Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 25, 2019, No. 4, 72–82
DOI: 10.7546/nntdm.2019.25.4.72-82

Distribution of constant terms of irreducible polynomials in $\mathbb{Z}_p[x]$

Sarah C. Cobb[1], Michelle L. Knox[2], Marcos Lopez[3], Terry McDonald[4] and Patrick Mitchell[5]

Department of Mathematics, Midwestern State University
3410 Taft Blvd, Wichita Falls, TX 76308 USA
e-mails: [1] sarah.cobb@msutexas.edu, [2] michelle.knox@msutexas.edu,
[3] marcos.lopez@msutexas.edu, [4] terry.mcdonald@msutexas.edu,
[5] patrick.mitchell@msutexas.edu

Received: 29 May 2019 **Accepted:** 12 September 2019

Abstract: We obtain explicit formulas for the number of monic irreducible polynomials with prescribed constant term and degree q^k over a finite field. These formulas are derived from work done by Yucas. We show that the number of polynomials of a given constant term depends only on whether the constant term is a residue in the underlying field. We further show that as k becomes large, the proportion of irreducible polynomials having each constant term is asymptotically equal.
Keywords: Irreducible polynomials, Finite fields.
2010 Mathematics Subject Classification: 11T06, 12E05.

1 Introduction

The distribution of primes across equivalence classes in modular arithmetic is a well-studied problem in number theory. According to Dirichlet's Theorem, the proportion of primes in each equivalence class for a given modulus is asymptotically equal. When only primes less than some finite bound are considered, however, there are usually more primes of the form $4n + 3$ than of the form $4n + 1$, a phenomenon known as Chebyshev's bias. Rubinstein and Sarnak show in [4] that, assuming the Generalized Riemann Hypothesis, this bias generalizes to other moduli: for a fixed k, primes of the form $kn + a$ are more common when a is not a quadratic residue mod k than when it is.

In this paper, we will show that a related bias holds for monic irreducible polynomials over $\mathbb{Z}_p$ whose degree is q^k for some odd prime q. In this case, the number of monic irreducible polynomials with a given constant term a is related to whether a is a residue in the underlying field. As the degree grows larger, however, the proportion of such polynomials ending in each possible constant term is asymptotically equal.

Throughout this paper, p and q are assumed to be odd primes, ϕ denotes the Euler phi function, and Φ_n denotes the nth cyclotomic polynomial. Much of the other notation follows Yucas in [5].

Let $N(n, a, p)$ denote the number of monic irreducible polynomials over $\mathbb{Z}_p$ of degree n with constant term $(-1)^n a$. We limit our discussion to polynomials where the degree is a power of an odd prime. To establish a formula for $N(n, a, p)$, Yucas considers the possible orders of irreducible polynomials. For $n \in \mathbb{N}$, define a set

$$D_n = \{r : r|p^n - 1 \text{ but } r \nmid p^m - 1 \text{ for } 1 \leq m < n\}.$$

Note that D_n is the set of possible orders of polynomials of degree n over $\mathbb{Z}_p^*$. For any $r \in D_n$, we can write $r = d_r m_r$ where $d_r = \gcd\left(r, \frac{p^n-1}{p-1}\right)$. When n is a power of a prime, we have the following characterization of D_n:

Lemma 1.1. *Let $n = q^k$ for some $k \in \mathbb{N}$, then*

$$D_n = \{r : r|p^{q^k} - 1 \textit{ but } r \nmid p^{q^{k-1}} - 1\}.$$

Proof. Note that $\gcd(p^{q^k} - 1, p^m - 1) = p^{\gcd(q^k, m)} - 1$ (see Lemma 12.6 in [1]). If $\gcd(q^k, m) = 1$ and $r \in D_n$ with $r|p^m - 1$, then $r|p - 1$. Otherwise, $r|p^m - 1$ for some divisor m of q^k, i.e., $r|p^{q^i}$ for some $0 \leq i < k$. But $p^{q^i} - 1$ divides $p^{q^{k-1}} - 1$ for any $0 \leq i \leq k - 1$. □

Lemma 1.1 allows us to focus our attention on divisors of $p^{q^{k-1}} - 1$ instead of looking for all possible values of m where $r|p^m - 1$. Using this set D_n and the order of the element $a \in \mathbb{Z}_p^*$, Yucas derives the following formula for $N(n, a, p)$:

Theorem 1.2 ([5, Theorem 3.5])**.** *Suppose $a \in \mathbb{Z}_p^*$ has order m. Then*

$$N(n, a, p) = \frac{1}{n\phi(m)} \sum_{\substack{r \in D_n \\ m_r = m}} \phi(r).$$

While this gives a method for computing $N(n, a, p)$ in any case, it does not provide a clear way to compare different cases. Our goal is to establish the distribution of constant terms for a fixed p and q^k for $k \in \mathbb{N}$. This depends on the distribution of qth powers in $\mathbb{Z}_p^*$.

Definition 1.3. *Let $a \in \mathbb{Z}_p^*$. If there is some $b \in \mathbb{Z}_p^*$ such that $b^q \equiv a \pmod p$, then a is a q-residue in $\mathbb{Z}_p^*$.*

As we see in Theorem 1.4, the distribution of q-residues in $\mathbb{Z}_p^*$ depends on whether q divides $p-1$, which allows us to determine the number of q-residues in $\mathbb{Z}_p^*$ in Proposition 1.5.

Theorem 1.4 ([3, Theorem 2.37]). *If p is a prime and $\gcd(a,p) = 1$, then the congruence $x^n \equiv a \pmod{p}$ has $\gcd(n, p-1)$ solutions or no solution according as $a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}$ or not.*

Proposition 1.5. *If $\gcd(q, p-1) = q$, then there are $\frac{p-1}{q}$ q-residues in $\mathbb{Z}_p^*$. Otherwise, every element of $\mathbb{Z}_p^*$ is a q-residue.*

Proof. Observe that $\gcd(a,p) = 1$ for every $a \in \mathbb{Z}_p^*$. If $\gcd(q, p-1) = q$, then $q | p-1$. By Theorem 1.4, for any $a \in \mathbb{Z}_p^*$, $x^q \equiv a \pmod{p}$ has $\gcd(q, p-1) = q$ solutions or no solutions. Hence $\frac{p-1}{q}$ values of a have a solution to that equation. If $\gcd(q, p-1) = 1$, then $a^{\frac{p-1}{1}} \equiv 1 \pmod{p}$ because $\mathbb{Z}_p^*$ has $p-1$ elements. So every $a \in \mathbb{Z}_p^*$ is a q-residue. $\square$

In Section 2, we will consider the case where $\gcd(q, p-1) = 1$. We will prove that for any $a \in \mathbb{Z}_p^*$,

$$N(q^k, a, p) = \frac{p^{q^k} - p^{q^{k-1}}}{q^k(p-1)}.$$

In the case where $\gcd(q, p-1) = q$, the value of $N(q^k, a, p)$ depends on whether or not a is a q-residue in $\mathbb{Z}_p^*$. We will address this in Sections 3 and 4. In particular, we will show that

$$N(q^k, a, p) = \frac{p^{q^k} - 1}{q^k(p-1)}$$

whenever a is not a q-residue in $\mathbb{Z}_p^*$ and

$$N(q^k, a, p) = \frac{p^{q^k} - qp^{q^{k-1}} + q - 1}{q^k(p-1)}$$

whenever a is a q-residue in $\mathbb{Z}_p^*$.

In Yucas's formula, $N(q^k, a, p)$ represents the number of irreducible monic polynomials with a constant term of $(-1)^{q^k} a$. In our case, we assume q is an odd prime, hence $N(q^k, a, p)$ is the number of monic irreducible polynomials with a constant term of $-a$. Since a is a q-residue if and only if $-a$ is a q-residue, $N(q^k, a, p)$ is the number of irreducible monic polynomials with constant term either a or $-a$.

2 A formula for $N(q^k, a, p)$ when $\gcd(q, p-1) = 1$

Before we can compute $N(q^k, a, p)$ when $\gcd(q, p-1) = 1$, we need to present some ancillary results. Recall that $r = d_r m_r$ where $d_r = \gcd\left(r, \frac{p^n-1}{p-1}\right)$ and m_r is the order of r in $\mathbb{Z}_p^*$.

Lemma 2.1. *Let $r \in D_n$. Then $r | \frac{p^n-1}{p-1}$ if and only if $m_r = 1$.*

Proof. If r divides $\frac{p^n-1}{p-1}$, then $d_r = r$ implies $m_r = 1$. Conversely, $m_r = 1$ implies $r = d_r$ and thus r divides $\frac{p^n-1}{p-1}$. $\square$

Theorem 2.2. *Let $n = q^k$ for some $k \in \mathbb{N}$, and let $R_1 = \{r \in D_n : m_r = 1\}$. Then*

$$R_1 = \left\{ r \in \mathbb{N} : r | \frac{p^{q^k} - 1}{p-1} \text{ and } r \nmid p^{q^{k-1}} - 1 \right\}.$$

Proof. Let $S = \left\{ r \in \mathbb{N} : r | \frac{p^{q^k}-1}{p-1} \text{ and } r \nmid p^{q^{k-1}} - 1 \right\}$. Let $r \in R_1$, then $m_r = 1$ implies $r | \frac{p^{q^k}-1}{p-1}$ by Lemma 2.1. By the definition of D_n, r does not divide $p^m - 1$ for any $1 \leq m < n$ and hence $r \nmid p^{q^{k-1}} - 1$. So $r \in S$ and $R_1 \subseteq S$.

Next suppose $r \in S$. By Lemma 1.1, $r \in D_n$, and $m_r = 1$ by Lemma 2.1. Thus, $S \subseteq R_1$. □

Corollary 2.2.1. *Let $k \in \mathbb{N}$, $n = q^k$, and $\gcd(q, p-1) = 1$. For any $r \in D_n$, $d_r \in R_1$.*

Proof. Since $r \in D_n$ with order m_r, $r \nmid p^{q^{k-1}} - 1$, say t is a prime dividing r but not $p^{q^{k-1}} - 1$. If $t | m_r$, then $t | p-1$ which means $t | p^{q^{k-1}} - 1$, a contradiction. So $t | d_r$, thus $d_r \nmid p^{q^{k-1}} - 1$. By definition of d_r, $d_r | \frac{p^{q^k}-1}{p-1}$, hence $d_r \in R_1$. □

Lemma 2.3. *For $i \in \mathbb{N}$, $\gcd(\Phi_q(p^i), p-1) \leq q$.*

Proof. Let $s = \gcd(\Phi_q(p^i), p-1)$. Then, we can write $p - 1 = st$ for some $t \in \mathbb{N}$. It follows that

$$\Phi_q(p^i) = \Phi_q((st+1)^i) = (st+1)^{i(q-1)} + (st+1)^{i(q-2)} + ... + (st+1)^i + 1.$$

Expanding this expression yields q ones, and since s divides the remaining terms on that side of the equation as well as $\Phi_q(p^i)$, $s | q$. □

Lemma 2.4. *For $k \in \mathbb{N}$,*

$$\gcd\left(\frac{p^{q^k} - 1}{p-1}, p^{q^{k-1}} - 1 \right) = \begin{cases} q \cdot \frac{p^{q^{k-1}}-1}{p-1} & \text{if } \gcd(q, p-1) = q \\ \frac{p^{q^{k-1}}-1}{p-1} & \text{if } \gcd(q, p-1) = 1 \end{cases}.$$

Proof. Observe that $p^{q^k} - 1 = (p-1) \prod_{i=0}^{k-1} \Phi_q\left(p^{q^i}\right)$. Hence

$$\begin{aligned} \gcd\left(\frac{p^{q^k} - 1}{p-1}, p^{q^{k-1}} - 1 \right) &= \gcd\left(\prod_{i=0}^{k-1} \Phi_q\left(p^{q^i}\right), (p-1) \prod_{i=0}^{k-2} \Phi_q\left(p^{q^i}\right) \right) \\ &= \left[\prod_{i=0}^{k-2} \Phi_q\left(p^{q^i}\right) \right] \gcd\left(\Phi_q\left(p^{q^{k-1}}\right), p-1 \right) \\ &= \left[\frac{p^{q^{k-1}} - 1}{p-1} \right] \gcd\left(\Phi_q\left(p^{q^{k-1}}\right), p-1 \right). \end{aligned}$$ □

By Lemma 2.3, $\gcd\left(\Phi_q\left(p^{q^{k-1}}\right), p-1 \right)$ equals 1 or q depending on whether q divides $p-1$.

Corollary 2.4.1. *For $k \in \mathbb{N}$, if $\gcd(q, p-1) = 1$, then $\gcd\left(\frac{p^{q^k}-1}{p-1}, p-1 \right) = 1$. If $\gcd(q, p-1) = q$, then q is the only prime divisor of $\gcd\left(\frac{p^{q^k}-1}{p-1}, p-1 \right)$.*

Proof. The results follow from the previous two lemmas and the fact that

$$p^{q^k} - 1 = (p-1)\prod_{i=0}^{k-1} \Phi_q\left(p^{q^i}\right). \qquad \square$$

Theorem 2.5. *Let* $k \in \mathbb{N}$, $\gcd(q, p-1) = 1$, *and* $a \in \mathbb{Z}_p^*$, *then*

$$N(q^k, a, p) = \frac{p^{q^k} - qp^{q^{k-1}}}{q^k(p-1)}.$$

Proof. Let $n = q^k$ and a have order m. By [5, Theorem 3.5], we have

$$N(q^k, a, p) = \frac{1}{q^k\phi(m)} \sum_{\substack{r\in D_n \\ m_r = m}} \phi(r).$$

For any $r \in D_n$ with $m_r = m$, we can write $r = m_r d_r$ with $\gcd(m_r, d_r) = 1$ by Corollary 2.4.1. Thus, we have

$$N(q^k, a, p) = \frac{1}{q^k\phi(m)} \sum_{\substack{r\in D_n \\ m_r = m}} \phi(m_r)\phi(d_r).$$

Recalling that $\sum_{d|n} \phi(d) = n$, we use Corollary 2.2.1 and properties of the Euler ϕ function to get

$$N(q^k, a, p) = \frac{1}{q^k} \sum_{\substack{d_r | \frac{p^n-1}{p-1} \\ d_r \nmid p^{q^{k-1}}-1}} \phi(d_r) = \frac{1}{q^k}\left[\sum_{d_r | \frac{p^n-1}{p-1}} \phi(d_r) - \sum_{d_r | \gcd(\frac{p^n-1}{p-1}, p^{q^{k-1}}-1)} \phi(d_r)\right].$$

From Lemma 2.4 we know

$$\gcd\left(\frac{p^{q^k}-1}{p-1}, p^{q^{k-1}} - 1\right) = \frac{p^{q^{k-1}}-1}{p-1},$$

thus

$$\begin{aligned} N(q^k, a, p) &= \frac{1}{q^k}\left[\frac{p^{q^k}-1}{p-1} - \frac{p^{q^{k-1}}-1}{p-1}\right] \\ &= \frac{p^{q^k} - 1 - (p^{q^{k-1}} - 1)}{q^k(p-1)} \\ &= \frac{p^{q^k} - qp^{q^{k-1}}}{q^k(p-1)}. \end{aligned} \qquad \square$$

3 Results when $\gcd(q, p-1) = q$ and a is not a q-residue

When $\gcd(q, p-1) = q$, $\mathbb{Z}_p^*$ contains non q-residues as well as q-residues. The value of $N(q^k, a, p)$ depends on whether or not a is a q-residue. In this section, we will prove $N(q^k, a, p) = \frac{p^{q^k}-1}{q^k(p-1)}$ when a is not a q-residue. Theorem 3.1 is important in proving this result, since it classifies the maximum power of q dividing m_r when r is not a q-residue.

Theorem 3.1. *Let $\mathbb{Z}_p^* = \langle a \rangle$ and let $p-1 = q^i s$ for some integer s with $\gcd(q,s) = 1$ and some $i \in \mathbb{N}$. Let $b = a^k$ for some $k \in \mathbb{Z}$ with the order of b being m_b. The following are equivalent.*

1. *b is not a q-residue.*

2. *$q^i | m_b$*

3. *$q \nmid \gcd(k, p-1)$.*

Proof. First, we will show $(1) \Rightarrow (2)$. Assume $q^i \nmid m_b$, then $m_b = q^j t$ for some $0 \leq j < i$ and integer t dividing s (since $m_r | p-1$) with $\gcd(q,t) = 1$. Notice

$$a^{p-1} \equiv 1 \equiv b^{m_b} \equiv a^{m_b k} \pmod{p}.$$

So, $p-1|m_b k$, that is, $(q^i s)|(q^j tk)$ where $j < i$, hence $q^{i-j}|k$, say $k = q^{i-j}u$ for some integer u. It follows that

$$b = a^k = a^{q^{i-j}u} = (a^{q^{i-j-1}u})^q$$

is a q-residue.

Next, we will prove $(2) \Rightarrow (3)$. Assume $q^i | m_b$, then $m_b = q^i t$ for some integer t dividing s with $\gcd(q,t) = 1$. It follows that

$$|a^k| = |b| = m_b = q^i t = \frac{p-1}{\gcd(k, p-1)} = \frac{q^i s}{\gcd(k, p-1)}$$

and thus $q \nmid \gcd(k, p-1)$.

Finally, to show that $(3) \Rightarrow (1)$, assume b is a q-residue, say $b = a^k = a^{qm}$ for some $m \in \mathbb{Z}$. Then $p-1|(k-qm)$ implies $(p-1)u = k - qm$ for some $u \in \mathbb{Z}$. Note $q^i su = k - qm$ implies $k = q^i su + qm$. Since $p-1$ and k are both divisible by q, so is $\gcd(k, p-1)$. □

Theorem 3.2. *Let $k \in \mathbb{N}$, $\gcd(q, p-1) = q$, and let $a \in \mathbb{Z}_p^*$ be a non q-residue. Then,*

$$N(q^k, a, p) = \frac{p^{q^k} - 1}{q^k(p-1)}.$$

Proof. Let $n = q^k$ and $r \in D_n$. Let $p - 1 = q^i s$ for some integer s with $\gcd(s,q) = 1$ and $i \in \mathbb{N}$. Since a is not a q-residue, and since $m_r | p-1$, by Theorem 3.1, $m_r = q^i v$ for some integer v such that $v|s$ and with $\gcd(v,q) = 1$. We can also write $\frac{p^{q^k}-1}{p-1} = q^j t$ for some integer t with $\gcd(q,t) = 1$ and $j \in \mathbb{N}$. We claim that $\gcd(v,t) = 1$. By Corollary 2.4.1, if $\gcd(p, q-1) = q$, then q is the only prime divisor of

$$\gcd\left(\frac{p^{q^k} - 1}{p-1}, p-1\right) = \gcd\left(q^j t, q^i s\right).$$

Since m_r divides $p-1$, then q must also be the only prime divisor of $\gcd(q^j t, q^i v)$. We note that since $\gcd(v,q) = \gcd(t,q) = 1$, and that q must be the only divisor of $\gcd(q^j t, q^i v)$, then we must have $\gcd(v,t) = 1$.

We claim that $r = q^{i+j}vu$ for some u that divides t. Recall $r = m_r d_r$ where $d_r = \gcd\left(r, \frac{p^{q^k}-1}{p-1}\right)$, and we have assumed $m_r = q^i v$. Since m_r has q^i as a factor, then d_r must have q^j as a factor as well. The reasoning for this is if $d_r = q^\ell u$ with $\gcd(q, u) = 1$ and $\ell < j$, then

$$d_r = \gcd\left(r, \frac{p^{q^k}-1}{p-1}\right) = \gcd(m_r d_r, q^j t) = \gcd((q^i v)(q^\ell u), q^j t) = q^\ell u$$

This implies that u must divide t. Observe that $j \geq \ell + 1$ and $i + \ell \geq \ell + 1$ (because $i \neq 0$), hence $\gcd((q^i v)(q^\ell u), q^j t)$ should be divisible by $q^{\ell+1}$, contradicting our assumption that $d_r = q^\ell u$. Thus, $q^j | d_r$, and we can write $d_r = q^j u$ for some integer u which divides t and where $\gcd(q, t) = 1$. It follows that $r = m_r d_r = (q^i v)(q^j u) = q^{i+j} vu$ where $u|t$. Note that Corollary 2.4.1 implies that $\gcd(s, t) = 1$. Thus, $\gcd(u, v) = 1$ since $u|t$ and $v|s$.

Now we can prove the theorem. By [5, Theorem 3.5], we have

$$N(q^k, a, p) = \frac{1}{q^k \phi(m)} \sum_{\substack{r \in D_n \\ m_r = m}} \phi(r).$$

The previous paragraph allows us to write

$$N(q^k, a, p) = \frac{1}{q^k \phi(q^i)\phi(v)} \sum_{\substack{r \in D_n \\ u|t}} \phi(q^{i+j} vu).$$

We can rewrite the $\phi(r)$ from this expression as $\phi(q^{i+i})\phi(v)\phi(u)$ since

$$\gcd(v, q) = \gcd(u, q) = \gcd(v, u) = \gcd(v, t) = \gcd(q, t) = 1.$$

Now such an r from D_n cannot divide $p^m - 1$ for any $m < q^k$, but Lemma 1.1 implies we need only check for divisors that come from $p^{q^{k-1}} - 1$. In this case, the fact that q^{i+j} divides r and

$$p^{q^k} - 1 = \left(\frac{p^{q^k}-1}{p-1}\right)(p-1) = (q^j t)(q^i s) = q^{i+j} st$$

prevents r from dividing $p^{q^\ell} - 1$ when $\ell < k$. Hence we can say

$$N(q^k, a, p) = \frac{1}{q^k \phi(q^i)\phi(v)} \sum_{u|t} \phi(q^{i+j})\phi(v)\phi(u).$$

Using properties of the Euler ϕ function, we get

$$\begin{aligned} N(q^k, a, p) &= \frac{\phi(q^{i+j})\phi(v)}{q^k \phi(q^i)\phi(v)} \sum_{u|t} \phi(u) \\ &= \frac{q^{i+j} - q^{i+j-1}}{q^k(q^i - q^{i-1})} \sum_{u|t} \phi(u) \\ &= \frac{q^{i+j-1}(q-1)}{q^k q^{i-1}(q-1)} \sum_{u|t} \phi(u) \\ &= \frac{q^j t}{q^k} \\ &= \frac{p^{q^k} - 1}{q^k(p-1)}. \end{aligned}$$

□

4 Results when $\gcd(q, p-1) = q$ and a is a q-residue

In Section 3, we were able to directly compute $N(p^k, a, p)$ when $\gcd(q, p-1) = q$ and a is not a q-residue. In order to compute $N(q^k, a, p)$ when $\gcd(q, p-1) = q$ and a is a q-residue, we will first compute $N(q^k, 1, p)$. We will then prove that $N(q^k, a, p) = N(q^k, 1, p)$ whenever a is a q-residue.

Theorem 4.1. *Let $k \in \mathbb{N}$ and $\gcd(q, p-1) = q$, then*

$$N(q^k, 1, p) = \frac{p^{q^k} - qp^{q^{k-1}} + q - 1}{q^k(p-1)}.$$

Proof. Let $n = q^k$ and let $r \in D_n$ with $m_r = 1$. By [5, Theorem 3.5], we have

$$N(q^k, 1, p) = \frac{1}{q^k \phi(1)} \sum_{\substack{r \in D_n \\ m_r = 1}} \phi(r).$$

By Theorem 2.2 and properties of the Euler ϕ function, we get

$$N(q^k, 1, p) = \frac{1}{q^k} \sum_{\substack{r \mid \frac{p^n - 1}{p-1} \\ r \nmid p^{q^{k-1}} - 1}} \phi(r) = \frac{1}{q^k} \left[\sum_{r \mid \frac{p^n-1}{p-1}} \phi(r) - \sum_{r \mid \gcd(\frac{p^n-1}{p-1}, p^{q^{k-1}} - 1)} \phi(r) \right].$$

From Lemma 2.4 we know

$$\gcd\left(\frac{p^{q^k} - 1}{p-1}, p^{q^{k-1}} - 1 \right) = q \cdot \frac{p^{q^{k-1}} - 1}{p-1},$$

thus

$$\begin{aligned} N(q^k, 1, p) &= \frac{1}{q^k} \left[\frac{p^{q^k} - 1}{p-1} - q \frac{p^{q^{k-1}} - 1}{p-1} \right] \\ &= \frac{p^{q^k} - 1 - q(p^{q^{k-1}} - 1)}{q^k(p-1)} \\ &= \frac{p^{q^k} - qp^{q^{k-1}} + q - 1}{q^k(p-1)}. \end{aligned}$$

□

Theorem 4.2. *Let $k \in \mathbb{N}$, $k \geq 2$, $\gcd(q, p-1) = q$, and a be a q-residue. Then*

$$N(q^k, 1, p) = N(q^k, a, p).$$

Proof. Let $p - 1 = q^j s$, where $\gcd(s, q) = 1$ and $j \in \mathbb{N}$. Since $p - 1 | p^{q^{k-1}} - 1$, this implies that $p^{q^{k-1}}$ is a multiple of $q^j s$. Furthermore, we can write $p^{q^{k-1}} - 1 = q^{i-1} st$ where $\gcd(s, t) = 1$, $\gcd(t, q) = 1$, and $i - 1 > j$. By Corollary 2.4.1, the only prime divisor of $\gcd\left(\frac{p^{q^{k-1}} - 1}{p-1}, p - 1 \right)$ is q, so $\gcd(s, t) = 1$ and $i - 1 > j$.

Now consider $p^{q^k}-1$. We have $p^{q^{k-1}}-1|p^{q^k}-1$, hence we can write $p^{q^k}-1 = q^i stu$ where $\gcd(u,q) = \gcd(s,tu) = 1$. Note by Lemma 2.4, since $q^{i-1}|p^{q^{k-1}}-1$, we have $q^i|p^{q^k}-1$.

Let $n = q^k$ and $r \in D_n$ be a q-residue. Recall $m_r|p-1$, that is, $m_r|q^j s$. We also have $r = m_r d_r$ where $d_r = \gcd\left(r, \frac{p^{q^k}-1}{p-1}\right) = \gcd(r, q^{i-j}tu)$. By Theorem 3.1, r being a q-residue implies q^j does not divide m_r (i.e., m_r can have any power of q except the maximum q^j).

First, let us evaluate $N(q^k,1,p)$. If $m_r = 1$, then $r|\frac{p^{q^k}-1}{p-1}$ by Lemma 2.1 and $r \nmid p^{q^{k-1}}-1$ because $r \in D_n$. In other words, $r|q^{i-j}tu$ and $r \nmid q^{i-1}st$. We claim that there exists $u' \neq 1$ such that $u'|r$ and $u'|u$. If not, then $\gcd(u,r) = 1$ implies $r|q^{i-j}st$. But then $r|q^{i-1}st$, which is a contradiction. Thus, $r = q^\ell t'u'$ for some $\ell \in \{0,\ldots,i-j\}$, $t'|t$, $u'|u$, $u' \neq 1$. Now we have

$$\begin{aligned} N(q^k,1,p) &= \frac{1}{q^k\phi(1)} \sum_{\substack{r\in D_n \\ m_r=1}} \phi(r) \\ &= \frac{1}{q^k} \sum_{\substack{\ell\in\{0,\ldots,i-j\} \\ t'|t,u'|u,u'\neq 1}} \phi(q^\ell)\phi(t')\phi(u') \\ &= \frac{q^{i-j}t(u-1)}{q^k} \\ &= \frac{t(u-1)}{q^{k-i+j}}. \end{aligned}$$

Now suppose $m_r \neq 1$, say $m_r = q^b s'$ for some $b \in \{0,\ldots,j-1\}$ and $s'|s$. Note that $b \leq j-1$ implies $q^j \nmid m_r$ and so $q^i \nmid r$. We claim that there exists $u'|u$, $u' \neq 1$, such that $u'|r$. If not, $\gcd(u,r) = 1$ and $r|p^{q^k}-1$ implies $r|q^i st$. But $q^i \nmid r$, so $r|q^{i-1}st$, contradicting $r \in D_n$. Thus, $r = q^\ell s't'u'$ for some $\ell \in \{0,\ldots,i-1\}$, $s'|s$, $t'|t$, $u'|u$, $u' \neq 1$. There are two cases to consider: $m_r = s'$ and $m_r = q^b s'$ for some $b \in \{0,\ldots,j-1\}$.

<u>Case 1: ($m_r = s'$)</u> In this case $\ell \in \{0,\ldots,i-j\}$. It follows that

$$\begin{aligned} N(q^k,a,p) &= \frac{1}{q^k\phi(s')} \sum_{\substack{r\in D_n \\ m_r=s'}} \phi(r) \\ &= \frac{1}{q^k\phi(s')} \sum_{\substack{\ell\in\{0,\ldots,i-j\} \\ t'|t,u'|u,u'\neq 1}} \phi(q^\ell)\phi(s')\phi(t')\phi(u') \\ &= \frac{q^{i-j}t(u-1)}{q^k} \\ &= \frac{t(u-1)}{q^{k-i+j}} \\ &= N(q^k,1,p). \end{aligned}$$

<u>Case 2: ($m_r = q^b s'$)</u> We claim $\ell = i-j+b$ for some $b \in \{1,\ldots,j-1\}$. If $\ell \leq i-j$, then $d_r = \gcd\left(r, \frac{p^{q^k}-1}{p-1}\right) = \gcd(q^\ell s't'u', q^{i-j}tu) = q^\ell t'u'$ implies $b = 0$, a contradiction. Hence, $\ell > i-j$ and we can write $\ell = i-j+b$ for some $b \in \{1,\ldots,j-1\}$. It follows that

$$
\begin{aligned}
N(q^k, a, p) &= \frac{1}{q^k \phi(q^b s')} \sum_{\substack{r \in D_n \\ m_r = q^b s'}} \phi(r) \\
&= \frac{1}{q^k \phi(q^b s')} \sum_{t' | t, u' | u, u' \neq 1} \phi(q^{i-j+b}) \phi(s') \phi(t') \phi(u') \\
&= \frac{1}{q^k \phi(s')(q^b - q^{b-1})} \sum_{t' | t, u' | u, u' \neq 1} (q^{i-j+b} - q^{i-j+b-1}) \phi(s') \phi(t') \phi(u') \\
&= \frac{(q^{i-j+b} - q^{i-j+b-1}) t(u-1)}{q^k (q^b - q^{b-1})} \\
&= \frac{t(u-1)}{q^{k-i+j}} \\
&= N(q^k, 1, p).
\end{aligned}
$$

□

It is worthwhile to note that Theorem 2.5, Theorem 4.1, and Theorem 4.2 each produce a formula for $N(q^k, a, p)$ that depends only on whether or not a is a q-residue. In particular, $N(q^k, a, p)$ takes only one or two distinct values for a given q^k and p. The following relationship is particularly interesting:

Corollary 4.2.1. *Let* $\gcd(q, p-1) = q$ *and* $k \in \mathbb{N}$. *If* a *is a non* q*-residue and* b *a* q*-residue in* $\mathbb{Z}_p^*$, *then*

$$N(q^k, a, p) - N(q^k, b, p) = N(q^{k-1}, a, p).$$

While this corollary shows that the difference between $N(q^k, a, p)$ and $N(q^k, b, p)$ increases as k increases, we will show that the ratio $\frac{N(q^k,a,p)}{N(q^k,b,p)}$ approaches one. If $\gcd(p-1, q) = 1$, then by Theorem 2.5 the constant terms of all monic irreducible polynomials are uniformly distributed. Thus, the ratio $\frac{N(q^k,a,p)}{N(q^k,b,p)}$ equals one for any $a, b \in \mathbb{Z}_p^*$.

Notice that by Theorem 3.2 the number of irreducible monic polynomials with constant term a, where a is not a q-residue and $\gcd(p-1, q) = q$, is given by

$$\frac{p^{q^k} - 1}{q^k(p-1)},$$

and when b is a q-residue, the number is

$$\frac{p^{q^k} - qp^{q^k - 1} + q - 1}{q^k(p-1)}.$$

Hence the ratio

$$\frac{N(q^k, a, p)}{N(q^k, b, p)} = \frac{p^{q^k} - 1}{q^k(p-1)} \cdot \frac{q^k(p-1)}{p^{q^k} - qp^{q^k-1} + q - 1}$$

approaches one as k approaches infinity.

This shows us that the proportions of constant terms of monic irreducible polynomials are asymptotically equal, as their limits show a uniform distribution among the constant terms.

References

[1] Krizek, M., Luca, F., & Somer, L. (2001). *17 Lectures on Fermat Numbers*, CMS Books in Mathematics, Springer-Verlag, New York.

[2] Lidl, R., & Niederreiter, H. (1994). *Introduction to Finite Fields and Their Application, Revised edition*, Cambridge University Press, Cambridge.

[3] Niven, I., Zuckerman, H., & Montgomery, H. (1991). *An Introduction to the Theory of Numbers, 5th edition*, Wiley and Sons, Inc., New York.

[4] Rubinstein, M., & Sarnak, P. (1994). Chebyshev's Bias, *Experimental Mathematics*, 3, 173–197.

[5] Yucas, J. L. (2006). Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields and Their Appl*, 12, 211–221.