\mathrm{Spl}(f)$ are equal, the speed of convergence for $f_{6.1}$ is slow compared to other two polynomials. The author does not know the reason.

First, we define a type number $1, 2, 3$ to a polynomial f with a root α as follows :

The type number of f is 2 if $\mathbb{Q}(\alpha)$ contains a quadratic subfield M_2 such that the trace of α to M_2 is rational.

The type number of f is 3 if $\mathbb{Q}(\alpha)$ contains a cubic subfield M_3 such that the discriminant D of the monic minimal quadratic polynomial $g_2(x)$ of α over M_3 is rational.

Otherwise, the type number is 1.

There are linear (resp. quadratic) relations among local roots r_i in (1) if the type number is 2 (resp. 3), and for a polynomial $f(x) = g\big(h(x)\big)$ with a cubic polynomial $h(x)$, the type number of f is 2 (cf. [1]).

It is not difficult to see that type numbers 2 and 3 are incompatible.

We checked the following : Let a polynomial BP be $f_{6.1}$ or $f_{6.2z}$, and α a root of it. We consider a polynomial f whose root is $\beta := \sum_{i=0}^{5} c_i\alpha^i$ with integers c_i $|c_i| \leq 1$. We skip reducible polynomials and decomposable ones of $f(x) = g\big(h(x)\big)$ with $\deg h = 2$. There is a large number X for which (4) is valid with $m = 1$ instead of $m = 10$ for the density (7) corresponding to the type of f.

(5) The case of $n = 7$. We checked for any irreducible polynomial $f(x) = x^7 + a_6x^6 + \cdots + a_0$ with $|a_i| \leq 1$ there is a large number X such that (4) with $m = 1$ holds for $\Pr^*(f)$ given by

$$[127, 120, 99, 64, 29, 8, 1]/128. \tag{8}$$

3. Remarks

3.1.

First, put

$$\hat{\mathfrak{D}}_n := \left\{(x_1, \ldots, x_n) \mid 0 < x_1 < \cdots < x_n < 1, \sum_{i=1}^{n} x_i \in \mathbb{Z}\right\},$$

$$\mathfrak{D}_n := \left\{(x_1, \ldots, x_{n-1}) \mid 0 < x_1 < \cdots < x_{n-1} < x_n := \left\lceil \sum_{i=1}^{n-1} x_i \right\rceil - \sum_{i=1}^{n-1} x_i \right\}$$

$$= \left\{(x_1, \ldots, x_{n-1}) \mid 0 < x_1 < \cdots < x_{n-1} < {}^{\exists}x_n < 1, \sum_{i=1}^{n} x_i \in \mathbb{Z}\right\}.$$

$\mathfrak{D}_n$ is a projection of $\hat{\mathfrak{D}}_n$, and the volume seems to be $1/n!$. We note that points $(r_1/p, \ldots, r_{n-1}/p)$ are in $\mathfrak{D}_n$ if p is sufficiently large, and let us consider the following property, which is a kind of uniformity:

$$\begin{aligned} \Pr_D(f) &= \frac{\mathrm{vol}(\{\mathrm{x} \in \mathfrak{D}_\mathrm{n} \mid \hat{\mathrm{x}} \in \overline{D}\})}{vol(\mathfrak{D}_n)} \\ &= \frac{\mathrm{vol}(\overline{D} \cap \hat{\mathfrak{D}}_\mathrm{n}\})}{\mathrm{vol}(\hat{\mathfrak{D}}_\mathrm{n})} \end{aligned} \tag{9}$$

for a domain $D \subset [0, 1)^n$. Here, $\Pr_D(f)$ is defined at (2), and we put, for $\boldsymbol{x} = (x_1, \ldots, x_{n-1})$,

$$\hat{\boldsymbol{x}} = (x_1, \ldots, x_{n-1}, x_n) \quad \text{for } x_n := \left\lceil \sum_{i=1}^{n-1} x_i \right\rceil - \sum_{i=1}^{n-1} x_i.$$

The first equality in (9) is an expectation, but the second equality is definite, since the angle of two hyperplanes T_c defined by $\sum_{i=1}^{n} x_i = c$ and H_n defined by $x_n = 0$ is $\arccos(1/\sqrt{n})$ independent of c. Theoretically the second is better, but numerically the first is easier to calculate.

For a polynomial $f = x^n + a_{n-1}x^{n-1} + \dots$, we put $tr(f) := -a_{n-1}$, and we note that the equation $r_1+\dots+r_n-tr(f) \equiv 0 \bmod p$ implies $r_1/p+\dots+r_n/p = tr(f)/p+C_p(f)$ for an integer $C_p(f)$. If $\mathrm{Pr}_D(f) \neq 0$ holds, then there are infinitely many primes $p \in \mathrm{Spl}(f)$ such that $(r_1/p,\dots,r_n/p) \in D$, whose accumulation points are in $\hat{\mathfrak{D}}_n$ by $r_1/p+\dots+r_n/p = C_p(f)+tr(f)/p$. Hence we have $\overline{D}\cap\hat{\mathfrak{D}}_n \neq \emptyset$ if $\mathrm{Pr}_D(f) \neq 0$. In other words, $\overline{D}\cap\hat{\mathfrak{D}}_n = \emptyset$ implies $\mathrm{Pr}_D(f) = 0$, therefore (9) is valid if $\overline{D}\cap\hat{\mathfrak{D}}_n = \emptyset$. It is inappropriate to put the restriction $D \subset \hat{\mathfrak{D}}_n$ from the beginning, because it implies $\mathrm{Pr}_D(f) = 0$ in the case of $tr(f) \neq 0$.

Suppose that $\deg f$ is odd prime: We expect

$$\mathrm{Pr}^*(f) = [a(n,1),\dots,a(n,n)]/a(n,0),$$

where

$$a(n,m) := \sum_{j=m}^{n}\binom{n}{j} = \sum_{J=0}^{n-m}\binom{n}{J} \quad (0 \le m \le n),$$

and $a(n,m) + a(n,n-m+1) = 2^n = a(n,0)$ $(1 \le m \le n)$ is easy to see (cf. Theorem 2). Relevant values are

$$[a(n,0),\dots,a(n,n)] = \begin{cases} [8,7,4,1] & (n=3),\\ [16,15,11,5,1] & (n=4),\\ [32,31,26,16,6,1] & (n=5),\\ [64,63,57,42,22,7,1] & (n=6),\\ [128,127,120,99,64,29,8,1] & (n=7). \end{cases}$$

The values in the case of $n = 3,5,7$ match with (3), (6), (8), however for $n = 4$, it does not match with (5), and for $n = 6$, it matches with $f_{6.2*}$, for which the uniformity (9) fails as we will see later.

Let D_j be as before. In case of $n = 3$, the equation (9) for D_j is consistent with Pr_3 as noted, and by approximating the volume by the Monte Carlo method in the case of $n = 5,7$, the equation (9) for D_j seems to be true.
Moreover, in case of $n = 5$, for any subset $S \subset \{1,2,3,4,5\}$ with $2 \le \#S \le 4$, we gave conjectural densities $\mathrm{Pr}_k(f,S)$ after proposition 4 in [1], which correspond to the region defined by $D_n(S,k) := \{(x_1,\dots,x_n) \in [0,1)^n \mid \lceil\sum_{i\in S} x_i\rceil = k\}$. They also support (9), as far as we approximate the volume of the region by the M. C. method.

In case of $n = 4$, after calculating volumes exactly, we can check that the conjecture Pr_4 is compatible with (9), and also conjectural densities $\mathrm{Pr}_k(f,S)$ after proposition 4 in [1] corresponding to the region $D_n(S,k)$ match with (9) by approximating volumes by the M. C. method.

In case of $n = 6$ and $f = f_{6.1}$, (7) and $\mathrm{Pr}_k(f, S)$ in the third section of [1] are consistent with (9) by approximating volumes by the M. C. method, but there is no information on the values of the density in [2] unfortunately.

3.2.

Let a polynomial $f(x)$ be of degree n and put $K := \mathbb{Q}(\alpha)$, where α is a root of $f(x)$. Let us see that an existence of a proper subfield of K may imply relations among local roots, which is a generalization of proposition 5 in [1] as follows.

Denote the ring of integers of K by O_K and prime ideals lying above p by $\mathfrak{P}_i$. Suppose that $p \in \mathrm{Spl}(f)$ is sufficiently large and $r_1, \ldots, r_n$ are roots of $f(x) \bmod p$, where we do not assume inequalities (1); then we have the prime ideal decomposition of $p : pO_K = \mathfrak{P}_1 \cdots \mathfrak{P}_n$ and we may suppose that, by renumbering

$$\mathfrak{P}_i = (\alpha - r_i)O_K + pO_K \text{ and } O_K/pO_K \cong O_K/\mathfrak{P}_1 \oplus \cdots \oplus O_K/\mathfrak{P}_n, \tag{10}$$

in particular $\alpha \equiv r_i \bmod \mathfrak{P}_i$. The isomorphism in (10) is given by

$$\beta \bmod pO_K \mapsto (\beta \bmod \mathfrak{P}_1, \ldots, \beta \bmod \mathfrak{P}_n)$$

and

$$O_K/\mathfrak{P}_i \cong \mathbb{Z}/p\mathbb{Z}.$$

Let F be a proper subfield of K and $m := [F : \mathbb{Q}]$, $k := n/m$, and we renumber roots r_i and ideals $\mathfrak{P}_i$ as follows :

$$\begin{aligned} pO_F &= \mathfrak{p}_1 \cdots \mathfrak{p}_m, \\ \mathfrak{p}_i O_K &= \mathfrak{P}_{i,1} \ldots \mathfrak{P}_{i,k} \quad (1 \le i \le m), \\ \alpha &\equiv r_{i,j} \bmod \mathfrak{P}_{i,j} \quad (1 \le i \le m, 1 \le j \le k). \end{aligned}$$

Let $g(x)$ be the monic minimal polynomial of α over F, whose degree is k; then $g(\alpha) = 0$ implies $g(r_{i,j}) \equiv 0 \bmod \mathfrak{P}_{i,j}$, i.e., $g(r_{i,j}) \in \mathfrak{P}_{i,j} \cap F = \mathfrak{p}_i$ $(1 \le j \le k)$, hence

$$g(x) \equiv \prod_{1 \le j \le k} (x - r_{i,j}) \bmod \mathfrak{p}_i \quad (1 \le i \le m).$$

If $tr(g)$ is a rational integer, then we have

$$tr(g) \equiv \sum_{j=1}^{k} r_{i,j} \bmod p \qquad (1 \le i \le m),$$

which implies

$$\sum_{j=1}^{k} r_{i,j}/p - \sum_{j=1}^{k} r_{1,j}/p \in \mathbb{Z} \qquad (2 \le i \le m).$$

hence, for a certain labeling of $x_1, \dots, x_n$ as $x_{i,j}$ ($1 \le i \le m, 1 \le j \le k$), a point $(r_1/p, \dots, r_n/p)$ is on a lower dimensional set

$$\left\{(x_1, \dots, x_n) \Big| \sum_{j=1}^{k} x_{i,j} - \sum_{j=1}^{k} x_{1,j} \in \mathbb{Z} \text{ for } 2 \le i \le m\right\}.$$

Hence the uniformity (9) breaks down (cf. Example 1 below).

If $g(x)$ is quadratic and the discriminant is a rational integer D, then we have $(r_{i,1} - r_{i,2})^2 \equiv D \bmod p$, which implies $r_{i,1} - r_{i,2} \equiv \pm(r_{1,1} - r_{1,2}) \bmod p$ ($2 \le i \le m$), hence

$$(r_{i,1}/p - r_{i,2}/p) \pm (r_{1,1}/p - r_{1,2}/p) \in \mathbb{Z} \quad (2 \le i \le m).$$

Similarly to the above, a point $(r_1/p, \dots, r_n/p)$ is on a lower dimensional set defined by a linear form, and the uniformity (9) breaks down (cf. Example 2 below).

Suppose that there are subfields F_1, F_2 of K such that $\mathbb{Q} \subset F_1 \subset F_2 \subset K$ and $g^{(i)}(x)$ is the minimal polynomial of α over F_i. Then $g^{(1)}$ is divisible by $g^{(2)}$ over F_2 by $g^{(1)}(\alpha) = g^{(2)}(\alpha) = 0$, and put $d_i = \deg g^{(i)}$. Renumber roots r_i and prime ideals as

$$pO_{F_1} = \prod_{i=1}^{[F_1:\mathbb{Q}]} \mathfrak{p}_i^{(1)}, \qquad \mathfrak{p}_i^{(1)} O_{F_2} = \prod_{j=1}^{[F_2:F_1]} \mathfrak{p}_{i,j}^{(2)},$$

$$g^{(1)}(x) \equiv \prod_{k=1}^{d_1} (x - r_{i,k}) \bmod \mathfrak{p}_i^{(1)} \qquad (1 \le i \le [F_1 : \mathbb{Q}]),$$

$$g^{(2)}(x) \equiv \prod_{k=1}^{d_2} (x - r_{i,k+(j-1)d_2}) \bmod \mathfrak{p}_{i,j}^{(2)} \qquad (1 \le j \le [F_2 : F_1]).$$

Suppose that $tr(g^{(2)}) \in F_1$ and $tr(g^{(2)}) = m \cdot tr(g^{(1)})$ ($m \in \mathbb{Z}$) hold; then $tr(g^{(2)}) \equiv \sum_{k=1}^{d_2} r_{i,k+(j-1)d_2} \bmod \mathfrak{p}_{i,j}^{(2)}$ and the condition $tr(g^{(2)}) \in F_1$ imply $tr(g^{(2)}) \equiv \sum_{k=1}^{d_2} r_{i,k+(j-1)d_2} \bmod \mathfrak{p}_i^{(1)}$. Now the condition $tr(g^{(2)}) = m \cdot tr(g^{(1)})$ implies

$$tr(g^{(2)}) \equiv \sum_{k=1}^{d_2} r_{i,k+(j-1)d_2} \equiv m \sum_{k=1}^{d_1} r_{i,k} \bmod \mathfrak{p}_i^{(1)}.$$

Therefore we have $\sum_{k=1}^{d_2} r_{i,k+(j-1)d_2} - m \sum_{k=1}^{d_1} r_{i,k} \equiv 0 \bmod p$, i.e.,

$$\sum_{k=1}^{d_2} r_{i,k+(j-1)d_2}/p - m \sum_{k=1}^{d_1} r_{i,k}/p \in \mathbb{Z} \quad (1 \le i \le [F_1 : \mathbb{Q}]),$$

Hence a point $(r_1/p, \dots, r_n/p)$ is on a lower dimensional set

$$\Big\{(x_1, \dots, x_n) \Big| \sum_{k=1}^{d_2} x_{i,k+(j-1)d_2} - m \sum_{k=1}^{d_1} x_{i,k} \in \mathbb{Z} \ ({}^\forall i, j)\Big\}$$

for an appropriate labeling $\{x_1, \dots, x_n\} = \{x_{i,j} \mid i, j\}$. This case occurs for a polynomial of degree 8.

For a polynomial $f = x^8 - 72x^7 + 1816x^6 - 19584x^5 + 94320x^4 - 59904x^3 - 1664x^2 - 69120x + 95488$, put $K = \mathbb{Q}(\alpha)$ for a root α, which is a Galois extension of $\mathbb{Q}$. K contains three quadratic subfields $F_1\big(\cong \mathbb{Q}(\sqrt{-1})\big), F_2\big(\cong \mathbb{Q}(\sqrt{3})\big), F_3\big(\cong \mathbb{Q}(\sqrt{-3})\big)$ and five quartic subfields $F_4\big(\cong \mathbb{Q}(\sqrt{-1}, \sqrt{3})\big), F_5, F_6, F_7, F_8$, where F_5, F_6 (resp. F_7, F_8) contain $\mathbb{Q}(\sqrt{3})$ (resp. $\mathbb{Q}(\sqrt{-3})$. Fields $F_5 \cong F_6$ (resp. $F_7 \cong F_8$) are defined by a polynomial $x^4 - 2x^3 - 2x + 1$ (resp. $x^4 - 3x^2 + 3$). Let a polynomial g_i be the minimal polynomial of α over F_i, and let α_i be the complex roots of f with $\alpha_1 = \alpha$ and

$$\begin{aligned}
g_1(x) &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_7)(x - \alpha_8), \\
g_2(x) &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4), \\
g_3(x) &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_5)(x - \alpha_6), \\
g_4(x) &= (x - \alpha_1)(x - \alpha_2), \\
g_5(x) &= (x - \alpha_1)(x - \alpha_3), \\
g_6(x) &= (x - \alpha_1)(x - \alpha_4), \\
g_7(x) &= (x - \alpha_1)(x - \alpha_5), \\
g_8(x) &= (x - \alpha_1)(x - \alpha_6).
\end{aligned}$$

Then for any prime $p \in \mathrm{Spl}(f)$, $g_i(x)$ is congruent to a polynomial replaced a complex root α_j by a local root r_j without (1) modulo the prime ideal of F_i below a fixed prime ideal of K above p, and we have linear relations

$$\begin{aligned}
2(-r_1 + r_2) + r_3 - r_4 - 2(r_5 - r_6) - \delta(r_7 - r_8) &\equiv 0 \bmod p, \\
-r_1 + r_2 + 2(r_3 - r_4) + (r_5 - r_6) + 2\delta(r_7 - r_8) &\equiv 0 \bmod p,
\end{aligned}$$

hence the uniformity (9) breaks down. The linear relations come from global identities of roots of f:

$$\begin{aligned}
2(-\alpha_1 + \alpha_2) + \alpha_3 - \alpha_4 - 2(\alpha_5 - \alpha_6) + \alpha_7 - \alpha_8 &= 0, \\
-\alpha_1 + \alpha_2 + 2(\alpha_3 - \alpha_4) + \alpha_5 - \alpha_6 - 2(\alpha_7 - \alpha_8) &= 0.
\end{aligned}$$

In the above, $\delta = \pm 1$ which depends on p. The sign ± 1 comes from the ambiguity of the choice of r_7, r_8. It seems to be equi-distributed under the condition $r_7 < r_8$.

Quite similarly to proposition 4 in [1], we can show : If local roots r_i without restriction (1) for infinitely many primes $p \in \mathrm{Spl}(f)$ satisfy $h(r_1, \ldots, r_n) \equiv 0 \bmod p$ for some polynomial with integer coefficients, there is a numbering $\alpha_1, \ldots, \alpha_n$ of complex roots of f satisfying $h(\alpha_1, \ldots, \alpha_n) = 0$.

For what kind of a region or a polynomial h above the uniformity (9) breaks down? One working hypothesis is that the above polynomial h is only a linear form if the uniformity (9) breaks down. If there is a relation $\sum m_i\alpha_i = m$ $(m_i, m \in \mathbb{Z})$, then accumulation points of $(r_1/p, \ldots, r_n/p)$ satisfies a relation $\sum m_i x_{\sigma(i)} = 0$ for a permutation σ dependent on the ordering of r_i. How can one find out a deformation from the uniformity?

Example 1. Polynomials $f_{6.2z}, f_{6.2n}$ have the following decomposition over $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-7})$, respectively.

$$\begin{aligned} f_{6.2z} &= (x^3 - 3\sqrt{-1}x - \sqrt{-1} - 1)(x^3 + 3\sqrt{-1}x + \sqrt{-1} - 1), \\ f_{6.2n} &= (x^3 - x^2 + (5 - \sqrt{-7})x + 8 - 3\sqrt{-7}) \\ &\quad \times (x^3 - x^2 + (5 + \sqrt{-7})x + 8 + 3\sqrt{-7}). \end{aligned}$$

As a numerical example, $\mathrm{Pr}_D(f_{6.2z})$ takes a non-zero value 10/144 for a lower dimensional set $D := \{(x_1, ..., x_6) \in [0, 1)^6 \mid x_1 + x_2 + x_3 = 1, x_4 + x_5 + x_6 = 2\}$. But, $\mathrm{Pr}_D(f) = 0$ holds for $f = f_{6.2n}, f_{6.2p}$, and putting $D_w := \{(x_1, ..., x_6) \in [0, 1)^6 \mid |x_1 + x_2 + x_3 - 1| < w, |x_4 + x_5 + x_6 - 2| < w\}$, we have

$$\mathrm{Pr}_{D_w}(f, 10^8) = \begin{cases} 0.1483 & (w = 0.1), \\ 0.0764 & (w = 0.01), \\ 0.0703 & (w = 0.001), \\ 0.0698 & (w = 0.0001). \end{cases}$$

These may suggest $\lim_{w\to 0} \mathrm{Pr}_{D_w}(f) = 10/144 = 0.069\dot{4}$.

Example 2. Let us consider a polynomial $f = f_{6.3}$. It decomposes over a field $F := \mathbb{Q}(\beta)$ defined by $\beta^3 - 9\beta^2 - 57\beta + 169 = 0$ as follows:

$$\begin{aligned} f_{6.3} =&(x^2 - \beta x + \beta^2/4 + 7/4) \\ &\times \left(x^2 + (-\beta^2/6 + 5\beta/3 + 17/6)x + \beta^2/6 - 19\beta/6 + 50/3\right) \\ &\times \left(x^2 + (\beta^2/6 - 2\beta/3 - 71/6)x - 5\beta^2/12 + 19\beta/6 + 427/12\right). \end{aligned}$$

The discriminant of each factor is -7.

Example 3. We use notations $g, \mathfrak{p}_i, r_{i,j}$ at the beginning of this subsection. Let $V(x_1, \ldots, x_k)$ be a polynomial over $\mathbb{Z}$ in $x_1, \ldots, x_k$ which vanishes at a point $(g_{k-1}, \ldots, g_0)$, putting $g(x) = x^k + g_{k-1}x^{k-1} + \cdots + g_0$. Such a polynomial exists, since coefficients of $g(x)$ are algebraic. Let v be a polynomial replacing variables of V by corresponding elementary symmetric functions in $r_{i,1}, \dots, r_{i,k}$. Then we have

$$v(r_{i,1}, \dots, r_{i,k}) \in \mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z} \quad (1 \le {}^{\forall} i \le m).$$

Note that a relation $v(r_{i,1}, \dots, r_{i,k}) \equiv 0 \bmod p$ does not necessarily imply relations among $r_{i,1}/p, \dots, r_{i,k}/p$. But, it implies $v(r_{1,1}, \dots, r_{1,k}) \equiv \cdots \equiv v(r_{m,1}, \dots, r_{m,k}) \bmod p$ and it may happen to reduce to linear relations. If all reduced linear relations have no constant term, then for some lower dimensional region D, $\mathrm{Pr}_D(f) > 0$ happens as example 1,2, hence the uniformity breaks down.
For $f = f_{6.1}$ let us give an example such that linear relations do not necessarily induce a break of uniformity. It decomposes over $\mathbb{Q}(\sqrt{-7})$ as follows:

$$\begin{aligned} f(x) \;&=\; \big(x^3 + (1-\sqrt{-7})x^2/2 - (1+\sqrt{-7})x/2 - 1\big) \\ &\quad \times \big(x^3 + (1+\sqrt{-7})x^2/2 - (1-\sqrt{-7})x/2 - 1\big). \end{aligned}$$

Since a polynomial $V(x) := (2x-1)^2 + 7$ vanishes at $(1 \pm \sqrt{-7})/2$, neglecting the order (1) we have

$$\big(-2(r_1 + r_2 + r_3) - 1\big)^2 + 7 \equiv \big(-2(r_4 + r_5 + r_6) - 1\big)^2 + 7 \equiv 0 \bmod p,$$

hence the difference of the left and the middle implies

$$r_1 + r_2 + r_3 \equiv r_4 + r_5 + r_6 \bmod p, \quad \text{or} \quad \sum_{i=1}^{6} r_i + 1 \equiv 0 \bmod p.$$

The left hand suggests to have to check whether $\mathrm{Pr}_E(f) = 0$ or not for a lower dimensional set E given by the union of

$$\{(x_1, \dots, x_6) \mid (x_{i_1} + x_{i_2} + x_{i_3}) - (x_{i_4} + x_{i_5} + x_{i_6}) \in \mathbb{Z}\} \text{ for } \{i_1, \dots, i_6\} = \{1, \dots, 6\}.$$

But the right hand is always satisfied by

$$f = x^6 + x^5 + \cdots + 1,$$

and if the left hand happens, we have $t := r_1 + r_2 + r_3 \equiv (p-1)/2 \bmod p$, which contradicts $(-2t-1)^2 + 7 \equiv 0 \bmod p$. Therefore we have $\mathrm{Pr}_E(f) = 0$, as we have expected.

REFERENCES

[1] KITAOKA,Y.: *Statistical distribution of roots of a polynomial modulo primes*, (submitted).
[2] *The On-Line Encyclopedia of Integer Sequences*, Published electronically, 2000, http://oeis.org

[3] SERRE, J. P.: *Quelques applications du théorème de densité de Chebotarev*, I.H.E.S., **54** (1981), 323–401.

Received October 4, 2016
Accepted January 12, 2017

Yoshiyuki Kitaoka
Uzunawa 1085-10, Asahi-cho,
Mie, 510-8104
JAPAN
E-mail: kitaoka@meijo-u.ac.jp