Uniform Distribution Theory **8** (2013), no.1, 17–30

uniform distribution theory

A STATISTICAL RELATION OF ROOTS OF A POLYNOMIAL IN DIFFERENT LOCAL FIELDS IV

Yoshiyuki Kitaoka

ABSTRACT. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots$ be an irreducible polynomial with integer coefficients, and L a natural number. For a prime p for which $f(x) \bmod p$ is completely decomposable, we consider the n roots r_i with $r_i \equiv 0 \bmod L$ and $0 \le r_i < pL$. We propose several conjectures on the distribution of integers $(a_{n-1} + \sum r_i)/p$ when p varies. We have studied the case $L = 1$ in previous papers, and this is a continuation.

Communicated by Shigeki Akiyama

1. Introduction

Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \tag{1}$$

be a 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 $p\,(> L)$ denotes prime numbers. For a prime $p \in Spl(f)$, we can take n integers $r_1, \cdots, r_n \in \mathbb{Z}$ such that

$$\begin{cases} f(r_i) \equiv 0 \bmod p, \\ r_i \equiv 0 \bmod L, \qquad\qquad (i = 1, \cdots, n) \\ 0 \le r_i \le pL - 1, \end{cases} \tag{2}$$

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

$$a_{n-1} + \sum_{i=1}^{n} r_i = C_p(f)p. \tag{3}$$

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

To study the distribution of $C_p(f)$, we put

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

where $Spl_X(f) = \{p \in Spl(f) \mid p \le X\}$.
When $L = 1$, numerical data suggest that the limit

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

exists, and we gave several observations in [6],[7],[8]. For example, $Pr(f,L)[k]$ ($L = 1$) is given by Eulerian numbers, and it suggests that the $n!$ arrangements $(r_{i_1}/p, \cdots, r_{i_{n-1}}/p)$ of all possible choices of $n-1$ roots among $r_1, \cdots, r_n$ seem to be uniformly distributed in $[0,1)^{n-1}$ if $f(x)$ is of deg ≥ 2, irreducible and not of the form $f(x) = g(h(x))$ with $1 < \deg h(x) < \deg f(x)$. When $n = 2$, it is true ([1],[9]). Even if $f(x)$ has the decomposition above, we can see how matters stand if the decomposition is essentially unique. Otherwise, we have no prospect.

In this paper, we are concerned with a case with congruence condition, that is $L > 1$.
We may replace the condition $r_i \equiv 0 \bmod L$ $(i = 1, \cdots, n)$ by $r_i \equiv a \bmod L$ for any fixed integer a. But, considering $g(x) = f(x+a)$, it is reduced to the case $a = 0$, since $C_p(f) = C_p(g)$ holds except finitely many primes $p \in Spl(f(x)) = Spl(g(x))$, if $f(x)$ has no integer roots.

Before observations, which are given in the next section, we give a following basic remark.

Proposition 1. *Let f be a monic polynomial with integer coefficients in* (1), *and let L, j be natural numbers, and put $N = (a_{n-1}, L)$. We denote Euler's function by φ. If $a_{n-1} \equiv 0 \bmod L$, 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 $a_{n-1} \not\equiv 0 \bmod L$, then we have

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

where the limit is not zero if and only if (i) $(j,L) = N$ *and* (ii) a_{n-1}/N *and j/N induce the same automorphism on the field $\mathbb{Q}(\zeta_{L/N}) \cap \mathbb{Q}(f)$. Here $\mathbb{Q}(f)$ is the field generated by all roots of $f(x)$ over the rational number field $\mathbb{Q}$, and ζ_a denotes an a-th primitive root of unity.*

Proof. Let $p \in Spl(f)$ and integers r_i satisfy (2). Then $C_p(f) \equiv j \bmod L$ is equivalent to $a_{n-1} \equiv jp \bmod L$ by the definition (3). Hence we have

$$\sum_{k \equiv j \bmod L} Pr_X(f, L)[k] = \frac{\#\{p \in Spl_X(f) \mid a_{n-1} \equiv jp \bmod L\}}{\#Spl_X(f)}.$$

Let us state conditions on p in words of Frobenius automorphisms : For a prime p in $Spl(f)$ with $a_{n-1} \equiv jp \bmod L$, let σ be a Frobenius automorphism of $\mathbb{Q}(f, \zeta_{L/N})$ over $\mathbb{Q}$ corresponding to p. If p does not divide the discriminant of $f(x)$, then p is unramified in the field $\mathbb{Q}(f)$, and moreover the condition $p \in Spl(f)$ means that p is completely decomposable in the field $\mathbb{Q}(f)$, that is σ is the identity mapping on a subfield $\mathbb{Q}(f)$. In addition, σ is an automorphism on $\mathbb{Q}(\zeta_{L/N})$ induced by $\zeta_{L/N} \to \zeta_{L/N}^p$.
The condition $a_{n-1} \equiv jp \bmod L$ means that j is divisible by $N = (a_{n-1}, L)$, and $(j, L) = N$.

If $a_{n-1} \equiv 0 \bmod L$, then we have $N = L$ and j is divisible by L, hence the statement of the proposition is true in this case.

Suppose that $a_{n-1} \not\equiv 0 \bmod L$; we have $(a_{n-1}/N, L/N) = 1$ and $a_{n-1}/N \equiv j/N \cdot p \bmod L/N$, which is equivalent to $(\zeta_{L/N})^{a_{n-1}/N} = \sigma(\zeta_{L/N})^{j/N}$. Therefore, in case that one of the conditions (i),(ii) in the proposition is not satisfied, the limit of the statement of the proposition is zero.

We note that the condition $(j/N, L/N) = 1$ implies that σ is uniquely determined by the condition $(\zeta_{L/N})^{a_{n-1}/N} = \sigma(\zeta_{L/N})^{j/N}$. Hence a conjugate class of σ in $Gal(\mathbb{Q}(f, \zeta_{L/N})/\mathbb{Q})$ consists of one element σ, since σ is trivial on $\mathbb{Q}(f)$.

Under the conditions (i),(ii), Chebotarev's density theorem implies

$$\begin{aligned}
&\lim_{X \to \infty} \sum_{k \equiv j \bmod L} Pr_X(f, L)[k] \\
&= \lim_{X \to \infty} \frac{\#\{p \in Spl_X(f) \mid a_{n-1} \equiv jp \bmod L\}}{\#\{p \mid p \in Spl(f), p \leq X\}} \\
&= \lim_{X \to \infty} \frac{\#\{p \in Spl_X(f) \mid a_{n-1} \equiv jp \bmod L\}/\#\{p < X\}}{\#Spl_X(f)/\#\{p < X\}} \\
&= \frac{[\mathbb{Q}(f) : \mathbb{Q}]}{[\mathbb{Q}(f, \zeta_{L/N}) : \mathbb{Q}]} \\
&= \frac{1}{[\mathbb{Q}(f, \zeta_{L/N}) : \mathbb{Q}(f)]} \\
&= \frac{1}{[\mathbb{Q}(\zeta_{L/N}) : \mathbb{Q}(\zeta_{L/N}) \cap \mathbb{Q}(f)]}
\end{aligned}$$

$$= \frac{[\mathbb{Q}(\zeta_{L/N}) \cap \mathbb{Q}(f) : \mathbb{Q}]}{\varphi(L/N)}.$$

□

Remark 1. *The proof of the proposition shows that if $p \in Spl(f)$ does not divide the discriminant of $f(x)$, then putting $j = C_p(f)$, which implies $Pr_X(f,L)[j] \neq 0$, we have* (i) *$(j, L) = N$, and* (ii) *a_{n-1}/N and j/N induce the same automorphism on the field $\mathbb{Q}(\zeta_{L/N}) \cap \mathbb{Q}(f)$, if $L \neq N$.*
The value $\lim_{X\to\infty} \sum_{k\equiv j \bmod L} Pr_X(f,L)[k]$ is independent of j if it is not zero.

In the rest of this paper, we assume that a polynomial $f(x)$ is irreducible and of $\deg(f) > 1$. Our basic conjecture is that the limit

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

exists.
It is easy to see $1 \leq C_p(f) \leq nL - 1$ with finitely many exceptional primes p, since $C_p(f) \leq 0$ (resp. $C_p(f) \geq nL$) implies $0 \leq \sum r_i \leq -a_{n-1}$ (resp. $0 < \sum(Lp - r_i) \leq a_{n-1}$), which implies that the polynomial $f(x)$ has an integer root. Therefore we write

$$Pr = Pr(f,L) = [Pr(f,L)[1], \cdots, Pr(f,L)[nL-1]], \tag{4}$$

or simply

$$Pr = [Pr[1], \cdots, Pr[nL-1]].$$

Moreover in view of the remark, we define a natural number T and a shrunk density SPr by

$$T = L/N, \quad SPr(f,L)[k] = Pr(f,L)[kN], \tag{5}$$

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

$$\sum_{k\equiv j \bmod T} SPr[k] = \frac{[\mathbb{Q}(\zeta_T) \cap \mathbb{Q}(f) : \mathbb{Q}]}{\varphi(T)}, \tag{6}$$

for any integer j satisfying the condition (iii) above.

The reducible case will be discussed in a subsequent paper.

2. Observations

When a polynomial $f(x)$ is of the form $g(h(x))$ with $1 < \deg g(x) < \deg f(x)$, we call $f(x)$ reduced. Otherwise, $f(x)$ is called non-reduced. Putting for a non-reduced irreducible monic polynomial $f(x)$ with integer coefficients and $\deg f = n$

$$N = (a_{n-1}, L),\ T = L/N,\ \Delta = (n-1)!\,\varphi(T^n),$$

our basic conjecture is that all components of $SPr(f, L)$ are rational numbers whose denominator divides Δ.

Our strategy to find the likely rational values of Pr from numerical data $Pr_X(f, L)$ is

(i) to find an integer c approximating $\Delta \cdot Pr_X(f, L)[k]$ for a large number X,

(ii) to confirm that $|\Delta \cdot Pr_X(f, L)[k] - c| < 1$ holds when X is reasonably large.

Hereafter statements are conjectures based on observations supported by numerical data [1] unless we give proofs.

2.1. $n = 2$ and $L > 1$

Suppose that $f(x) = x^2 + ax + b$ is a monic irreducible polynomial of degree 2 and $L(> 1)$ is a natural number.

In case of $a \equiv 0 \bmod L$, i.e. $T = L/N = 1$, $SPr = SPr(f, L)$ is given by

$$SPr[1] = 1,\ SPr[j] = 0 \text{ if } j \neq 1. \tag{7}$$

Next, suppose that $a \not\equiv 0 \bmod L$, then our observation is that $SPr(f, L)$ is equal to the following distribution table SPr : denoting the discriminant of a quadratic field $\mathbb{Q}(f)$ by D, for $1 \leq j \leq T-1$

$$SPr[j] = \begin{cases} \dfrac{2j}{T \cdot \varphi(T)} & \text{if } (j, T) = 1, D \mid T,\ \chi_D(a/N) = \chi_D(j), \\[2ex] \dfrac{j}{T \cdot \varphi(T)} & \text{if } (j, T) = 1, D \nmid T, \end{cases}$$

and

$$SPr[T+j] = \begin{cases} \dfrac{2(T-j)}{T \cdot \varphi(T)} & \text{if } (j, T) = 1, D \mid T,\ \chi_D(a/N) = \chi_D(j), \\[2ex] \dfrac{T-j}{T \cdot \varphi(T)} & \text{if } (j, T) = 1, D \nmid T, \end{cases}$$

and $SPr[k] = 0$ except the above, where $\chi_D(m)$ means Kronecker's symbol $(\frac{D}{m})$.

[1] Data were made by PARI/GP.

We note that the condition $D \mid T$ is equivalent to $\mathbb{Q}(f) \subset \mathbb{Q}(\zeta_T)$ and the above observations are compatible with (6). If $\chi_D(-1) = -1$, then Pr is not symmetric. This is checked by the method referred above for irreducible polynomials with $0 \le a \le 50$, $|b| \le 50$ and $X < 10^{10}$.

In case of $n = 2$, we can give following theoretical results.

Theorem 1. *Let $f(x) = x^2 + Ax + B$ be a monic irreducible polynomial of degree 2, and $L(> 1)$ a natural number. Supposing that $A \equiv 0 \bmod L$, we have $C_p(f) = L$ except finitely many primes in $Spl(f)$, hence the observation (7) above is true.*

Proof. We divide the proof into two cases $f(x) = (x + a)^2 + c$ or $f(x) = (x + a)^2 + x + c$ $(a, c \in \mathbb{Z})$. First, suppose that $f(x) = (x + a)^2 + c$; then the assumption $A \equiv 0 \bmod L$ implies that $2a \equiv 0 \bmod L$. Let R be an integer such that

$$f(R) \equiv 0 \bmod p, \ R \equiv 0 \bmod L, \text{ and } 0 \le R < pL, \tag{8}$$

where $p \in Spl(f)$, in particular $p > L \ge 2$.
Let us see that for

$$R_1 = pL - R - 2a,$$

conditions $f(R_1) \equiv 0 \bmod p$, $R_1 \equiv 0 \bmod L$, $R_1 \not\equiv R \bmod pL$ and $0 \le R_1 < pL$ are satisfied except finitely many primes in $Spl(f)$. Once they had been proved, $C_p(f) = (2a + R + R_1)/p = L$ is obvious, and the proof is over in this case. The first follows from $f(-R - 2a) = (-R - a)^2 + c = f(R) \equiv 0 \bmod p$. The second is easy. If $R_1 \equiv R \bmod pL$ holds, then we have $2(R + a) \equiv 0 \bmod p$, and so $f(R) \equiv f(-a) \equiv c \bmod p$, which implies $p \mid c$. Thus $R_1 \equiv R \bmod pL$ does not happen if $p > c$.
Let us confirm $0 \le R_1 < pL$; suppose that there are infinitely many primes $p \in Spl(f)$ such that $R_1 < 0$; this implies $-2a < R - pL < 0$, and so there is an integer r between $-2a$ and 0 such that $r = R - pL$ holds for infinitely many primes $p \in Spl(f)$. Therefore we have $f(r) = f(R - pL) \equiv 0 \bmod p$ for infinitely many primes p, that is $f(r) = 0$, which contradicts the irreducibility of $f(x)$. Next, suppose that $R_1 \ge pL$ and so $0 \le R \le -2a$ for infinitely many primes $p \in Spl(f)$; then there is an integer r between 0 and $-2a$ such that $r = R$ holds for infinitely many primes $p \in Spl(f)$. This implies $f(r) = f(R) \equiv 0 \bmod p$, which contradicts the irreducibility of $f(x)$ again.

Second, we assume that $f(x) = (x + a)^2 + x + c$. Then $A = 2a + 1 \equiv 0 \bmod L$ follows from the assumption. For a prime $p \in Spl(f)$, take an integer R satisfying (8); then an integer $R_1 = pL - R - 2a - 1$ satisfies conditions $f(R_1) \equiv 0 \bmod p$, $R_1 \equiv 0 \bmod L$, $R_1 \not\equiv R \bmod pL$ and $0 \le R_1 < pL$ except finitely many primes similarly to the above, hence we have $C_p(f) = L$. □

Theorem 2. *Let $f(x) = x^2+Ax+B$ be a monic irreducible polynomial of degree 2, and $L(>1)$ an integer. Suppose that $A \not\equiv 0 \bmod L$. For a prime $p \in Spl(f)$, define an integer t by*

$$pt \equiv A \bmod L \text{ and } 1 \leq t \leq L-1.$$

Then we have

$$C_p(f) = \begin{cases} t & \text{if} \quad R \leq tp, \\ t+L & \text{if} \quad R \geq tp+1 \end{cases} \tag{9}$$

except finitely many primes p, where an integer R is defined by

$$f(R) \equiv 0 \bmod p,\ R \equiv 0 \bmod L,\ 0 \leq R \leq pL-1. \tag{10}$$

Proof. First, let us assume that $f(x) = x^2 + 2ax + b$ $(a, b \in \mathbb{Z})$ with $A = 2a \not\equiv 0 \bmod L$. To evaluate $C_p(f)$, we must find another integer R', which satisfies (10). First, we show that $-R-2a$ is another solution of $f(x) \equiv 0 \bmod p$. Put $s = -R-2a$; then $f(s) = f(R) \equiv 0 \bmod p$ is easy. If $s \equiv R \bmod p$, then we have $2a \equiv -2R \bmod p$, and hence $R \equiv -a \bmod p$, which implies $f(R) \equiv -a^2+b \bmod p$. Thus p is a divisor of $b - a^2 (\neq 0)$. Excluding such a finite number of primes, we have shown

$$f(-R-2a) \equiv 0 \bmod p, \quad -R-2a \not\equiv R \bmod p.$$

Now, to look for another solution R' with $R' \equiv 0 \bmod L,\ 0 \leq R' \leq pL-1$ explicitly, we put

$$R' := -R - 2a + p\alpha \quad (\alpha \in \mathbb{Z}).$$

Since $R' \equiv 0 \bmod L$ is equivalent to $p\alpha \equiv 2a \equiv A \bmod L$, we have $\alpha \equiv t \bmod L$. Hence R' is of the form

$$R' = -R - 2a + p(t + \beta L)$$

for an integer β. The inequality $0 \leq R' \leq pL-1$ means

$$0 \leq -R - 2a + tp + \beta Lp \leq pL-1, \tag{11}$$

from which follows

$$(R + 2a - tp)/(Lp) \leq \beta \leq 1 + (R + 2a - tp - 1)/(Lp),$$

and so conditions $1 \leq t \leq L-1$ and $0 \leq R \leq pL-1$ imply

$$2a/(Lp) - 1 + 1/L \leq \beta \leq 1 + (pL - 1 + 2a - p - 1)/(Lp),$$

which implies $\beta = 0, 1$ except finitely many primes p. Thus we have

$$C_p(f) = (R + R' + 2a)/p = \begin{cases} t & \text{if} \quad \beta = 0, \\ t+L & \text{if} \quad \beta = 1. \end{cases}$$

Since we have, by (11)

$$\begin{cases} 0 & \le -R-2a+tp \le pL-1 & \text{if} \quad \beta=0, \\ -pL & \le -R-2a+tp \le -1 & \text{if} \quad \beta=1, \end{cases}$$

we have

$$C_p(f) = \begin{cases} t & \text{if} \quad -R-2a+tp \ge 0, \\ t+L & \text{if} \quad -R-2a+tp \le -1, \end{cases}$$

hence

$$C_p(f) = \begin{cases} t & \text{if} \quad R \le tp-2a, \\ t+L & \text{if} \quad R \ge tp-2a+1. \end{cases}$$

Now, let us show that the number of primes p for satisfying $|R-tp| \le 2|a|$ is finite, which completes a proof. Suppose that there are infinitely many primes p so that $|R-tp| \le 2|a|$, which implies that there are infinitely many primes satisfying $R-tp=r$ for some integer r with $|r| \le 2|a|$. Therefore we have a contradiction $f(r) \equiv f(R) \equiv 0 \bmod p$ for infinitely many primes, i.e. $f(r)=0$.

The case of $f(x)=x^2+(2a+1)x+b$ is similarly proved. $\square$

Remark 2. *For $1 \le t \le L-1$, Theorem 2 implies*

$$Pr(f,L)[t]$$
$$= \lim_{X\to\infty} \frac{\#\left\{p \in Spl_X(f) \;\middle|\; \begin{array}{l} pt \equiv A \bmod L, \exists R \ s.t.\ f(R) \equiv 0 \bmod p, \\ R \equiv 0 \bmod L, 0 < R \le tp \end{array} \right\}}{\#Spl_X(f)}.$$

Our observation suggests that if $((A^2-4B)t, L)=1$, it is equal to

$$\frac{t}{L\varphi(L)},$$

and if we neglect the condition $pt \equiv A \bmod L$, we may expect

$$\lim_{X\to\infty} \frac{\#\left\{p \in Spl_X(f) \;\middle|\; \begin{array}{l} \exists R \ s.t.\ f(R) \equiv 0 \bmod p, \\ R \equiv 0 \bmod L, 0 < R \le tp \end{array} \right\}}{\#Spl_X(f)} = t/L.$$

2.2. The case that $n \ge 3$ and f is non-reduced

In this subsection, we assume that $f(x)$ is irreducible, of $n = \deg f(x) \ge 3$ and non-reduced moreover. Before stating observations, let us recall a distribution table by Eulerian numbers introduced in [7], which are defined by the following rules : Let $A(1,1)=1$ and let $A(n,k)$ $(1 \le k \le n)$ be defined by

$$A(n,k) = (n-k+1)A(n-1,k-1) + kA(n-1,k).$$

The Eulerian table E_n is defined by

$$E_n(k) = \frac{A(n-1,k)}{(n-1)!} \quad (1 \le k \le n-1).$$

The first conjecture is that for $T = 1$,

$$SPr = E_n, \text{ i.e. } SPr(f,L)[k] = E_n(k) \quad (1 \le k \le n-1).$$

Suppose $T > 1$. We introduce a function $F_n(x)$ by

$$F_n(x) = \frac{1}{(n-1)!} \sum_{0 \le i \le x} (-1)^i \binom{n}{i} (x-i)^{n-1} \quad (i \in \mathbb{Z}),$$

which is the volume of

$$\{(x_1, \cdots, x_{n-1}) \mid 0 \le {}^{\forall} x_i < 1, x - 1 < \sum_{i=1}^{n-1} x_i \le x\}$$

and

$$E_n(k) = F_n(k) \quad (1 \le k \le n-1).$$

(See I.9 in [2],[3].)

Our conjecture is

$$SPr[j] = \begin{cases} \frac{[\mathbb{Q}(f) \cap \mathbb{Q}(\zeta_T):\mathbb{Q}]}{\varphi(T)} F_n(j/T) & \text{if } (j,T) = 1 \text{ and } [[j]] = [[a_{n-1}/N]], \\ 0 & \text{otherwise,} \end{cases}$$

where for an integer j relatively prime to T, $[[j]]$ denotes an automorphism of $\mathbb{Q}(f) \cap \mathbb{Q}(\zeta_T)$ which is the restriction of an automorphism of $\mathbb{Q}(\zeta_T)$ induced by $\zeta_T \to \zeta_T^j$.

For a natural number $j < nT$, we put

$$v[j] = (n-1)!\, T^{n-1} F_n(j/T),$$

and we define a table R_T by

$$R_T[j] = \begin{cases} v[j] & \text{if } (j,T) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

The sum $\sum_{j=1}^{nT-1} R_T[j]$ is equal to Δ and the mean and the variance of the distribution R_T/Δ are $nT/2$ and $nT^2/12$, respectively.

The following shows that the above conjecture is compatible with Proposition 1.

Proposition 2. *For a table v above and an integer k not divisible by T, we have*

$$\sum_{j \equiv k \bmod T} v[j] = (n-1)!\, T^{n-1}, \ \textit{i.e.} \ \sum_{j \equiv k \bmod T} F_n(j/T) = 1.$$

To prove the proposition, we need the following:

Lemma 1. *For a natural number N, we have*

$$\sum_{\ell=0}^{N}(-1)^{\ell}\binom{N}{\ell}P(\ell)=0, \tag{13}$$

where $P(x)$ is any polynomial of $\deg P(x) \le N-1$, *and*

$$\sum_{\ell=0}^{N}(-1)^{\ell}\binom{N}{\ell}(N-\ell)^{N}=N!\,,\ \sum_{\ell=0}^{N}(-1)^{\ell}\binom{N}{\ell}\ell^{N}=(-1)^{N}N!\,. \tag{14}$$

Proof. Put

$$f_0(x)=1,\ f_k(x)=x(x-1)\cdots(x-(k-1))\ \ (k>0),$$

and differentiating $(x+1)^N=\sum_{\ell=0}^{N}\binom{N}{\ell}x^{\ell}$ k-times $(0\le k\le N-1)$ and substituting $x=-1$, we get

$$0=\sum_{\ell=0}^{N}(-1)^{\ell}\binom{N}{\ell}f_k(\ell)\quad(0\le k\le N-1)$$

by $f_k(0)=\cdots=f_k(k-1)=0$ $(k>0)$. Since a polynomial P of $\deg P(x)\le N-1$ is a linear combination of $f_0,\cdots,f_{N-1}$, we get (13).
We use induction on N to prove (14). It is obvious when $N=1$. Suppose $N>1$; then we have

$$\begin{aligned}
&\sum_{\ell=0}^{N}(-1)^{\ell}\binom{N}{\ell}(N-\ell)^{N}\\
=&\sum_{\ell=0}^{N-1}(-1)^{\ell}\binom{N}{\ell}(N-\ell)^{N}\\
=&N\sum_{\ell=0}^{N-1}(-1)^{\ell}\binom{N-1}{\ell}(N-\ell)^{N-1}
\end{aligned}$$

applying (13) to a polynomial $P(\ell)=(N-\ell)^{N-1}-(-\ell)^{N-1}$ of $\deg\le N-2$ and $N-1$ instead of N

$$\begin{aligned}
=&N\sum_{\ell=0}^{N-1}(-1)^{\ell}\binom{N-1}{\ell}(-\ell)^{N-1}\\
=&N\sum_{\ell=0}^{N-1}(-1)^{\ell+N-1}\binom{N-1}{\ell}\ell^{N-1}
\end{aligned}$$

$$
\begin{aligned}
&= N\sum_{\ell=0}^{N-1}(-1)^{\ell}\binom{N-1}{N-1-\ell}(N-1-\ell)^{N-1}\\
&= N\sum_{\ell=0}^{N-1}(-1)^{\ell}\binom{N-1}{\ell}(N-1-\ell)^{N-1}\\
&= N!.
\end{aligned}
$$

□

We remark that (13) implies $v[j] = v[nT - j]$ for $1 \le j \le nT - 1$ if j is not divisible by T.
Proof of Proposition 2.
Assume $0 < k < T$; then we have

$$
\begin{aligned}
\sum_{j\equiv k \bmod T} v[j] &= \sum_{m=0}^{n-1} v[mT+k]\\
&= \sum_{m=0}^{n-1}\sum_{i=0}^{m}(-1)^i\binom{n}{i}(mT+k-iT)^{n-1}\\
&= \sum_{i=0}^{n-1}\sum_{m=i}^{n-1}(-1)^{m-i}\binom{n}{m-i}(iT+k)^{n-1}
\end{aligned}
$$

using $\sum_{r=0}^{m}(-1)^r\binom{n}{r} = (-1)^m\binom{n-1}{m}$ $(0 \le m \le n-1)$

$$
\begin{aligned}
&= \sum_{i=0}^{n-1}(-1)^{n-1-i}\binom{n-1}{n-1-i}(iT+k)^{n-1}\\
&= \sum_{j=0}^{n-1}(-1)^{j}\binom{n-1}{j}((n-1-j)T+k)^{n-1},
\end{aligned}
$$

applying (13)

$$
\begin{aligned}
&= \sum_{j=0}^{n-1}(-1)^{j}\binom{n-1}{j}(-jT)^{n-1},\\
&= (n-1)!\,T^{n-1} \quad \text{by (14).}
\end{aligned}
$$

□

Here, let us refer to how to be convinced of the truth of conjectures by calculation by computer. For a polynomial f, we calculate a shrunk density

$$SPr_X(f,L)[k] = Pr_X(f,L)[kN] \quad (1 \le k < nT)$$

for a large number X, then we define V as follows : If $SPr_X(f,L)[k] \neq 0$, then $V[k] = A(n-1,k)$ if $T=1$, or $V[k] = v[k]$ if $T>1$. If $SPr_X(f,L)[k] = 0$, we put $V[k]=0$. Put $s = \sum_k V[k]$ and $D[k] = r(s \cdot SPr_X(f,L)[k]) - V[k]$, where $r(x)$ means the rounded integer of x. If $D[k]=0$, then $SPr_X(f,L)[k]$ is well-approximated by $V[k]/s$. We have only to observe that $|D[k]|\,(\in \mathbb{Z})$ decreases to 0 when X increases. The convergence is relatively slow.

2.2.1. The case that $n=4$ and f is reduced

In this case, an irreducible polynomial $f(x)$ is reduced, i.e. of the form $(x^2+ax)^2+b(x^2+ax)+c$ $(a,b,c\in\mathbb{Z})$, and entries of SPr seem rational numbers whose denominators are a divisor of $12\varphi(T^4)=2\Delta$.
When $T=1$, i.e. $2a\equiv 0 \bmod L$, we conjecture that

$$SPr = [0,1,0] \text{ or } [1/4,1/2,1/4],$$

and it is likely that $SPr=[0,1,0]$ if and only if L divides a. Even if $SPr=[0,1,0]$ holds, $Pr_X(f,L)[2L]\neq 1$ may happen.
Suppose that $T>1$; put

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

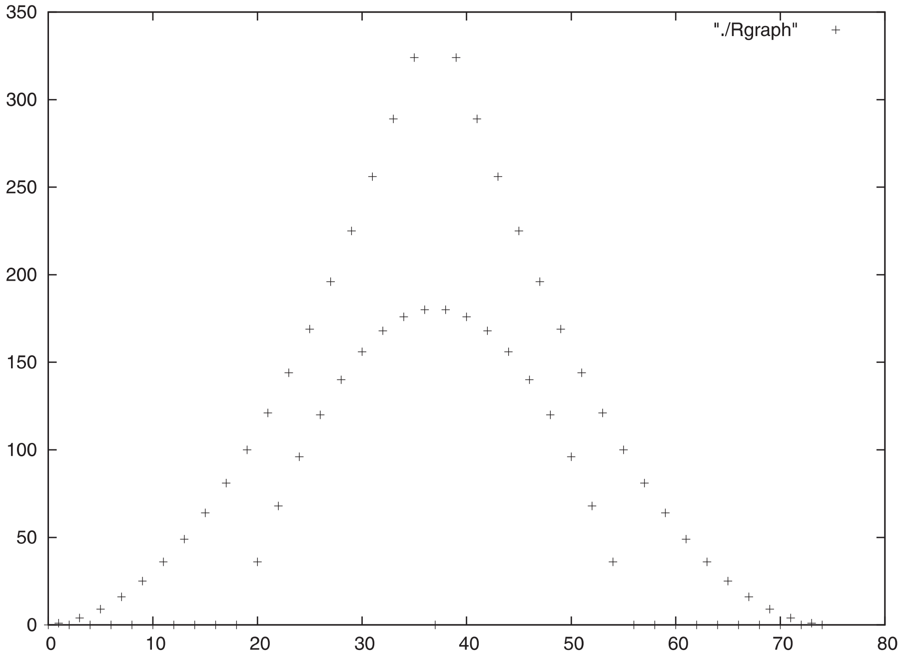
We conjecture that there is a constant c such that for $k=1,\cdots,T-1$, a sub-vector $c(SPr[k], SPr[T+k], SPr[2T+k], SPr[3T+k])$ is equal to one of

$$\begin{aligned}
&(0,0,0,0),\\
&(k^2, f_2(T+k), (4T-(2T+k))^2, 0),\\
&(0, (T+k)^2, f_2(4T-(2T+k)), (T-k)^2),\\
&(k^2, f_3(T+k), f_3(4T-(2T+k)), (4T-(3T+k))^2).
\end{aligned}$$

The sum of entries of the second, the third and the last is equal to $4T^2$, $4T^2$ and $8T^2$, respectively. Therefore Proposition 1 implies that the last line does not appear together with the second and the third at the same time. If T is odd, the last does not occur, and there is a non-zero constant c such that every non-zero $cSPr[j]$ is equal to $R_T[j]$ defined by

$$R_T[j] = \begin{cases} j^2 & \text{if } j\equiv 0 \bmod 2, \quad\quad 2\le j\le 2T-2,\\ f_2(j) & \text{if } j\equiv 1 \bmod 2,\ T+2\le j\le 2T-1,\\ 0 & \text{if } 1\le j\le 2T \text{ and except the above,}\end{cases}$$
$$R_T[4T-j] = R_T[j] \text{ if } 1\le j\le 2T.$$

Let us give a graph of R_{19}.



The author does not know the meaning of polynomials f_2, f_3.

BIBLIOGRAPHIE

[1] W. Duke, J.B. Friedlander and H. Iwaniec: *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math., **141**(1995), 423-441.

[2] W. Feller: *An introduction to probability theory and its applications*, Vol. 2, J. Wiley, New York, 1966.

[3] D. Foata: *Distributions eulériennes et mahoniennes sur le groupe des permutations,* in "Higher Combinatorics, Proceedings of the NATO Advanced Study Institute, Berlin, West Germany, September 1-10, 1976" (M.Aigner, Ed), 27-49, Reidel, Dordrecht/Boston, 1977.

[4] H. Iwaniec, E. Kowalski: *Analytic Number Theory*, American Mathematical Society, Colloquium Publications textbf53(2004).

[5] T. Hadano, Y. Kitaoka, T. Kubota, M. Nozaki: *Densities of sets of primes related to decimal expansion of rational numbers*, Number Theory: Tradition and Modernization, pp. 67-80, W. Zhang and Y. Tanigawa, eds. ©2006 Springer Science + Business Media,Inc.

[6] Y. Kitaoka: *A statistical relation of roots of a polynomial in different local files*, Math. of Comp. **78**(2009), 523-536.

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

[8] Y. Kitaoka: *A statistical relation of roots of a polynomial in different local files III*, Osaka J. Math. 49 (2012), 393-420.

[9] Á. Tóth: *Roots of Quadratic congruences*, Internat. Math. Res. Notices 2000, 719-739.

Received August 3, 2011
Accepted April 24, 2012

Yoshiyuki Kitaoka
Department of Mathematics
Meijo University Tenpaku
Nagoya, 468-8502, Japan.
E-mail, kitaoka@meijo-u.ac.jp: