

Exact Primary Kernels for Groups Generated by Linear Polynomials

Alper Ferudun*

24 October 2026

Abstract

Let p be prime, let $S \subset \mathbb{F}_p$ have $d > 0$ elements, and let $h \in \mathbb{F}_p[X]$ be a nonconstant polynomial with no zero in S . Write G_h for the subgroup of $(\mathbb{F}_p[X]/(h))^\times$ generated by the classes of $X - s$, $s \in S$. We determine the order, invariant factors, and relation lattice of the kernel K_h of reduction to $G_{\text{rad}(h)}$. If $h = \prod_i f_i^{e_i}$ with distinct monic irreducible factors, then

$$\log_p |K_h| = \sum_{a \geq 0} \min \left\{ d, \sum_i \deg(f_i) (\lceil e_i/p^a \rceil - 1) \right\}.$$

The nontrivial cyclic factors have at most two adjacent exponents. The proof combines logarithmic differentiation with Frobenius descent, ending in one linear relation space over $\mathbb{F}_p$. It gives uniform divergent-base growth whenever the excess degree $\deg h - \deg \text{rad}(h)$ is a fixed positive fraction of d . The reduced subgroup remains undetermined; in particular, this does not resolve the squarefree or irreducible AKS-related growth problem.

1 Context and notation

For a finite field $\mathbb{F}_q$, groups generated by the residues of $X - s$ modulo a polynomial occur in primality proving and finite-field algorithms. Voloch studies this precise family and proves lower bounds using polynomial counting, rational-function counting, and algebraic curves [2]. Bernstein improves the congruence-counting bounds using the Stothers–Mason theorem [3]. AIM’s 2003 workshop Question 2 asks about uniform divergence of $\log |G_h|/|S|$ in an AKS-related setting [1].

We consider a prime field throughout:

$$p \text{ prime, } S \subset \mathbb{F}_p, \quad d = |S| > 0, \quad h(s) \neq 0 \quad (s \in S).$$

The polynomial h is nonconstant and may be taken monic. Write

$$h = \prod_{i=1}^m f_i^{e_i}, \quad n_i = \deg f_i, \quad h_0 = \text{rad}(h) = \prod_{i=1}^m f_i,$$

where the f_i are distinct monic irreducible polynomials and $e_i \geq 1$. Set $R_h = \mathbb{F}_p[X]/(h)$ and $G_h = \langle X - s : s \in S \rangle$. All generators are units by the hypothesis on $h(s)$.

Reduction induces a surjection $G_h \rightarrow G_{h_0}$. Its kernel K_h is a p -group, while G_{h_0} has order prime to p . The ambient principal-unit order $p^{\deg h - \deg h_0}$ is standard and is recorded in Voloch’s

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>. Unrefereed preprint, version 1.0. Licensed under CC BY 4.0.

discussion of repeated factors [2, p. 236]. It need not equal $|K_h|$. Our result determines the generated kernel exactly, including its integer relation lattice. It makes no assertion that the same generators are independent in different residue-field components.

The literal AIM sentence admits a linear-modulus obstruction if no further degree conditions are imposed: for $h = X - a$ and $S = \mathbb{F}_p \setminus \{a\}$, one has $|G_h| = p - 1$. This elementary observation is not a new claim here, nor does it refute the intended AKS regime. The theorem below isolates the multiplicity-dependent contribution; it supplies no additional bound when h is squarefree.

2 The kernel formula

For $a \geq 0$, define

$$e_i(a) = \left\lceil \frac{e_i}{p^a} \right\rceil, \quad L_a = \sum_i n_i(e_i(a) - 1), \quad \tau = \min\{a \geq 0 : L_a < d\}, \quad \lambda = L_\tau. \quad (1)$$

The sequence eventually vanishes, so τ is defined.

Theorem 1. *Under the preceding hypotheses,*

$$K_h \cong (\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\lambda \times (\mathbb{Z}/p^\tau\mathbb{Z})^{d-\lambda}, \quad (2)$$

with factors of order 1 omitted. In particular,

$$|G_h| = |G_{h_0}| p^{d\tau+\lambda} = |G_{h_0}| p^{\sum_{a \geq 0} \min(d, L_a)}. \quad (3)$$

Thus the isomorphism type of the kernel depends on S only through its cardinality, and on the irreducible factors only through their degrees and multiplicities. The reduced subgroup G_{h_0} need not enjoy either independence property.

3 Principal relations

The proof uses the lattice of relations among principal projections, which differs from the lattice of full relations in G_h .

Lemma 2. *The kernel K_h is the Sylow p -subgroup of G_h . There is a surjection $\rho_h : \mathbb{Z}^S \rightarrow K_h$ sending the standard basis vector at s to the principal projection of $X - s$. For $c = (c_s) \in \mathbb{Z}^S$, set $F_c(X) = \prod_{s \in S} (X - s)^{c_s}$. Its relation lattice $\Lambda_h = \ker \rho_h$ is characterized by*

$$c \in \Lambda_h \iff \frac{F_c(\alpha + t)}{F_c(\alpha)} \equiv 1 \pmod{t^{e_i}} \quad \text{for every root } \alpha \text{ of every } f_i. \quad (4)$$

Proof. Let $J = \ker(R_h \rightarrow R_{h_0})$. The reduced unit group is $\prod_i \mathbb{F}_{p^{n_i}}^\times$, of order prime to p . The group $1 + J$ is a p -group since $(1 + j)^{p^b} = 1 + jp^b = 1$ for large b . Reduction maps G_h onto G_{h_0} , because it sends each generator to the corresponding generator. Hence its kernel is exactly the Sylow p -subgroup.

In a finite abelian group the projection onto a primary component is a power map, by the Chinese remainder theorem on the component exponents. It therefore preserves every subgroup. The principal projections of the generators generate K_h , proving surjectivity of ρ_h .

Choose a finite splitting field k of h_0 . Finite fields are perfect, and injective base change followed by Chinese remaindering gives

$$R_h \otimes_{\mathbb{F}_p} k \cong \prod_i \prod_{f_i(\alpha)=0} k[t]/(t^{e_i}), \quad X \mapsto \alpha + t.$$

The prime-to- p units in each factor are exactly the nonzero constants; the principal units form its Sylow p -subgroup. The normalized series in (4) is precisely the principal projection of F_c . This proves the equivalence. Negative exponents cause no problem because F_c has neither a zero nor a pole at any root of h . $\square$

Put $P(X) = \prod_{s \in S} (X - s)$, and reduce integer coefficients modulo p using a bar. Logarithmic differentiation gives

$$\frac{F'_c}{F_c} = \sum_{s \in S} \frac{\bar{c}_s}{X - s} = \frac{N_c}{P}, \quad N_c = \sum_{s \in S} \bar{c}_s \frac{P}{X - s}. \quad (5)$$

The map $c \bmod p \mapsto N_c$ is an isomorphism $\mathbb{F}_p^S \rightarrow \mathbb{F}_p[X]_{<d}$: evaluating at s gives $N_c(s) = \bar{c}_s P'(s)$, and $P'(s) \neq 0$.

Lemma 3. *If $c \in \Lambda_h$, then*

$$\prod_i f_i^{e_i-1} \mid N_c. \quad (6)$$

Consequently $L_0 \geq d$ implies $\Lambda_h \subset p\mathbb{Z}^S$. If all $e_i \leq p$, condition (6) is also sufficient for $c \in \Lambda_h$.

Proof. Differentiate each congruence in (4). The logarithmic derivative vanishes at every root of f_i to order at least $e_i - 1$. The denominator P is coprime to h , giving (6). If its divisor has degree at least d , then $N_c = 0$, since $\deg N_c < d$. The isomorphism just established forces all c_s to be divisible by p .

For sufficiency, let $U = 1 + \sum_{j \geq 1} u_j t^j$ be one of the normalized series, and suppose $U'/U \in t^{e-1}k[[t]]$ with $e \leq p$. Multiplication by the unit U implies $U' \in t^{e-1}k[[t]]$. Thus $ju_j = 0$ for $1 \leq j < e$. All those integers are nonzero in k , so $U \equiv 1 \pmod{t^e}$. Apply this to every root and use Lemma 2. $\square$

Lemma 4. *Put $h^{[a]} = \prod_i f_i^{e_i(a)}$. For any integer vector b ,*

$$pb \in \Lambda_{h^{[a]}} \iff b \in \Lambda_{h^{[a+1]}}.$$

If $L_a \geq d$, then $\Lambda_{h^{[a]}} = p\Lambda_{h^{[a+1]}}$.

Proof. One has $F_{pb} = F_b^p$. For $U \in 1 + tk[[t]]$, $\text{ord}_t(U^p - 1) = p \text{ord}_t(U - 1)$, including infinite order. Hence the required order $e_i(a)$ for $U^p - 1$ is equivalent to the required order $\lceil e_i(a)/p \rceil = e_i(a+1)$ for $U - 1$. If $L_a \geq d$, Lemma 3 says that every relation vector is divisible by p ; the equivalence then gives the stated lattice equality. $\square$

Proof of Theorem 1. Repeatedly applying Lemma 4 yields

$$\Lambda_h = p^\tau \Lambda_{h^{[\tau]}}. \quad (7)$$

At the final layer, $\lambda = L_\tau < d \leq p$. Since $n_i \geq 1$, each $e_i(\tau) \leq p$. Define $D = \prod_i f_i^{e_i(\tau)-1}$, of degree λ . The sufficient part of Lemma 3 now applies:

$$\Lambda_{h^{[\tau]}} = \{b \in \mathbb{Z}^S : D \mid N_b\}.$$

Under the isomorphism $\mathbb{F}_p^S \cong \mathbb{F}_p[X]_{<d}$, its reduction modulo p is the subspace of multiples of D , of dimension $d - \lambda$. The lattice contains $p\mathbb{Z}^d$ and has index p^λ . Its Smith diagonal therefore consists of $d - \lambda$ entries 1 and λ entries p . Equation (7) multiplies each entry by p^τ . As $K_h \cong \mathbb{Z}^d/\Lambda_h$, formula (2) follows.

Moreover $e_i(\tau) \leq p$ implies $L_{\tau+1} = 0$. All earlier L_a , $a < \tau$, are at least d , so $\sum_a \min(d, L_a) = d\tau + \lambda$. Surjectivity of $G_h \rightarrow G_{h_0}$ proves (3). $\square$

Corollary 5. *A vector $c \in \mathbb{Z}^S$ is a relation among the principal projections if and only if*

$$p^\tau \mid c_s \quad (s \in S), \quad \sum_{s \in S} \left(\frac{c_s}{p^\tau} \bmod p \right) \frac{P(X)}{X - s} \equiv 0 \pmod{D}.$$

The matrix of remainders $P/(X - s) \bmod D$ has rank λ .

Proof. These are precisely the scaled lattice and final divisibility conditions in the proof. The remainder map from polynomials of degree below d onto $\mathbb{F}_p[X]/(D)$ is surjective because $\lambda < d$. $\square$

A full relation in G_h must additionally vanish in G_{h_0} . Neither the theorem nor the corollary assumes that this reduced relation is known.

4 Growth consequences and examples

Corollary 6. *If $L_0 < d$, the group G_h contains the entire ambient principal-unit group $1 + J$. In all cases,*

$$\frac{\log |G_h|}{d} \geq \min \left(1, \frac{\deg h - \deg h_0}{d} \right) \log p.$$

Consequently, if $d \rightarrow \infty$ and $\deg h - \deg h_0 \geq \epsilon d$ for some fixed $\epsilon > 0$, then $\log |G_h|/d \rightarrow \infty$, uniformly over those moduli.

Proof. If $L_0 < d$, Theorem 1 gives $|K_h| = p^{L_0}$. This equals $|1 + J|$, and $K_h \subset 1 + J$, proving equality. The first summand in (3) gives $|G_h| \geq p^{\min(d, L_0)}$. Finally $p \geq d \rightarrow \infty$. $\square$

Combining the theorem with the classical collision-free count gives

$$|G_h| \geq p^{d\tau + \lambda} \binom{d + \deg h_0 - 1}{d}. \quad (8)$$

Indeed, products $\prod_s (X - s)^{a_s}$ with $a_s \geq 0$ and total degree below $\deg h_0$ have distinct residues modulo h_0 ; their count is the binomial coefficient. This familiar argument is credited to AKS in Voloch's section 1 [2].

For $p = 2$, $S = \{0, 1\}$, and $h = (X^2 + X + 1)^5$, one has

$$(L_0, L_1, L_2, L_3) = (8, 4, 2, 0), \quad K_h \cong (\mathbb{Z}/8\mathbb{Z})^2.$$

The reduced group is $\mathbb{F}_4^\times$, so $|G_h| = 3 \cdot 64 = 192$. The ambient principal-unit group has order $2^8 = 256$; it is strictly larger than K_h . For $p = 3$, $S = \{0, 2\}$, and $h = (X - 1)^{10}$, the levels are 9, 3, 1, 0, giving $K_h \cong \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.

Remark 7. The prime-field hypothesis is essential to this formulation. Over $\mathbb{F}_4$, the choices $S = \{1\}$ and $h = X^2$ give a principal kernel of order 2, not 4; one cannot replace p by q in the formula. The proof uses both the $\mathbb{F}_p$ -linear numerator isomorphism and $d \leq p$.

Remark 8. For squarefree h , the theorem gives only $K_h = 1$. If the degree excess is too small, the reduced subgroup may supply the dominant contribution. No general lower bound beyond the credited earlier methods is established for that subgroup here.

5 Computational checks and scope

A companion exact-arithmetic checker enumerates generated subgroups directly in finite quotient rings, independently of the derivative proof. It checks 7,484 admissible instances, including 850 with repeated factors, 5,418 with nonsplit factors, and 1,846 with multiple distinct factors. Across these instances it enumerates 379,582 group elements and verifies 8,359 torsion counts. The tested primes are 2, 3, 5, 7, with additional higher-multiplicity cases; these are finite checks, not a replacement for the proof.

A second checker compares Corollary 5 with direct ring powering in ten configurations, including prime 101. It checks 7,730 exponent vectors and the same number of signed-period translates. Small cases exhaust the principal periods; larger cases use a fixed seed and a specified critical-layer grid. Normal and optimized Python runs produce identical receipts. Both scripts, receipts, and audit notes accompany the source package.

The stated kernel classification is complete. The broader AIM growth question is not settled by it. The use of logarithmic derivatives, Frobenius, and Smith form is standard; the targeted comparison with [2, 3] does not certify absolute novelty or priority. The author used AI assistance for mathematical exploration, proof development, drafting, literature comparison, and computational checks, and remains responsible for the statements and proofs. This preprint is unrefereed; no independent expert review or proof-assistant verification is claimed.

References

- [1] American Institute of Mathematics, *Future directions in algorithmic number theory*, workshop notes, 24–28 March 2003, version 30 April 2003, Question 2, pp. 24–25. <https://aimath.org/WWN/primesinp/primesinp.pdf>.
- [2] J. F. Voloch, On some subgroups of the multiplicative group of finite rings, *J. Theorie Nombres Bordeaux* **16** (2004), 233–239. [doi:10.5802/jtnb.445](https://doi.org/10.5802/jtnb.445).
- [3] D. J. Bernstein, Sharper ABC-based bounds for congruent polynomials, *J. Theorie Nombres Bordeaux* **17** (2005), 721–725. [doi:10.5802/jtnb.515](https://doi.org/10.5802/jtnb.515).