Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2024, Volume 30, Number 1, 195–210
DOI: 10.7546/nntdm.2024.30.1.195-210

Distribution of constant terms of irreducible polynomials in $\mathbb{Z}_p[x]$ whose degree is a product of two distinct odd primes

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

[1] Department of Mathematics, Midwestern State University
3410 Taft Blvd, Wichita Falls, TX, 76308 United States
e-mail: sarah.cobb@msutexas.edu

[2] Department of Mathematics, Midwestern State University
3410 Taft Blvd, Wichita Falls, TX, 76308 United States
e-mail: michelle.knox@msutexas.edu

[3] Department of Mathematics, Midwestern State University
3410 Taft Blvd, Wichita Falls, TX, 76308 United States
e-mail: marcos.lopez@msutexas.edu

[4] Department of Mathematics, Midwestern State University
3410 Taft Blvd, Wichita Falls, TX, 76308 United States
e-mail: terry.mcdonald@msutexas.edu

[5] Department of Mathematics, Midwestern State University
3410 Taft Blvd, Wichita Falls, TX, 76308 United States
e-mail: patrick.mitchell@msutexas.edu

Received: 27 September 2023 **Accepted:** 6 March 2024 **Online First:** 28 March 2024

Abstract: We obtain explicit formulas for the number of monic irreducible polynomials with prescribed constant term and degree q_1q_2 over a finite field, where q_1 and q_2 are distinct odd primes.

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 q_1-residue and/or a q_2-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. This paper continues work done in [1].

Keywords: Irreducible polynomials, Finite fields.
2020 Mathematics Subject Classification: 11T06, 12E05.

1 Introduction

In [1], we looked at the distribution of constant terms of monic irreducible polynomials over $\mathbb{Z}_p$ whose degree was a power of an odd prime q, and we found that 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. In this paper, we will determine the number of monic irreducible polynomials with a given constant term a for polynomials whose degree is a product of two distinct odd primes, and we will use these values to show that the proportion of such polynomials remains asymptotically equal as the degree grows larger.

Throughout this paper, p, q_1 and q_2 are assumed to be distinct odd primes and ϕ denotes the Euler phi function. Let $n \in \mathbb{N}$, then $N(n,p)$ denotes the number of monic irreducible polynomials over $\mathbb{Z}_p$ of degree n, and $N(n,a,p)$ denotes the number of monic irreducible polynomials over $\mathbb{Z}_p$ of degree n with constant term $(-1)^n a$.

The next theorem from [3] is a well known result providing the number of monic irreducible polynomials in $\mathbb{Z}_p[x]$ of degree n.

Theorem 1.1. *The number $N(n,p)$ of monic irreducible polynomials in $\mathbb{Z}_p[x]$ of degree n is given by*

$$N(n,p) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

As we investigate polynomials over $\mathbb{Z}_p$ with prescribed constant term, we will follow the notation laid out in Yucas [5]. 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

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

then D_n is the set of possible orders of polynomials in $N(n,p)$. Let $r \in D_n$, and let $a \in \mathbb{Z}_p^*$ be an element of order m_r, then we can write $r = d_r m_r$ where $d_r = \gcd(r, \frac{p^n-1}{p-1})$. The following theorem from Yucas (Theorem 3.5 of [5]) will form the basis of most of the calculations in this paper.

Theorem 1.2. *The number $N(n,a,p)$ if monic irreducible polynomials over $\mathbb{Z}_p$ of degree n with constant term $(-1)^n a$ is*

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

As we consider the possible values of $N(n,a,p)$ specifically when $n = q_1q_2$, this value will depend on whether or not a is an n-residue. Just as an element of $c \in \mathbb{Z}_p$ is a quadratic residue if $c = d^2$ for some $d \in \mathbb{Z}_p$, $c \in \mathbb{Z}_p$ is an n-residue if $c = d^n$ for some $d \in \mathbb{Z}_p$. The following theorem will be used several times in this paper and is based on Lemma 2 from [4].

Theorem 1.3. *Let $n \in \mathbb{N}$ with $n > 1$, and assume $c, d \in \mathbb{Z}_p^*$ are both n-residues. Then $N(n,c,p) = N(n,d,p)$.*

Proof. Let $P(n,a,p)$ denote the set of monic irreducible polynomials of degree n in $\mathbb{Z}_p^*$ with constant term a, so that the cardinality of $P(n,a,p)$ is $N(n,a,p)$. We will prove the theorem by defining a bijection between $P(n,c,p)$ and $P(n,d,p)$.

Let $g = dc^{-1}$. Since g is the product of two n-residues, g must be an n-residue. Therefore there is some element $h \in \mathbb{Z}_p^*$ such that $h^n = g$.

Define a function $\varphi : P(n,c,p) \to P(n,d,p)$ by

$$\varphi(f(x)) = gf(h^{-1}x).$$

To show that if $f(x) \in P(n,c,p)$, then $\varphi(f(x)) \in P(n,d,p)$, we must show that $\varphi(f(x))$ is monic, irreducible, of degree n, and has constant term d. Let $f(x) \in P(n,c,p)$ with $f(x) = \sum_{i=0}^{n} a_i x^i$. Note that $a_0 = c$ and $a_n = 1$. Then

$$\begin{aligned}\varphi(f(x)) &= gf(h^{-1}x)\\ &= g\sum_{i=0}^{n} a_i(h^{-1}x)^i\\ &= \sum_{i=0}^{n} ga_ih^{-i}x^i.\end{aligned}$$

The leading term of $\varphi(f(x))$ is $gh^{-n}x^n = gg^{-1}x^n = x^n$, demonstrating that $\varphi(f(x))$ is monic and of degree n.

The constant term of $\varphi(f(x))$ is $ga_0 = gc = d$, showing that $\varphi(f(x))$ has constant term d.

To show that $\varphi(f(x))$ is irreducible, we proceed by contraposition. Suppose that $\varphi(f(x))$ is reducible, so that $\varphi(f(x)) = f_1(x)f_2(x)$ for some $f_1, f_2 \in \mathbb{Z}_p[x]$. It follows that

$$\begin{aligned}gf(h^{-1}x) &= f_1(x)f_2(x)\\ f(h^{-1}x) &= g^{-1}f_1(x)f_2(x)\\ f(hh^{-1}x) &= g^{-1}f_1(hx)f_2(hx)\\ f(x) &= g^{-1}f_1(hx)f_2(hx)\end{aligned}$$

showing that f is reducible.

Therefore $\varphi(f(x)) \in P(n,d,p)$. It remains to show that φ is a bijection.

Let $f_1, f_2 \in P(n,c,p)$ with $\varphi(f_1(x)) = \varphi(f_2(x))$. Then $gf_1(h^{-1}x) = gf_2(h^{-1}x)$ and therefore $f_1(h^{-1}x) = f_2(h^{-1}x)$. Since $h^{-1}\mathbb{Z}_p = \mathbb{Z}_p$, this demonstrates that $f_1(x) = f_2(x)$ for every $x \in \mathbb{Z}_p$. It follows that φ is injective. To see that φ is surjective, let $\hat{f} \in P(n,d,p)$. Then $g^{-1}\hat{f}(hx) \in P(n,c,p)$ and $\varphi(g^{-1}\hat{f}(hx)) = \hat{f}(x)$. □

As we begin to calculate $N(q_1q_2, a, p)$, there are three possibilities we will consider:

Case 1: $p \equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$

Case 2: $p \not\equiv 1 \pmod{q_1}$ and $p \not\equiv 1 \pmod{q_2}$

Case 3: $p \not\equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$

Case 1 will be addressed in Section 2, and Cases 2 and 3 will be addressed in Section 3.

2 The case $p \equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$

First, if $p \equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$, then the following theorems provide the possible values of $N(q_1q_2, a, p)$, and we will devote this section to proving the theorems:

Theorem 2.2 If $a \in \mathbb{Z}_p^*$ is neither a q_1-residue nor a q_2-residue, then

$$N(q_1q_2, a, p) = \frac{p^{q_1q_2} - 1}{q_1q_2(p-1)}.$$

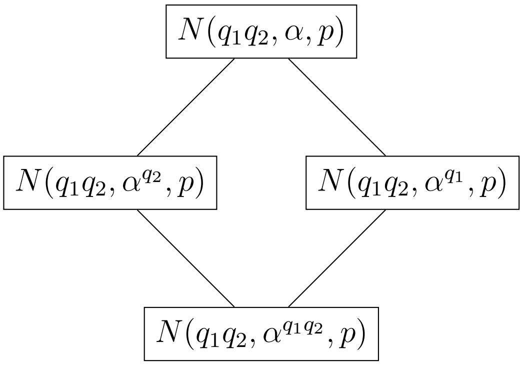
Theorem 2.3 If $a \in \mathbb{Z}_p^*$ is a q_2-residue but not a q_1-residue, then

$$N(q_1q_2, a, p) = \frac{p^{q_1q_2} - 1}{q_1q_2(p-1)} - \frac{p^{q_1} - 1}{q_1(p-1)}.$$

Theorem 2.4 If $a \in \mathbb{Z}_p^*$ is both q_1-residue and a q_2-residue, then

$$N(q_1q_2, a, p) = \frac{p^{q_1q_2} - 1}{q_1q_2(p-1)} - \frac{p^{q_1} - 1}{q_1(p-1)} - \frac{p^{q_2} - 1}{q_2(p-1)} + 1.$$

Because of the way the values of $N(q_1q_2, a, p)$ are created by subtracting from the value $\frac{p^{q_1q_2}-1}{q_1q_2(p-1)}$, we can represent the values in the following lattice. Observe that if α is a generator of $\mathbb{Z}_p^*$, then α is neither a q_1-residue nor a q_2-residue. On the sides of the lattice, α^{q_1} is a q_1-residue that is not a q_2-residue, and α^{q_2} is a q_2-reside that is not a q_1-residue. Finally, on the bottom, $\alpha^{q_1q_2} = 1$ is both a q_1-residue and a q_2-residue. We will revisit this lattice in Section 4 when we compare the values along each edge of the lattice. The value from Theorem 2.2 provides the value at the top of the lattice, the value from Theorem 2.3 provides the values on the sides of the lattice, and the value from Theorem 2.4 provides the value at the bottom of the lattice.


$N(q_1q_2, \alpha, p)$
$N(q_1q_2, \alpha^{q_2}, p)$
$N(q_1q_2, \alpha^{q_1}, p)$
$N(q_1q_2, \alpha^{q_1q_2}, p)$

Our proof of Lemma 2.2 will require the following result regarding the p-adic valuation. Recall that the p-adic valuation $\nu_p : \mathbb{Z} \to \mathbb{N}$ is defined by $\nu_p(n) = max\{\nu \in \mathbb{N} : p^\nu | n\}$ if $n \neq 0$ and $\nu_p(0) = \infty$.

Lemma 2.1. *Let $a, b \in \mathbb{Z}_{\geq 0}$. If t is a prime with $t|(p^a - 1)$ and $t \nmid b$, then $\nu_t(p^a - 1) = \nu_t(p^{ab} - 1)$.*

Proof. Note that $p^{ab} - 1$ can be factored as

$$p^{ab} - 1 = (p^a - 1) \sum_{i=1}^{b} p^{a(b-i)}$$

Since $t|(p^a - 1)$, there is some integer u such that $p^a = tu + 1$. This allows us to write

$$\sum_{i=1}^{b} p^{a(b-i)} = \sum_{i=1}^{b} (tu + 1)^{(b-i)}$$

When the expression on the right is expanded, the only terms not divisible by t are the powers of 1. Therefore the expression gives a multiple of t plus

$$\sum_{i=1}^{b} 1^{(b-i)} = b$$

Therefore there is some integer w such that

$$\sum_{i=1}^{b} p^{a(b-i)} = tw + b.$$

We know t does not divide b, thus t does not divide $\sum_{i=1}^{b} p^{a(b-i)}$ and so $\nu_t\left(\sum_{i=1}^{b} p^{a(b-i)}\right)$ equals zero. Hence $\nu_t(p^{ab} - 1) = \nu_t(p^a - 1) + \nu_t\left(\sum_{i=1}^{b} p^{a(b-i)}\right) = \nu_t(p^a - 1)$. □

Yucas's formula requires calculations involving $r \in D_{q_1 q_2}$, and these values rely heavily on the values of $p - 1$, $p^{q_1} - 1$, $p^{q_2} - 1$, and $p^{q_1 q_2} - 1$. The information in the next lemma will aid us in those calculations.

Lemma 2.2. *For primes p, q_1, and q_2, we may write*

$$\begin{aligned} p - 1 &= q_1^{k_1} q_2^{k_2} s_1 \\ p^{q_1} - 1 &= q_1^{k_1 + j_1} q_2^{k_2} s_1 s_{q_1} \\ p^{q_2} - 1 &= q_1^{k_1} q_2^{k_2 + j_2} s_1 s_{q_2} \\ p^{q_1 q_2} - 1 &= q_1^{k_1 + j_1} q_2^{k_2 + j_2} s_1 s_{q_1} s_{q_2} s_{q_1 q_2} \end{aligned}$$

where all variables represent positive integers and $s_1, s_{q_1}, s_{q_2}, s_{q_1 q_2}, q_1$, and q_2 are pairwise relatively prime.

It is worth noting a few things about the factorizations above. Clearly $p - 1$ divides the other three expressions, and $p^{q_1} - 1$ and $p^{q_2} - 1$ both divide $p^{q_1 q_2} - 1$. The significant claims here are that q_1 and q_2 are the only prime factors that appear with potentially different exponents in the factorizations of the four expressions and that those exponents increase only when p is raised to a power divisible by that prime.

Proof. The following statements together suffice for the proof:

(i) For any prime t dividing s_1, $\nu_t(p-1) = \nu_t(p^{q_1}-1) = \nu_t(p^{q_2}-1) = \nu_t(p^{q_1q_2}-1)$

(ii) For any prime t dividing s_{q_1}, $\nu_t(p^{q_1}-1) = \nu_t(p^{q_1q_2}-1)$

(iii) For any prime t dividing s_{q_2}, $\nu_t(p^{q_2}-1) = \nu_t(p^{q_1q_2}-1)$

(iv) $\gcd(s_{q_1}, s_{q_2}) = 1$

(v) $\nu_{q_1}(p-1) = \nu_{q_1}(p^{q_2}-1)$

(vi) $\nu_{q_2}(p-1) = \nu_{q_2}(p^{q_1}-1)$

(vii) $\nu_{q_1}(p^{q_1}-1) = \nu_{q_1}(p^{q_1q_2}-1)$

(viii) $\nu_{q_2}(p^{q_2}-1) = \nu_{q_2}(p^{q_1q_2}-1)$

The first four statements establish that s_1, s_{q_1}, s_{q_2}, and $s_{q_1q_2}$ are pairwise relatively prime. The next four show that the exponents of q_1 and q_2 vary only depending on whether the prime in question is a factor of the exponent of p. With the exception of (iv), each of these statements follows directly from Lemma 2.1. Statement (iv) follows from the fact that

$$\gcd(p^{q_1}-1, p^{q_2}-1) = p^{gcd(q_1,q_2)} - 1 = p - 1$$

(see Lemma 12.6 in [2]). □

For example, consider $\mathbb{Z}_{31}$ with $q_1 = 3$ and $q_2 = 5$. Then, as in the previous lemma, we can write $p-1$, $p^{q_1}-1$, $p^{q_2}-1$, and $p^{q_1q_2}-1$ accordingly:

	power of $q_1 = 3$	**power of $q_2 = 5$**	s_1	s_{q_1}	s_{q_2}	$s_{q_1q_2}$
$p-1$	3^1	5^1	2			
p^3-1	3^2	5^1	2	331		
p^5-1	3^1	5^2	2		$11 \cdot 17351$	
$p^{15}-1$	3^2	5^2	2	331	$11 \cdot 17351$	$2521 \cdot 327412201$

Observe that the values of s_{q_2} and $s_{q_1q_2}$ are composite in this example, and note that 3 and 5 are the only values whose powers change.

The proof of the next proposition uses properties of the Euler phi function and is omitted.

Proposition 2.1. *Let $q, a, b \in \mathbb{N}$ with q being prime. Then $\frac{\phi(q^{a+b})}{q\phi(q^a)} = q^{b-1}$.*

Theorem 2.2 (Top of Lattice). *Let $c \in \mathbb{Z}_p^*$, where c is neither a q_1-residue nor a q_2-residue. Then*

$$N(q_1q_2, c, p) = \frac{p^{q_1q_2}-1}{q_1q_2(p-1)}.$$

Proof. Let α be a generator of $\mathbb{Z}_p^*$ and $c \in \mathbb{Z}_p^*$ such that c is neither a q_1-residue nor a q_2-residue. Then $c = \alpha^k$ for some integer k with $0 < k \leq p-1$. Since c is neither a q_1 nor a q_2 residue, neither q_1 nor q_2 divides k. Let m denote the order of c in $\mathbb{Z}_p^*$. Since $|\alpha^k| = \frac{|\alpha|}{\gcd(|\alpha|,k)} = \frac{p-1}{\gcd(p-1,k)}$, we have $m = q_1^{k_1}q_2^{k_2}s_1'$ for some s_1' dividing s_1.

Let $r \in D_{q_1q_2}$ with $m_r = m$, recalling that $r = m_r d_r$ where $d_r = \gcd(r, \frac{p^{q_1q_2}-1}{p-1})$. Since $q_1^{k_1}q_2^{k_2}$ divides m_r and $q_1^{j_1}q_2^{j_2}$ divides $\frac{p^{q_1q_2}-1}{p-1}$, it must be the case that $q_1^{k_1+j_1}q_2^{k_2+j_2}$ divides r. Moreover, any divisor of $p^{q_1q_2}-1$ that is divisible by $q_1^{k_1+j_1}q_2^{k_2+j_2}$ is an element of $D_{q_1q_2}$, since $q_1^{k_1+j_1}q_2^{k_2+j_2}$ is not a divisor of $p^a - 1$ for any $a < q_1q_2$. Therefore the subset of $D_{q_1q_2}$ with $m_r = m$ is exactly the set of divisors r of $p^{q_1q_2}-1$ with $q_1^{k_1+j_1}q_2^{k_2+j_2}|r$.

It follows from [5] that

$$\begin{aligned} N(q_1q_2, c, p) &= \frac{1}{q_1q_2\phi(m)} \sum_{\substack{r \in D_n \\ m_r = m}} \phi(r) \\ &= \frac{1}{q_1q_2\phi(m)} \sum_{s'_{q_1}|s_{q_1}, s'_{q_2}|s_{q_2}, s'_{q_1q_2}|s_{q_1q_2}} \phi(q_1^{k_1+j_1}q_2^{k_2+j_2}s'_1 s'_{q_1} s'_{q_2} s'_{q_1q_2}) \\ &= \frac{1}{q_1q_2\phi(m)} \sum_{u|s_{q_1}s_{q_2}s_{q_1q_2}} \phi(q_1^{k_1+j_1}q_2^{k_2+j_2}s'_1 u). \end{aligned}$$

Since the values of $q_1^{k_1+j_1}$, $q_2^{k_2+j_2}$, s'_1, and u are pairwise relatively prime, we can write

$$\begin{aligned} N(q_1q_2, c, p) &= \frac{1}{q_1q_2\phi(q_1^{k_1}q_2^{k_2}s'_1)} \sum_{u|s_{q_1}s_{q_2}s_{q_1q_2}} \phi(q_1^{k_1+j_1})\phi(q_2^{k_2+j_2})\phi(s'_1)\phi(u) \\ &= \frac{\phi(q_1^{k_1+j_1})\phi(q_2^{k_2+j_2})\phi(s'_1)}{q_1q_2\phi(q_1^{k_1})\phi(q_2^{k_2})\phi(s'_1)} \sum_{u|s_{q_1}s_{q_2}s_{q_1q_2}} \phi(u). \end{aligned}$$

Note that the summation above is over all divisors of $s_{q_1}s_{q_2}s_{q_1q_2}$, which gives us

$$\begin{aligned} N(q_1q_2, c, p) &= \frac{\phi(q_1^{k_1+j_1})}{q_1\phi(q_1^{k_1})} \cdot \frac{\phi(q_2^{k_2+j_2})}{q_2\phi(q_2^{k_2})} \cdot s_{q_1}s_{q_2}s_{q_1q_2} \\ &= \frac{q_1^{k_1+j_1}q_2^{k_2+j_2}s_1 s_{q_1}s_{q_2}s_{q_1q_2}}{q_1q_2(q_1^{k_1}q_2^{k_2}s_1)} \\ &= \frac{p^{q_1q_2}-1}{q_1q_2(p-1)}. \end{aligned}$$

□

The next lemma follows from the fact that the only prime divisor of $\gcd(\frac{p^{q^k}-1}{p-1}, p-1)$ is q (see Corollary 2.4 of [1]), so the proof is omitted.

Lemma 2.3. *For $k \in \mathbb{N}$, if $\gcd(q, p-1) = q$, then $\gcd(\frac{p^{q^k}-1}{p-1}, p-1) = q$.*

Theorem 2.3 (Sides of Lattice)**.** *If $a \in \mathbb{Z}_p^*$ is a q_2-residue but not a q_1-residue, then*

$$N(q_1q_2, a, p) = \frac{p^{q_1q_2}-1}{q_1q_2(p-1)} - \frac{p^{q_1}-1}{q_1(p-1)}.$$

Proof. Let α be a generator of $\mathbb{Z}_p^*$ and $c \in \mathbb{Z}_p^*$ such that c is a q_1-residue but not a q_2-residue. Then $c = \alpha^k$ for some integer k with $0 < k \leq p-1$. Since c is a q_1-residue but not a q_2-residue, we have $q_1|k$ and $q_2 \not| k$. Let m denote the order of c in $\mathbb{Z}_p^*$. Since $|\alpha^k| = \frac{|\alpha|}{\gcd(|\alpha|,k)} = \frac{p-1}{\gcd(p-1,k)}$, we have $m = q_1^u q_2^{k_2} s'_1$ for some s'_1 dividing s_1 and $0 \leq u < k_1$.

Let $r \in D_{q_1q_2}$ with $m_r = m$, recalling that $r = m_r d_r$ where $d_r = \gcd(r, \frac{p^{q_1q_2}-1}{p-1})$. Since $q_2^{k_2}$ divides m_r and $q_2^{j_2}$ divides $\frac{p^{q_1q_2}-1}{p-1}$, it must be the case that $q_2^{k_2+j_2}$ divides r. We may therefore write $r = q_1^t q_2^{k_2+j_2} s_1' s_{q_1}' s_{q_2}' s_{q_1q_2}'$ for some $s_{q_1}', s_{q_2}', s_{q_1q_2}'$ dividing s_{q_1}, s_{q_2}, and $s_{q_1q_2}$ respectively and $u \le t < k_1 + j_1$. Note that u and s_1' depend only on m, whereas t, s_{q_1}, s_{q_2}, and $s_{q_1q_2}$ also depend on r.

Since $q_2^{k_2+j_2}$ divides r, it is clear that $r \nmid p - 1$ and $r \nmid p^{q_1} - 1$. In order for r to be in the set $D_{q_1q_2}$, we also need $r \nmid p^{q_2} - 1$. Therefore one of the following must be true: $s_{q_1}' \ne 1$, $s_{q_1q_2}' \ne 1$, or $t > k_1$.

We will consider two cases: first the case with $q_1 \nmid m$ and then $q_1 | m$.

Suppose first that $q_1 \nmid m$. In this case, $u = 0$ and $m = q_2^{k_2} s_1'$. Moreover, since the value of $\nu_{q_1}\left(\frac{p^{q_1q_2}-1}{p-1}\right)$ is j_1, we have $\nu_{q_1}(r) \le j_1$. By Theorem 1.2,

$$\begin{aligned}
N(q_1q_2, c, p) &= \frac{1}{q_1q_2\phi(m)} \sum_{\substack{r \in D_n \\ m_r = m}} \phi(r) \\
&= \frac{1}{q_1q_2\phi(q_2^{k_2}s_1')} \sum_{\substack{0 \le t \le j_1 \\ s_{q_1}'|s_{q_1}, s_{q_2}'|s_{q_2}, s_{q_1q_2}'|s_{q_1q_2} \\ s_{q_1}'s_{q_1q_2}' \ne 1 \text{ or } t > k_1}} \phi(q_1^t)\phi(q_2^{k_2+j_2})\phi(s_1')\phi(s_{q_1}')\phi(s_{q_2}')\phi(s_{q_1q_2}') \\
&= \frac{\phi(q_2^{k_2+j_2})\phi(s_1')}{q_1q_2\phi(q_2^{k_2})\phi(s_1')} \sum_{\substack{0 \le t \le j_1 \\ s_{q_1}'|s_{q_1}, s_{q_2}'|s_{q_2}, s_{q_1q_2}'|s_{q_1q_2} \\ s_{q_1}'s_{q_1q_2}' \ne 1 \text{ or } t > k_1}} \phi(q_1^t)\phi(s_{q_1}')\phi(s_{q_2}')\phi(s_{q_1q_2}').
\end{aligned}$$

Again we apply properties of the Euler phi function to get

$$\begin{aligned}
N(q_1q_2, c, p) &= \frac{q_2^{j_2}}{q_1q_2}\left(\sum_{x | q_1^{j_1} s_{q_1}s_{q_2}s_{q_1q_2}} \phi(x) - \sum_{\substack{0 \le t \le j_1 \\ s_{q_1}'|s_{q_1}, s_{q_2}'|s_{q_2}, s_{q_1q_2}'|s_{q_1q_2} \\ s_{q_1}'s_{q_1q_2}' = 1 \text{ and } t \le k_1}} \phi(q_1^t)\phi(s_{q_1}')\phi(s_{q_2}')\phi(s_{q_1q_2}') \right) \\
&= \frac{q_2^{j_2}}{q_1q_2}\left(q_1^{j_1} s_{q_1}s_{q_2}s_{q_1q_2} - \sum_{\substack{0 \le t \le j_1 \\ t \le k_1 \\ s_{q_1}'|s_{q_1}}} \phi(q_1^t)\phi(s_{q_2}') \right).
\end{aligned}$$

By Lemma 2.3, we know that either $j_1 = 1$ or $k_1 = 1$. Therefore if $t \le j_1$ and $t \le k_1$, it follows that $t \le 1$. This allows us to write:

$$\begin{aligned}
N(q_1q_2, c, p) &= \frac{q_2^{j_2}}{q_1q_2}\left(q_1^{j_1} s_{q_1}s_{q_2}s_{q_1q_2} - \sum_{\substack{t \in \{0,1\} \\ s_{q_2}'|s_{q_2}}} \phi(q_1^t)\phi(s_{q_2}') \right) \\
&= \frac{q_2^{j_2}}{q_1q_2}\left(q_1^{j_1} s_{q_1}s_{q_2}s_{q_1q_2} - \sum_{x | q_1 s_{q_2}} \phi(x) \right).
\end{aligned}$$

Applying the property of the Euler phi regarding the sum of $\phi(x)$ for divisors x of $n \in \mathbb{N}$ allows us to rewrite the summation as:

$$
\begin{aligned}
&= \frac{q_2^{j_2}}{q_1 q_2}\left(q_1^{j_1} s_{q_1} s_{q_2} s_{q_1 q_2} - q_1 s_{q_2}\right) \\
&= \frac{q_1^{j_1} q_2^{j_2} s_{q_1} s_{q_2} s_{q_1 q_2}}{q_1 q_2} - \frac{q_1 q_2^{j_2} s_{q_2}}{q_1 q_2} \\
&= \frac{p^{q_1 q_2} - 1}{q_1 q_2 (p-1)} - \frac{p^{q_2} - 1}{q_2 (p-1)}.
\end{aligned}
$$

It remains to examine the case where $q_1 | m$. Recall that $m = q_1^u q_2^{k_2} s_1'$ for some s_1' dividing s_1 and $0 \leq u < k_1$ and $r = q_1^t q_2^{k_2+j_2} s_1' s_{q_1}' s_{q_2}' s_{q_1 q_2}'$ for some $s_{q_1}', s_{q_2}', s_{q_1 q_2}'$ dividing s_{q_1}, s_{q_2}, and $s_{q_1 q_2}$ respectively and $u \leq t < k_1 + j_1$, with u and s_1' depending only on m, whereas t, s_{q_1}, s_{q_2}, and $s_{q_1 q_2}$ also depend on r.

Note as above that either j_1 or k_1 must be 1. Suppose by way of contradiction that $k_1 = 1$. Then we have $0 \leq t < 1 + j_1$ and therefore $t \leq j_1$. In this case, q_1^t is a divisor of both r and $\frac{p^{q_1 q_2 - 1}}{p-1}$ and therefore of d_r. This implies that $q_1^t \nmid m$, contradicting our assumption in this case. We therefore have $j_1 = 1$. This allows us to compute

$$
\begin{aligned}
d_r &= \gcd\left(r, \frac{p^{q_1 q_1} - 1}{p-1}\right) \\
&= \gcd\left(q_1^t q_2^{k_2+j_2} s_1' s_{q_1}' s_{q_2}' s_{q_1 q_2}', q_1^{j_1} q_2^{j_1} s_{q_1} s_{q_2} s_{q_1 q_2}\right) \\
&= q_1^{j_1} q_2^{j_2} s_{q_1}' s_{q_2}' s_{q_1 q_2}' \\
&= q_1 q_2^{j_2} s_{q_1}' s_{q_2}' s_{q_1 q_2}'.
\end{aligned}
$$

Since $r = m_r d_r$, we have $m_r = q_1^{t-1} q_2^{k_2} s_1'$, implying that $t = u + 1$. This is significant since u depends only on m and not on r. As in the first case, in order for r to be in the set D_r, we also need either $s_{q_1}' \neq 1$, $s_{q_1 q_2}' \neq 1$, or $t > k$. Since $t < k_1 + j_1$ and $j_1 = 1$, it is not possible to have $t > k_1$. Thus we have either $s_{q_1}' \neq 1$ or $s_{q_1 q_2}' \neq 1$. Again by Theorem 1.2,

$$
\begin{aligned}
N(q_1 q_2, c, p) &= \frac{1}{q_1 q_2 \phi(m)} \sum_{\substack{r \in D_n \\ m_r = m}} \phi(r) \\
&= \frac{1}{q_1 q_2 \phi(q_1^u q_2^{k_2} s_1')} \sum_{\substack{s_{q_1}' | s_{q_1}, s_{q_2}' | s_{q_2}, s_{q_1 q_2}' | s_{q_1 q_2} \\ s_{q_1}' s_{q_1 q_2}' \neq 1}} \phi(q_1^{u+1}) \phi(q_2^{k_2+j_2}) \phi(s_1') \phi(s_{q_1}') \phi(s_{q_2}') \phi(s_{q_1 q_2}') \\
&= \frac{\phi(q_1^{u+1}) \phi(q_2^{k_2+j_2}) \phi(s_1')}{q_1 q_2 \phi(q_1^u) \phi(q_2^{k_2}) \phi(s_1')} \sum_{\substack{s_{q_1}' | s_{q_1}, s_{q_2}' | s_{q_2}, s_{q_1 q_2}' | s_{q_1 q_2} \\ s_{q_1}' s_{q_1 q_2}' \neq 1}} \phi(s_{q_1}' s_{q_2}' s_{q_1 q_2}').
\end{aligned}
$$

Again applying the property of the Euler phi regarding the sum of $\phi(x)$ for divisors x of $n \in \mathbb{N}$, we have

$$\begin{aligned}N(q_1q_2,c,p) &= \frac{q_1q_2^{j_2}}{q_1q_2}\left(\sum_{x|s_{q_1}s_{q_2}s_{q_1q_2}}\phi(x) - \sum_{x|s_{q_2}}\phi(x)\right)\\ &= \frac{q_1q_2^{j_2}}{q_1q_2}\left(s_{q_1}s_{q_2}s_{q_1q_2} - s_{q_2}\right)\\ &= \frac{q_1^{j_1}q_2^{j_2}s_{q_1}s_{q_2}s_{q_1q_2}}{q_1q_2} - \frac{q_1q_2^{j_2}s_{q_2}}{q_1q_2}\\ &= \frac{p^{q_1q_2}-1}{q_1q_2(p-1)} - \frac{p^{q_2}-1}{q_2(p-1)}.\end{aligned}$$ □

Now we are ready to prove the following theorem.

Theorem 2.4 (Bottom of lattice)**.** *If $a \in \mathbb{Z}_p^*$ is both q_1-residue and a q_2-residue, then*

$$N(q_1q_2,a,p) = \frac{p^{q_1q_2}-1}{q_1q_2(p-1)} - \frac{p^{q_1}-1}{q_1(p-1)} - \frac{p^{q_2}-1}{q_2(p-1)} + 1$$

Proof. Since every irreducible polynomial has nonzero constant term, $N(q_1q_2,p)$ can be expressed as the sum

$$N(q_1q_2,p) = \sum_{a\in\mathbb{Z}_p^*} N(q_1q_2,a,p)$$

By Theorem 1.1, the left side of the equation is

$$N(q_1q_2,p) = \frac{1}{q_1q_2}\left(p^{q_1q_2} - p^{q_1} - p^{q_2} + p\right)$$

In order to rewrite the right side of the equation, we begin by classifying the elements of $\mathbb{Z}_p^*$ according to whether they are q_1-residues, q_2-residues, both, or neither. Let α be a generator of $\mathbb{Z}_p^*$. If $a \in \mathbb{Z}_p^*$ is both a q_1- and a q_2-residue, then $a = \alpha^{kq_1q_2}$ for some $0 \le k < \frac{p-1}{q_1q_2}$. Therefore there are $\frac{p-1}{q_1q_2}$ elements of $\mathbb{Z}_p^*$ that are both q_1-residues and q_2-residues.

If $a \in \mathbb{Z}_p^*$ is a q_1-residue but not a q_2-residue, then $a = \alpha^{kq_1}$ for some $0 \le k < \frac{p-1}{q_1}$ with $q_2 \nmid k$. Thus there are $\frac{p-1}{q_1} - \frac{p-1}{q_1q_2}$ elements of $\mathbb{Z}_p^*$ that are q_1-residues but not q_2-residues. Similarly, there are $\frac{p-1}{q_2} - \frac{p-1}{q_1q_2}$ elements of $\mathbb{Z}_p^*$ that are q_1-residues but not q_2-residues.

The remaining elements of $\mathbb{Z}_p^*$ are neither q_1-residues nor q_2 residues. Therefore the number of elements in this collection is given by

$$(p-1) - \left(\frac{p-1}{q_2} - \frac{p-1}{q_1q_2}\right) - \left(\frac{p-1}{q_1} - \frac{p-1}{q_1q_2}\right) - \frac{p-1}{q_1q_2}$$

which simplifies to

$$(p-1) - \frac{p-1}{q_2} - \frac{p-1}{q_1} + \frac{p-1}{q_1q_1}.$$

Theorems 2.2 and 2.3 and 1.3 demonstrate that $N(q_1q_2,a,p)$ depends only on whether a is a q_1-residue and/or q_2-residue. It follows that

$$\begin{aligned}N(q_1q_2,p) = &\frac{p-1}{q_1q_2}N(q_1q_2,\alpha^{q_1q_2},p)\\&+\left(\frac{p-1}{q_1}-\frac{p-1}{q_1q_2}\right)N(q_1q_2,\alpha^{q_1},p)\\&+\left(\frac{p-1}{q_2}-\frac{p-1}{q_1q_2}\right)N(q_1q_2,\alpha^{q_2},p)\\&+\left(p-1-\frac{p-1}{q_1}-\frac{p-1}{q_2}+\frac{p-1}{q_1q_2}\right)N(q_1q_2,\alpha,p)\end{aligned}$$

Using the results of Theorems 2.2, 2.3, and 1.1, we obtain

$$\begin{aligned}\frac{1}{q_1q_2}\left(p^{q_1q_2}-p^{q_1}-p^{q_2}+p\right) = &\frac{p-1}{q_1q_2}N(q_1q_2,\alpha^{q_1q_2},p)\\&+\left(\frac{p-1}{q_1}-\frac{p-1}{q_1q_2}\right)\left(\frac{p^{q_1q_2}-1}{q_1q_2(p-1)}-\frac{p^{q_2}-1}{q_2(p-1)}\right)\\&+\left(\frac{p-1}{q_2}-\frac{p-1}{q_1q_2}\right)\left(\frac{p^{q_1q_2}-1}{q_1q_2(p-1)}-\frac{p^{q_1}-1}{q_1(p-1)}\right)\\&+\left(p-1-\frac{p-1}{q_1}-\frac{p-1}{q_2}+\frac{p-1}{q_1q_2}\right)\left(\frac{p^{q_1q_2}-1}{q_1q_2(p-1)}\right).\end{aligned}$$

which can be simplified to

$$\begin{aligned}\frac{p^{q_1q_2}-p^{q_1}-p^{q_2}+p}{q_1q_2} = &\frac{p-1}{q_1q_2}N(q_1q_2,\alpha^{q_1q_2},p)+\left(\frac{1}{q_1}-\frac{1}{q_1q_2}\right)\left(\frac{p^{q_1q_2}-1}{q_1q_2}-\frac{p^{q_2}-1}{q_2}\right)\\&+\left(\frac{1}{q_2}-\frac{1}{q_1q_2}\right)\left(\frac{p^{q_1q_2}-1}{q_1q_2}-\frac{p^{q_1}-1}{q_1}\right)\\&+\left(1-\frac{1}{q_1}-\frac{1}{q_2}+\frac{1}{q_1q_2}\right)\left(\frac{p^{q_1q_2}-1}{q_1q_2}\right).\end{aligned}$$

Multiplying by q_1q_2 gives

$$\begin{aligned}(p^{q_1q_2}-p^{q_1}-p^{q_2}+p) = (p-1)N(q_1q_2,\alpha^{q_1q_2},p)+(q_2-1)\left(\frac{p^{q_1q_2}-1}{q_1q_2}-\frac{p^{q_2}-1}{q_2}\right)\\+(q_1-1)\left(\frac{p^{q_1q_2}-1}{q_1q_2}-\frac{p^{q_1}-1}{q_1}\right)+(q_1q_2-q_1-q_2+1)\left(\frac{p^{q_1q_2}-1}{q_1q_2}\right).\end{aligned}$$

This can in turn be simplified to give

$$p-1=(p-1)N(q_1q_2,\alpha^{q_1q_2},p)+\frac{p^{q_2}-1}{q_2}+\frac{p^{q_1}-1}{q_1}-\frac{p^{q_1q_2}-1}{q_1q_2}.$$

Dividing both sides by $(p-1)$ leaves

$$1=N(q_1q_2,\alpha^{q_1q_2},p)+\frac{p^{q_2}-1}{q_2(p-1)}+\frac{p^{q_1}-1}{q_1(p-1)}-\frac{p^{q_1q_2}-1}{q_1q_2(p-1)}.$$

This is equivalent to

$$\frac{p^{q_1q_2}-1}{q_1q_2(p-1)}-\frac{p^{q_1}-1}{q_1(p-1)}-\frac{p^{q_2}-1}{q_2(p-1)}+1=N(q_1q_2,\alpha^{q_1q_2},p),$$

which completes the proof. □

Let us consider again $\mathbb{Z}_{31}$ with $q_1 = 3$ and $q_2 = 5$. Theorems 2.2, 2.3, and 2.4 show that the set

$$D_{15} = \{r : r|31^{15} - 1, r \nmid 31^3 - 1, r \nmid 31^5 - 1\}$$

can be partitioned into the following sets:

$$\begin{aligned}
D_{top} &= \{r \in D_{15} : q_1^{k_1+j_1}|r \text{ and } q_2^{k_2+j_2}|r\} = \{r \in D_{15} : 3^2|r \text{ and } 5^2|r\}\\
D_{side3} &= \{r \in D_{15} : q_1^{k_1+j_1}|r \text{ and } q_2^{k_2+j_2} \nmid r\} = \{r \in D_{15} : 3^2|r \text{ and } 5^2 \nmid r\}\\
D_{side5} &= \{r \in D_{15} : q_1^{k_1+j_1} \nmid r \text{ and } q_2^{k_2+j_2}|r\} = \{r \in D_{15} : 3^2 \nmid r \text{ and } 5^2|r\}\\
D_{bottom} &= \{r \in D_{15} : q_1^{k_1+j_1} \nmid r \text{ and } q_2^{k_2+j_2} \nmid r\} = \{r \in D_{15} : 3^2 \nmid r \text{ and } 5^2 \nmid r\}
\end{aligned}$$

The sums computed in the proofs of Theorems 2.2, 2.3, and 2.4 are sums over these subsets of D_{15}.

3 The case $p \not\equiv 1 \pmod{q_1}$

Let us consider when $p \not\equiv 1 \pmod{q_1}$ and $p \not\equiv 1 \pmod{q_2}$, In fact, we have the following more general result, which follows directly from Theorem 1.3.

Theorem 3.1. *Assume* $n \in \mathbb{N}$ *and* $\gcd(n, p-1) = 1$. *Then for any* $a \in \mathbb{Z}_p^*$,

$$N(n, a, p) = \frac{1}{p-1}N(n, p) = \frac{1}{n(p-1)}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d.$$

Corollary 3.1. *Assume* $n = q_1q_2$ *and* $\gcd(n, p) = 1$. *Then* $N(n, a, p) = \frac{p^{q_1q_2} - p^{q_1} - p^{q_2} + p}{q_1q_2(p-1)}$ *for any* $a \in \mathbb{Z}_p^*$.

Finally we will consider when $p \not\equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$. Then we will have two possibilities, depending on whether or not the constant term is a q_2-residue. In other words, a constant term a is either a q_1-residue and not a q_2-residue, or a is both a q_1-residue and a q_2-residue.

Theorem 3.2. *Assume* $p \not\equiv 1 \pmod{q_1}$ *and* $p \equiv 1 \pmod{q_2}$.

1. *If* $a \in \mathbb{Z}_p^*$ *is not a* q_2*-residue, then*

$$N(q_1q_2, a, p) = \frac{p^{q_1q_2} - 1}{q_1q_2(p-1)} - \frac{p^{q_2} - 1}{q_1q_2(p-1)} = \frac{p^{q_1q_2} - p^{q_2}}{q_1q_2(p-1)}.$$

2. *If* $a \in \mathbb{Z}_p^*$ *is a* q_2*-residue, then*

$$N(q_1q_2, a, p) = \frac{p^{q_1q_2} - 1}{q_1q_2(p-1)} - \frac{p^{q_2} - 1}{q_1q_2(p-1)} - \frac{p^{q_1} - p}{q_2(p-1)}.$$

Before we begin this proof, we need a modification of Lemma 2.2.

Lemma 3.1. *For primes $p, q_1,$ and q_2 with $p \not\equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$, we may write*

$$\begin{aligned} p-1 &= q_2^{k_2} s_1 \\ p^{q_2}-1 &= q_2^{k_2+j_2} s_1 s_{q_2} \\ p^{q_1q_2}-1 &= q_2^{k_2+j_2} s_1 s_{q_2} s_{q_1q_2} \end{aligned}$$

where all variables represent positive integers, the integers $s_1, s_{q_2}, s_{q_1q_2}, q_1$,and q_2 are pairwise relatively prime, and $\gcd(q_1, s_1) = 1$.

Note that q_1 cannot be a factor of s_1 but it can potentially be a factor of s_{q_2} or $s_{q_1q_2}$ The proof of this lemma follows from that of Lemma 2.2 and is omitted. Now we are ready to prove Theorem 3.2.

Proof. To prove (1), assume $a \in \mathbb{Z}_p^*$ is not a q_2-residue. We will use Lemma 3.1 to write

$$\begin{aligned} p-1 &= q_2^{k_2} s_1 \\ p^{q_2}-1 &= q_2^{k_2+j_2} s_1 s_{q_2} \\ p^{q_1q_2}-1 &= q_2^{k_2+j_2} s_1 s_{q_2} s_{q_1q_2}. \end{aligned}$$

Let $c \in \mathbb{Z}_p^*$ where c is not a q_2-residue, and let m be the order of c. Then, as argued in the proof of Theorem 2.2, $m = q_2^{k_2} s'_1$ for some s'_1 dividing s_1.

Let $r \in D_{q_1q_2}$ with $m_r = m$, where $r = m_r d_r$ and $d_r = \gcd(r, \frac{p^{q_1q_2}-1}{p-1})$. Since $q_2^{k_2}$ divides m_r and $q_2^{j_2}$ divides $\frac{p^{q_1q_2}-1}{p-1}$, it must be the case that $q_2^{k_2+j_2}$ divides r. Since $q_2^{k_2+j_2}$ divides $p^{q_2}-1$, the only way to ensure $r|p^{q_1q_2}-1$ and not $p-1$ or $p^{q_2}-1$ is the presence of a prime from $s_{q_1q_2}$. It follows from Theorem 1.2 that

$$\begin{aligned} N(q_1q_2, c, p) &= \frac{1}{q_1q_2\phi(m)} \sum_{\substack{r \in D_n \\ m_r = m}} \phi(r) \\ &= \frac{1}{q_1q_2\phi(m)} \sum_{s'_{q_2}|s_{q_2}, s'_{q_1q_2}|s_{q_1q_2}, s'_{q_1q_2}\neq 1} \phi(q_2^{k_2+j_2} s'_1 s'_{q_2} s'_{q_1q_2}) \\ &= \frac{1}{q_1q_2\phi(q_2^{k_2} s'_1)} \sum_{s'_1|s_1, s'_{q_2}|s_{q_2}, s'_{q_1q_2}|s_{q_1q_2}, s'_{q_1q_2}\neq 1} \phi(q_2^{k_2+j_2})\phi(s'_1)\phi(s'_{q_2} s'_{q_1q_2}) \\ &= \frac{\phi(q_2^{k_2+j_2})}{q_1q_2\phi(q_2^{k_2})} \sum_{s'_{q_2}|s_{q_2}, s'_{q_1q_2}|s_{q_1q_2}, s'_{q_1q_2}\neq 1} \phi(s'_{q_2} s'_{q_1q_2}) \end{aligned}$$

Again using properties of the Euler phi function, we can rewrite this summation as follows:

$$N(q_1q_2, c, p) = \frac{q_2^{j_2}}{q_1q_2}(s_{q_2}s_{q_1q_2} - s_{q_2}) = \frac{p^{q_1q_2}-1}{q_1q_2(p-1)} - \frac{p^{q_2}-1}{q_1q_2(p-1)}$$

which proves (1).

To prove (2), first note that by Theorem 3.1, for any two elements $a, b \in \mathbb{Z}_p^*$ which are both q_2-residues, $N(n, a, p) = N(n, b, p)$. Theorem 1.1, tells us $N(q_1q_2, p) = \frac{p^{q_1q_2}-p^{q_1}-p^{q_2}+p}{q_1q_2}$. Since there are $\frac{p-1}{q_2}$ elements of $\mathbb{Z}_p^*$ which are q_2-residues (with $N(q_1q_2, c, p) = \frac{p^n - p^{q_2}}{n(p-1)}$) and $p - 1 - \frac{p-1}{q_2} = (p-1)(1 - \frac{1}{q_2})$ which are not, we can compute $N(q_1q_2, a, p)$ by finding the following.

$$
\begin{aligned}
N(q_1q_2,a,p) &= \frac{\frac{p^{q_1q_2}-p^{q_1}-p^{q_2}+p}{q_1q_2} - \left(\frac{p^{q_1q_2}-p^{q_2}}{q_1q_2(p-1)}\right)(p-1)(1-\frac{1}{q_2})}{\frac{p-1}{q_2}} \\
&= \frac{1}{q_1q_2(p-1)}\left[q_2(p^{q_1q_2}-p^{q_1}-p^{q_2}+p)-(p^{q_1q_2}-p^{q_2})(q_2-1)\right] \\
&= \frac{1}{q_1q_2(p-1)}[-q_2p^{q_1}+q_2p+p^{q_1q_2}-p^{q_2}] \\
&= \frac{1}{q_1q_2(p-1)}[(p^{q_1q_2}-1)-(p^{q_2}-1)-q_2(p^{q_1}-p)] \\
&= \frac{p^{q_1q_2}-1}{q_1q_2(p-1)} - \frac{p^{q_2}-1}{q_1q_2(p-1)} - \frac{p^{q_1}-p}{q_1(p-1)}. \qquad \square
\end{aligned}
$$

4 Conclusion

Consider the case when q_1 and q_2 both divide $p-1$. While considering values of $N(q_1q_2,a,p)$ when q_1 and q_2 both divide $p-1$, we found it useful to visualize these values in the following lattice. This is the same lattice from Section 1 with the edges labeled. The edges of the lattice are labeled with values of $N(q_1,a,p)$ or $N(q_2,a,p)$ to represent the difference between the vertices of that edge. For example, $N(q_1q_2,\alpha,p)-N(q_1q_2,\alpha^{q_1},p)=N(q_2,\alpha^{q_1},p)$.

$$\begin{tikzcd}
 & \boxed{N(q_1q_2,\alpha,p)} \arrow[dl, dash, "N(q_1,\alpha^{q_2},p)"'] \arrow[dr, dash, "N(q_2,\alpha^{q_1},p)"] & \\
\boxed{N(q_1q_2,\alpha^{q_2},p)} \arrow[dr, dash, "N(q_2,\alpha^{q_1q_2},p)"'] & & \boxed{N(q_1q_2,\alpha^{q_1},p)} \arrow[dl, dash, "N(q_1,\alpha^{q_1q_2},p)"] \\
 & \boxed{N(q_1q_2,\alpha^{q_1q_2},p)} &
\end{tikzcd}$$

The values on the edges were computed in [1] and are summarized in the next theorem.

Theorem 4.1. *Let* $k \in \mathbb{N}$.

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

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

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

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

3. *(Theorem 4.1 and 4.2) Let* $\gcd(q,p-1)=q$, *and let* $a \in \mathbb{Z}_p^*$ *be a q-residue, then*

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

Since the next two theorems are easy corollaries of Theorem 4.1, Theorem 2.2, Theorem 2.3, and Theorem 2.4, we leave the proofs to the reader.

Theorem 4.2. $N(q_1q_2, \alpha, p) - N(q_1q_2, \alpha^{q_1}, p) = N(q_2, \alpha^{q_1}, p)$

Theorem 4.3. $N(q_1q_2, \alpha^{q_1}, p) - N(q_1q_2, \alpha^{q_1q_2}, p) = N(q_1, \alpha^{q_1q_2}, p)$

In the case where q_1 divides $p-1$, but q_2 does not, we get a much simpler lattice. Notice that the lattice representation of Case 2 is identical to the top right portion of the lattice representation of the first case.

$$\begin{tikzcd}
\boxed{N(q_1q_2, \alpha, p)} \arrow[dr, dash, "N(q_2, \alpha^{q_1}, p)"] & \\
& \boxed{N(q_1q_2, \alpha^{q_1}, p)}
\end{tikzcd}$$

The proof of the next theorem is also a corollary of Theorem 4.1 and Theorem 3.2 and is left to the reader.

Theorem 4.4. $N(q_1q_2, \alpha, p) - N(q_1q_2, \alpha^{q_1}, p) = N(q_2, \alpha^{q_1}, p)$.

Now we are ready to consider the ratios of $N(q_1q_2, a, p)$ for varying values of a. When $p \equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$, there are three possible values of $N(q_1q_2, a, p)$ depending on whether a is a q_1-residue and/or a q_2-residue. The largest possible value would be $\frac{p^{q_1q_2}-1}{q_1q_2(p-1)}$ when a is neither residue, and the smallest value would be $\frac{p^{q_1q_2}-1}{q_1q_2(p-1)} - \frac{p^{q_1}-1}{q_1(p-1)} - \frac{p^{q_2}-1}{q_2(p-1)} + 1$ when a is both residues. Observe that the ratio of these terms would be

$$\frac{N(q_1q_2, \alpha^{q_1q_2}, p)}{N(q_1q_2, \alpha, p)} = 1 - \frac{q_2(p^{q_1}-1)}{p^{q_1q_2}-1} - \frac{q_1(p^{q_2}-1)}{p^{q_1q_2}-1} + \frac{q_1q_2(p-1)}{p^{q_1q_2}-1}.$$

As $q_1q_2 \to \infty$, this ratio will approach one. Hence the other two possible ratios will also approach one as $q_1q_2 \to \infty$.

Next, when $p \not\equiv 1 \pmod{q_1}$ and $p \equiv 1 \pmod{q_2}$, we have the following ratio

$$\frac{N(q_1q_2, \alpha, p)}{N(q_1q_2, \alpha^{q_1}, p)} = \frac{p^{q_1q_2} - p^{q_2}}{p^{q_1q_2} - p^{q_2} - p^{q_1} + q_1p}$$

which also approaches one as $q_1q_2 \to \infty$. Finally, the case when $p \not\equiv 1 \pmod{q_1}$ and $p \not\equiv 1 \pmod{q_2}$ automatically yields a ratio $\frac{N(q_1q_2,a,p)}{N(q_1q_2,b,p)} = 1$ as these values $N(q_1q_2, a, p)$ are identical for any $a \in \mathbb{Z}_p^*$.

Therefore the proportions of constant terms of these monic irreducible polynomials of degree q_1q_2 are asymptotically equal, as their limits show a uniform distribution among the constant terms.

Acknowledgements

We would like to give special thanks to Catherine Stringfellow and Richard Simpson, our colleagues from Midwestern State University, whose work on calculating irreducible polynomials helped us confirm our results.

References

[1] Cobb, S., Knox, M., Lopez, M., McDonald, T., & Mitchell, P. (2019). Distribution of constant terms of polynomials in $\mathbb{Z}_p[x]$. *Notes on Number Theory and Discrete Mathematics*, 25(4), 72–82.

[2] Křížek, M., Luca, F., & Somer, L. (2001). *17 Lectures on Fermat Numbers. From Number Theory to Geometry.* CMS Books in Mathematics, Springer-Verlag, New York.

[3] Lidl, R., & Niederreiter, H. (1994). *Introduction to Finite Fields and Their Applications (Revised ed.).* Cambridge UP, Cambridge.

[4] Omidi Koma, B., Panario, D., & Wang, Q. (2010). The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms. *Discrete Mathematics*, 310, 1282–1292.

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