Uniform Distribution Theory **10** (2015), no.2, 1–10

uniform distribution theory

STATISTICAL DISTRIBUTION OF ROOTS MODULO PRIMES OF AN IRREDUCIBLE AND DECOMPOSABLE POLYNOMIAL OF DEGREE 4

Yoshiyuki Kitaoka

Dedicated to Professor Harald Niederreiter on the occasion of his 70th birthday

ABSTRACT. For an irreducible polynomial $f(x) = (x^2 + ax)^2 + b(x^2 + ax) + c$ of degree 4 and a natural number L, we propose a conjecture of distribution of roots r_1, r_2, r_3, r_4 of f modulo a prime p satisfying $r_i \equiv 0 \bmod L$ and $0 \le r_i \le pL - 1$.

Communicated by Shigeki Akiyama

1. Introduction

Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

be an irreducible monic polynomial with integer coefficients, and let L be a natural number. Put

$$Spl(f) = \{p \mid f(x) \bmod p \text{ is completely decomposable}\},$$

where a letter p denotes prime numbers larger than L. This is an infinite set, and the natural density is given by Chebotarev's density theorem. For a prime $p \in Spl(f)$, we can take n integers $r_1, \ldots, r_n \in \mathbb{Z}$ such that

$$\begin{cases} f(r_i) \equiv 0 \bmod p, \\ r_i \equiv 0 \bmod L, \qquad (i = 1, \ldots, n) \\ 0 \le r_i \le pL - 1, \end{cases} \tag{1}$$

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

by Chinese Remainder Theorem. Then we have $a_{n-1} + \sum r_i \equiv 0 \bmod p$, hence there exists an integer $C_p(f)$ such that

$$a_{n-1} + \sum_{i=1}^{n} r_i = C_p(f)p\,. \tag{2}$$

We note that $-a_{n-1}$ is the global trace of a root α of $f(x) = 0$ and $\sum r_i$ is the sum of local traces in $\mathbb{Q}(\alpha) \otimes \mathbb{Q}_p$ modulo p, hence $C_p(f)$ involves the difference of the global trace and the sum of local traces. The condition

$$1 \le C_p(f) < nL \tag{3}$$

holds with finitely many exceptional primes p, and we studied the distribution of $C_p(f)$ for an irreducible and indecomposable[1] polynomial f in the previous paper [5]. Putting

$$Pr_X(f, L)[k] = \frac{\#\{p \in Spl_X(f) \mid C_p(f) = k\}}{\#Spl_X(f)},$$

where $Spl_X(f) = \{p \in Spl(f) \mid p \le X\}$, we are concerned with the limit

$$Pr(f, L)[k] := \lim_{X \to \infty} Pr_X(f, L)[k]\,.$$

Numerical data suggest that the limit exists, and we gave several observations ([1] in the case related to the decimal expansion of a rational number, [2], [3], [4] in the case of $L = 1$, and [5] in the case of $L > 1$ and an irreducible and indecomposable polynomial). By a remark on $C_p(f)$ above, $Pr(f, L)[k] = 0$ if $k \le 0$ or $k \ge nL$.

In the subsection 2.2.1 of [5], we gave conjectures for an irreducible and decomposable(= reduced there) polynomial of degree 4, but they were observations based on insufficient data. In fact, one of them is false. Here we correct it and give a definite result in the easiest case and conjectures based on more data in the next section. In the third section, we give a proof of the easiest case and theoretical partial evidences of conjectures.

2. Conjectures

First, let us recall some necessary results in [5]. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be an irreducible polynomial with integer coefficients. Hereafter, $\mathbb{Q}(f)$ denotes

[1] A polynomial f is called indecomposable unless $f(x) = g(h(x))$ holds for polynomials g, h with $1 < \deg g < \deg f$. In [5], it was called non-reduced.

the Galois extension of the rational number field $\mathbb{Q}$ generated by all roots of $f(x)=0$ and ζ_T is a primitive Tth root of unity.

The following is Proposition 1 in [5] :

Proposionion 1. *Let f be a polynomial above, and let L, j be natural numbers, and put $N=(a_{n-1},L)$ and $T=L/N$. We denote Euler's function by φ. If $T=1$, i. e., $a_{n-1}\equiv 0 \bmod L$, then we have*

$$\lim_{X\to\infty}\sum_{k\equiv j \bmod L} Pr_X(f,L)[k]=\begin{cases}1 & \text{if } j\equiv 0 \bmod L,\\ 0 & \text{otherwise.}\end{cases}$$

If $T>1$, then we have

$$\lim_{X\to\infty}\sum_{k\equiv j \bmod L} Pr_X(f,L)[k]=\frac{[\mathbb{Q}(f)\cap\mathbb{Q}(\zeta_T):\mathbb{Q}]}{\varphi(T)} \text{ or } 0,$$

where the limit is not zero if and only if (i) $(j,L)=N$ *and* (ii) *mappings* $\zeta_T\to\zeta_T^{a_{n-1}/N}$ *and* $\zeta_T\to\zeta_T^{j/N}$ *induce the same automorphism on the subfield* $\mathbb{Q}(f)\cap\mathbb{Q}(\zeta_T)$ *of* $\mathbb{Q}(\zeta_T)$.

Although the existence of the limit of each factor $Pr_X(f,L)[k]$ is a conjecture, the limit of the sum $\sum_{k\equiv j \bmod L} Pr_X(f,L)[k]$ exists. Hereafter as in the proposition, we put

$$N:=(a_{n-1},L),\ T:=L/N, \tag{4}$$

hence $(a_{n-1}/N,T)=1$. The proposition says that the non-vanishing condition $Pr(f,L)[k]\neq 0$ implies $(k,L)=N$, hence we introduce the shrunk density

$$SPr(f,L)[k]:=Pr(f,L)[kN]\quad(1\le k<nT).$$

Under the basic conjecture of the existence of the limit $Pr(f,L)$, the condition $SPr[k]\neq 0$ implies that (i) $1\le k<nT$ and (ii) $(k,T)=1$, and (iii) k and a_{n-1}/N induce the same automorphism on the field $\mathbb{Q}(f)\cap\mathbb{Q}(\zeta_T)$, and furthermore

$$\sum_{j\equiv k \bmod T} SPr[j]=\frac{[\mathbb{Q}(f)\cap\mathbb{Q}(\zeta_T):\mathbb{Q}]}{\varphi(T)} \tag{5}$$

for any integer k satisfying the three conditions above.

From now on, we specialize a polynomial f to *an irreducible and decomposable polynomial of degree* 4, i. e.,

$$f(x)=(x^2+ax)^2+b(x^2+ax)+c\quad(a,b,c\in\mathbb{Z}), \tag{6}$$

whence $n=4, a_{n-1}=2a$ and $(2a/N,T)=1$.

The case of $T = 1$, i. e., $L \mid 2a$ is as follows:

Theorem 1. *If $a \equiv 0 \bmod L$, then*

$$SPr(f,L)[2] = 1, \quad SPr(f,L)[1] = SPr(f,L)[3] = 0.$$

Conjecture 1. *If $2a \equiv 0 \bmod L, a \not\equiv 0 \bmod L$, then*

$$SPr(f,L)[2] = 1/2, \quad SPr(f,L)[1] = SPr(f,L)[3] = 1/4.$$

The proof and the comment are given in the next section.

Next, suppose that $T > 1$ and put

$$f_2(x) = -2x^2 + 8Tx - 6T^2, \quad f_3(x) = f_2(x) + x^2.$$

Fixing T, we introduce basic vectors $v_i[k]$ for $k = 1, \ldots, T-1$:

$$\begin{aligned} v_1[k] &:= (0,0,0,0), \\ v_2[k] &:= \big(k^2, f_2(T+k), (2T-k)^2, 0\big), \\ v_3[k] &:= \big(0, (T+k)^2, f_2(2T-k), (T-k)^2\big), \\ v_4[k] &:= \big(k^2, f_3(T+k), f_3(2T-k), (T-k)^2\big). \end{aligned}$$

We expect that for $1 \le k < T$, a vector

$$V[k] := \big(SPr[k], SPr[T+k], SPr[2T+k], SPr[3T+k]\big)$$

is proportional to one of vectors $v_i[k]$. Since the sum of entries of the second, the third and the last is equal to $4T^2$, $4T^2$ and $8T^2$, respectively, the equation (5) suggests that $V[k]$ is equal to one of

$$v_1[k], \quad 2q_T v_2[k], \quad 2q_T v_3[k], \quad q_T v_4[k],$$

where

$$q_T := \frac{[\mathbb{Q}(f) \cap \mathbb{Q}(\zeta_T) : \mathbb{Q}]}{8T^2\varphi(T)}.$$

The data suggest that the proportional constant is independent of k, hence v_4 does not appear together with v_2, v_3 at the same time. We note that $v_2[k] + v_3[k] = v_4[k]$ and entries in $v_i[k]$ are positive if "0" is not put.

Let F be an abelian extension of $\mathbb{Q}$ and let C_F be the conductor of F, that is the least positive integer C_F such that $\mathbb{Q}(\zeta_{C_F})$ contains F. If an integer k is relatively prime to C_F, we denote by $[[k]]$ an automorphism of F induced by $\zeta_{C_F} \to \zeta_{C_F}^k$.

Now we can state conjectures in case of $T > 1$. Note that the order of the Galois group $Gal(\mathbb{Q}(f)/\mathbb{Q})$ is 4, 8 and Proposition 1 implies that $V[k] \ne (0,0,0,0)$ if and only if $(k,T) = 1$ and $[[k]] = [[2a/N]]$ on $\mathbb{Q}(f) \cap \mathbb{Q}(\zeta_T)$.

Hereafter integers k are supposed to satisfy

$$1 \le k \le T-1, \ (k,T) = 1 \quad \textit{and} \quad [[k]] = [[2a/N]] \ \textit{on} \ \mathbb{Q}(f) \cap \mathbb{Q}(\zeta_T). \tag{7}$$

If one of the above is not satisfied, we have $V[k] = (0,0,0,0)$ by Proposition 1.

(I) The case of $T \equiv 1 \bmod 2$ [2]:

$V[k] = q_T v_4[k]$ does not occur, and

$$V[k] = 2q_T \times \begin{cases} v_2[k] & \text{if } k \equiv 2a/N \bmod 2, \\ v_3[k] & \text{if } k \not\equiv 2a/N \bmod 2. \end{cases}$$

(II) The case of $T \equiv 0 \bmod 2$:

Let F be the maximal abelian subfield of $\mathbb{Q}(f)$, which is quartic.

(II.a) The case of $[F \cap \mathbb{Q}(\zeta_{2T}) : F \cap \mathbb{Q}(\zeta_T)] = 2$:

$$V[k] = 2q_T \times \begin{cases} v_2[k] & \text{if } [[k]] = [[2a/N]] \text{ on } F \cap \mathbb{Q}(\zeta_{2T}), \\ v_3[k] & \text{if } [[k]] \neq [[2a/N]] \text{ on } F \cap \mathbb{Q}(\zeta_{2T}). \end{cases}$$

(II.b) The case of $[F \cap \mathbb{Q}(\zeta_{2T}) : F \cap \mathbb{Q}(\zeta_T)] \neq 2$:

$V[k] = q_T v_4[k]$ holds for every k.

The (conjectural) density depends not on the field $\mathbb{Q}(f)$ but on the maximal abelian subfield F.

Our checking method by pari/gp[3] is to watch that numerical data $Pr_X(f, L)$ multiplied by $8T^2\varphi(T)$ approach the conjectural densities multiplied by the same $8T^2\varphi(T)$, which are integers. Let us give numerical data of ratios $Pr_X(f, L)[k]$ to the conjectural density $Pr[k]$ in case of $a = 4$, $b = 13$, $c = 41$, $N = 8$, $21 \leq T \leq 30$, $L = NT$, $X = 10^{10}$: By $\mathbb{Q}(f) = \mathbb{Q}(\zeta_5)$, the maximal abelian subfield F is $\mathbb{Q}(f)$ itself and $F \cap \mathbb{Q}(\zeta_T) = \mathbb{Q}(\zeta_{(5,T)})$. Hence, in the case of $5 \mid T$, the condition $[[k]] = [[2a/N]]$ is $k \equiv 2a/N \bmod 5$. We define er by

$$er = \max_{\substack{1 \leq k \leq 4L-1 \\ Pr[k] \neq 0}} |Pr_X(f, L)[k]/Pr[k] - 1|.$$

In the following table, T is on the upper row, $1/q_T$ is on the middle line and er is on the lower row, where the value er is rounded off to the third decimal place.

T	21	22	23	24	25
$1/q_T$	42336	38720	93104	36864	25000
er	0.011	0.048	0.022	0.009	0.004

T	26	27	28	29	30
$1/q_T$	64896	104976	75264	188384	14400
er	0.027	0.034	0.017	0.026	0.003

[2] In [5], the case of $2a/N \equiv 1 \bmod 2$ was missing.

[3] The PARI Group, PARI/GP version 2.7.0 Bordeaux, 2014, `http://pari.math.u-bordeaux.fr/`

We note that in case of $T \equiv 0 \bmod 2$,

$$
\begin{aligned}
&[F \cap \mathbb{Q}(\zeta_{2T}) : F \cap \mathbb{Q}(\zeta_T)] = 2 \\
\Leftrightarrow &\begin{cases} 2 \,|\, C_F,\ F \cap \mathbb{Q}(\zeta_{2T}) \neq \mathbb{Q} & \text{if } [F \cap \mathbb{Q}(\zeta_T) : \mathbb{Q}] = 1, \\ C_F = 2(C_F, T) & \text{if } [F \cap \mathbb{Q}(\zeta_T) : \mathbb{Q}] = 2. \end{cases}
\end{aligned}
$$

P r o o f. Suppose first, $[F \cap \mathbb{Q}(\zeta_{2T}) : F \cap \mathbb{Q}(\zeta_T)] = 2$. If $F \cap \mathbb{Q}(\zeta_T) = \mathbb{Q}$, then two equations

$$
\begin{aligned}
[F(\zeta_{2T}) : \mathbb{Q}] &= [F : F \cap \mathbb{Q}(\zeta_{2T})][\mathbb{Q}(\zeta_{2T}) : F \cap \mathbb{Q}(\zeta_{2T})] \cdot 2 \\
&= 2 \cdot \varphi(2T)/2 \cdot 2 = \varphi(4T)
\end{aligned}
$$

and

$$
\begin{aligned}
[F(\zeta_{2T}) : \mathbb{Q}] &= [F(\zeta_{2T}) : F(\zeta_T)][F : \mathbb{Q}][\mathbb{Q}(\zeta_T) : \mathbb{Q}] \\
&= [F(\zeta_{2T}) : F(\zeta_T)] \cdot 4\varphi(T) = [F(\zeta_{2T}) : F(\zeta_T)]\varphi(4T)
\end{aligned}
$$

imply

$$[F(\zeta_{2T}) : F(\zeta_T)] = 1, \quad \text{i.e.,} \ F(\zeta_{2T}) = F(\zeta_T),$$

hence

$$\mathbb{Q}(\zeta_{C_F}, \zeta_{2T}) = \mathbb{Q}(\zeta_{C_F}, \zeta_T).$$

Thus C_F should be even, since T is even. If $F \cap \mathbb{Q}(\zeta_T) \neq \mathbb{Q}$, then $F \cap \mathbb{Q}(\zeta_T)$ is quadratic and $F \cap \mathbb{Q}(\zeta_{2T})$ is quartic, that is $F \cap \mathbb{Q}(\zeta_{2T}) = F$, hence

$$F \not\subset \mathbb{Q}(\zeta_T) \quad \text{and} \quad F \subset \mathbb{Q}(\zeta_{2T}),$$

which imply

$$C_F = 2(C_F, T).$$

Conversely, suppose that $2 \,|\, C_F$, $F \cap \mathbb{Q}(\zeta_{2T}) \neq \mathbb{Q}, [F \cap \mathbb{Q}(\zeta_T) : \mathbb{Q}] = 1$; we have only to show $F \not\subset \mathbb{Q}(\zeta_{2T})$. If $F \subset \mathbb{Q}(\zeta_{2T})$, then we have

$$[F(\zeta_T) : \mathbb{Q}] = [F : \mathbb{Q}][\mathbb{Q}(\zeta_T) : \mathbb{Q}] = 4\varphi(T),$$

hence

$$\varphi(2T) = [\mathbb{Q}(\zeta_{2T}) : \mathbb{Q}] = [F(\zeta_{2T}) : \mathbb{Q}] = [F(\zeta_{2T}) : F(\zeta_T))] \cdot 4\varphi(T),$$

which is a contradiction. Last, assume $C_F = 2(C_F, T), [F \cap \mathbb{Q}(\zeta_T) : \mathbb{Q}] = 2$; the odd part of C_F divides T and the 2-factor of C_F is twice the 2-factor of T, i.e., $C_F \,|\, 2T$. Thus $F \subset \mathbb{Q}(\zeta_{C_F}) \subset \mathbb{Q}(\zeta_{2T})$, that is $F \cap \mathbb{Q}(\zeta_{2T}) = F$. □

3. Proof of Theorem 1 and comments

We recall that an irreducible polynomial f is given by (6) and note that the equation $x^2 + ax = (-x-a)^2 + a(-x-a)$ implies the equivalence of

$$f(r) \equiv 0 \bmod p \quad \text{and} \quad f(-r-a) \equiv 0 \bmod p.$$

A basic lemma is

Lemma 1. *Let an integer r be a root of $f(x) \equiv 0 \bmod p$ with* (1)*; then we can take an integer δ so that for $R := p\delta - r - a$*

$$f(R) \equiv 0 \bmod p,\ 0 \le R < pL,\ R \equiv 0 \bmod L, \qquad (8)$$
$$R \not\equiv r \bmod p,$$
$$0 < \delta < 2L,$$

with finitely many exceptional primes p.

Proof. The existence of an integer δ satisfying (8) for a prime $p\,(> L)$ follows from Chinese Remainder Theorem. Suppose $R \equiv r \bmod p$ for an odd prime p; then we have $2r \equiv -a \bmod p$, therefore for an irreducible polynomial $F(x) := 2^4 f(x/2)$ with integer coefficients, we have $F(-a) \equiv F(2r) \equiv 2^4 f(r) \equiv 0 \bmod p$. Thus, such a prime p is a divisor of non-zero integer $F(-a)$, hence the possibility of p is finite. Next, the condition $0 \le R < pL$ implies $(\delta - L)p - a < r \le p\delta - a$. By the assumption $0 \le r < pL$, we have $(\delta - 2L)p < a \le p\delta$, which implies $a/p \le \delta < a/p + 2L$, i. e., $0 \le \delta \le 2L$ with finitely many exceptional primes p. Suppose $\delta = 0$ for infinitely many primes p; then $0 \le R = -r-a$, i. e., $0 \le r \le -a$ follows for infinitely many primes. Thus there is an integer $M\,(= r)$ between 0 and $-a$ such that $f(M) \equiv 0 \bmod p$ for infinitely many primes, which implies a contradiction $f(M) = 0$. Last, suppose $\delta = 2L$ for infinitely many primes p; then $R = 2Lp - r - a < pL$, i. e., $-a \le r - pL < 0$ follows for infinitely many primes. Thus there is an integer $M\,(= r - pL)$ such that $f(M) \equiv f(r) \equiv 0 \bmod p$ for infinitely many primes, which implies a contradiction $f(M) = 0$. □

Proposionion 2. *For a prime $p \in Spl(f)$, let $r_1, \dots, r_4$ be roots of $f(x) \equiv 0 \bmod p$ with* (1)*, and using the previous lemma, we may suppose that they satisfy*

$$r_1 + r_3 = \delta_1 p - a,\ r_2 + r_4 = \delta_2 p - a\,(0 < \delta_1 \le \delta_2 < 2L). \qquad (9)$$

Then we have $\delta_1 = \delta_2 = C_p(f)/2$ or $\delta_1 = (C_p(f) - L)/2$, $\delta_2 = (C_p(f) + L)/2$, where $C_p(f)$ is defined by (2)*.*

P r o o f. Since the assumption $r_i \equiv 0 \bmod L$ $(i = 1, \ldots, 4)$ implies $\delta_1 p - a \equiv \delta_2 p - a \equiv 0 \bmod L$, we have $\delta_1 \equiv \delta_2 \bmod L$, assuming $p > L$. Thus $\delta_1 = \delta_2$ or $\delta_2 = \delta_1 + L$ follows from $0 < \delta_1 \le \delta_2 < 2L$, and by $(\delta_1 + \delta_2)p = 2a + \sum r_i = C_p(f)p$, we get the statement of the proposition. □

(1) and (2) imply a fundamental relation $C_p(f)p \equiv 2a \bmod L$, hence for some natural number k

$$C_p(f) = kN, \quad \text{and} \quad (k, T) = 1,\ kp \equiv 2a/N \bmod T. \tag{10}$$

Moreover, we have

Corollary 1. *Continuing the previous proposition, we have, for $C_p(f) = kN$ above*

$$\begin{cases} kp \equiv 2a/N \bmod 2T & \text{if} \quad \delta_2 = \delta_1, \\ (k - T)p \equiv 2a/N \bmod 2T & \text{if} \quad \delta_2 = \delta_1 + L. \end{cases}$$

If either $C_p(f) \le L$ or $C_p(f) \ge 3L$, then only the case $\delta_2 = \delta_1$ holds.

P r o o f. By (1) and (9), we have $\delta_1 p \equiv a \bmod L$, hence

$$kN/2 \cdot p \equiv a \bmod L \quad \text{if} \quad \delta_2 = \delta_1,$$
$$(kN - L)/2 \cdot p \equiv a \bmod L \quad \text{if} \quad \delta_2 = \delta_1 + L.$$

Since $L = NT$, and $2a$ is divisible by N, the statement follows easily. If the condition $\delta_2 = \delta_1 + L$ happens, then the previous proposition implies

$$(C_p(f) - L)/2 > 0 \quad \text{and} \quad (C_p(f) + L)/2 < 2L, \quad \text{i.e.,} \quad L < C_p(f) < 3L,$$

which completes the proof. □

The corollary says that if either $C_p(f) \le L$ or $C_p(f) \ge 3L$, we have a stronger condition $kN/2 \cdot p \equiv a \bmod L$ than (10), which elucidates the entry "0" in vectors v_2, v_3 as stated later.

P r o o f o f T h o e r e m 1. By the assumption $a \equiv 0 \bmod L$, δ_1, δ_2 in (9) are divisible by L, hence are equal to L. Thus we have $C_p(f) = 2L$, hence

$$SPr(f, L)[2] = Pr(f, L)[2N] = Pr(f, L)[2L] = 1$$

and

$$SPr(f, L)[1] = SPr(f, L)[3] = 0.$$

□

Next, let us study the meaning of Conjecture 1, i.e.,

$$SPr(f, L) = (1/4, 1/2, 1/4) \quad \text{if } 2a \equiv 0 \bmod L \quad \text{but } a \not\equiv 0 \bmod L\,.$$

We use notations in Proposition 2. By the equation (2), we see $C_p(f) \equiv 0 \bmod L$, which implies $C_p(f) = L, 2L$ or $3L$ by (3). We see that $\delta_1 = \delta_2 = L/2$ holds in the case of $C_p(f) = L$, second $\delta_1 = L/2, \delta_2 = 3L/2$ in the case of $C_p(f) = 2L$ since $\delta_1 = \delta_2 = L$ with (9) implies a contradiction $a \equiv 0 \bmod L$, and last $\delta_1 = \delta_2 = 3L/2$ holds in the case of $C_p(f) = 3L$. Thus we have

$$2a + \sum r_i = Lp \times \begin{cases} 1 & \text{if} \quad \delta_1 = \delta_2 = L/2, \\ 2 & \text{if} \quad \delta_1 = L/2, \delta_2 = 3L/2, \\ 3 & \text{if} \quad \delta_1 = \delta_2 = 3L/2. \end{cases}$$

Here let us see that $\delta_2 = L/2$ (resp. $\delta_2 = 3L/2$) is equivalent to $r_2, r_4 \in [0, Lp/2]$ (resp. $r_2, r_4 \in [Lp/2, Lp]$) except finitely many primes p. Suppose $\delta_2 = L/2$; then $r_2, r_4 \le r_2 + r_4 = Lp/2 - a$ implies $r_2, r_4 \in [0, Lp/2 - a]$. By using the pigeon hole principle as in the proof of Lemma 1, we see $r_2, r_4 \in [0, Lp/2]$ except finitely many primes p. The equivalence of the conditions $\delta_1 = L/2$ and $r_1, r_3 \in [0, Lp/2]$ is similar. If $\delta_2 = 3L/2$, then the condition $r_2 < pL$ implies

$$r_4 = 3Lp/2 - a - r_2 > Lp/2 - a \quad \text{and similarly} \quad r_2 > Lp/2 - a,$$

hence we have $r_2, r_4 \in [Lp/2, Lp]$ except finitely many primes p, similarly. Thus, if pairs r_1, r_3 and r_2, r_4 distribute uniformly on $[0, Lp/2]$ and $[Lp/2, Lp]$, we have $SPr(f, L) = (1/4, 1/2, 1/4)$.

Let us assume $T > 1$ hereafter, and we show that cases of the density zero in the conjecture are affirmative.

We are still assuming $1 \le k \le T - 1$.
The case of $T \equiv 1 \bmod 2$: We have to show

$$SPr[3T + k] = 0 \qquad \text{if } k \equiv 2a/N \bmod 2, \tag{11}$$

$$SPr[k] = 0 \qquad \text{if } k \not\equiv 2a/N \bmod 2. \tag{12}$$

By Corollary 1, we have $\delta_2 = \delta_1$ for $C_p(f) = kN, (3T + k)N$. Thus the condition $SPr[3T + k] = Pr(f, L)[(3T + k)N] \ne 0$ implies $(3T + k)p \equiv 2a/N \bmod 2T$, which implies $1 + k \equiv 2a/N \bmod 2$. This concludes (11).
Suppose that $SPr[k] = Pr(f, L)[kN] \ne 0$; then we have $kp \equiv 2a/N \bmod 2T$, which implies $k \equiv 2a/N \bmod 2$, and (12) has been proved.

Let us assume that $T \equiv 0 \bmod 2$. Keeping notations in the previous section, we must show that in case of $[F \cap \mathbb{Q}(\zeta_{2T}) : F \cap \mathbb{Q}(\zeta_T)] = 2$,

$$SPr[3T + k] = 0 \qquad \text{if } [[k]] = [[2a/N]] \text{ on } F \cap \mathbb{Q}(\zeta_{2T}), \tag{13}$$

$$SPr[k] = 0 \qquad \text{if } [[k]] \ne [[2a/N]] \text{ on } F \cap \mathbb{Q}(\zeta_{2T}). \tag{14}$$

We are assuming that an integer k is relatively prime to T and T is even, thus $[[k]]$ is well-defined on $F \cap \mathbb{Q}(\zeta_{2T})\,(\subset \mathbb{Q}(\zeta_{2T}))$.

On (13): Suppose $SPr[3T + k] = Pr[(3T + k)N] \ne 0$; we have $\delta_2 = \delta_1$, hence $(T + k)p \equiv 2a/N \bmod 2T$ for a prime p with $C_p(f) = (3T + k)N$, hence $\zeta_{2T}^{2a/N} = -\zeta_{2T}^{kp} = -\sigma(\zeta_{2T})^k$, where σ is a Frobenius automorphism of p at $\mathbb{Q}(f)(\zeta_{2T})$. The condition $p \in Spl(f)$ implies that σ is the identity mapping on $F\,(\subset \mathbb{Q}(f))$. Since $K := F \cap \mathbb{Q}(\zeta_{2T}) \neq F \cap \mathbb{Q}(\zeta_T)$, there is an element $\alpha \in K$, which is not expressed by a linear combination of powers ζ_T with rational coefficients, therefore $\alpha^{[[2a/N]]} \neq \sigma(\alpha)^{[[k]]} = \alpha^{[[k]]}$, that is $[[2a/N]] \neq [[k]]$ on K.

On (14): Suppose $SPr[k] = Pr[kN] \neq 0$; then we have $kp \equiv 2a/N \bmod 2T$. Thus we have $[[k]] = [[2a/N]]$ by the fact that p decompose at $F(\subset \mathbb{Q}(f))$ completely. This completes the proof of (14).

REFERENCES

[1] 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 (W. Zhang and Y. Tanigawa, eds.), Springer Science + Business Media, Inc. 2006, pp. 67–80.

[2] KITAOKA, Y.: *A statistical relation of roots of a polynomial in different local fields*, Math. of Comp. **78**(2009), 523–536.

[3] KITAOKA Y.: *A statistical relation of roots of a polynomial in different local fields II*, Number Theory : Dreaming in Dreams (Series on Number Theory and Its Application Vol. 6), World Scientific, 2010. pp. 106–126.

[4] KITAOKA, Y.: *A statistical relation of roots of a polynomial in different local fields III*, Osaka J. Math. **49** (2012), 393–420.

[5] KITAOKA, Y.: *A statistical relation of roots of a polynomial in different local fields IV.* Uniform Distribution Theory **8** (2013), no.1, 17–30

Received June 30, 2014
Accepted February 2, 2015

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