THE EXACT MULTIPLICITY OF THE WILSON SUPERCONGRUENCE IN $\mathbb{F}_Q[T]$

DAVID NIEDBALA GIRAUDIN

Abstract. Let $q = p^s$ with p an odd prime, and let $\wp$ be a monic irreducible polynomial of degree $d \geq 2$ in $\mathbb{F}_q[t]$. The Wilson analogue $F_d \equiv -1 \pmod{\wp}$ holds for the product F_d of all nonzero polynomials of degree less than d, and Thakur proved that $\wp$ is a Wilson prime, i.e. $F_d \equiv -1 \pmod{\wp^2}$, exactly when all exponents of $\wp$ are $\equiv 0$ or $1 \pmod{p}$, in which case the congruence holds modulo $\wp^{p-1}$. He asked whether it can hold modulo a higher power, and what the exact multiplicities are. Let r be the largest integer such that all exponents of $\wp$ are $\equiv 0$ or 1 modulo p^r. We prove that the exact multiplicity $m = v_\wp(F_d + 1)$ is 1 if $r = 0$, $p^r - 1$ if $1 \leq r \leq s$, and $q+1$ if $r > s$. In particular $m \leq q+1$, and the multiplicity of a Wilson prime in the numerator of $\sum_{i<d} 1/(t^{q^i} - t)$ is exactly $m - 1$. Examples over $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_9$ show that all regimes occur. A script checks the theorem on all primes of small degree and on these examples.

hexagon:2611.00076v1

1. Introduction

Let $q = p^s$ with p an odd prime, $A = \mathbb{F}_q[t]$, and $[i] = t^{q^i} - t$. For a monic irreducible $\wp \in A$ of degree d let F_d be the product of all nonzero polynomials of degree less than d. Then $F_d \equiv -1 \pmod{\wp}$, the analogue of Wilson's theorem, and

$$F_d = (-1)^d \frac{D_d}{L_d} = (-1)^d \prod_{i=1}^{d-1} [i]^{\,q^{d-i}-1}, \tag{1}$$

where $D_d = \prod_{i=1}^{d} [i]^{q^{d-i}}$ and $L_d = \prod_{i=1}^{d} [i]$ [Th13, p. 1842]. Following Thakur, $\wp$ is a *Wilson prime* if $F_d \equiv -1 \pmod{\wp^2}$. We write

$$m(\wp) = v_\wp(F_d + 1)$$

for the exact multiplicity of the Wilson congruence. For $d = 1$ one has $F_1 = -1$, so we assume $d \geq 2$ throughout.

Thakur proved that $\wp$ is a Wilson prime if and only if $d^2\wp/dt^2 = 0$, that is, all exponents of $\wp$ are $\equiv 0$ or $1 \pmod{p}$, and that in this case the congruence holds modulo $\wp^{p-1}$ [Th13, Thm. 2.9]; see also the remarks after [Th24, Thm. 5.1]. For the primes $t^p - t - a$ over $\mathbb{F}_p$ the exponent $p - 1$ was already known to be exact [SSTT]; see also [Th13, Rem. 2.12]. Thakur also reported numerical data of G. Todd suggesting that $p - 1$ is exact even when q is not prime, and noted that it was unclear whether the power can be increased [Th13, Rem. 2.11]. In Question (1) of the closing list of questions of [Th24], he asked whether, for $d > 1$ and $p > 2$, the congruence ever (or infinitely often) holds modulo a higher power, and what the exact multiplicities are.

Definition. The *depth* $r(\wp)$ is the largest integer $r \geq 0$ such that every exponent n with a nonzero coefficient in $\wp$ satisfies $n \equiv 0$ or $1 \pmod{p^r}$. Since $d \geq 2$ is an exponent of $\wp$, the depth is finite. Equivalently, $r(\wp) \geq \rho$ if and only if $\wp = U(t^{p^\rho}) + t\,V(t^{p^\rho})$ for some polynomials U, V.

Theorem 1. *Let $\wp$ be monic irreducible of degree $d \geq 2$ in $\mathbb{F}_q[t]$, $q = p^s$, p odd, and $r = r(\wp)$. Then*

$$v_\wp(F_d + 1) = \begin{cases} 1 & \text{if } r = 0, \\ p^r - 1 & \text{if } 1 \leq r \leq s, \\ q + 1 & \text{if } r > s. \end{cases}$$

Date: 3 November 2026.

Thus the only possible exact multiplicities are $1,\ p-1,\ p^2-1,\ \ldots,\ q-1$ and $q+1$, and the Wilson congruence never holds modulo $\wp^{q+2}$. Over $\mathbb{F}_p$ the only possible values are 1, $p-1$ and $p+1$. Since depth r forces $d \geq p^r$, the depth is at most 1 when $d < p^2$, and then the value $p-1$ of [Th13] is exact, in agreement with the data of [Th13, Rem. 2.11]. The case $r=1$ of Lemma 4 below is [Th13, Thm. 2.9(iii)]. We assume p odd, as in the question; for $p=2$ see [Th13, Thm. 2.9(iv)]. The answer to the first part of the question is positive: the examples of Section 4 have multiplicity $q+1$ for $q=3,5,9$, and $p^2-1=8$ for $q=9$. We do not address the infinitude of such primes.

Thakur also proved [Th24, Thm. 7.1] that the primes of degree d dividing the numerator of $H_d = 1/[1] + \cdots + 1/[d-1]$ are exactly the Wilson primes, with multiplicity at least $p-2$. Theorem 1 makes this exact.

Corollary 2. *If $\wp$ is a Wilson prime of degree d and depth r, then $v_\wp(H_d) = p^r - 2$ if $r \leq s$ and $v_\wp(H_d) = q$ if $r > s$. In all cases $v_\wp(H_d) = m(\wp) - 1$.*

Proof. Since $[i]' = -1$ and $q^{d-i} - 1 \equiv -1 \pmod p$, logarithmic differentiation of (1) gives $F_d' = F_d H_d$. As $\wp \nmid F_d$, $v_\wp(H_d) = v_\wp(F_d') = v_\wp\big((F_d+1)'\big)$. Write $F_d + 1 = \wp^m G$ with $\wp \nmid G$; then $(F_d+1)' = \wp^{m-1}(m\wp' G + \wp G')$, and $\wp \nmid \wp'$ because $\wp$ is separable. Since none of the values $p^r - 1$, $q+1$ is divisible by p, the valuation is $m-1$. The primes $\wp$ of degree d do not divide $L_{d-1} = [1]\cdots[d-1]$, so $v_\wp(H_d)$ is also the valuation of the numerator of H_d. □

2. Local expansion at a root

Fix $\wp$ as in Theorem 1 and a root θ of $\wp$, so that $\mathbb{F}_q(\theta) = \mathbb{F}_{q^d}$ and $\theta^{q^d} = \theta$. Put

$$\beta_i = \theta^{q^i} - \theta \qquad (1 \leq i \leq d-1);$$

these are nonzero, and $\beta_1, \ldots, \beta_{d-1}$ together with 0 are the roots of $\wp(X+\theta)$. For a polynomial $G \in \mathbb{F}_q[t]$, the Hasse derivatives $G^{[k]}$ are defined by $G(t+u) = \sum_k G^{[k]}(t) u^k$. Since $\wp$ is separable, $v_\wp(G)$ is the order of vanishing of G at θ, that is

$$v_\wp(G) = \min\{k \geq 0 :\ G^{[k]}(\theta) \neq 0\}. \tag{2}$$

Lemma 3. *With $e_i = q^{d-i} - 1$,*

$$F_d(\theta + u) = (-1)^d \prod_{i=1}^{d-1} \big(\beta_i - u + u^{q^i}\big)^{e_i} \qquad \text{in } \mathbb{F}_{q^d}[u].$$

Proof. In characteristic p, $[i](\theta+u) = \theta^{q^i} + u^{q^i} - \theta - u = \beta_i - u + u^{q^i}$; apply (1). □

Lemma 4. *Let $x_i = \beta_i^{-1}$ and let $h_k = h_k(x_1, \ldots, x_{d-1})$ be the complete homogeneous symmetric polynomials, so $\sum_{k\geq 0} h_k u^k = \prod_i (1 - x_i u)^{-1}$. Then*

$$\sum_{k \geq 0} h_k\, u^k = \frac{\wp'(\theta)}{\sum_{j \geq 1} \wp^{[j]}(\theta)\, u^{j-1}}.$$

Moreover $\wp^{[j]}(\theta) = 0$ for $2 \leq j \leq p^r - 1$, and $\wp^{[p^r]}(\theta) \neq 0$ if $r \geq 1$. Consequently $h_1 = \cdots = h_{p^r-2} = 0$ and $h_{p^r-1} \neq 0$ when $r \geq 1$, and $h_1 \neq 0$ when $r = 0$.

Proof. We have $\wp(u+\theta) = \sum_j \wp^{[j]}(\theta) u^j = u \prod_{i=1}^{d-1}(u - \beta_i)$, so $Q(u) := \sum_{j\geq 1} \wp^{[j]}(\theta) u^{j-1} = \prod_i (u - \beta_i)$ and $Q(0) = \wp'(\theta)$. Hence $\prod_i (1 - x_i u) = Q(u)/Q(0)$, which is the first identity.

Write $\wp = \sum_n c_n t^n$, so that $\wp^{[j]} = \sum_n \binom{n}{j} c_n t^{n-j}$. For $j \geq 1$ this polynomial has degree less than d, so it vanishes at θ if and only if it is zero, that is, if and only if $p \mid \binom{n}{j}$ for every n with $c_n \neq 0$. Let $2 \leq j \leq p^r - 1$ and $c_n \neq 0$. The lowest r base-p digits of n are all 0, or are $1, 0, \ldots, 0$; since $j < p^r$ has $j \geq 2$, some digit of j exceeds the corresponding digit of n, and Lucas' theorem gives $p \mid \binom{n}{j}$. If $r \geq 1$, by maximality of r some exponent n has $n \bmod p^{r+1} \notin \{0, 1\}$; as $n \equiv 0$ or $1 \pmod{p^r}$, its digit n_r is nonzero, and Lucas' theorem gives $\binom{n}{p^r} \equiv n_r \not\equiv 0$. Distinct n give distinct monomials t^{n-p^r}, so $\wp^{[p^r]} \neq 0$. Finally $\wp'(\theta) \neq 0$ by separability, and if $r = 0$ some exponent has $n \not\equiv 0, 1 \pmod p$, so $\binom{n}{2} = n(n-1)/2 \not\equiv 0$ and $\wp^{[2]}(\theta) \neq 0$.

If $r \geq 1$, the denominator in the first identity is $\wp'(\theta)\big(1 + cu^{p^r-1} + O(u^{p^r})\big)$ with $c = \wp^{[p^r]}(\theta)/\wp'(\theta) \neq 0$, so the quotient is $1 - cu^{p^r-1} + O(u^{p^r})$. If $r = 0$, the same computation gives $h_1 = -\wp^{[2]}(\theta)/\wp'(\theta) \neq 0$. □

3. Proof of Theorem 1

Let $f_k = F_d^{[k]}(\theta)$, the coefficient of u^k in $F_d(\theta + u)$. By (2), $m = \min\{k \geq 1 : f_k \neq 0\}$ and $f_0 = F_d(\theta) = -1$.

Step 1: $f_k = -h_k$ for $0 \leq k \leq q-1$. Modulo u^q all terms u^{q^i} in Lemma 3 vanish. Moreover $(\beta_i - u)^{e_i} = (\beta_i - u)^{q^{d-i}}/(\beta_i - u) = (\beta_i^{q^{d-i}} - u^{q^{d-i}})/(\beta_i - u)$, and $q^{d-i} \geq q$. Hence, modulo u^q,

$$F_d(\theta + u) \equiv (-1)^d \prod_{i=1}^{d-1} \frac{\beta_i^{q^{d-i}}}{\beta_i - u} = (-1)^d \prod_{i=1}^{d-1} \beta_i^{e_i} \cdot \prod_{i=1}^{d-1} (1 - x_i u)^{-1} = F_d(\theta) \sum_k h_k u^k = -\sum_k h_k u^k.$$

Step 2: the case $r \leq s$. If $r = 0$, Step 1 and Lemma 4 give $f_1 = -h_1 \neq 0$, so $m = 1$. If $1 \leq r \leq s$, then $p^r - 1 \leq q - 1$, and Step 1 with Lemma 4 gives $f_1 = \cdots = f_{p^r-2} = 0$ and $f_{p^r-1} \neq 0$, so $m = p^r - 1$.

Step 3: the case $r > s$. Then $p^r - 1 \geq pq - 1 \geq q + 2$, so Lemma 4 gives $h_1 = \cdots = h_{q+1} = 0$, and by Step 1 $f_1 = \cdots = f_{q-1} = 0$. We compute modulo u^{q+2}. For $i \geq 2$ the term u^{q^i} vanishes, since $q^2 \geq q + 2$. As in Step 1, $\big(\beta_i - u + \delta_{i,1}u^q\big)^{e_i} = N_i/D_i$ with $D_i = \beta_i - u + \delta_{i,1}u^q$ and $N_i = D_i^{q^{d-i}}$. Modulo u^{q+2}, $N_i = \beta_i^{q^{d-i}}$ for $i \leq d-2$, since $q^{d-i} \geq q^2$, while $N_{d-1} = \beta_{d-1}^q - u^q$; here $d \geq p^r \geq pq \geq 9$, so the factors $i = 1$ and $i = d-1$ are distinct. Hence, with $y = \beta_{d-1}^{-q}$,

$$F_d(\theta + u) \equiv -(1 - yu^q)\, \frac{1}{1 - x_1 u + x_1 u^q} \prod_{i=2}^{d-1} \frac{1}{1 - x_i u}.$$

Now $(1 - x_1 u + x_1 u^q)^{-1} = (1 - x_1 u)^{-1} - x_1 u^q (1 - x_1 u)^{-2} + O(u^{2q})$, so

$$\begin{aligned} F_d(\theta + u) &\equiv -(1 - yu^q)\Big(\sum_k h_k u^k - x_1 u^q (1 - x_1 u)^{-1} \sum_k h_k u^k\Big) \\ &\equiv -(1 - yu^q)\Big(\sum_k h_k u^k - x_1 u^q \big(1 + (x_1 + h_1)u\big)\Big). \end{aligned}$$

Reading off coefficients,

$$f_q = -(h_q - x_1 - y), \qquad f_{q+1} = -\big(h_{q+1} - (x_1 + y)h_1 - x_1^2\big).$$

Since $\theta^{q^d} = \theta$, we have $\beta_{d-1}^q = \theta^{q^d} - \theta^q = -\beta_1$, so $y = -x_1$. With $h_q = h_{q+1} = h_1 = 0$ we get $f_q = 0$ and $f_{q+1} = x_1^2 = \beta_1^{-2} \neq 0$. Hence $m = q + 1$. □

Remark 5. In Step 3 the vanishing of f_q depends on the identity $\beta_{d-1}^q = -\beta_1$, which links the factors $i = 1$ and $i = d-1$ of Lemma 3: the term $-x_1$ coming from $i = 1$ cancels the term $-y$ coming from $i = d-1$.

4. Examples and verification

We write $\mathbb{F}_9 = \mathbb{F}_3[a]/(a^2 - a - 1)$. The following polynomials are irreducible, with the stated depth and multiplicity:

q	$\wp$	r	regime	m
3	$t^3 - t - 1$	1	$r \leq s$	2
3	$t^{18} - t^{10} + 1$	2	$r > s$	4
5	$t^5 - t - 1$	1	$r \leq s$	4
5	$t^{51} - 2t^{50} - t^{26} + 1$	2	$r > s$	6
9	$t^3 - (a+1)t - (a+1)$	1	$r \leq s$	2
9	$t^{10} + (a+1)t^9 + t + 1$	2	$r = s$	8
9	$t^{54} - a\,t^{28} + a\,t^{27} + a\,t + 1$	3	$r > s$	10

The ancillary file `verify_wilson_multiplicity.py` (Python 3, no dependency, exact arithmetic in $\mathbb{F}_q[t]$, about fifteen seconds) checks:

- the product formula (1) against the definition of F_d over $\mathbb{F}_3$ for $d = 2, 3$;
- for every monic irreducible $\wp$ of degree $2 \leq d \leq 7$ over $\mathbb{F}_3$, $2 \leq d \leq 4$ over $\mathbb{F}_5$ and $2 \leq d \leq 3$ over $\mathbb{F}_9$ (981 primes in all): the valuation $v_\wp(F_d + 1)$, computed in $\mathbb{F}_q[t]$ modulo a power of $\wp$ from (1), equals the value of Theorem 1, and $v_\wp(H_d)$ equals $m - 1$ (Corollary 2);
- for the examples above: irreducibility (Rabin's test), the depth, and the same two valuations computed directly in $\mathbb{F}_q[t]$ for the five examples of degree at most 18;
- for all the examples, the coefficients f_k of $F_d(\theta + u)$ computed in the residue field $\mathbb{F}_q[t]/\wp$ from Lemma 3: the first nonzero one is f_m; $f_k = -h_k$ for $k < q$, with h_k computed from the first identity of Lemma 4; the vanishing of $\wp^{[j]}(\theta)$ for $2 \leq j \leq \min(p^r - 1, q + 3)$, and $\wp^{[p^r]} \neq 0$; $\beta_{d-1}^q = -\beta_1$; and, when $r > s$, $f_q = 0$ and $f_{q+1} = \beta_1^{-2}$.

In small degree only the depths 0 and 1 occur, and the multiplicity $p - 1$ of [Th13] is then exact. These computations check the statements; the proofs do not depend on them.

Acknowledgement. Technical assistance: Claude (Anthropic).

References

[SSTT] J. Sauerberg, L. Shu, D. S. Thakur and G. Todd, Infinitude of Wilson primes for $\mathbb{F}_q[t]$, *Acta Arith.* **157** (2013), 91–100.

[Th13] D. S. Thakur, Differential characterization of Wilson primes for $\mathbb{F}_q[t]$, *Algebra Number Theory* **7** (2013), 1841–1848.

[Th24] D. S. Thakur, Fermat–Wilson supercongruences, arithmetic derivatives and strange factorizations, *J. Théor. Nombres Bordeaux* **36** (2024), no. 2, 481–491, doi:10.5802/jtnb.1285; arXiv:2211.01076.

ORCID 0009-0009-1526-1178