hexagon:2611.01007v2

WILSON PRIMES FOR AN ELLIPTIC COORDINATE RING OF CLASS NUMBER ONE

DAVID NIEDBALA GIRAUDIN

Abstract. Thakur characterised the Wilson primes of $\mathbb{F}_q[t]$ (q odd) as the primes with vanishing second derivative, and asked for generalisations to other function fields, for instance of class number one. Let $A = \mathbb{F}_3[x,y]/(y^2 - x^3 + x + 1)$, the coordinate ring of an elliptic curve with a single rational point; it is a principal ideal domain. We define a Wilson product $W_d \in A$ which is the analogue of Thakur's F_d and satisfies $W_d \equiv -1 \pmod{\pi}$ for every prime π of degree d. We prove that π is a Wilson prime, i.e. $W_d \equiv -1 \pmod{\pi^2}$, if and only if $D^2\pi = 0$ and the coefficient of the monomial of degree $d-1$ in π vanishes, where D is the invariant derivation. The second condition has no counterpart in genus 0; it is automatic for $d \equiv 2 \pmod 3$ and for $d = 3$, and is a genuinely additional condition in degrees 6 and 9. There is no Wilson prime of degree $d \equiv 1 \pmod 3$, and $y^{4\cdot 25^k} + y^{25^k} - 1$ ($k \geq 0$) is an infinite family of Wilson primes. The criterion is confirmed by exact computation on all 25 430 primes of degree at most 11.

1. Statement

Let $k = \mathbb{F}_3$, $f = x^3 - x - 1$, and $A = k[x,y]/(y^2 - f)$, the affine coordinate ring of the elliptic curve $E\colon y^2 = x^3 - x - 1$ with its point ∞ removed. Since f takes the value -1 on $\mathbb{F}_3$, we have $E(\mathbb{F}_3) = \{\infty\}$, hence the class number of A is $\#E(\mathbb{F}_3) = 1$: A is a principal ideal domain with $A^\times = k^\times$. Put $\deg = -\operatorname{ord}_\infty$, so $\deg x = 2$, $\deg y = 3$, and for a prime π, $\deg \pi = \dim_k A/\pi$. The monomials $m_{2i} = x^i$, $m_{2i+3} = x^i y$ ($i \geq 0$) form a k-basis of A, with exactly one monomial m_j of each degree $j \geq 0$, $j \neq 1$. For $a \in A$ we write $a = \sum_j a_j m_j$, with the convention $a_1 = 0$.

Definition 1. For $d \geq 2$ let V_d be the k-span of the m_j with $0 \leq j \leq d+1$, $j \neq d$, and

$$W_d = \prod_{v \in V_d \setminus \{0\}} v \ \in A.$$

Lemma 2. *For every prime π of degree $d \geq 2$, reduction $V_d \to A/\pi$ is bijective, and $W_d \equiv -1 \pmod{\pi}$.*

Proof. $\dim_k V_d = d$. A non-zero multiple $g\pi$ has degree $d + \deg g \in \{d\} \cup [d+2, \infty)$, and if it has degree d it is $c\pi$, $c \in k^\times$, whose coefficient on m_d is non-zero. So $V_d \cap \pi A = 0$. The product of the non-zero elements of a finite field is -1. □

In $\mathbb{F}_q[t]$ the analogous recipe (all monomials of degree $< d$) gives Thakur's F_d, the product of all non-zero polynomials of degree less than d [3, 4]; infinitely many Wilson primes in $\mathbb{F}_q[t]$ were exhibited for many q in [2] and for every q in [3]. The space V_d is stable under the automorphisms $(x,y) \mapsto (x+a, \pm y)$, $a \in \mathbb{F}_3$, of A.

Definition 3. A prime π of degree $d \geq 2$ is a *Wilson prime* if $W_d \equiv -1 \pmod{\pi^2}$.

Date: 24 November 2026.

Let D be the k-derivation of A with $Dx = -y$, $Dy = -1$ (it respects $y^2 = f$ because $D(y^2) = -2y = y$ and $D(f) = -Dx = y$). Since $2y\,dy = f'(x)\,dx = -dx$, we have $dx = y\,dy$, so $\Omega_{A/k} = A\,dy$ and $D = -d/dy$. For π of degree d put

$$c(\pi) = \pi_{d-1}/\pi_d.$$

Theorem 4. *Let π be a prime of A of degree $d \geq 2$.*

1. *π is a Wilson prime if and only if π divides $D^2\pi + c(\pi)\,D\pi$.*
2. *π is a Wilson prime if and only if $D^2\pi = 0$ and $c(\pi) = 0$.*
3. *There is no Wilson prime of degree $d \equiv 1 \pmod 3$. If $d \equiv 2 \pmod 3$, then $D^2\pi = 0$ implies $c(\pi) = 0$.*

In degree 3 every prime is $\pm(y + \alpha x + \beta)$ and $D^2\pi = \alpha\pi_3 = \pi_2$, so $D^2\pi = 0$ again implies $c(\pi) = 0$. In degrees 6 and 9 the condition $c(\pi) = 0$ is not a consequence of $D^2\pi = 0$: in degree 6 there are 12 primes with $D^2\pi = 0$, of which 6 are Wilson primes; in degree 9, 56 and 14. We do not know what happens for general $d \equiv 0 \pmod 3$.

Theorem 5. *Let $P \in \mathbb{F}_3[y]$ be monic irreducible with $P'' = 0$ and $\deg P \equiv 1 \pmod 3$. Then $P(y)$ is a Wilson prime of A of degree $3 \deg P$. In particular $y^{4\cdot 25^k} + y^{25^k} - 1$ is a Wilson prime of degree $12 \cdot 25^k$ for every $k \geq 0$.*

2. Preliminaries

Expansions at infinity. Let $u = x/y$, a uniformiser at ∞. From $y^2 = f(x)$ one gets $x = u^{-2}(1 + O(u^4))$ and $y = u^{-3}(1 + O(u^4))$, hence $m_j = u^{-j}(1 + O(u^4))$ for all j. Consequently, for $a \in A$ of degree n,

$$a = \sum_{j=n-3}^{n} a_j u^{-j} + O(u^{-n+4}). \tag{1}$$

Moreover $dy = (1 + O(u^2))\,du$ (the term $-3u^{-4}$ vanishes), so dy has neither zero nor pole on E, and

$$D(u^{-j}) = j\,u^{-j-1}(1 + O(u^2)). \tag{2}$$

The derivation. D^3 is a derivation (characteristic 3) killing x and y, so $D^3 = 0$. If $Da = 0$ then $da = 0$, so a is a cube in the fraction field, hence in A (A is normal): $\ker D = A^3$. If π is prime, its zeros on $E(\bar{k})$ are simple and dy does not vanish there, so $D\pi$ is a unit modulo π.

3. Reduction to a linear coefficient

Fix a prime π of degree $d \geq 2$, $\kappa = A/\pi$, and let $\rho\colon V_d \to \kappa$ be the bijection of Lemma 2. Define the k-linear map $\partial\colon \kappa \to \kappa$ by $\partial(\rho(v)) = D(v) \bmod \pi$. Every k-linear endomorphism of κ is uniquely $z \mapsto \sum_{j=0}^{d-1} \lambda_j z^{3^j}$, $\lambda_j \in \kappa$; let $\lambda_0 = \lambda_0(\pi)$ be the coefficient of z for ∂.

Proposition 6. *$W_d \equiv -1 + \pi\,\lambda_0/D\pi \pmod{\pi^2}$. In particular π is Wilson if and only if $\lambda_0 = 0$.*

Proof. The completion of A at π is $\kappa[[\pi]]$, with κ embedded by Teichmüller representatives. For $a \in A$ write $a \equiv \bar{a} + \delta(a)\pi \pmod{\pi^2}$ with $\bar{a}, \delta(a) \in \kappa$. Then δ is a k-derivation $A \to \kappa$ with $\delta(\pi) = 1$; as $\Omega_{A/k} = A\,dy$, $\delta = \overline{D(\cdot)}/\overline{D\pi}$. Let $e(z) = \prod_{v \in V_d}(z - v) \in A[z]$. It is an additive polynomial, monic of degree 3^d, and its coefficient of z is $\prod_{v \neq 0}(-v) = W_d$. Modulo π it is $z^{3^d} - z$, so $e(z) \equiv z^{3^d} - z + \pi g(z) \pmod{\pi^2}$ with $g \in \kappa[z]$ additive of degree $< 3^d$. For $v \in V_d$, $v^{3^d} \equiv \bar{v}^{3^d} = \bar{v} \pmod{\pi^2}$, so $0 = e(v) \equiv \bar{v} - v + \pi g(\bar{v})$, i.e. $g(\bar{v}) = \delta(v)$. Hence

$g(z) = \partial(z)/\overline{D\pi}$ for all $z \in \kappa$, and both sides being additive polynomials of degree $< 3^d$, they coincide. Comparing coefficients of z gives the claim. □

Lemma 7. *For $a \in \kappa$ let M_a be multiplication by a. Then $\operatorname{tr}_k(M_a \circ \partial) = \operatorname{Tr}_{\kappa/k}(a\lambda_0)$. Hence $\lambda_0 = 0$ if and only if $\operatorname{tr}_k(M_a \circ \partial) = 0$ for all $a \in \kappa$.*

Proof. Let φ be the Frobenius of κ/k. It suffices to show $\operatorname{tr}_k(M_b\varphi^j) = 0$ for $0 < j < d$. This trace is k-linear in b, so equals $\operatorname{Tr}_{\kappa/k}(c_j b)$ for some c_j. Conjugating by M_ζ, $\zeta \in \kappa^\times$, gives $\operatorname{Tr}(c_j b) = \operatorname{Tr}(c_j b \zeta^{3^j-1})$ for all b, so $c_j(1 - \zeta^{3^j-1}) = 0$; taking ζ a generator of $\kappa^\times$ gives $c_j = 0$. □

4. The residue pairing and the kernel

For $b, c \in A$ put $\langle b, c\rangle = -\operatorname{Res}_\infty\big(bc\,dy/\pi\big)$.

Lemma 8. *$\langle b, c\rangle = \operatorname{Tr}_{\kappa/k}\big(b\bar{c}/\bar{\pi}_y\big)$ with $\pi_y = -D\pi$. So $\langle\ ,\ \rangle$ induces a non-degenerate symmetric k-bilinear form on κ, and $\langle ab, c\rangle = \langle a, bc\rangle$.*

Proof. The differential $bc\,dy/\pi$ has poles only at ∞ and at the zeros of π, which are simple and form one Galois orbit. As $d\pi = \pi_y\,dy$, its residue at a zero Q is $(bc/\pi_y)(Q)$. Apply the residue theorem. □

Write $a_1 = a \otimes 1$, $a_2 = 1 \otimes a$ in $A \otimes_k A$, the coordinate ring of $(E \setminus \infty)^2$.

Lemma 9. *Let $C = (y_1 + y_2)/(x_1 - x_2)$. Then*

$$C = \frac{1}{y_2 - y_1} - \frac{(x_2 - x_1)^2}{y_2 - y_1}, \tag{3}$$

and $R_0 := (\pi_2 - \pi_1)\,C$ belongs to $A \otimes_k A$.

Proof. $(y_1 + y_2)(y_2 - y_1) - (x_1 - x_2) = f(x_2) - f(x_1) + (x_2 - x_1) = x_2^3 - x_1^3 = (x_2 - x_1)^3$; divide by $(x_1 - x_2)(y_2 - y_1)$. The function $x_1 - x_2$ vanishes simply on the diagonal Δ and on the graph Δ^- of $[-1]$, and $y_1 + y_2$ vanishes on Δ^-; so on the smooth affine surface the only possible pole of C is a simple pole along Δ, where $\pi_2 - \pi_1$ vanishes. (The surface is smooth, hence normal, so a function without polar divisor is regular; the points of $\Delta \cap \Delta^-$ have codimension 2. The denominator $y_2 - y_1$ in (3) creates no further pole: away from Δ it vanishes only where $x_2 - x_1 = \pm 1$, and there $1 - (x_2 - x_1)^2 = 0$.) □

Lemma 10. *Write $R_0 = \sum_i r_i \otimes s_i$. For every $b \in A$, $\sum_i \langle b, s_i\rangle\, r_i \equiv b \pmod{\pi}$.*

Proof. As π is separable it suffices to evaluate at a zero $P \in E(\bar{k})$ of π, the pairing being extended $\bar{k}$-linearly in the second variable. There $R_0(P, \cdot) = \pi \cdot C(P, \cdot)$, so the left side is $-\operatorname{Res}_{Q=\infty}\big(b(Q)C(P,Q)\,dy_Q\big)$. The differential $b\,C(P,\cdot)\,dy$ has poles only at P and ∞: at $Q = -P \neq P$ the numerator of C vanishes, and if $P = -P$ then $x - x_P$ has a double zero and y a simple zero at P. By (3), and because $y - y(P)$ is a uniformiser at P, its residue at P is $b(P)$. Conclude by the residue theorem. □

Proposition 11. *Let $(m_j)_{j\in J}$ be the monomial basis of V_d. Then $R := R_0 + c(\pi)\,\pi_1$ lies in $V_d \otimes_k A$; writing $R = \sum_{j\in J} m_j \otimes t_j$, we have $\langle m_i, t_j\rangle = \delta_{ij}$, and*

$$\Theta := \sum_{j\in J} D(m_j)\,t_j \;=\; D^2\pi + c(\pi)\,D\pi \quad \text{in } A.$$

Proof. Expand in the first variable at ∞, with $u = u_1$ and coefficients in A (second variable). We have $C = u^{-1}(1 + y_2/y_1)(1 - x_2/x_1)^{-1} = u^{-1}(1 + O(u^2))$, hence, by (1) and $d \geq 2$,

$$R_0 = -\pi_d\, u^{-d-1} - \pi_{d-1} u^{-d} + O(u^{-d+1}).$$

So $R_0 \in L_{d+1} \otimes A$, where L_n is the span of the m_j, $j \leq n$, and its coefficient on m_d is $-\pi_{d-1} \otimes 1$; adding $c(\pi)\pi_1$ removes it, so $R \in V_d \otimes A$. Since $R - R_0 = c(\pi)\,\pi \otimes 1$ contributes a multiple of π, Lemma 10 gives $\sum_j \langle m_i, t_j\rangle m_j \equiv m_i \pmod{\pi}$, and $V_d \cap \pi A = 0$ gives $\langle m_i, t_j\rangle = \delta_{ij}$.

Let $\mu\colon A \otimes A \to A$ be the multiplication (restriction to Δ) and $D_1 = D \otimes 1$. Then $\Theta = \mu(D_1 R) = \mu(D_1 R_0) + c(\pi) D\pi$. By (3), $R_0 = \Phi \cdot (1 - (x_2 - x_1)^2)$ with $\Phi = (\pi_2 - \pi_1)/(y_2 - y_1)$, regular near Δ; the second factor is 1 on Δ and its D_1-derivative vanishes on Δ, so $\mu(D_1 R_0) = \mu(D_1 \Phi)$. Applying D_1 twice to $\Phi\,(y_2 - y_1) = \pi_2 - \pi_1$, with $D_1(y_2 - y_1) = 1$, gives

$$D_1^2 \Phi \cdot (y_2 - y_1) + 2 D_1 \Phi = -(D^2\pi)_1,$$

so on Δ: $2\mu(D_1\Phi) = -D^2\pi$, i.e. $\mu(D_1\Phi) = D^2\pi$ in characteristic 3. □

5. Proof of Theorem 4

Part (1). The trace of an endomorphism T of κ is $\sum_j \langle T\bar{m}_j, \bar{t}_j\rangle$, by Proposition 11. With $T = M_a \circ \partial$ and Lemma 8,

$$\operatorname{tr}_k(M_a \circ \partial) = \sum_j \langle a\, D(m_j), t_j\rangle = \langle a, \Theta\rangle.$$

By Proposition 6 and Lemma 7, π is Wilson iff $\langle a, \Theta\rangle = 0$ for all a, iff $\Theta \equiv 0 \pmod{\pi}$ (non-degeneracy), iff $\pi \mid D^2\pi + c(\pi) D\pi$, since $\Theta = D^2\pi + c(\pi) D\pi$.

Parts (2) and (3). Normalise $\pi_d = 1$, $c = c(\pi)$, and let $\Theta' = D^2\pi + cD\pi$. By (1) and (2),

$$D\pi = d\, u^{-d-1} + (d-1)c\, u^{-d} + \cdots, \qquad D^2\pi = d(d+1)u^{-d-2} + d(d-1)c\, u^{-d-1} + \cdots,$$

$$\Theta' = d(d+1)\, u^{-d-2} + d^2 c\, u^{-d-1} + O(u^{-d}).$$

Assume $\pi \mid \Theta'$. As $\deg \Theta' \leq d + 2$, $\Theta' = (a + bx)\pi$ with $a, b \in \mathbb{F}_3$, and $(a + bx)\pi = b\, u^{-d-2} + bc\, u^{-d-1} + O(u^{-d})$. Comparing: $b = d(d+1)$ and $d^2 c = d(d+1)c$, i.e. $dc = 0$.

Case $d \equiv 1 \pmod 3$. Then $c = 0$, $b = -1$, and $D^2\pi = (a - x)\pi$. Applying D^2 and using $D^3 = 0$, $D(a - x) = y$, $D^2(a - x) = -1$:

$$0 = (a - x)D^2\pi + 2y\, D\pi - \pi \equiv 2y\, D\pi \pmod{\pi},$$

because $(a - x)D^2\pi = (a - x)^2\pi$. As $D\pi$ is a unit modulo π, $\pi \mid y$, so $d \leq 3$, contradicting $d \geq 4$. So there is no Wilson prime of degree $\equiv 1 \pmod 3$.

Case $d \equiv 0, 2 \pmod 3$. Then $b = 0$ and $\Theta' = a\pi$. Applying D^2: $0 = D^4\pi + cD^3\pi = a\, D^2\pi$. If $a \neq 0$ then $D^2\pi = 0$, so $cD\pi = a\pi$, which forces $c = 0$ ($D\pi$ is a unit modulo π) and then $a\pi = 0$, absurd. So $a = 0$ and $D^2\pi = -cD\pi$. Applying D: $0 = D^3\pi = -cD^2\pi$. If $c \neq 0$ then $D^2\pi = 0$, hence $D\pi = 0$ and $\pi \in A^3$, which is impossible for a prime. So $c = 0$ and $D^2\pi = 0$. The converse is clear.

Finally, if $D^2\pi = 0$ the coefficient $d(d-1)c$ vanishes, which gives $c = 0$ when $d \equiv 2 \pmod 3$. □

Remark 12. Carrying out the same argument in $\mathbb{F}_q[t]$, q odd, with $C = 1/(t_2 - t_1)$ and V the polynomials of degree $< d$, one finds $\Theta \equiv \pm\frac{1}{2}\wp''$, which recovers Thakur's criterion $\wp'' = 0$ [3]. The term $c(\pi)D\pi$ comes from the simple pole of C at infinity, which is absent in genus 0.

6. Proof of Theorem 5

Let $n = \deg P \equiv 1 \pmod 3$, θ a root of P, $\kappa_0 = \mathbb{F}_3(\theta)$. Since $A = \mathbb{F}_3[y][x]/(x^3 - x - (y^2+1))$, the element $P(y)$ is prime in A iff $x^3 - x - (\theta^2+1)$ is irreducible over κ_0, iff $\mathrm{Tr}_{\kappa_0/\mathbb{F}_3}(\theta^2+1) \neq 0$ (Artin–Schreier). The coefficient of y^{n-4} in P'' is $(n-2)(n-3)$ times the coefficient e_2 of y^{n-2} in P, and $(n-2)(n-3) \neq 0$ in $\mathbb{F}_3$ because $n \equiv 1 \pmod 3$; as $P'' = 0$, $e_2 = 0$ (for $n = 1$ there is nothing to prove), so by Newton's identity $\mathrm{Tr}(\theta^2) = e_1^2$ with $-e_1$ the coefficient of y^{n-1}, and $\mathrm{Tr}(\theta^2+1) = e_1^2 + n = e_1^2 + 1 \neq 0$ in $\mathbb{F}_3$. So $\pi = P(y)$ is a prime of degree $d = 3n$. It satisfies $D^2\pi = P''(y) = 0$, and $\pi = u^{-3n}(1 + O(u^3))$ because $y^j = u^{-3j}(1 + O(u^4))$, so $c(\pi) = 0$ by (1). Theorem 4 applies.

Let $P_0 = y^4 + y - 1$. It is irreducible over $\mathbb{F}_3$ and its roots have multiplicative order 80. By [1, Theorem 3.35], $P_0(y^s)$ is irreducible for $s = 25^k$, $k \geq 1$ (the only prime factor of s divides 80, $(3^4 - 1)/80 = 1$, and $4 \nmid s$). Its degree is $4 \cdot 25^k \equiv 1 \pmod 3$, and $P_0(y^s)'' = 0$ because $4s \equiv s \equiv 1 \pmod 3$. □

7. Numerical verification

The following was computed in exact arithmetic over $\mathbb{F}_3$; the counts of primes agree with the zeta function of E.

d	2	3	4	5	6	7	8	9	10	11
primes	3	9	21	54	125	324	819	2184	5853	16038
Wilson primes	0	3	0	6	6	0	45	14	0	198

For every one of these 25 430 primes, the Wilson property was decided from the definition, by computing W_d exactly in A and testing divisibility of $W_d + 1$ by π^2, and compared with the criterion of Theorem 4(2): no discrepancy. For $d \leq 7$ the Wilson property was computed a second time by a different route (W_d modulo π^2 after Hensel lifting), with the same result. The identity of Proposition 11 was checked directly, modulo π, on the 518 primes $a(x) + b(x)y$, $b \neq 0$, of degree 4 to 7 (this check is not part of the ancillary script), and $y^4 + y - 1$ was confirmed to be a Wilson prime of degree 12 from the definition. The ancillary script `verify_wilson_elliptic.py` reproduces the table up to degree 9 and the checks of Theorem 5. The Wilson primes of degree 3 are $y,\ y+1,\ y-1$.

8. Status and questions

Theorems 4 and 5 are proved above. Nothing in this note has been checked by a third party. Open: the other coordinate rings of class number one, in particular in characteristic 2; the exact power of π dividing $W_d + 1$ for Wilson primes; and whether Wilson primes exist in every degree $d \equiv 0, 2 \pmod 3$, $d \geq 3$.

Acknowledgement. This work was carried out with the AI system Claude (Anthropic), which performed the computations and the drafting under the author's direction.

References

[1] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, 1997.

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

[3] D. S. Thakur, Differential characterization of Wilson primes for $\mathbb{F}_q[t]$, Algebra Number Theory **7** (2013), no. 8, 1841–1848.

[4] D. S. Thakur, Fermat–Wilson supercongruences, arithmetic derivatives and strange factorizations, J. Théor. Nombres Bordeaux **36** (2024), no. 2, 481–491.

Independent researcher, France. ORCID 0009-0009-1526-1178