Number of Non–Zero Coefficients of $(1 + x^a + x^b)^n$ over $\mathbf{F}_p$

Andy Zhuang

Abstract

The paper studies explicit formulas for $N_p(n; a, b)$, the count of coefficients that remain non–zero modulo a prime p in the trinomial power $(1+x^a+x^b)^n$ with $0 < a < b < p$. Leveraging Lucas' digit–wise criterion and the matrix–automaton framework of Amdeberhan–Stanley, we first prove a *carry-free theorem*: if every base-p digit of n does not exceed $\lfloor (p-1)/b \rfloor$ and the generated x-exponents do not overlap at every digit position, then no cross-digit carries occur and the exponents are unique for each digit position. This leads to $N_p(n; a, b)$ being factorized as $\prod_l \binom{n_l+2}{2}$, where n_l are digits of n under base-p.

The paper next derives a upper bound $N_p(n; a, b) \le 3^{\,w_p(n)}$, where $w_p(n)$ is the sum of the base-p digits of n, and shows that equality holds precisely when every digit of n is 0 or 1. Worked examples—including the case $(1 + x + x^3)^n$ over $\mathbb{F}_7$—demonstrate the formulas in practice, and the discussion shows our contributions within earlier studies on automatic sequences and multinomial Lucas theorems.

1 Preliminaries

The problem of deciding when a coefficient of a polynomial power $f(x)^n \in \mathbb{F}_p[x]$ disappears modulo a fixed prime (or prime power) sits at the intersection of additive number theory, automatic sequences, and algebraic combinatorics. We summarize the main results of prior work that our work builds upon.

1.1 Digit–wise carry criteria: Kummer and Lucas

Kummer's paper [5] on ideal factorizations already contains a *carry interpretation* for p-adic valuations of binomial coefficients. Lucas [2] made the idea explicit for residues mod p: in modern language, writing $n = \sum n_j p^j,\ k = \sum k_j p^j$, one has

$$\binom{n}{k} \equiv \prod_j \binom{n_j}{k_j} \pmod{p},$$

so $\binom{n}{k} \not\equiv 0$ iff every digit satisfies $k_j \le n_j$.

In an extended form, Lucas' theorem also works for multinomials.

Let p be a prime, and let

$$n = n_0 + n_1 p + \cdots + n_r p^r$$

$$k_j = k_{j0} + k_{j1} p + \cdots + k_{jr} p^r \quad \text{for } j = 1, 2, \ldots, m$$

with $\sum_{j=1}^{m} k_{ji} = n_i$ for all $i = 0, 1, \ldots, r$.

Then

$$\binom{n}{k_1, k_2, \ldots, k_m} \equiv \prod_{i=0}^{r} \binom{n_i}{k_{1i}, k_{2i}, \ldots, k_{mi}} \pmod{p}$$

Clear explanation and other extensions (e.g. to multinomial coefficients) can be found in Riddle's survey [6].

1.2 Automatic sequences and matrix automata

Lucas's digit test implies that the *indicator sequence* $\left[\binom{n}{k} \not\equiv 0\right]_{n\geq 0}$ is p-automatic. Allouche and Shallit's theory of regular sequences [3] provides a linear-algebraic description: reading the base-p digits of n drives a finite automaton whose transition matrices $A_0, \ldots, A_{p-1}$ count admissible digit patterns.

For *general* polynomials f, Amdeberhan & Stanley constructed such matrices in their paper on *Polynomial Coefficient Enumeration* [1].

They showed that $N_p(n; f) := \#\{\text{coefficients } \not\equiv 0 \pmod{p}\}$ admits the factorization $N_p(n; f) = uA_{a_t} \cdots A_{a_0} v$ for $n = \sum a_j p^j$. This matrix viewpoint is the foundation of this paper. We specialized or refined their general framework.

1.3 Fractal growth and sparse trinomials

For the specific trinomial $1+x+x^2$ over $\mathbb{F}_3$, Ellison's undergraduate thesis empirically observed a *power-law* growth $N_3(n) \asymp n^{\beta}$ and proved $\beta = \log_3 \rho(A)$ where $\rho(A)$ is the Perron eigenvalue of the 3×3 transition matrix [4]. Her limit theorem clarified earlier numerical evidence of fractal self-similarity in trinomial Pascal triangles.

1.4 Notations

Throughout this paper

$$p \text{ is prime}, \qquad 0 < a < b < p, \qquad N_p(n; a, b) := \#\big\{\text{non–zero coefficients of } (1 + x^a + x^b)^n\big\}.$$

Write the base-p expansion $n = \sum_{j=0}^{s} n_j p^j$ and denote $w_p(n) := \sum_j n_j$ as its digit-sum.

2 Theorem for the Carry-free Case

In this section, we will prove a formula for calculating $N_p(n; a, b)$ in a special case when there is no carry in the base-p expression of n.

Lemma 2.1. *let a, b, p, n be positive integers, which satisfy $0 < a < b < p$ and $n \leq \lfloor (p-1)/b \rfloor$. For integer i, j satisfying $0 \leq i, j \leq n$ and $i+j \leq n$, the number of unique values for $a*j+b*k$ can be written as:*

$$N(n) = \begin{cases} \dfrac{(n+1)(n+2)}{2}, & 0 \leq n < b_0, \\ b_0(n+1) - \dfrac{b_0(b_0-1)}{2}, & n \geq b_0. \end{cases}$$

where, $d = \gcd(a, b)$ *and* $b_0 = b/d$.

Proof. **1. Remove the common factor.** Write $a = d\,a_0$ and $b = d\,b_0$ with $\gcd(a_0, b_0) = 1$; then let

$$X_{j,k} = d\,Y_{j,k}, \qquad Y_{j,k} := a_0\,j + b_0\,k.$$

Multiplication by the positive constant d is injective, so it suffices to count the distinct values of $Y_{j,k}$.

2. Characterize collisions. Suppose two pairs (j_1, k_1) and (j_2, k_2) give the same value, i.e. $a_0 j_1 + b_0 k_1 = a_0 j_2 + b_0 k_2$. Because a_0 and b_0 are coprime,

$$(j_1 - j_2,\ k_1 - k_2) = t\,(b_0,\ -a_0) \qquad (t \in \mathbb{Z}).$$

Hence all lattice points that give the *same* Y form a translate of the one–dimensional lattice generated by $\Delta := (b_0, -a_0)$. Each such class therefore contains a unique representative whose first coordinate lies in the range

$$0 \le j \le b_0 - 1.$$

3. Count the representatives. Fix a residue j with $0 \le j \le \min\{n, b_0 - 1\}$. The admissible values of k satisfy $0 \le k \le n - j$, giving $n - j + 1$ lattice points. Summing over all eligible j we get

$$N(n) = \sum_{j=0}^{\min\{n, b_0 - 1\}} (n - j + 1).$$

4. Evaluate the sum. If $n < b_0$ the upper limit is $j = n$, and

$$N(n) = \sum_{j=0}^{n} (n - j + 1) = \frac{(n+1)(n+2)}{2}.$$

If $n \ge b_0$ the upper limit is $j = b_0 - 1$, and

$$N(n) = \sum_{j=0}^{b_0 - 1} (n - j + 1) = b_0(n+1) - \frac{b_0(b_0 - 1)}{2}.$$

5. No modular coincidences. Because $j + k \le n$ we have $X_{j,k} \le b\,n \le p - 1$ by the assumption on n; therefore two values coincide modulo p iff they coincide as ordinary integers, and the count above is indeed the desired number of distinct values.

□

Theorem 2.2 (Carry-free)**.** *Let p be a prime, $0 < a < b < p$ and $\gcd(a, b) = 1$. Write the exponent $n = \sum_{l=0}^{s} n_l p^l$ with base–p digits $0 \le n_l \le p - 1$. Let*

$$\tau \ := \ \Big\lfloor \frac{p-1}{b} \Big\rfloor.$$

If every digit satisfies $n_l \le \tau$ and $\tau < b$, then the number

$$N_p(n; a, b) \ = \ \#\big\{\textit{coefficients} \ \not\equiv 0 \pmod p \ \textit{in} \ (1 + x^a + x^b)^n\big\}$$

is

$$N_p(n; a, b) \ = \ \prod_{l=0}^{s} \binom{n_l + 2}{2}. \tag{1}$$

Proof. We expand $(1+x^a+x^b)^n = \sum_{i+j+k=n} \binom{n}{i,j,k} x^{aj+bk}$, where $i, j, k \geq 0$ and $\binom{n}{i,j,k} = \dfrac{n!}{i!\, j!\, k!}$ denotes a trinomial coefficient. A term contributes to $N_p(n; a, b)$ precisely when $\binom{n}{i,j,k} \not\equiv 0 \pmod{p}$. We prove four claims as follows.

(i) Digit conditions for the existence of a term. Write $i = \sum i_l p^l$, $j = \sum j_l p^l$, $k = \sum k_l p^l$ with $0 \leq i_l, j_l, k_l \leq p-1$. Lucas's theorem for multinomials [2] says

$$\binom{n}{i,j,k} \not\equiv 0 \pmod{p} \iff i_l + j_l + k_l = n_j \quad \text{for all } l.$$

Equivalently, *no base-p carry occurs* when adding the digit triples.

(ii) Absence of carries for the exponent under the hypothesis $n_l \leq \tau$**.** Fix a digit position l. Because $i_l + j_l + k_l = n_l \leq \tau$, we have $aj_l + bk_l \leq b(j_l + k_l) \leq bn_l \leq b\tau \leq p-1$, so $aj_l + bk_l < p$. Thus, when we multiply the lth-place exponents aj_l and bk_l and add them, *no carry is propagated* to the next higher digit of the total exponent $aj + bk$.

(iii) For the l***'s digit, each*** $aj_l + bk_l$ ***is unique*** This can be proved with contradiction. if we have $aj_{l1} + bk_{l1} = aj_{l2} + bk_{l2}$, where $j_{l1} \neq j_{l2}$ and $k_{l1} \neq k_{l2}$. Let's assume $j_{l1} > j_{l2}$, It can be written as:

$$a(j_{l1} - j_{l2}) = b(k_{l2} - k_{l1})$$

Since $gcd(a, b) = 1$, $j_{l1} - j_{l2}$ must be a multiple of b. This is impossible because $0 < j_{l1} - j_{l2} < n_l \leq \tau < b$.

(iv) Counting valid digit triples. For a fixed digit n_l, the number of non-negative integer solutions to $i_l + j_l + k_l = n_l$ can be derived from Lemma 2.1. It is the first case, since $gcd(a, b) = 1 \to b_0 = b$ and $n_l < b$ is given as one of the conditions. So, it is the formula below: $\frac{(n_l+2)(n_l+1)}{2} = \binom{n_l+2}{2}$.

Because carries never arise, choices in different digit positions are *independent*. The multiplication principle therefore gives $N_p(n; a, b) = \prod_l \binom{n_l+2}{2}$, which is equation (1). □

Remark 2.3. Both (ii) and (iii) are necessary. Without (iii), two terms might get the same exponent of x, and their coefficients are added together, which might create a carry.

Illustrative examples for Theorem 2.2

Below are three concrete computations.

Example 2.4 ($p = 7,\ a = 1,\ b = 3$)**.** Here $\tau = \lfloor (7-1)/3 \rfloor = 2$. Choose $n = 2$ so the base–7 digit is $2 \leq \tau$. Also $b > \tau$.

Applying formula (1),

$$N_7(2; 1, 3) \ = \ \binom{2+2}{2} \ = \ 6.$$

Indeed, a direct expansion of $(1 + x + x^3)^2$ confirms that exactly 6 coefficients are non-zero mod 7.

Example 2.5 ($p = 7,\ a = 1,\ b = 3$)**.** Now $\tau = \lfloor (7-1)/3 \rfloor = 2$. Take $n = 9 = 1 \cdot 7^1 + 2$, with digits $(n_1, n_0) = (1, 2) \leq \tau < b$. Theorem 2.2 gives

$$N_7(9; 1, 3) \ = \ \binom{1+2}{2} \binom{2+2}{2} \ = \ 3 \ \cdot \ 6 \ = \ 18.$$

Expanding $(1 + x + x^3)^9$ modulo 7 and counting non–zero coefficients yields the same value.

Example 2.6 ($p = 13,\ a = 3,\ b = 5$)**.** Here $\tau = \lfloor (13-1)/5 \rfloor = 2$. Let $n = 27 = 2 \cdot 13^1 + 1$, so $(n_1, n_0) = (2, 1) \leq \tau < b$. Equation (1) gives

$$N_{13}(27; 3, 5) \ = \ \binom{2+2}{2} \binom{1+2}{2} \ = \ 6 \ \cdot \ 3 \ = \ 18.$$

A brute–force computation verifies that exactly 18 coefficients of $(1 + x^3 + x^5)^{27}$ are non–zero modulo 13.

These examples illustrate how Theorem 2.2 provides a *digit-by-digit* solution for counting non–zero coefficients—one can simply check the base–p digits of n are each $\leq \tau$. As long as $gcd(a, b) = 1$ and $\tau < b$, we can just evaluates a product of small binomial numbers.

Corollary 2.7. ***Binary-digit exponents***
Let p be a prime, $0 < a < b < p$ If every digit $n_l \in \{0, 1\}$ (i.e. n is written with binary *digits in base p), then*

$$N_p(n;\ a, b) \ = \ 3^{\,w_p(n)}. \tag{2}$$

Proof. The proof is similar to the proof for Theorem 2.2, except for step (iii). Since each digit of j and k can be either 0 or 1, $aj_i + bk_l$ can take four values: 0, a, b,$a + b$. They are all different. This does not require $gcd(a, b)$ to be 1. Because a single digit contains at most one "1'' and $\binom{1+2}{2} = 3$. Given there are $w_p(n)$ 3s multiplied together, the final result is $3^{\,w_p(n)}$ □

Illustrative examples for Corollary 2.7

Below are three concrete computations.

Example 2.8 ($p = 7,\ a = 2,\ b = 4$)**.** Here $\tau = \lfloor (7-1)/4 \rfloor = 1$. Let $n = 8 = 1 \cdot 7^1 + 1$, so $(n_1, n_0) = (1, 1)$, $w_p(n) = 2$.

Applying formula (2),

$$N_7(8; 2, 4) \ = \ 3^2 \ = \ 9.$$

Indeed, a direct expansion of $(1 + x^2 + x^4)^8$ confirms that exactly 9 coefficients are non-zero mod 7.

3 Upper bound of $N_p(n; a, b)$

Lemma 3.1. *Let*

$$C(t) := \binom{t+2}{2} = \frac{(t+1)(t+2)}{2}.$$

We claim

$$C(t) \le 3^t \qquad (t \ge 0), \tag{3}$$

with equality $\iff t \in \{0, 1\}$.

Proof. Define $f(t) := \frac{C(t)}{3^t}$. Compute the ratio

$$\frac{f(t+1)}{f(t)} = \frac{(t+2)(t+3)}{(t+1)(t+2)} \cdot \frac{1}{3} = \frac{t+3}{3(t+1)} < 1 \quad (t \ge 1).$$

Therefore $f(t)$ is strictly *decreasing* for $t \ge 1$, while $f(0) = 1$ and $f(1) = 1$ directly. Thus, $C(t) < 3^t$ for every $t \ge 2$, establishing (3) and its equality clause.

□

Theorem 3.2. *Let p be a prime and $0 < a < b < p$. Write n in base p,*

$$n = \sum_{l=0}^{s} n_l\, p^l, \qquad 0 \le n_l \le p-1, \qquad w_p(n) := \sum_{l=0}^{s} n_l, \qquad \tau := \left\lfloor \frac{p-1}{b} \right\rfloor$$

If every digit satisfies $n_l \le \tau$, and denote

$$N_p(n; a, b) := \#\Big\{ \textit{coefficients } \not\equiv 0 \pmod p \textit{ in } (1 + x^a + x^b)^n \Big\}.$$

Then

$$N_p(n; a, b) \le \prod_{l=0}^{s} \binom{n_l + 2}{2} \le 3^{\,w_p(n)}, \tag{4}$$

The equality holds in the upper bound $\big(N_p(n; a, b) = 3^{h(n)}\big)$ iff *every digit* $n_l \in \{0, 1\}$.

Proof.

1. Independent digit contribution using Lucas's theorem Similar to the proof for Theorem 2.2, we expand

$$(1 + x^a + x^b)^n = \sum_{i+j+k=n} \binom{n}{i, j, k} x^{a\,j + b\,k},$$

and write the summation indices digit-wise, $i = \sum i_l p^l$, $j = \sum j_l p^l$, $k = \sum k_l p^l$. Lucas's theorem for multinomials states that $\binom{n}{i,j,k} \not\equiv 0 \pmod p$ iff

$$i_l + j_l + k_j = n_l \quad \text{for every } l \quad \big(\text{no digit-carry in } i + j + k\big).$$

Thus each digit $t := n_l$ contributes *independently* of all others if there is no carry.

2. No carry across different digits when $n_l \le \tau$. This is the same as step (ii) in the proof for Theorem 2.2. That is, for a digit position l, $aj_l + bk_l < p$, no carry happens.

3. Counting number of triples in one column Fix a digit value n_l at digit position l, the number of integer solutions to $i_l + j_l + k_l = n_l$, $i_l, j_l, k_l \ge 0$, is the stars-and-bars number

$$\binom{n_l + 2}{2}.$$

Note: some of those triples might get the same $aj_l + bk_l$ value. For example, if $a = 1, b = 2$ $2 \cdot a + 0 \cdot b = 0 \cdot a + 1 \cdot b$. It gets the same value as $a = 0, b = 1$. x gets the same exponent and the two terms merged together, the resulting coefficient might exceed $p - 1$ and be a multiple of p and disappear. Therefore, $\binom{n_l+2}{2}$ is an *absolute upper bound* on how many distinct (non-zero) coefficients a single digit can produce.

Since each digit position is independent (no carry) as proved previous, this proves the first inequality in (4) that:

$$N_p(n; a, b) \ \le \ \prod_{l=0}^{s} \binom{n_l + 2}{2}$$

4. Proof for the upper bound For each digit position l, it follows directly from Lemma 3.1 that

$$\binom{n_l + 2}{2} \le 3^{n_l}$$

Multiplying over all digits positions, we get:

$$N_p(n; a, b) \ \le \ \prod_{l=0}^{s} \binom{n_l + 2}{2} \le \prod_{l=0}^{s} 3^{n_l} = \ 3^{w_p(n)}$$

which is the desired upper bound.

5. When equality holds From Lemma 3.1, the second inequality in (4) holds if and only if $n_l \in 0, 1$. We only need to consider when $n_l = 1$. In that case, (j_l, k_l) can be either $(0, 0), (1, 0)$ or $(0, 1)$. $aj_l + bk_l$ are all different for the three cases: $0, a, b$, and all of them are less than p, so they generate separate power of x for that digit position. That is 3 possibilities for each digit of n that is 1. Each digit position is independent, therefore:

$$N_p(n; a, b) \ = \ 3^{w_p(n)}$$

In other words, when the second inequality in (4) holds, the first inequality also holds.

□

Acknowledgements

The digit-automaton viewpoint and equation are adapted from Amdeberhan & Stanley [1]; Lucas' theorem proof follows Riddle's article [6].

References

[1] T. Amdeberhan and R. P. Stanley. *Polynomial Coefficient Enumeration*. Unpublished manuscript, 59 pp., 2008. Available online at `http://math.mit.edu/~rstan/papers/pcenum.pdf`.

[2] É. Lucas. *Théorie des fonctions numériques simplement périodiques*. *American Journal of Mathematics* **1** (1878), 184–196, 197–240, 289–321. Part III (pp. 289–321).

[3] Jean-Paul Allouche and Jeffrey Shallit. *Automatic Sequences: Theory, Applications, Generalizations*. Cambridge University Press, 2003.

[4] C. Ellison. *The Number of Non-Zero Coefficients of Powers of a Polynomial over a Finite Field*. Undergraduate thesis, Stanford University, 2016.

[5] E. E. Kummer. *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*. *Journal für die reine und angewandte Mathematik* (Crelle's Journal) **44** (1852), 93–146.

[6] L. Riddle. *Proof of Lucas's Theorem*. Available at `https://larryriddle.agnesscott.org/ifs/siertri/LucasProof.htm`, last accessed 2 Aug 2025.