MATHEMATICS OF COMPUTATION
Volume 78, Number 265, January 2009, Pages 523–536
S 0025-5718(08)02133-9
Article electronically published on May 12, 2008

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

YOSHIYUKI KITAOKA

ABSTRACT. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. We observe a statistical relation of roots of $f(x)$ in different local fields $\mathbb{Q}_p$, where $f(x)$ decomposes completely. Based on this, we propose several conjectures.

1. INTRODUCTION AND CONJECTURES

Let n be an odd natural number, and consider prime numbers p such that $p-1$ is divisible by n. Then the sum of n-th roots of unity in $(\mathbb{Z}/p\mathbb{Z})^\times$ is divisible by p, and the quotient $\mathfrak{s}(p)$ lies in the interval $[1, n-2]$. In the previous paper ([1]), we proposed a few conjectures on the distribution of $\mathfrak{s}(p)$.

In this paper, we give a comprehensive viewpoint. For a polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x], \tag{1.1}$$

we put

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

where p denotes prime numbers. Let $r_1, \ldots, r_n$ ($r_i \in \mathbb{Z}$, $0 \le r_i \le p-1$) be solutions of $f(x) \equiv 0 \bmod p$ for $p \in Spl(f)$; then $a_{n-1} + \sum r_i \equiv 0 \bmod p$ is clear. Thus there exists an integer $C_p(f)$ such that

$$a_{n-1} + \sum_{i=1}^{n} r_i = C_p(f)p. \tag{1.2}$$

We stress that the local solutions are supposed to satisfy

$$0 \le r_i \le p-1 \quad (r_i \in \mathbb{Z}). \tag{1.3}$$

To survey the situation, the proofs of the following will be gathered in the next section.

Proposition 1.1. *Let $f(x) = x + a$ ($a \in \mathbb{Z}$); then we have, for primes p with finitely many possible exceptions,*

$$C_p(f) = \begin{cases} 1 & \text{if } a > 0, \\ 0 & \text{if } a \le 0. \end{cases} \tag{1.4}$$

The range of $C_p(f)$ for a general case is given by

Received by the editor May 7, 2007 and, in revised form, December 10, 2007.
2000 *Mathematics Subject Classification.* Primary 11K99, 11C08, 11Y05.
Key words and phrases. Statistics, roots of polynomial, local field.
The author was partially supported by Grant-in-Aid for Scientific Research (C), The Ministry of Education, Science, Sports and Culture.

Proposition 1.2. *Suppose that* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ *does not have a linear factor in* $\mathbb{Q}[x]$. *Then we have, for* $p \in Spl(f)$,

$$1 \le C_p(f) \le n-1 \tag{1.5}$$

except finitely many possible primes.

Remark 1.3. We have chosen the local solutions under the condition (1.3). When we adopt the condition $-1/2 \le r_i/p < 1/2$, we have

$$C_p(x+a) = 0$$

for any prime $p\,(> |a|)$. Although it may seem desirable, in return, we lose our good expectation in Section 4.

The following is the second exceptional case where we can evaluate $C_p(f)$ explicitly.

Theorem 1.4. *Let* n *be a natural number and let*

$$f(x) = \sum_{i=0}^{2n} a_i x^i \in \mathbb{Z}[x]$$

be a monic polynomial such that (i) $f(x)$ *does not have a linear factor in* $\mathbb{Q}[x]$ *and* (ii) *there are polynomials* $f_1(x), f_2(x)$ *such that* $f(x) = f_1(f_2(x))$ *with* $\deg f_2(x) = 2$. *Then we have*

$$C_p(f) = n \;(= \frac{1}{2}\deg f(x)) \tag{1.6}$$

for primes $p \in Spl(f)$ *with finitely many possible exceptions.*

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. To study the distribution of the values $C_p(f)$, we put, for $1 \le c \le \deg f(x) - 1$ and a positive number X,

$$\begin{aligned} Pr(c, f, X) &= \frac{\#\{p \in Spl(f) \mid p \le X, C_p(f) = c\}}{\#\{p \in Spl(f) \mid p \le X\}}, \\ \mu(f, X) &= \frac{\sum_{p \in Spl(f), p \le X} C_p(f)}{\#\{p \in Spl(f) \mid p \le X\}}, \\ \sigma^2(f, X) &= \frac{\sum_{p \in Spl(f), p \le X} C_p(f)^2}{\#\{p \in Spl(f) \mid p \le X\}} - \mu(f, X)^2. \end{aligned}$$

Let us give one more definition.

Definition 1.5. Let $f(x)$ be a monic polynomial of $\deg f(x) \ge 2$ in $\mathbb{Z}[x]$; then there are monic polynomials $f_1(x), f_2(x) \in \mathbb{Z}[x]$ which satisfy $f(x) = f_1(f_2(x))$ and $\deg f_2(x) \ge 2$. We call the minimum among $\deg f_2(x)$ the reduced degree of $f(x)$, and denote it by $rd(f)$.

The reduced degree of the polynomial in Theorem 1.4 is 2, and the reduced degree of $x^n - a$ is the least prime divisor of n. By definition, the reduced degree is greater than 1, and the reduced degree of a polynomial of prime degree p is p. Using this notation, the theorem above is rephrased as follows.

Corollary 1.6. *Let $f(x)\,(\in \mathbb{Z}[x])$ be a monic polynomial of $rd(f)=2$ and suppose that it does not have a linear factor in $\mathbb{Q}[x]$. Then we have*

$$\begin{array}{lcl} \lim_{X\to\infty} Pr(c,f,X) & = & \begin{cases} 1 & \textit{if } c=\frac{1}{2}\deg f(x), \\ 0 & \textit{otherwise,} \end{cases} \\ \lim_{X\to\infty} \mu(f,X) & = & \frac{1}{2}\deg f(x), \\ \lim_{X\to\infty} \sigma^2(f,X) & = & 0. \end{array}$$

This case seems exceptional.

Now we propose a conjecture based on data in Section 5 :

Conjecture 1.7. *Let $f(x)$ be a monic irreducible polynomial of degree $n\,(\geq 3)$ in $\mathbb{Z}[x]$. We assume that the reduced degree of $f(x)$ is not 2. Then*

$$\begin{aligned} \mu(f) &:= \lim_{X\to\infty} \mu(f,X) \ = n/2, \\ \sigma^2(f) &:= \lim_{X\to\infty} \sigma^2(f,X) = n/12, \end{aligned} \tag{1.7}$$

and putting

$$Pr(c,f) := \lim_{X\to\infty} Pr(c,f,X),$$

the array of densities $[Pr(1,f),\dots,Pr(n-1,f)]$ depends only on the reduced degree $rd(f)$ of $f(x)$. Moreover, the following is likely:

$$Pr(c,f)=0 \ \textit{unless}\ (\deg f(x))/rd(f) \leq c \leq \deg f(x) - (\deg f(x))/rd(f)$$

and

$$Pr(k,f) = Pr(n-k,f) \quad \textit{for all } k,$$

$$Pr(1,f) \leq Pr(2,f) \leq \cdots \geq Pr(n-2,f) \geq Pr(n-1,f),$$

that is, a symmetric unimodal sequence.

Remark 1.8. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. We denote by K and K_f its minimal splitting field of $f(x)$ and the Galois closure of K over $\mathbb{Q}$, respectively. For a prime number p, we know that with finitely many possible exceptions, $f(x) \bmod p$ decomposes completely if and only if p decomposes fully in K, and hence in K_f. Thus Chebotarev's Density Theorem tells us that

$$\frac{\#\{p \in Spl(f) \mid p \leq X\}}{X/\log X} \sim \frac{1}{[K_f:\mathbb{Q}]},$$

and hence

$$\begin{aligned} Pr(c,f,X) &= \frac{\#\{p\in Spl(f) \mid p\leq X, C_p(f)=c\}}{\#\{p\in Spl(f)\mid p\leq X\}} \\ &\sim [K_f:\mathbb{Q}]\frac{\#\{p\in Spl(f) \mid p\leq X, C_p(f)=c\}}{X/\log X}. \end{aligned}$$

If $f(x)=g(x)h(x)$ for monic polynomials $g(x),h(x)\in\mathbb{Z}[x]$, then

$$C_p(f) = C_p(g)+C_p(h)$$

is easy to see. Numerical data suggests that

$$Pr(c,g) = \lim_{X\to\infty} \frac{\#\{p\in Spl(g)\cap Spl(h) \mid p\leq X, C_p(g)=c\}}{\#\{p\in Spl(g)\cap Spl(h)\mid p\leq X\}}.$$

2. Proofs

Proof of Proposition 1.1. Suppose that a prime number p is greater than $|a|$. If $a > 0$, then the local solution mod p is $p - a$, and so $C_p(f) = 1$. If $a \leq 0$, then the local solution is $-a$, and $C_p(f) = 0$. □

Proof of Proposition 1.2. Let $p \in Spl(f)$ and let $r_i \in \mathbb{Z}$ be integral solutions of $f(x) \equiv 0 \bmod p$ with $0 \leq r_i \leq p - 1$. By the definition (1.2), we have

$$C_p(f)p \geq a_{n-1},$$

which yields $C_p(f) \geq 0$ with finite exceptions. If $C_p(f) = 0$, then we have by (1.2),

$$0 \leq r_1 = -a_{n-1} - \sum_{i=2}^{n} r_i \leq -a_{n-1}.$$

Therefore, if there exist infinitely many primes $p \in Spl(f)$ such that $C_p(f) = 0$, then there is an integer r by the pigeon hole principle such that $0 \leq r \leq -a_{n-1}$ and $r = r_1$ for infinitely many primes, which means $f(r) = 0$ by $f(r) = f(r_1) \equiv 0 \bmod p$. This contradicts the assumption, and hence $C_p(f) \geq 1$ with finitely many possible exceptions.

Next, (1.2) implies

$$C_p(f)p \leq a_{n-1} + n(p-1),$$

and so $C_p(f) \leq n$ with finitely many possible exceptions. If $C_p(f) = n$, then we have by (1.2),

$$np \leq a_{n-1} + r_1 + (n-1)(p-1),$$

and hence

$$1 \leq p - r_1 \leq a_{n-1} - (n-1) \leq a_{n-1}.$$

Hence, if there exist infinitely many primes p such that $C_p(f) = n$, then there is an integer R such that $1 \leq R \leq a_{n-1}$ and $R = p - r_1$ for infinitely many primes p. For such primes, we have $f(-R) \equiv f(r_1) \equiv 0 \bmod p$, and so $f(-R) = 0$, which contradicts the assumption on $f(x)$. Thus we have $C_p(f) \leq n - 1$ with finitely many possible exceptions. □

Proof of Theorem 1.4. We may suppose that f_1, f_2 are monic and $f_2(x) = (x + a)^2$ for some rational number a. Then we have

$$f(x) = ((x+a)^2)^n + c_{n-1}((x+a)^2)^{n-1} + \cdots (c_i \in \mathbb{Q}),$$

and hence $a_{2n-1} = 2na$. The above means that $g(x) := f(x - a)$ is an even polynomial and then $g(x) = g(-x)$, i.e., $f(x - a) = f(-x - a)$. Substituting $x = a$, we have $f(0) = f(-2a)$, which means that $-2a$ is a root of a monic polynomial $f(x) - f(0) \in \mathbb{Z}[x]$. Thus $2a$ is an integer:

$$a = a_{2n-1}/2n \in \mathbb{Z}/2. \tag{2.1}$$

Let $p \in Spl(f)$ and $f(-a) \notin p\mathbb{Z}_p$. First we assume $a \in \mathbb{Z}$ and let $\pm r_i$ $(i = 1, \ldots, n)$ be solutions of $f(x - a) \equiv 0 \bmod p$; then $-a \pm r_i$ are solutions of $f(x) \equiv 0 \bmod p$. Take an integer R_i such that

$$-a + r_i \equiv R_i \bmod p \text{ and } 0 \leq R_i \leq p - 1.$$

Then we have $-a - r_i \equiv -2a - R_i \bmod p$, and $R_i, -2a - R_i$ $(i = 1, \ldots, n)$ are solutions of $f(x) \equiv 0 \bmod p$. Let us show that

$$-p + 1 \leq -2a - R_i \leq -1 \tag{2.2}$$

with finitely many possible exceptions. If $-2a - R_i \geq 0$ for infinitely many primes $p \in Spl(f)$, then we have $0 \leq R_i \leq -2a$ for the same primes, and hence there is an integer R such that $0 \leq R \leq -2a$ and $R = R_i$ for infinitely many primes $p \in Spl(f)$. This R satisfies $f(R) = f(R_i) \equiv 0 \bmod p$ for infinitely many primes p, which yields $f(R) = 0$. Thus we have the contradiction, and hence $-2a - R_i \leq -1$. If $-2a - R_i \leq -p$ for infinitely many primes $p \in Spl(f)$, then we have $-2a \leq R_i - p \leq -1$ for the same primes, and hence there is an integer R' such that $-2a \leq R' \leq -1$ and $R' = R_i - p$ for infinitely many primes $p \in Spl(f)$. This R' satisfies $f(R') \equiv f(R_i) \equiv 0 \bmod p$ for infinitely many primes p, which yields the contradiction $f(R') = 0$. Thus we have shown (2.2) with finitely many possible exceptions, and then $R_1, \ldots, R_n$ and $p - 2a - R_1, \ldots, p - 2a - R_n$ are all roots in $[0, p-1]$ of $f(x) \bmod p$. Hence we have

$$\begin{aligned} C_p(f) &= (a_{n-1} + \sum R_i + \sum (p - 2a - R_i))/p \\ &= (a_{n-1} + np - 2an)/p \\ &= n \end{aligned}$$

by (2.1).

Next, we assume $a \in \mathbb{Z}/2 \setminus \mathbb{Z}$ and put $a = b + 1/2$ ($b \in \mathbb{Z}$). We consider the above argument over $\mathbb{Z}_p/p\mathbb{Z}_p$ instead of $\mathbb{Z}/p\mathbb{Z}$; then $a \equiv b - (p-1)/2 \bmod p$ is clear. Let $\pm r_i$ ($i = 1, \ldots, n$) be solutions of $f(x - a) \equiv 0 \bmod p$; then $-b + (p-1)/2 \pm r_i$ ($\equiv -a \pm r_i \bmod p$) are all integral solutions of $f(x) \equiv 0 \bmod p$. Take an integer R_i such that

$$-b + (p-1)/2 + r_i \equiv R_i \bmod p \text{ and } 0 \leq R_i \leq p - 1.$$

Then we have $-b + (p-1)/2 - r_i \equiv -2b - 1 - R_i \bmod p$ and $R_i, -2b - 1 - R_i$ ($i = 1, \ldots, n$) are all solutions of $f(x) \equiv 0 \bmod p$. Let us show

$$0 \leq p - 2b - 1 - R_i \leq p - 1 \tag{2.3}$$

with finitely many exceptions. Suppose $p - 2b - 1 - R_i \geq p$; then we have $0 \leq R_i \leq -2b - 1$. If this is true for infinitely many primes p, then there is an integer R such that $0 \leq R \leq -2b - 1$ and $R = R_i$ for infinitely many primes. Therefore, $f(R) = f(R_i) \equiv 0 \bmod p$ for infinitely many primes, which implies the contradiction $f(R) = 0$.

Suppose $p - 2b - 1 - R_i \leq -1$; then $-2b \leq R_i - p \leq -1$. If there exist infinitely many such primes, then there exists an integer R' such that $-2b \leq R' \leq -1$ and $R' = R_i - p$ for infinitely many primes. Hence $f(R') \equiv f(R_i) \equiv 0 \bmod p$ for infinitely many primes. This is the contradiction and we have shown (2.3). Now we have, with the condition (2.3),

$$\begin{aligned} C_p(f) &= (a_{n-1} + \sum R_i + \sum (p - 2b - 1 - R_i))/p \\ &= (a_{n-1} + np - 2an)/p \\ &= n, \end{aligned}$$

which completes the proof. □

3. Miscellaneous remarks

Let us give some remarks. The following conjecture was stated in Remark 2 in [1].

Conjecture 3.1. *Let $F = \mathbb{Q}(\alpha)\,(\neq \mathbb{Q})$ be an algebraic number field with an algebraic integer α, and let k be a non-negative integer. For a prime number p which decomposes fully in F and a prime ideal $\mathfrak{p}$ lying above p, we write in $F_{\mathfrak{p}} = \mathbb{Q}_p$*

$$\alpha = c_{\mathfrak{p}}(0) + c_{\mathfrak{p}}(1)p + \cdots (c_{\mathfrak{p}}(i) \in \mathbb{Z}, 0 \leq c_{\mathfrak{p}}(i) < p).$$

Then the points $(c_{\mathfrak{p}}(0)/p, c_{\mathfrak{p}}(1)/p, \ldots, c_{\mathfrak{p}}(k)/p)(\in [0,1)^{k+1})$ distribute uniformly when $p, \mathfrak{p}$ run over those above.

The conjectures of the average and the variance in Conjecture 1.7 are intuitively supported by Conjecture 3.1 and Theorem 2 in [1], which is quoted below for convenience as

Theorem 3.2. *Let $x_1, x_2, \ldots, x_n$ be random variables on $\mathbb{R}$ obeying the uniform distribution $I(0,1)$, or what amounts to the same, their distribution functions are all equal to the set-theoretical characteristic function of $[0,1]$. Then, putting*

$$X_n = \frac{1}{\sqrt{n}}(x_1 + x_2 + \cdots + x_n - n/2),$$

$X = \lim_{n\to\infty} X_n$ determines a normal distribution on $\mathbb{R}$ with mean 0 and with variance $\frac{1}{12}$.

Indeed, we can show that Conjecture 3.1 yields the assertion on the average as follows.

Proposition 3.3. *Let $f(x)$ be a monic irreducible polynomial in $\mathbb{Z}[x]$ and suppose $n = \deg f(x) \geq 2$. Assuming Conjecture 3.1, we have*

$$\mu(f) = n/2.$$

The proof is quite similar to the proof of Proposition 1 in [1].

The following gives a connection between Conjecture 4 in [1] and the viewpoint in this paper.

Proposition 3.4. *Let $m\,(\geq 2)$ be a natural number and put $n = 3m$ and $f(x) = (x^3)^{m-1} + \cdots + x^3 + 1, g(x) = x^n - 1$. Then*

$$\mu(g) = (\deg g(x) - 1)/2,\ \sigma^2(g) = (\deg g(x) - 3)/12 \tag{3.1}$$

is true if and only if

$$\mu(f) = \frac{1}{2}\deg f(x),\ \sigma^2(f) = \frac{1}{12}\deg f(x).$$

Proof. First, we note that

$$g(x) = (x^3 - 1)f(x).$$

$Spl(g) \subset Spl(f)$ is clear. To see the converse, let $p \in Spl(f)$. Suppose that the order of any solution r of $f(x) \equiv 0 \bmod p$ is relatively prime to 3; then any solution r of $f(x) \equiv 0 \bmod p$ is a root of $x^m - 1 \equiv 0 \bmod p$, since $r^n \equiv 1 \bmod p$. This is the contradiction, because $\deg f(x) = 3m - 3 > m$. Thus there is a root r such that the order of $\langle r\rangle$ is divisible by 3 and hence $x^3 - 1 \bmod p$ is completely decomposable, and hence $Spl(g) = Spl(f)$. Let r_i $(0 \leq r_i \leq p-1)$ be roots of $f(x) \bmod p$ and let

$\{1, R_1, R_2\}$ $(0 \le R_i \le p-1)$ be roots of $x^3 - 1 = (x-1)(x^2+x+1) \bmod p$; then we have, by the definition

$$C_p(g) = (1 + R_1 + R_2 + \sum r_i)/p = C_p(x^2+x+1) + C_p(f).$$

Hence Theorem 1.4 implies $C_p(g) = 1 + C_p(f)$ with finitely many exceptional primes p, which yields

$$\mu(g) = \mu(f) + 1, \sigma^2(g) = \sigma^2(f),$$

which completes the proof. □

Remark 3.5. In the above proposition, (3.1) is the assertion in Conjecture 4 in [1], if n is odd.

Remark 3.6. Although we considered carrying at the first digit only, it is possible to consider it at every digit. Let $r_1, \ldots, r_n$ be solutions of $f(x) \equiv 0 \bmod p^i$; then $a_{n-1} + \sum r_j \equiv 0 \bmod p^i$ holds, and so we can consider $(a_{n-1} + \sum r_j)/p^i$ instead of $C_p(f)$. Let $\mu_i(f), \sigma_i^2(f), Pr_i(c, f)$ be those defined at the i-th digit similarly to the case $i = 1$. We expect that they are independent of i and the product $Pr_1(c_1, f) \cdots Pr_m(c_m, f)$ is equal to the density $Pr([c_1, \ldots, c_m], f)$, which is the density similarly defined for the array $[c_1, \ldots, c_m]$ with the carried integer c_i at the i-th digit.

4. Rational approximation of expected density

In this section, we discuss approximating the expected densities by rationals.

Let $f(x)$ be a monic polynomial of $rd(f) = 2$ such that $f(x)$ does not have a linear factor in $\mathbb{Q}[x]$; then we already know by Theorem 1.4 that

$$C_p(f) = \frac{1}{2} \deg f(x).$$

Let f be an irreducible monic polynomial of degree $3m$ in $\mathbb{Z}[x]$. If the reduced degree is 3, $Pr(c, f)$ is likely to be as follows:

$$Pr(c, f) = \begin{cases} 2^{-m}\dbinom{m}{c-m} & \text{if } m \le c \le 2m, \\ 0 & \text{otherwise.} \end{cases}$$

The data for $n = 3, 6, 9, 12, 15$ in the next section support this.

Similarly, in Tables 5 and 6 in [1], when $n = 3m$, densities seem to be approximated by

$$\begin{cases} 2^{-(m-1)}\dbinom{m-1}{s-m} & \text{if } m \le s \le 2m-1, \\ 0 & \text{otherwise.} \end{cases}$$

Professor Yukari Kosugi perceived that the densities in Tables 10 and 6 of [1] are approximated by Eulerian numbers if n is a prime number. Let us introduce this. Let $A(1, 1) = 1$ and let $A(n, k)$ $(1 \le k \le n)$ be defined by

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

Their values are:

$n \setminus k$	1	2	3	4	5	6	7	8	9
2	1	1							
3	1	4	1						
4	1	11	11	1					
5	1	26	66	26	1				
6	1	57	302	302	57	1			
7	1	12	1191	2416	1191	12	1		
8	1	247	4293	15619	15619	4293	247	1	
9	1	502	14608	88234	15619	88234	14608	502	1

In the tables referred above, the densities are well approximated by

$$A(n-2,s)/(n-2)!$$

when n is prime. Following her great insight, we easily see that the density $Pr(c,f)$ is well approximated by

$$A(\deg f(x)-1,c)/(\deg f(x)-1)!$$

if $rd(f)=\deg f(x)$ (cf. Section 5 below).

What is expected if $4 \le rd(f) < \deg f$? (Cf. f_3, f_4 in 5.6.)

5. Numerical data

5.1. $n=3$**.** In the following table, $\mu, \sigma^2, Pr(c)$ are the abbreviation of $\mu(f,10^9)$, $\sigma^2(f,10^9)$, $Pr(c,f,10^9)$ and $\#Spl = \#Spl(f,10^9)$. The expected values of $\mu(f)$, $\sigma^2(f)$, $Pr(c,f)$ are in the last line. We use these abbreviations hereafter if we do not refer, and the values are rounded off to four decimal places.

f	μ	σ^2	$Pr(1)$	$Pr(2)$	$\#Spl$
x^3-x-1	1.500	0.2500	0.4998	0.5002	8474030
x^3+x^2+x-1	1.500	0.2500	0.5002	0.4998	8472910
x^3-3x+1	1.500	0.2500	0.4999	0.5001	16949354
x^3+x^2-4x+1	1.500	0.2500	0.4999	0.5001	16948980
	$n/2=1.5$	$n/12=0.25$	1/2	1/2	

5.2. $n=4$**.** The reduced degrees of the following polynomials are 4. We put

$$\begin{aligned} f_1 &= x^4-x^3-x^2-x-1, \\ f_2 &= x^4-x^3-x^2+x+1, \\ f_3 &= x^4+x^3+x^2+x+1. \end{aligned}$$

f	μ	σ^2	$Pr(1)$	$Pr(2)$	$Pr(3)$	$\#Spl$
f_1	2.000	0.3333	0.1664	0.6667	0.1669	2118177
f_2	2.000	0.3333	0.1667	0.6667	0.1666	6354490
f_3	2.000	0.3333	0.1666	0.6667	0.1667	12711386
	$n/2=2$	$n/12=0.3333$	1/6	4/6	1/6	

Since $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$, we have $C_p(x^5-1)=C_p(x^4+x^3+x^2+x+1)$ and so the average, the variance, and the density are the same for x^5-1 and $x^4+x^3+x^2+x+1$. Indeed, the data for $x^4+x^3+x^2+x+1$ here and the data for $n=5, x=10^9$ in [1] are compatible.

5.3. $n = 5$. We put

$$\begin{aligned} f_1 &= x^5 - x^3 - x^2 - x + 1, \\ f_2 &= x^5 - x^4 - x^2 - x + 1, \\ f_3 &= x^5 + x^4 - x^2 - x + 1, \\ f_4 &= x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1. \end{aligned}$$

f	μ	σ^2
f_1	2.501	0.4169
f_2	2.497	0.4177
f_3	2.501	0.4161
f_4	2.500	0.4169
	$n/2 = 2.5$	$n/12 = 0.4167$

$Pr(1)$	$Pr(2)$	$Pr(3)$	$Pr(4)$	$\#Spl$
0.04160	0.4578	0.4587	0.04187	423981
0.04228	0.4600	0.4561	0.04157	423719
0.04110	0.4590	0.4579	0.04193	422711
0.04180	0.4582	0.4584	0.04167	10169695
$1/24 = 0.04167$	$11/24 = 0.4583$	$11/24$	$1/24$	

5.4. $n = 6$. We put

$$\begin{aligned} f_1 &= x^6 + x + 1, \\ f_2 &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\ f_3 &= x^6 + 2x^5 + x^4 + x^3 + x^2 + 1 = (x^3 + x^2)^2 + (x^3 + x^2) + 1, \\ f_4 &= x^6 + 2x^4 + x^3 + x^2 + x + 2 = (x^3 + x)^2 + (x^3 + x) + 2. \end{aligned}$$

The reduced degree of f_1, f_2 is 6.

f	μ	σ^2
f_1	3.005	0.5012
f_2	3.000	0.5000
	$6/2$	$6/12$

$Pr(1)$	$Pr(2)$	$Pr(3)$	$Pr(4)$	$Pr(5)$	$\#Spl$
0.0086	0.2135	0.5513	0.2177	0.0089	70292
0.0084	0.2164	0.5501	0.2167	0.0083	8474221
$1/120$ $= 0.0083$	$26/120$ $= 0.2167$	$66/120$ $= 0.5500$	$26/120$	$1/120$	

Since $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x-1)f_2$, we have $C_p(x^7 - 1) = C_p(f_2)$ and so the average, the variance, and the density are the same for $x^7 - 1$ and f_2. Indeed, the data for f_2 here and the data for $n = 7, x = 10^9$ in [1] are compatible.

The reduced degree of f_3, f_4 is 3.

f	μ	σ^2
f_3	3.001	0.5003
f_4	2.999	0.5004
	6/2	6/12

$Pr(1)$	$Pr(2)$	$Pr(3)$	$Pr(4)$	$Pr(5)$	$\#Spl$
0	0.2497	0.4997	0.2506	0	705553
0	0.2506	0.4996	0.2498	0	706369
0	1/4	1/2	1/4	0	

5.5. $n = 7$**.** We put

$$\begin{aligned} f_1 &= x^7 - x^5 - x^4 - x^3 - x^2 - x + 1, \\ f_2 &= x^7 + x^6 - x^5 - x^4 - x^3 - x^2 - x + 1, \\ f_3 &= x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1. \end{aligned}$$

f	μ	σ^2
f_1	3.495	0.5969
f_2	3.501	0.5792
f_3	3.500	0.5832
	7/2	$7/12 = 0.5833$

$Pr(1)$	$Pr(2)$	$Pr(3)$	$Pr(4)$	$Pr(5)$	$Pr(6)$	$\#Spl$
0.0016	0.0823	0.4206	0.4113	0.0832	0.0011	10076
0.0017	0.0779	0.4189	0.4228	0.0775	0.0014	9994
0.0014	0.0790	0.4192	0.4198	0.0792	0.0014	7264359
$1/6!$ $= 0.0014$	$57/6!$ $= 0.0792$	$302/6!$ $= 0.4194$				

5.6. $n = 8$**.** We put

$$\begin{aligned} f_1 &= x^8 + x + 2, \\ f_2 &= x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1, \\ f_3 &= (x^4 + x)^2 + 1, \\ f_4 &= (x^4 + x^2 + x)^2 + 2. \end{aligned}$$

The reduced degree of f_1, f_2 (resp. f_3, f_4) is 8 (resp. 4).

f	μ	σ^2
f_1	3.989	0.6587
f_2	3.999	0.6671
	$8/2 = 4$	$8/12 = 0.6667$

$Pr(1)$	$Pr(2)$	$Pr(3)$	$Pr(4)$	$Pr(5)$	$Pr(6)$	$Pr(7)$	$\#Spl$
0	0.0204	0.2514	0.4686	0.2376	0.0220	0	1225
0.0002	0.0240	0.2364	0.4793	0.2361	0.0238	0.0002	6354766
0.0002	0.0238	0.2363	0.4794	0.2363	0.0238	0.0002	

Here the last row is $A(7,c)/7!$.

f	μ	σ^2
f_3	4.004	0.6599
f_4	3.994	0.6655
	$8/2 = 4$	$8/12 = 0.6667$

$Pr(1)$	$Pr(2)$	$Pr(3)$	$Pr(4)$	$Pr(5)$	$Pr(6)$	$Pr(7)$	$\#Spl$
0	0.0267	0.2203	0.5028	0.2227	0.0276	0	44089
0	0.0288	0.2221	0.5020	0.2200	0.0270	0	44112
0	1/36	8/36	18/36	8/36	1/36	0	

For a reducible polynomial $f = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^2 + x + 1)(x^6 + x^3 + 1)$, the data for $n = 9$ in [1] means the following:

$Pr(1)$	$Pr(2)$	$Pr(3)$	$Pr(4)$	$Pr(5)$	$Pr(6)$	$Pr(7)$
0	0	0.24993	0.50014	0.24993	0	0

Put $g = x^2+x+1, h = x^6+x^3+1$; since $Spl(h) \subset Spl(g)$ and $C_p(c,f) = 1+C_p(h)$, the table above is compatible with the expectation in Section 4, noting that the reduced degree of $h(x)$ is three.

5.7. $n = 9$**.** We put

$$\begin{aligned} f_1 &= x^9 + x + 1, \\ f_2 &= x^9 + x^8 - 8x^7 - 7x^6 + 21x^5 + 15x^4 - 20x^3 - 10x^2 + 5x + 1, \\ f_3 &= (x^3 + x)^3 + 2, \\ f_4 &= (x^3 + x)^3 + (x^3 + x)^2 + 1. \end{aligned}$$

The reduced degree of f_1, f_2 (resp. f_3, f_4) is 9 (resp. 3).

f	μ	σ^2
f_1	4.506	0.6859
f_2	4.500	0.7500
f_3	4.491	0.7448
f_4	4.502	0.7499
	$9/2 = 4.5$	$9/12 = 0.75$

	f_1	f_2	f_3	f_4
$Pr(1)$	0	0.0000	0	0
$Pr(2)$	0.0064	0.0061	0	0
$Pr(3)$	0.1026	0.1064	0.1267	0.1240
$Pr(4)$	0.3654	0.3871	0.3768	0.3763
$Pr(5)$	0.4295	0.3877	0.3758	0.3737
$Pr(6)$	0.0962	0.1065	0.1208	0.1259
$Pr(7)$	0	0.0061	0	0
$Pr(8)$	0	0.0000	0	0
$\#Spl$	156	5649358	38912	38802

The following is the table of $A(8,c)/8!$:

c	1	2	3	4	5	6	7	8
	0.0000	0.0061	0.1065	0.3874	0.3874	0.1065	0.0061	0.0000

5.8. $n = 10$. We put

$$\begin{aligned} f_1 &= x^{10}+x+1, \\ f_2 &= x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1, \\ f_3 &= x^{10}+x^5+2, \\ f_4 &= x^{10}+3x^5+3. \end{aligned}$$

The reduced degree of f_1, f_2 is 10, and the one of f_3, f_4 is 5.

f	μ	σ^2
f_1	5.364	0.7769
f_2	5.000	0.8339
f_3	4.998	0.8362
f_4	5.000	0.8339
	$10/2=5$	$10/12=0.8333$

	f_1	f_2	f_3	f_4
$Pr(1)$	0	0.0000	0	0
$Pr(2)$	0	0.0014	0.0018	0.0018
$Pr(3)$	0	0.0403	0.0387	0.0383
$Pr(4)$	0.1818	0.2432	0.2483	0.2477
$Pr(5)$	0.3636	0.4302	0.4235	0.4239
$Pr(6)$	0.3636	0.2432	0.2475	0.2483
$Pr(7)$	0.0909	0.0404	0.0385	0.0382
$Pr(8)$	0	0.0014	0.0017	0.0017
$Pr(9)$	0	0.0000	0	0
$\#Spl$	11	5084435	254385	1271165

The following is the table of $A(9,c)/9!$:

c	1	2	3	4	5	6	7	8	9
	0.0000	0.0014	0.0403	0.2431	0.4304	0.2431	0.0403	0.0014	0.0000

5.9. $n = 12$. We put

$$\begin{aligned} f_1 &= (x^{13}-1)/(x-1), \\ f_2 &= (x^6+x)^2+(x^6+x)+1, \\ f_3 &= (x^4+x)^3-3(x^4+x)+1, \\ f_4 &= (x^3+x)^4+(x^3+x)^3+(x^3+x)^2+(x^3+x)+1. \end{aligned}$$

The reduced degree of f_1, f_2, f_3, f_4 is $12, 6, 4, 3$, respectively.

f	μ	σ^2
f_1	6.000	0.9993
f_2	5.796	1.125
f_3	6.073	1.004
f_4	5.996	0.9891
	$12/2=6$	$12/12=1$

	f_1	f_2	f_3	f_4	
$Pr(1)$	0.0000	0	0	0	0
$Pr(2)$	0.0001	0	0	0	0
$Pr(3)$	0.0038	0	0.0031	0	0
$Pr(4)$	0.0550	0.1296	0.0541	0.0605	0.0625
$Pr(5)$	0.2444	0.2593	0.2085	0.2556	0.25
$Pr(6)$	0.3938	0.3333	0.4093	0.3707	0.375
$Pr(7)$	0.2438	0.2407	0.2556	0.2537	0.25
$Pr(8)$	0.0553	0.0370	0.0649	0.0594	0.0625
$Pr(9)$	0.0038	0	0.0046	0	0
$Pr(10)$	0.0001	0	0	0	0
$Pr(11)$	0	0	0	0	0
$\#Spl$	4237228	54	1295	9862	

On the right column, the values $2^{-4}\binom{4}{k-4}$ for $4 \leq k \leq 8$ are given, and the following is the table of $A(11,c)/11!$ for $1 \leq c \leq 6$:

c	1	2	3	4	5	6
	0.0000	0.0001	0.0038	0.0552	0.2440	0.3939

5.10. $n = 15$**.** We put

$$\begin{aligned} f_1 &= x^{15} + x^{14} - 14x^{13} - 13x^{12} + 78x^{11} + 66x^{10} - 220x^9 \\ &\quad -165x^8 + 330x^7 + 210x^6 - 252x^5 - 126x^4 + 84x^3 \\ &\quad +28x^2 - 8x - 1, \\ f_2 &= x^{15} - 3x^5 + 1, \\ f_3 &= x^{15} + x^{10} - 2x^5 - 1, \\ f_4 &= x^{15} + x^{12} - 4x^9 - 3x^6 + 3x^3 + 1, \\ f_5 &= x^{15} + x^{12} - 12x^9 - 21x^6 + x^3 + 5, \end{aligned}$$

The reduced degree of f_1 is 15, and the reduced degrees of f_2, f_3 (resp. f_4, f_5) are 5 (resp. 3).

f	μ	σ^2
f_1	7.500	1.250
f_2	7.502	1.245
f_3	7.502	1.250
f_4	7.498	1.246
f_5	7.514	1.239
	$15/2 = 7.5$	$15/12 = 1.25$

	f_1	f_2	f_3	f_4	f_5	
$Pr(1)$	0.0000	0	0	0	0	0
$Pr(2)$	0	0	0	0	0	0
$Pr(3)$	0.0001	0.0001	0.0001	0	0	0
$Pr(4)$	0.0023	0.0025	0.0024	0	0	0
$Pr(5)$	0.0295	0.0278	0.0280	0.0314	0.0312	$1/32 = 0.0313$
$Pr(6)$	0.1472	0.1491	0.1495	0.1553	0.1504	$5/32 = 0.1563$
$Pr(7)$	0.3206	0.3195	0.3200	0.3139	0.3117	$10/32 = 0.3125$
$Pr(8)$	0.3212	0.3205	0.3190	0.3139	0.3171	$10/32 = 0.3125$
$Pr(9)$	0.1474	0.1498	0.1500	0.1542	0.1590	$5/32 = 0.1563$
$Pr(10)$	0.0294	0.0283	0.0284	0.0314	0.0305	$1/32 = 0.0313$
$Pr(11)$	0.0023	0.0024	0.0026	0	0	0
$Pr(12))$	0.0000	0.0000	0.0001	0	0	0
$Pr(13)$	0	0	0	0	0	0
$Pr(14)$	0	0	0	0	0	0
$\#Spl$	3389785	169310	169660	62503	20581	

The following is the table of $A(14,c)/14!$ for $1 \leq c \leq 7$:

c	1	2	3	4	5	6	7
	0.0000	0.0000	0.0001	0.0023	0.0295	0.1473	0.3209

References

1. 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., Springer, New York, 2006. MR2213829 (2007b:11110)

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