International Journal of Statistics and Probability; Vol. 7, No. 1; January 2018
ISSN 1927-7032 E-ISSN 1927-7040
Published by Canadian Center of Science and Education

Statistical Distribution of Roots of a Polynomial Modulo Primes III

Yoshiyuki Kitaoka[1]

Correspondence: Yoshiyuki Kitaoka, E-mail: kitaoka@meijo-u.ac.jp

Received: November 19, 2017 Accepted: December 5, 2017 Online Published: December 15, 2017

doi:10.5539/ijsp.v7n1p115 URL: https://doi.org/10.5539/ijsp.v7n1p115

Abstract

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ $(a_{n-1}, \ldots, a_0 \in \mathbb{Z})$ be a polynomial with complex roots $\alpha_1, \ldots, \alpha_n$ and suppose that a linear relation over $\mathbb{Q}$ among $1, \alpha_1, \ldots, \alpha_n$ is a multiple of $\sum_i \alpha_i + a_{n-1} = 0$ only. For a prime number p such that $f(x) \bmod p$ has n distinct integer roots $0 < r_1 < \cdots < r_n < p$, we proposed in a previous paper a conjecture that the sequence of points $(r_1/p, \ldots, r_n/p)$ is equi-distributed in some sense. In this paper, we show that it implies the equi-distribution of the sequence of $r_1/p, \ldots, r_n/p$ in the ordinary sense and give the expected density of primes satisfying $r_i/p < a$ for a fixed suffix i and $0 < a < 1$.

Keywords: polynomial, equi-distribution

1. Introduction

Let

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

be a monic polynomial of degree n (≥ 2) over the ring $\mathbb{Z}$ of integers with complex roots $\alpha_1, \ldots, \alpha_n$. We put

$$Spl_X(f) := \{p \leq X \mid f(x) \text{ is fully splitting modulo } p\}$$

for a positive number X and $Spl(f) := Spl_\infty(f)$. Here the letter p denotes a prime number, and a polynomial $f(x)$ is fully splitting modulo p if and only if

$$f(x) \equiv \prod_{i=1}^{n}(x - r_i) \bmod p \tag{2}$$

for some integers r_i. We know that $Spl(f)$ is an infinite set and that the density theorem due to Chebotarev holds; that is,

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

where $\mathbb{Q}$ is the rational number field and $\mathbb{Q}(f)$ is a finite Galois extension field of $\mathbb{Q}$ generated by all roots of $f(x)$. In this note, we require the following condition on the above local roots $r_1, \ldots, r_n$:

$$0 \leq r_1 \leq r_2 \leq \cdots \leq r_n < p. \tag{3}$$

The condition (3) determines the ith local root r_i uniquely. As a basic assumption, we assume that there is no non-trivial linear relation over $\mathbb{Q}$ among roots $\alpha_1, \ldots, \alpha_n$ and 1 except for a trivial relation $\sum \alpha_i + a_{n-1} = 0$ in this paper. We know that any irreducible polynomial of prime degree, or a polynomial f of degree n with $[\mathbb{Q}(f) : \mathbb{Q}] = n!$ has no non-trivial linear relation among roots and 1. An irreducible polynomial f of degree 4 has a non-trivial linear relation among roots and 1 if and only if $f(x)$ is of the form $g(h(x))$ for quadratic polynomials g, h (Kitaoka, 2017). When the degree is greater than 5, there is no such a simple classification.

We consider the following two kinds of uniformity: Put

$$\hat{\mathfrak{D}}_n := \{(x_1 \ldots, x_n) \in [0, 1)^n \mid 0 \leq x_1 \leq \cdots \leq x_n < 1, \sum_{i=1}^{n} x_i \in \mathbb{Z}\} \tag{4}$$

which is on the union of hyper-planes defined by $\sum x_i = k \in \mathbb{Z}$ in $\mathbb{R}^n$ and for a set $D \subset [0, 1)^n$ with $D = \overline{D^\circ}$

$$Pr_D(f, X) := \frac{\#\{p \in Spl_X(f) \mid (r_1/p, \ldots, r_n/p) \in D\}}{\#Spl_X(f)},$$

where local roots r_i are supposed to satisfy properties (2), (3). We proposed (Kitaoka, 2017)

Conjecture 1

$$\lim_{X\to\infty} Pr_D(f,X) = \frac{vol(D\cap\hat{\mathfrak{D}}_n)}{vol(\hat{\mathfrak{D}}_n)}. \tag{5}$$

Here, "*vol*" is the volume on the hyper-plane in $\mathbb{R}^n$. On the other hand, the classical concept of the uniformity is

Conjecture 2

$$\lim_{X\to\infty} \frac{\sum_{p\in Spl_X(f)} \#\{i \mid r_i/p \le a, 1\le i\le n\}}{n\cdot \#Spl_X(f)} = a \tag{6}$$

for a real number $a\in[0,1)$.

Due to (Duke, Friedlander & Iwaniec, 1995) and (Tóth, 2000), Conjecture 2 is true for a quadratic polynomial, however nothing is known if $n>2$.

We stated in (Kitaoka, 2017) that Conjecture 2 follows from Conjecture 1 as far as we checked by the Monte Carlo method. We give the rigorous proof here, that is,

Theorem 1. *Let $f(x)$ be a monic polynomial over $\mathbb{Z}$ of degree n. Under the assumption that there is no non-trivial linear relation over $\mathbb{Q}$ among roots of $f(x)$ and* 1*, Conjecture 1 implies Conjecture 2.*

To prove this, putting $D_{i,a} := \{(x_1,\ldots,x_n)\in[0,1)^n \mid x_i\le a\}$ for a given number $a\in[0,1)$, we have only to show

$$\sum_{i=1}^{n} \frac{vol(D_{i,a}\cap\hat{\mathfrak{D}}_n)}{n\cdot vol(\hat{\mathfrak{D}}_n)} = a \tag{7}$$

by (Kitaoka, 2017). To show it, we evaluate $\frac{vol(D_{i,a}\cap\hat{\mathfrak{D}}_n)}{vol(\hat{\mathfrak{D}}_n)}$ (Proposition 1), which gives as a by-product the density of primes p satisfying $r_i/p<a$:

Theorem 2. *Let $f(x)$ be a monic polynomial over $\mathbb{Z}$ of degree n. Under the assumption that there is no non-trivial linear relation over $\mathbb{Q}$ among roots of $f(x)$ and* 1*. Then Conjecture 1 implies for* $1\le i\le n$

$$\begin{aligned}&\lim_{X\to\infty}\frac{\#\{p\in Spl_X(f)\mid r_i/p<a\}}{\#Spl_X(f)}\\ =&\frac{1}{(n-1)!}\sum_{\substack{0\le h\le n\\ 1\le l\le n-1}}\sum_{k=i}^{n}(-1)^{h+k+n}\binom{n}{k}\sum_{m=1}^{n-1}\binom{k}{n-h-m+l}\binom{n-k}{m-l}M(l-ha)^{n-1},\end{aligned}$$

where the binomial coefficient $\binom{A}{B}$ is supposed to vanish unless $0\le B\le A$, and $M(x) := \max(x,0)$.

When $i=1$, a simpler formula is given in Proposition 1 in the next section. Let us give numerical data for a polynomial $f(x) = x^6+x^5+\cdots+1 = (x^7-1)/(x-1)$. Put

$$Ex(a,m,i) := \frac{\#\{p\in Spl_X(f)\mid r_i/p<a\}}{\#Spl_X(f)} \quad (X = 10^{10}\cdot m)$$

and denote the expected limit given by the above theorem by $T(a,i)$ and the error by

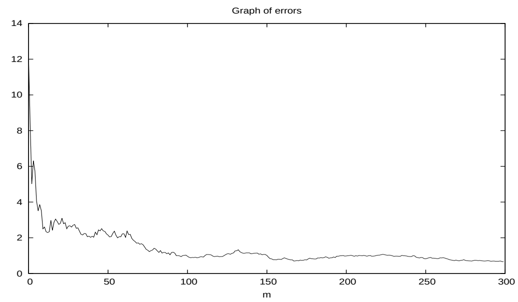
$$er(m) := 10^5 \max_{1\le k\le 100, 1\le i\le 6} |Ex(k/100,m,i) - T(k/100,i)|.$$

The graph of $er(m)$ $(m=1,\ldots,300)$ is below.

Conjecture 1 is generalized to a polynomial with a non-trivial linear relation among roots (Kitaoka, 2017). To treat such a polynomial, a more intrinsic proof of Theorem 1 independent of evaluation is desirable.

2. Proof

Hereafter, a real number a satisfies $0\le a<1$.



Lemma 1. *For an integer k with $1 \le k \le n$, let*

$$V(k) := vol\left(\left\{ \boldsymbol{x} \in [0,1)^n \,\middle|\, x_1, \dots, x_k \le a < x_{k+1}, \dots, x_n, \sum_{j=1}^{n} x_j \in \mathbb{Z} \right\}\right) \cos\theta, \tag{8}$$

for the angle θ of two hyper-planes defined by $x_j = 0$ and by $x_1 + \cdots + x_n = 0$ in $\mathbb{R}^n$. Then we have

$$\frac{vol(D_{i,a} \cap \hat{\mathfrak{D}}_n)}{vol(\hat{\mathfrak{D}}_n)} = \sum_{k=i}^{n} \binom{n}{k} V(k). \tag{9}$$

Proof. It is easy to see

$$\begin{aligned}
& vol(D_{i,a} \cap \hat{\mathfrak{D}}_n) \\
&= \sum_{k=i}^{n} vol\{\boldsymbol{x} \mid 0 \le x_1 \le \cdots \le x_k \le a < x_{k+1} \le \cdots \le x_n < 1, \sum x_j \in \mathbb{Z}\} \\
&= \sum_{k=i}^{n} \frac{1}{k!(n-k)!} vol\{\boldsymbol{x} \mid 0 \le x_1, \dots, x_k \le a < x_{k+1}, \dots, x_n < 1, \sum x_j \in \mathbb{Z}\} \\
&= \frac{1}{n!} \sum_{k=i}^{n} \binom{n}{k} vol\left\{ \boldsymbol{x} \,\middle|\, 0 \le x_1, \dots, x_k \le a < x_{k+1}, \dots, x_n < 1, \sum_{j} x_j \in \mathbb{Z} \right\} \\
&= vol(\hat{\mathfrak{D}}_n) \sum_{k=i}^{n} \binom{n}{k} V(k),
\end{aligned}$$

using $vol(\hat{\mathfrak{D}}_n) = \frac{1}{n! \cos\theta}$. □

To evaluate $V(k)$, we quote the following (Feller, 1966):

Lemma 2. *For a natural number k, the volume of a subset of the unit cube $[0,1)^k$ defined by $\{(x_1, \dots, x_k) \mid x_1 + \cdots + x_k \le x\}$ is given by*

$$U_k(x) := \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} M(x-i)^k.$$

Lemma 3. *For $k = n$, we have*

$$V(n) = \frac{1}{(n-1)!} \sum_{\substack{0 \le i \le n, \\ 1 \le k \le n-1}} (-1)^i \binom{n}{i} M(k - ia)^{n-1}. \tag{10}$$

Proof. It is easy to see that

$$\begin{aligned}
V(n) &= vol(\{\boldsymbol{x} \in \mathbb{R}^n \mid 0 \le x_1, \dots, x_n \le a, \sum_{i=1}^{n} x_i \in \mathbb{Z}\}) \cos\theta \\
&= \sum_{k=1}^{n-1} vol(\{\boldsymbol{x} \in \mathbb{R}^n \mid 0 \le x_1, \dots, x_n \le a, \sum_{i=1}^{n} x_i = k\}) \cos\theta
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=1}^{n-1} vol(\{\boldsymbol{x} \in \mathbb{R}^{n-1} \mid 0 \le x_1, \ldots, x_{n-1} \le a, 0 \le k - \sum_{i=1}^{n-1} x_i \le a\}) \\
&= \sum_{k=1}^{n-1} vol(\{\boldsymbol{x} \in \mathbb{R}^{n-1} \mid 0 \le x_1, \ldots, x_{n-1} \le a, \sum_{i=1}^{n-1} x_i \le k\}) \\
&\qquad - \sum_{k=1}^{n-1} vol(\{\boldsymbol{x} \in \mathbb{R}^{n-1} \mid 0 \le x_1, \ldots, x_{n-1} \le a, \sum_{i=1}^{n-1} x_i \le k-a\}).
\end{aligned}
$$

The volume of the set $\{\boldsymbol{x} \in \mathbb{R}^{n-1} \mid 0 \le x_1, \ldots, x_{n-1} \le a, \sum_{i=1}^{n-1} x_i \le K\}$ is equal to

$$
\begin{aligned}
& a^{n-1} vol(\{\boldsymbol{x} \in \mathbb{R}^{n-1} \mid 0 \le t_1, \ldots, t_{n-1} \le 1, \sum_{i=1}^{n-1} t_i \le K/a\}) \\
&= a^{n-1} U_{n-1}(K/a) \\
&= \frac{a^{n-1}}{(n-1)!} \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} M(K/a - i)^{n-1} \\
&= \frac{1}{(n-1)!} \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} M(K - ia)^{n-1}.
\end{aligned}
$$

Therefore we have

$$
\begin{aligned}
V(n) =& \frac{1}{(n-1)!} \sum_{k=1}^{n-1} \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} \{M(k-ia)^{n-1} - M(k-(i+1)a)^{n-1}\} \\
=& \frac{1}{(n-1)!} \sum_{k=1}^{n-1} \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} M(k-ia)^{n-1} \\
+& \frac{1}{(n-1)!} \sum_{k=1}^{n-1} \sum_{i=1}^{n} (-1)^i \binom{n-1}{i-1} M(k-ia)^{n-1} \\
=& \frac{1}{(n-1)!} \sum_{k=1}^{n-1} \sum_{i=0}^{n} (-1)^i \binom{n}{i} M(k-ia)^{n-1}.
\end{aligned}
$$

□

Lemma 4. *In case of* $1 \le k \le n-1$, *we have*

$$
V(k) = \sum_{m=1}^{n-1} (U_{k,n-1}(m-a) - U_{k,n-1}(m-1)), \tag{11}
$$

where

$$
U_{k,r}(t) := vol\{\boldsymbol{x} \in [0,1)^r \mid x_1, \ldots, x_k \le a < x_{k+1}, \ldots, x_r, \sum_{j=1}^{r} x_j < t\}. \tag{12}
$$

Proof. We see that

$$
\begin{aligned}
V(k) &= \sum_{m=1}^{n-1} vol \left\{ \boldsymbol{x} \in [0,1)^n \;\middle|\; x_1, \ldots, x_k \le a < x_{k+1}, \ldots, x_n, \sum_{j=1}^{n} x_j = m \right\} \cos\theta \\
&= \sum_{m=1}^{n-1} vol \left\{ \boldsymbol{x} \in [0,1)^{n-1} \;\middle|\; x_1, \ldots, x_k \le a < x_{k+1}, \ldots, x_{n-1}, a < m - \sum_{j=1}^{n-1} x_j < 1 \right\} \\
&= \sum_{m=1}^{n-1} (U_{k,n-1}(m-a) - U_{k,n-1}(m-1)).
\end{aligned}
$$

□

Lemma 5. *For integers r, k with $1 \le k \le r$, we have*

$$U_{k,r+1}(t) = \int_a^1 U_{k,r}(t-w)dw.$$

Proof. This follows from the equation

$$U_{k,r+1}(t) = \int_{x_{r+1}=a}^1 (\int_D dx_1, \dots dx_r)dx_{r+1}$$

where the domain D is given by the conditions $0 \le x_1, \dots, x_k \le a < x_{k+1}, \dots, x_r, \sum_{j=1}^r x_j < t - x_{r+1}$. □

Lemma 6.

$$\int_a^1 M(t-w)^m dw = \frac{1}{m+1}\{M(t-a)^{m+1} - M(t-1)^{m+1}\}.$$

Proof. The left-hand side is equal to

$$\begin{aligned}
&\int_a^1 \max(t-w,0)^m dw \\
=&\int_{t-a}^{t-1} \max(W,0)^m(-dW) \\
=&-\int_{-\infty}^{t-1} \max(W,0)^m dW + \int_{-\infty}^{t-a} \max(W,0)^m dW \\
=&-\frac{1}{m+1}M(t-1)^{m+1} + \frac{1}{m+1}M(t-a)^{m+1}.
\end{aligned}$$

□

Lemma 7. *For integers j, k with $j \ge 0, k \ge 1$, $U_{k,k+j}(t)$ is equal to*

$$\frac{1}{(k+j)!}\sum_{i=0}^k (-1)^i \binom{k}{i} \sum_{h=0}^j (-1)^{j+h}\binom{j}{h} M(t+h-j-(i+h)a)^{k+j}. \tag{13}$$

Proof. Suppose that $j = 0$; then $U_{k,k}(t)$ equals

$$\begin{aligned}
&vol\{\boldsymbol{x} \in [0,1)^k \mid x_1, \dots, x_k \le a, \sum_{j=1}^k x_j < t\} \\
=&a^k U_k(t/a) \\
=&\frac{1}{k!}\sum_{i=0}^k (-1)^i \binom{k}{i} M(t-ia)^k.
\end{aligned}$$

Second, suppose that the equation (13) is true; then we see that $U_{k,k+j+1}(t)$ equals

$$\begin{aligned}
&\int_a^1 U_{k,k+j}(t-w)dw \\
=&\frac{1}{(k+j)!}\sum_{i=0}^k (-1)^i \binom{k}{i} \sum_{h=0}^j (-1)^{j+h}\binom{j}{h} \int_a^1 M(t-w+h-j-(i+h)a)^{k+j} dw \\
=&\frac{1}{(k+j)!}\sum_{i=0}^k (-1)^i \binom{k}{i} \sum_{h=0}^j (-1)^{j+h}\binom{j}{h} \times
\end{aligned}$$

$$
\begin{aligned}
&\frac{1}{k+j+1}\{M(t+h-j-(i+h+1)a)^{k+j+1}-M(t+h-j-1-(i+h)a)^{k+j+1}\}\\
=&\frac{1}{(k+j+1)!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}\times\\
&\left\{\sum_{h=1}^{j+1}(-1)^{j+h+1}\binom{j}{h-1}M(t+h-j-1-(i+h)a)^{k+j+1}-\sum_{h=0}^{j}(-1)^{j+h}\binom{j}{h}M(t+h-j-1-(i+h)a)^{k+j+1}\right\}\\
=&\frac{1}{(k+j+1)!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}\times\left\{\sum_{h=1}^{j}(-1)^{j+h+1}\left(\binom{j}{h-1}+\binom{j}{h}\right)M(t+h-j-1-(i+h)a)^{k+j+1}\right.\\
&\qquad\left.+M(t-(i+j+1)a)^{k+j+1}-(-1)^jM(t-j-1-ia)^{k+j+1}\right\}\\
=&\frac{1}{(k+j+1)!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}\times\\
&\left\{\sum_{h=1}^{j}(-1)^{j+h+1}\binom{j+1}{h}M(t+h-j-1-(i+h)a)^{k+j+1}+M(t-(i+j+1)a)^{k+j+1}-(-1)^jM(t-j-1-ia)^{k+j+1}\right\},
\end{aligned}
$$

which completes the induction. □

Lemma 8. *For* $1 \le k \le n-1$, *we have*

$$
V(k)=\frac{1}{(n-1)!}\sum_{\substack{0\le h\le n\\1\le l\le n-1}}(-1)^{n+k+h}\sum_{m=1}^{n-1}\binom{k}{n-h-m+l}\binom{n-k}{m-l}M(l-ha)^{n-1}.
$$

Proof. For $1 \le k, m \le n-1$, we have

$$
\begin{aligned}
&(n-1)!\{U_{k,n-1}(m-a)-U_{k,n-1}(m-1)\}\\
=&\sum_{i,h\in\mathbb{Z}}(-1)^i\binom{k}{i}(-1)^{n-1-k+h}\binom{n-1-k}{h}M(m-a+h-(n-1-k)-(i+h)a)^{n-1}\\
&\quad-\sum_{i,h\in\mathbb{Z}}(-1)^i\binom{k}{i}(-1)^{n-1-k+h}\binom{n-1-k}{h}M(m-1+h-(n-1-k)-(i+h)a)^{n-1}\\
=&\sum_{h,l\in\mathbb{Z}}(-1)^{n+k+h}\binom{k}{n+l-h-m}\left\{\binom{n-1-k}{m-l}+\binom{n-1-k}{m-l-1}\right\}M(l-ha)^{n-1}\\
=&\sum_{\substack{0\le h\le n,\\1\le l\le n-1}}(-1)^{n+k+h}\binom{k}{n+l-h-m}\binom{n-k}{m-l}M(l-ha)^{n-1},
\end{aligned}
$$

where the restrictions on h, l follow from conditions $1 \le k, m \le n-1, 0 \le n+l-h-m \le k, 0 \le m-l \le n-k$. Lemma 4 completes the proof. □

Lemma 9. *Let* m, n *be integers satisfying* $0 \le m \le n-1$. *Then we have*

$$
\sum_{k=0}^{m}(-1)^k\binom{n}{k}=(-1)^m\binom{n-1}{m}. \tag{14}
$$

For a polynomial $P(x)=c_nx^n+\cdots+c_0$, *we have*

$$
\sum_{k=0}^{n}(-1)^kP(k)\binom{n}{k}=c_n(-1)^n\,n!. \tag{15}
$$

These are well-known and we omit the proof.

Proposition 1. *For an integer i with $1 \le i \le n$ and a real number $a \in [0,1)$, we have*

$$(n-1)!\,vol(D_{i,a} \cap \hat{\mathfrak{D}}_n)/vol(\hat{\mathfrak{D}}_n)$$
$$= \sum_{\substack{0\le h\le n\\ 1\le l\le n-1}} \sum_{k=i}^{n} (-1)^{h+k+n} \binom{n}{k} \left(\binom{n}{h} - \sum_{h\le q\le \max(l,h-1)} \binom{k}{q-h}\binom{n-k}{n-q} \right) M(l-ha)^{n-1}.$$

In particular, we have for $i = 1$

$$vol(D_{1,a} \cap \hat{\mathfrak{D}}_n)/vol(\hat{\mathfrak{D}}_n) = \sum_{\substack{0\le h\le n,\\ 1\le l\le n-1}} C_1(l,h) M(l-ha)^{n-1}, \tag{16}$$

where

$$C_1(l,h) = \frac{1}{(n-1)!} \begin{cases} (-1)^{n+h+1}\binom{n}{h} & \text{if } h \ge l+1, \\ 0 & \text{if } 1 \le h \le l, \\ (-1)^{n+l+1}\binom{n-1}{l} & \text{if } h = 0. \end{cases}$$

Proof. By Lemma 1, we have

$$\begin{aligned}
&(n-1)!\,vol(D_{i,a} \cap \hat{\mathfrak{D}}_n)/vol(\hat{\mathfrak{D}}_n) \\
=&(n-1)! \sum_{k=i}^{n} \binom{n}{k} V(k) \\
=&(n-1)!\,V(n) + (n-1)! \sum_{k=i}^{n-1} \binom{n}{k} V(k) \\
=& \sum_{\substack{0\le h\le n\\ 1\le l\le n-1}} (-1)^h \binom{n}{h} M(l-ha)^{n-1} \\
&+ \sum_{k=i}^{n-1} \binom{n}{k} \sum_{\substack{0\le h\le n\\ 1\le l\le n-1}} (-1)^{n+k+h} \sum_{m=1}^{n-1} \binom{k}{n-h-m+l} \binom{n-k}{m-l} M(l-ha)^{n-1} \\
=& \sum_{k=i}^{n} \binom{n}{k} \sum_{\substack{0\le h\le n\\ 1\le l\le n-1}} (-1)^{n+k+h} \sum_{m=1}^{n-1} \binom{k}{n-h-m+l} \binom{n-k}{m-l} M(l-ha)^{n-1},
\end{aligned}$$

since the binomial coefficient $\binom{0}{m-l}$ vanishes unless $m = l$. The partial sum $\sum_{m=1}^{n-1} \binom{k}{n-h-m+l}\binom{n-k}{m-l}$ is equal to

$$\begin{aligned}
&\sum_{1-l\le q\le n-1-l} \binom{k}{n-h-q}\binom{n-k}{q} \\
=& \sum_{0\le q\le \min(n-1-l,n-h)} \binom{k}{n-h-q}\binom{n-k}{q} \\
=& \binom{n}{n-h} - \sum_{\min(n-1-l,n-h)+1\le q\le n-h} \binom{k}{n-h-q}\binom{n-k}{q} \\
=& \binom{n}{h} - \sum_{h\le q\le \max(l,h-1)} \binom{k}{q-h}\binom{n-k}{n-q}.
\end{aligned} \tag{17}$$

Let us assume that $i = 1$ to show (16). Putting

$$\begin{aligned}
T(l,h) :=& \sum_{k=1}^{n} (-1)^{h+k+n} \binom{n}{k} \left(\binom{n}{h} - \sum_{h\le q\le \max(l,h-1)} \binom{k}{q-h}\binom{n-k}{n-q} \right) \\
=& -(-1)^{h+n}\binom{n}{h} - \sum_{k=1}^{n} (-1)^{h+k+n} \binom{n}{k} \sum_{q=h}^{\max(l,h-1)} \binom{k}{q-h}\binom{n-k}{n-q},
\end{aligned}$$

we have only to prove $T(l,h) = (n-1)!\,C_1(l,h)$. It is obviously true if $h \geq l+1$, since the partial sum on q is empty. In case of $h = 0$, we see that $T(l,0)$ is equal to

$$\begin{aligned}
&-(-1)^n - \sum_{k=1}^{n}(-1)^{k+n}\binom{n}{k}\sum_{q=0}^{l}\binom{k}{q}\binom{n-k}{n-q}\\
=&-(-1)^n - \sum_{k=1}^{n}(-1)^{k+n}\binom{n}{k}\sum_{q=0}^{l}\delta_{k,q}\\
=&-(-1)^n - \sum_{k=1}^{l}(-1)^{k+n}\binom{n}{k}\\
=&-\sum_{k=0}^{l}(-1)^{k+n}\binom{n}{k}\\
=&-(-1)^{n+l}\binom{n-1}{l}.
\end{aligned}$$

Lastly assume that $1 \leq h \leq l$. The sum $T(l,h) + (-1)^{h+n}\binom{n}{h}$ is equal to

$$\begin{aligned}
&-\sum_{k=1}^{n}(-1)^{h+k+n}\binom{n}{k}\sum_{q=h}^{l}\binom{k}{q-h}\binom{n-k}{n-q}\\
=&\ -\sum_{q=h}^{l}(-1)^{h+n}\binom{n}{h}\binom{n-h}{q-h}\sum_{k=1}^{n}(-1)^{k}\binom{h}{q-k}\\
=&\ -\sum_{q=h}^{l}(-1)^{h+n}\binom{n}{h}\binom{n-h}{q-h}(-1)^{q}\sum_{K=0}^{q-1}(-1)^{K}\binom{h}{K}\\
=&\ -\sum_{q=h}^{l}(-1)^{h+n}\binom{n}{h}\binom{n-h}{q-h}(-1)^{q}(-1)^{q-1}\binom{h-1}{q-1}\\
=&\ \sum_{q=h}^{l}(-1)^{h+n}\binom{n}{h}\binom{n-h}{q-h}\binom{h-1}{q-1}\\
=&\,(-1)^{h+n}\binom{n}{h},
\end{aligned}$$

which implies $T(l,h) = 0$. □

The proposition gives Theorem 2 by (17), and we see that the left-hand side of (7) is the sum of $C(l,h)M(l-ha)^{n-1}$ over integers l,h satisfying

$$1 \leq l \leq n-1, 0 \leq h \leq n, \tag{18}$$

where

$$\begin{aligned}
C(l,h) :=&\frac{1}{n!}\sum_{1\leq i\leq k\leq n}(-1)^{h+k+n}\binom{n}{k}\left(\binom{n}{h} - \sum_{h\leq q\leq \max(l,h-1)}\binom{k}{q-h}\binom{n-k}{n-q}\right)\\
=&\frac{1}{n!}\sum_{0\leq k\leq n}(-1)^{h+k+n}\,k\binom{n}{k}\left(\binom{n}{h} - \sum_{h\leq q\leq \max(l,h-1)}\binom{k}{q-h}\binom{n-k}{n-q}\right)\\
=&\frac{-1}{n!}\sum_{0\leq k\leq n}(-1)^{h+k+n}\,k\binom{n}{k}\sum_{h\leq q\leq \max(l,h-1)}\binom{k}{q-h}\binom{n-k}{n-q}.
\end{aligned}\tag{19}$$

To prove (7), we will show

$$C(l,h) = \begin{cases} \dfrac{-(-1)^{n-l}}{(n-1)!}\dbinom{n-2}{l-1} & \text{if } h = 0, \\ \dfrac{(-1)^{n-l}}{(n-1)!}\dbinom{n-2}{l-1} & \text{if } h = 1, \\ 0 & \text{if } h \geq 2. \end{cases} \tag{20}$$

Under the equations (20), Theorem 1 is proved as follows: The left-hand side of (7) is equal to

$$\begin{aligned}
&\sum_{l=1}^{n-1} \frac{-(-1)^{n-l}}{(n-1)!}\binom{n-2}{l-1} M(l)^{n-1} + \sum_{l=1}^{n-1} \frac{(-1)^{n-l}}{(n-1)!}\binom{n-2}{l-1} M(l-a)^{n-1} \\
=&\sum_{l=1}^{n-1} \frac{-(-1)^{n-l}}{(n-1)!}\binom{n-2}{l-1}(l^{n-1} - (l-a)^{n-1}) \\
=&\sum_{l=0}^{n-2} \frac{(-1)^{n+l}}{(n-1)!}\binom{n-2}{l}((n-1)al^{n-2} + O(l^{n-3})) \\
=&\, a.
\end{aligned}$$

Suppose $h = 0$; we see that

$$\begin{aligned}
C(l,0) =& \frac{-1}{n!} \sum_{0 \leq k \leq n} (-1)^{k+n}\, k \binom{n}{k} \sum_{0 \leq q \leq l} \binom{k}{q}\binom{n-k}{n-q} \\
=& \frac{-1}{n!} \sum_{0 \leq k \leq n} (-1)^{k+n}\, k \binom{n}{k} \sum_{0 \leq q \leq l} \delta_{k,q} \\
=& \frac{-1}{n!} \sum_{0 \leq k \leq l} (-1)^{k+n}\, k \binom{n}{k} \\
=& \frac{-1}{(n-1)!} \sum_{0 \leq k \leq l} (-1)^{k+n}\binom{n-1}{k-1} \\
=& \frac{-1}{(n-1)!} \sum_{0 \leq k \leq l-1} (-1)^{k+n+1}\binom{n-1}{k} \\
=& \frac{(-1)^{n+l+1}}{(n-1)!}\binom{n-2}{l-1},
\end{aligned}$$

which is (20).

Second we see that

$$C(l,1) = \frac{-1}{n!} \sum_{0 \leq k \leq n} (-1)^{1+k+n}\, k \binom{n}{k} \sum_{1 \leq q \leq l} \binom{k}{q-1}\binom{n-k}{n-q}.$$

Unless $q - 1 \leq k$ and $n - q \leq n - k$, binomial coefficients vanish, hence we may assume that $q = k$ or $q = k + 1$, and we see

$$\begin{aligned}
C(l,1) =& \frac{-1}{n!} \sum_{0 \leq k \leq n} (-1)^{1+k+n}\, k \binom{n}{k} \sum_{1 \leq q \leq l} (k\delta_{q,k} + (n-k)\delta_{q,k+1}) \\
=& \frac{-1}{n!} \sum_{0 \leq k \leq l} (-1)^{1+k+n}\, k^2 \binom{n}{k} + \frac{-1}{n!} \sum_{0 \leq k \leq l-1} (-1)^{1+k+n}\, k(n-k)\binom{n}{k} \\
=& \frac{(-1)^n}{(n-1)!} \sum_{0 \leq k \leq l-1} (-1)^k k \binom{n}{k} + \frac{1}{n!}(-1)^{l+n} l^2 \binom{n}{l}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{(-1)^n n}{(n-1)!} \sum_{0 \le k \le l-1} (-1)^k \binom{n-1}{k-1} + \frac{1}{n!}(-1)^{l+n} l^2 \binom{n}{l} \\
&= \frac{(-1)^{n+1} n}{(n-1)!} (-1)^{l-2} \binom{n-2}{l-2} + \frac{1}{n!}(-1)^{l+n} l^2 \binom{n}{l} \\
&= \frac{(-1)^{n+l}}{(n-1)!} \binom{n-2}{l-1}.
\end{aligned}
$$

Finally, assume that $h \ge 2$; hence $1 \le l \le n-1, 2 \le h \le n$ are supposed. By (19), we have

$$
\begin{aligned}
&- n!C(l,h) \\
&= \sum_{h \le q \le \max(l,h-1)} (-1)^{h+n} \binom{n}{h} \binom{n-h}{n-q} \sum_{0 \le k \le n} (-1)^k k \binom{h}{q-k} \\
&= \sum_{h \le q \le \max(l,h-1)} (-1)^{h+n} \binom{n}{h} \binom{n-h}{n-q} \sum_{0 \le K \le q} (-1)^{q+K} (q-K) \binom{h}{K} \\
&= 0,
\end{aligned}
$$

since

$$
\sum_{0 \le K \le q} (-1)^{q+K} (q-K) \binom{h}{K} = (-1)^q \sum_{0 \le K \le h} (-1)^K (q-K) \binom{h}{K} = 0
$$

by $h \ge 2$. Thus we have completed the proof.

References

Duke, W., Friedlander, J. B., & Iwaniec, H. (1995). Equidistribution of roots of a quadratic congruence to prime moduli. *Ann. of Math., 141,* 423-441. https://doi.org/10.2307/2118527

Feller, W. (1966). *An introduction to probability theory and its applications.* vol. 2, New York, J. Wiley.

Kitaoka, Y. (2017). Notes on the distribution of roots modulo a prime of a polynomial. *Unif. Distrib. Theory, 12,* 91-117.

Tóth. Á. (2000). Roots of Quadratic congruences, *Internat. Math. Res. Notices,* 719-739. https://doi.org/10.1155/S1073792800000404

Copyrights