hexagon:2611.01011v1

# WILSON PRIMES FOR COORDINATE RINGS OF HYPERELLIPTIC CURVES WITH ONE POINT AT INFINITY

DAVID NIEDBALA GIRAUDIN

Abstract. Let $A = \mathbb{F}_q[x,y]/(y^2 + h(x)y - f(x))$ be the coordinate ring of a smooth affine curve of genus $g \geq 1$ with one point at infinity ($\deg f = 2g+1$, $\deg h \leq g$), in any characteristic; $A$ need not be principal. With the Wilson product $W_d$ of [2, 3], a prime element $\pi$ of degree $d$ is called a Wilson prime if $W_d \equiv -1 \pmod{\pi^2}$. We prove that $W_d \equiv -1 + \pi\,(E(\pi) + K_\pi D\pi)/(D\pi)^2 \pmod{\pi^2}$, so that $\pi$ is a Wilson prime if and only if $\pi$ divides $E(\pi) + K_\pi D\pi$, where $D$ is the invariant derivation, $E = (h^2+4f)\,\partial_x^{(2)} + (f' + h'(y+h))\,\partial_x$ is a second order operator written with Hasse derivatives, the same in every characteristic, and $K_\pi \in A$ is defined by a canonical decomposition; for $d \geq 2g$ it is a polynomial in $x$ of degree less than $g$, given by an explicit recipe in terms of the leading coefficients of $\pi$. This contains the divisibility criteria of [2, 3] for the four rings of class number one, and Thakur's criterion for $\mathbb{F}_q[t]$ has the same shape. The statement is confirmed by exact computation on 17 curves of genus $1, 2, 3$ in characteristics $2, 3, 5, 7$.

## 1. Setting and statements

Let $k = \mathbb{F}_q$ of characteristic $p$, and $h, f \in k[x]$ with $f$ monic of odd degree $\gamma = 2g+1 \geq 3$ and $\deg h \leq g$. We assume that the affine curve $C\colon F(x,y) := y^2 + h(x)y - f(x) = 0$ is smooth over $\bar{k}$. Let $A = k[x,y]/(F)$ and $K$ its fraction field. This is the imaginary model of a hyperelliptic curve of genus $g$ [1, Chapter 14]: $C$ has a unique point $\infty$ at infinity, it is $k$-rational, $A$ is the ring of functions regular outside $\infty$, a Dedekind domain with $A^\times = k^\times$, and $\deg := -\operatorname{ord}_\infty$ satisfies $\deg x = 2$, $\deg y = \gamma$ (the condition $\deg h \leq g$ is what makes $y^2$ dominate $hy$ at infinity). Let $S = \{0, 2, 4, \dots\} \cup \{\gamma, \gamma+2, \dots\}$; for $j \in S$ put $m_j = x^{j/2}$ ($j$ even), $m_j = x^{(j-\gamma)/2} y$ ($j$ odd). The $m_j$ form a $k$-basis of $A$, $\deg m_j = j$; we write $a = \sum_j a_j m_j$, and $a_j = 0$ for $j \notin S$. A *prime element* is a $\pi \in A$ such that $A/\pi$ is a field; its *degree* is $d = \dim_k A/\pi = \deg \pi \in S$. We do not assume that $A$ is principal.

**Definition 1.** For $d \in S$, $d \geq 2$, $V_d$ is the $k$-span of the $m_j$ with $j \in S$, $j - d \notin S$, and $W_d = \prod_{v \in V_d \setminus \{0\}} v$. A prime element $\pi$ of degree $d$ is a *Wilson prime* if $W_d \equiv -1 \pmod{\pi^2}$.

**Lemma 2.** *$A = V_d \oplus \pi A$ for every prime element $\pi$ of degree $d$. Hence $V_d \to A/\pi$ is bijective and $W_d \equiv -1 \pmod{\pi}$.*

*Proof.* The degree of a non-zero element of $V_d$ lies in $S \setminus (d+S)$, which has $d$ elements, and the degree of a non-zero multiple of $\pi$ lies in $d+S$. So $V_d \cap \pi A = 0$ and $\dim V_d = d = \dim A/\pi$. □

The space $V_d$, hence $W_d$ and the notion of Wilson prime, depend on the model, i.e. on $x, y$. For the four rings of class number one this is the definition of [2, 3]; in $\mathbb{F}_q[t]$ the analogous product is Thakur's $F_d$ [5, 6], and the generalisation to other function fields is asked for in [6, §7.5, Question (2)].

*Date*: 24 November 2026.

**The operators $D$ and $E$.** Put $w = 2y + h = \partial F/\partial y$. As $C$ is smooth, $w$ and $f' - h'y = -\partial F/\partial x$ have no common zero, and $w \neq 0$ in $A$ (if $p = 2$ and $h = 0$, then $f'$ has a root $x_0$ and the point with $x = x_0$ is singular). So $\Omega_{A/k}$ is free on $\omega = dx/w = dy/(f' - h'y)$, which has neither zero nor pole on $C$, and there is a unique $k$-derivation $D$ of $A$ with $da = D(a)\,\omega$:

$$Dx = w, \qquad Dy = f' - h'y.$$

For a prime element $\pi$, the zeros of $\pi$ are simple, so $D\pi$ is a unit modulo $\pi$. Let $\partial = \partial^{(1)}$, $\partial^{(2)}$ be the first two Hasse derivatives of $K$ with respect to $x$ (a separating element, as $w \neq 0$); they are the coefficients of the $k$-algebra homomorphism $K \to K[[t]]$, $a \mapsto \sum_n \partial^{(n)} a\, t^n$, which extends $x \mapsto x + t$ [4]. So $D = w\,\partial$. Define

$$E(a) = w^2\,\partial^{(2)}a + \bigl(f' + h'(y + h)\bigr)\,\partial a, \qquad w^2 = h^2 + 4f. \tag{1}$$

If $p$ is odd, $E = \frac{1}{2}(D^2 + h'D)$. We shall see (Lemma 13) that $E$ maps $A$ into $A$. Explicitly, for $a, b \in k[x]$, with $a^{[2]} = \partial^{(2)}a$ and $\Delta = h^2 + 4f$,

$$\begin{aligned} D(a + by) &= (ha' + 2fb' + f'b) + (2a' - hb' - h'b)y, \\ E(a + by) &= (\Delta a^{[2]} + (f' + hh')a' + (hf' - h'f)b' + (hf^{[2]} - 2h^{[2]}f)b) \\ &\quad + \bigl(h'a' + \Delta b^{[2]} + (3f' + hh')b' + (2f^{[2]} + hh^{[2]})b\bigr)\,y. \end{aligned} \tag{2}$$

**The element $K_\pi$.** In $A \otimes_k A$ write $a_1 = a \otimes 1$, $a_2 = 1 \otimes a$, let $\mu\colon A \otimes A \to A$ be the multiplication and $G = y_1 + y_2 + h(x_1)$. By Lemma 11 below there is a unique $R_0 \in A \otimes A$ with

$$(x_1 - x_2)R_0 = (\pi_1 - \pi_2)\,G. \tag{3}$$

By Lemma 2, $A \otimes A = (V_d \otimes A) \oplus (\pi A \otimes A)$, so there are unique $R \in V_d \otimes A$ and $\varkappa \in A \otimes A$ with

$$R_0 = R + \pi_1 \varkappa. \tag{4}$$

We put $K_\pi = -\mu(\varkappa) \in A$.

**Theorem 3.** *Let $\pi$ be a prime element of $A$ of degree $d \geq 2$. Then*

$$W_d \equiv -1 + \pi\,\frac{E(\pi) + K_\pi D\pi}{(D\pi)^2} \pmod{\pi^2}.$$

*In particular $\pi$ is a Wilson prime if and only if $\pi$ divides $E(\pi) + K_\pi\, D\pi$.*

**Proposition 4.** *Let $d \geq \gamma - 1 = 2g$ and normalise $\pi_d = 1$. Let $\rho = \pi\,(y + h) = \sum_n \rho_n m_n$. For $a = g - 1, g - 2, \ldots, 0$ define $c_a \in k[x]$ by*

$$c_a = \sum_{i \geq 0} \rho_{d+2a+2+2i}\, x^i - \sum_{a < a' \leq g-1} \pi_{d-2(a'-a)}\, c_{a'}.$$

*Then $\varkappa = \sum_{a=0}^{g-1} x^a \otimes c_a$ and $K_\pi = -\sum_{a=0}^{g-1} c_a\, x^a$, a polynomial in $x$ of degree at most $g - 1$.*

**Corollary 5.** *Let $g = 1$, $h = h_1 x + h_0$. For every prime element $\pi$ of degree $d \geq 2$ with $\pi_d = 1$, $K_\pi = -\pi_{d-1} - \varepsilon h_1$, where $\varepsilon = 1$ if $d$ is even and $\varepsilon = 0$ if $d$ is odd. So $\pi$ is a Wilson prime if and only if $\pi$ divides $E(\pi) - (\pi_{d-1} + \varepsilon h_1)D\pi$.*

**Corollary 6.** *Let $g = 2$ and $d \geq 4$, $\pi_d = 1$. Then $K_\pi = -\rho_{d+2} - (2x - \pi_{d-2})\,\rho_{d+4}$.*

*Remark* 7. (a) For $p = 3$, $h = 0$, $f = x^3 - x - 1$: $E = -D^2$ and $K_\pi = -\pi_{d-1}$, so the criterion is $\pi \mid D^2\pi + \pi_{d-1}D\pi$, which is [2, Theorem 4(1)] (there $Dx = -y = 2y$). (b) For $p = 2$, $h = 1$: $D = \partial$, $E = \partial^{(2)} + f'\partial$; Corollary 5 gives $K_\pi = \pi_{d-1}$, and Corollary 6 with $f = x^5 + x^3 + 1$ gives $K_\pi = \pi_{d-3} + \pi_{d-1}\pi_{d-2}$: this is [3, Theorem 3]. (c) In $\mathbb{F}_q[t]$, with $V$ the polynomials of degree less than $d$, the same argument applies with $R_0 = (\wp_1 - \wp_2)/(t_1 - t_2) \in V \otimes A$ and no correction term; it gives the vanishing of the second Hasse derivative of $\wp$, which is Thakur's criterion [5]. We do not give the details.

## 2. Reduction to a linear coefficient

Fix a prime element $\pi$ of degree $d$, $\mathbf{F}_\pi = A/\pi$, $\rho_\pi \colon V_d \to \mathbf{F}_\pi$ the bijection of Lemma 2, and define the $k$-linear map $\delta_\pi \colon \mathbf{F}_\pi \to \mathbf{F}_\pi$ by $\delta_\pi(\rho_\pi(v)) = D(v) \bmod \pi$. Every $k$-linear endomorphism of $\mathbf{F}_\pi$ is uniquely $z \mapsto \sum_{j=0}^{d-1} \lambda_j z^{q^j}$; let $\lambda_0$ be the coefficient of $z$ for $\delta_\pi$.

**Proposition 8.** *$W_d \equiv -1 + \pi\lambda_0/D\pi \pmod{\pi^2}$. So $\pi$ is a Wilson prime if and only if $\lambda_0 = 0$.*

*Proof.* The completion of $A$ at $\pi$ is $\mathbf{F}_\pi[[\pi]]$. For $a \in A$ write $a \equiv \bar{a} + \delta(a)\pi \pmod{\pi^2}$ with $\bar{a}, \delta(a) \in \mathbf{F}_\pi$. Then $\delta$ is a $k$-derivation with $\delta(\pi) = 1$, so $\delta = \overline{D(\cdot)}/\overline{D\pi}$ because $\Omega_{A/k} = A\omega$. The polynomial $e(z) = \prod_{v \in V_d}(z - v)$ is $k$-linear, monic of degree $q^d$, and its coefficient of $z$ is $\prod_{v \neq 0}(-v) = (-1)^{q^d - 1}W_d = W_d$ ($q^d - 1$ is even if $p$ is odd, and $-1 = 1$ if $p = 2$). Modulo $\pi$ it is $z^{q^d} - z$, so $e(z) \equiv z^{q^d} - z + \pi g(z) \pmod{\pi^2}$ with $g$ a $k$-linear polynomial over $\mathbf{F}_\pi$ of degree $< q^d$. For $v \in V_d$, $v^{q^d} \equiv \bar{v} \pmod{\pi^2}$, so $0 = e(v) \equiv \bar{v} - v + \pi g(\bar{v})$, i.e. $g(\bar{v}) = \delta(v)$. Hence $g = \delta_\pi/\overline{D\pi}$ as functions on $\mathbf{F}_\pi$, hence as polynomials. Compare the coefficients of $z$. □

**Lemma 9.** *$\operatorname{tr}_k(M_a \circ \delta_\pi) = \operatorname{Tr}_{\mathbf{F}_\pi/k}(a\lambda_0)$ for $a \in \mathbf{F}_\pi$, where $M_a$ is multiplication by $a$. So $\lambda_0 = 0$ if and only if $\operatorname{tr}_k(M_a \circ \delta_\pi) = 0$ for all $a$.*

*Proof.* Let $\phi$ be the $q$-Frobenius. For $0 < j < d$ the trace $\operatorname{tr}_k(M_b\phi^j)$ is $k$-linear in $b$, hence equal to $\operatorname{Tr}(c_j b)$ for some $c_j$; conjugation by $M_\zeta$ gives $\operatorname{Tr}(c_j b) = \operatorname{Tr}(c_j b\zeta^{q^j - 1})$ for all $b$, so $c_j(1 - \zeta^{q^j - 1}) = 0$, and $c_j = 0$ on taking $\zeta$ a generator of $\mathbf{F}_\pi^\times$. Finally $\operatorname{tr}_k(M_b) = \operatorname{Tr}_{\mathbf{F}_\pi/k}(b)$. □

## 3. The pairing and the kernel

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

**Lemma 10.** *$\langle b, c\rangle = \operatorname{Tr}_{\mathbf{F}_\pi/k}(\bar{b}\bar{c}/\overline{D\pi})$. It induces a non-degenerate symmetric $k$-bilinear form on $\mathbf{F}_\pi$ with $\langle ab, c\rangle = \langle a, bc\rangle$.*

*Proof.* $bc\,\omega/\pi$ has poles only at $\infty$ and at the zeros of $\pi$, which are simple and form one Galois orbit. As $d\pi = D\pi\,\omega$, the residue at a zero $Q$ is $(bc/D\pi)(Q)$. Apply the residue theorem. □

**Lemma 11.** *For every $a \in A$ there is a unique $R_0(a) \in A \otimes A$ with $(x_1 - x_2)R_0(a) = (a_1 - a_2)G$.*

*Proof.* $C$ is geometrically integral, so $A \otimes A$ is a domain; uniqueness follows. We have $A \otimes A/(x_1 - x_2) \cong A[Y]/\big((Y - y)(Y + y + h)\big)$, with $Y$ the image of $y_2$. Let $N \in A[Y]$ represent $(a_1 - a_2)G$. It vanishes at $Y = y$, because $a_1 - a_2$ does, so $N = (Y - y)Q$ with $Q \in A[Y]$. It vanishes at $Y = -y - h$, because $G = y + Y + h$; so $-w\,Q(-y - h) = 0$, hence $Q(-y - h) = 0$ as $w \neq 0$, and $Q$ is divisible by $Y + y + h$. □

**Lemma 12.** *Write $R_0 = R_0(\pi) = \sum_i r_i \otimes s_i$. Then $\sum_i \langle b, s_i\rangle\, r_i \equiv b \pmod{\pi}$ for every $b \in A$.*

*Proof.* As $\pi$ generates a radical ideal, it suffices to evaluate at a zero $P \in C(\bar{k})$ of $\pi$, the pairing being extended $\bar{k}$-linearly in the second variable. By (3) and $\pi(P) = 0$, $R_0(P, \cdot) = -\pi \cdot C_P$

with $C_P = (y + y(P) + h(x(P)))/(x(P) - x)$, so the left side is $\mathrm{Res}_\infty(b\, C_P\, \omega)$. Let $\bar{P}$ be the conjugate of $P$: $x(\bar{P}) = x(P)$, $y(\bar{P}) = -y(P) - h(x(P))$. The affine poles of $C_P$ are among $P, \bar{P}$.

If $w(P) \neq 0$, then $\bar{P} \neq P$, $x - x(P)$ is a uniformiser at $P$ and at $\bar{P}$, the numerator of $C_P$ vanishes at $\bar{P}$ and equals $w(P)$ at $P$. So $b\, C_P\, \omega = b\, C_P\, dx/w$ has, on the affine curve, only a simple pole at $P$, with residue $-b(P)$.

If $w(P) = 0$, then $\bar{P} = P$, $s = y - y(P)$ is a uniformiser at $P$, the numerator of $C_P$ is $s$, and expanding $F(x(P) + \xi, y(P) + s) = 0$ gives $\xi = x - x(P) = s^2/(f' - h'y)(P) + O(s^3)$. With $\omega = dy/(f' - h'y)$ we get again a simple pole with residue $-b(P)$.

In both cases the residue theorem gives $\mathrm{Res}_\infty(b\, C_P\, \omega) = b(P)$. □

**Lemma 13.** *Let $\tau\colon A \otimes A \to K[[t]]$ be the ring homomorphism $\tau(a \otimes b) = b \sum_n \partial^{(n)} a\, t^n$, and let $D_1 = D \otimes 1$. For $\Phi \in A \otimes A$ write $\tau(\Phi) = \Phi_0 + \Phi_1 t + \cdots$. Then $\mu(\Phi) = \Phi_0$ and $\mu(D_1\Phi) = w\, \Phi_1$. Consequently, for every $a \in A$,*

$$\mu(R_0(a)) = D(a), \qquad \mu\big(D_1 R_0(a)\big) = E(a);$$

*in particular $E(A) \subset A$.*

*Proof.* $\mu(\Phi) = \Phi_0$ is clear. The maps $\tau \circ D_1$ and $\tau(w_1)\, \frac{d}{dt} \circ \tau$ are derivations of $A \otimes A$ into $K[[t]]$ over $\tau$; both vanish on $1 \otimes A$ and both send $x_1$ to $\tau(w_1)$. As $\tau(w_1)$ has constant term $w \neq 0$, the relation $\tau(w_1)\, \vartheta(y_1) = \tau((f' - h'y)_1)\vartheta(x_1)$, valid for both derivations $\vartheta$ because $F(x_1, y_1) = 0$, shows that they agree on $y_1$; so they are equal, and taking constant terms gives $\mu(D_1\Phi) = w\Phi_1$. Now $\tau(x_1 - x_2) = t$, $\tau(a_1 - a_2) = \partial a\, t + \partial^{(2)} a\, t^2 + \cdots$ and $\tau(G) = w + (\partial y + h')t + \cdots$, so $\tau(R_0(a)) = w\, \partial a + (w\, \partial^{(2)} a + (\partial y + h')\partial a)t + \cdots$. Hence $\mu(R_0(a)) = w\, \partial a = D(a)$ and $\mu(D_1 R_0(a)) = w^2 \partial^{(2)} a + (Dy + h'w)\, \partial a = E(a)$, because $Dy + h'w = f' - h'y + h'(2y + h)$. □

Formula (2) follows from (1) by a direct computation, using $w\, \partial y = f' - h'y$ and $w\, \partial^{(2)} y = f^{[2]} - h^{[2]} y - (\partial y)^2 - h' \partial y$, which give $E(y) = w\, (f^{[2]} - h^{[2]} y)$.

## 4. Proof of Theorem 3

Let $R$, $\varkappa$ be as in (4), and write $R = \sum_j m_j \otimes t_j$, the sum over the monomials of $V_d$. As $R - R_0 \in \pi A \otimes A$, Lemma 12 gives $\sum_j \langle m_i, t_j \rangle m_j \equiv m_i \pmod{\pi}$, hence $\langle m_i, t_j \rangle = \delta_{ij}$ by Lemma 2. So $\mathrm{tr}_k(T) = \sum_j \langle T \bar{m}_j, \bar{t}_j \rangle$ for every endomorphism $T$ of $\mathbf{F}_\pi$, and with Lemma 10

$$\mathrm{tr}_k(M_a \circ \delta_\pi) = \sum_j \langle a\, D(m_j), t_j \rangle = \langle a, \Theta \rangle, \qquad \Theta := \sum_j D(m_j)\, t_j = \mu(D_1 R).$$

By (4) and Lemma 13,

$$\Theta = \mu(D_1 R_0) - \mu\big(D_1(\pi_1 \varkappa)\big) = E(\pi) - D\pi \cdot \mu(\varkappa) - \pi\, \mu(D_1 \varkappa) \equiv E(\pi) + K_\pi D\pi \pmod{\pi}.$$

By Lemmas 9 and 10, $\mathrm{Tr}(a\lambda_0) = \langle a, \Theta \rangle = \mathrm{Tr}(a\, \Theta/D\pi)$ for all $a \in \mathbf{F}_\pi$, so $\lambda_0 = \Theta/D\pi$ in $\mathbf{F}_\pi$, and Proposition 8 gives the theorem. □

## 5. Proof of Proposition 4 and of the corollaries

Write $R_0 = \sum_{j \in S} m_j \otimes r_j$. We have $x\, m_j = m_{j+2}$, so the coefficient of $m_n$ (first variable) in $(x_1 - x_2)R_0$ is $r_{n-2} - x\, r_n$, with $r_j = 0$ for $j \notin S$. On the other side $(\pi_1 - \pi_2)G = \big(\pi(y + h)\big)_1 + \pi_1 y_2 - \pi_2 G$, where $\pi_1 y_2$ has degree $d$ and $\pi_2 G$ has degree at most $\gamma \leq d + 1$

in the first variable (recall $\deg h(x) \le 2g < \gamma$). As $d \ge 2g$, every $j \ge d$ belongs to $S$. So for $n \ge d+2$ we get $r_{n-2} - x\, r_n = \rho_n$, and as $R_0$ has finite support,

$$r_j = \sum_{i \ge 0} \rho_{j+2+2i}\, x^i \qquad (j \ge d),$$

in particular $r_j = 0$ for $j > d + \gamma - 2$. The indices $j \ge d$ with $j - d \in S$ and $j \le d + \gamma - 2$ are $j = d + 2a$, $0 \le a \le g - 1$. For $\varkappa' = \sum_a x^a \otimes c_a$ the coefficient of $m_{d+2a}$ in $\pi_1 \varkappa'$ is $\sum_{a' \ge a} \pi_{d-2(a'-a)} c_{a'}$, which equals $r_{d+2a}$ by the definition of the $c_a$ (recall $\pi_d = 1$). So $R_0 - \pi_1 \varkappa'$ has no component on $m_j$ with $j - d \in S$, i.e. it lies in $V_d \otimes A$, and $\varkappa = \varkappa'$ by uniqueness in (4). This proves Proposition 4.

For $g = 2$: $c_1 = \rho_{d+4}$ and $c_0 = \rho_{d+2} + x\rho_{d+4} - \pi_{d-2}\rho_{d+4}$, which gives Corollary 6. For $g = 1$: $K_\pi = -c_0 = -\rho_{d+2}$. Here $f = x^3 + \cdots$, and $y \cdot x^i y = x^i f - h\, x^i y$. If $d$ is odd, $m_d = x^i y$ and the terms of degree $d+2$ of $m_d(y+h)$ are $-h_1 x^{i+1} y + h_1 x^{i+1} y = 0$, while $m_{d-1} y = m_{d+2}$; so $\rho_{d+2} = \pi_{d-1}$. If $d$ is even, $m_d\, h$ contributes $h_1 m_{d+2}$, and for $d \ge 4$, $m_{d-1} = x^j y$ with $2j + 3 = d - 1$ and $m_{d-1}(y+h) = x^j f$ has leading term $m_{d+2}$ (for $d = 2$, $\pi_1 = 0$); so $\rho_{d+2} = \pi_{d-1} + h_1$. The monomials $m_j$, $j \le d - 2$, contribute in degree at most $d + 1$. This proves Corollary 5. □

## 6. Numerical verification

The ancillary script `verify_wilson_hyperelliptic.py` (pure Python) treats the 17 curves below over $\mathbb{F}_p$ (prime elements are counted up to units). For every prime element $\pi$ of degree $d$ in the indicated range it computes $W_d$ modulo $\pi^2$ from the definition (and also as a plain product when $p^d \le 300$), builds $R_0$, $R$ and $\varkappa$, and checks that $W_d \equiv -1 \pmod{\pi}$, that $\mu(D_1 R_0) = E(\pi)$ with $E$ given by (2), that $K_\pi$ agrees with Proposition 4 when $d \ge 2g$, and the congruence of Theorem 3. There is no failure on the 1377 prime elements of degree at most the bound given in the table, of which 59 are Wilson primes.

| $p$ | $g$ | $h$ | $f$ | $d \le$ | primes | Wilson | degrees with Wilson primes |
|---|---|---|---|---|---|---|---|
| 3 | 1 | 0 | $x^3 + 2x + 2$ | 6 | 212 | 15 | 3, 5, 6 |
| 2 | 1 | 1 | $x^3 + x + 1$ | 10 | 218 | 12 | 2, 5, 10 |
| 5 | 1 | 0 | $x^3 + x + 1$ | 4 | 22 | 1 | 3 |
| 7 | 1 | 0 | $x^3 + 3$ | 3 | 10 | 2 | 2, 3 |
| 2 | 1 | $x$ | $x^3 + 1$ | 12 | 184 | 4 | 12 |
| 3 | 1 | $x + 1$ | $x^3 + x^2 + 1$ | 6 | 38 | 3 | 3, 5 |
| 5 | 1 | $x + 2$ | $x^3 + x^2 + 3x + 1$ | 4 | 73 | 1 | 3 |
| 3 | 1 | 0 | $x^3 + x^2 + 2x + 1$ | 6 | 60 | 8 | 2, 3, 6 |
| 2 | 2 | 1 | $x^5 + x^3 + 1$ | 10 | 234 | 7 | 2, 4, 9 |
| 3 | 2 | 0 | $x^5 + x^2 + 2$ | 6 | 31 | 2 | 2 |
| 5 | 2 | 0 | $x^5 + 2x + 1$ | 4 | 8 | 0 | – |
| 2 | 2 | $x$ | $x^5 + x^2 + 1$ | 10 | 119 | 0 | – |
| 3 | 2 | $x^2 + 1$ | $x^5 + x^3 + x + 2$ | 6 | 20 | 0 | – |
| 3 | 2 | $x + 1$ | $x^5 + x^3 + 2$ | 6 | 42 | 0 | – |
| 2 | 3 | 1 | $x^7 + x + 1$ | 10 | 43 | 2 | 2, 10 |
| 3 | 3 | 0 | $x^7 + x + 2$ | 7 | 22 | 2 | 7 |
| 2 | 3 | $x + 1$ | $x^7 + 1$ | 10 | 41 | 0 | – |

A second program, written with the FLINT library, tested the criterion further on nine of these curves and one other (up to degree 14 for $p = 2$, 9 for $p = 3$, 6 for $p = 5$, 5 for $p = 7$): 5334 prime elements, no failure. For $q = 4$ see [3]. Fourteen of the 17 curves have class number greater than one.

## 7. Status and questions

Theorem 3, Proposition 4 and the corollaries are proved above. Nothing in this note has been checked by a third party. The computations cover prime fields only, apart from the case $q = 4$ of [3]. Open: a criterion for the prime ideals of $A$ that are not principal; an expression of $K_\pi$ for $d < 2g$; the set of degrees carrying Wilson primes and their infinitude.

**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] H. Cohen, G. Frey et al., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2006.

[2] D. Niedbala Giraudin, Wilson primes for an elliptic coordinate ring of class number one, Hexagon 2611.01007 (2026).

[3] D. Niedbala Giraudin, Wilson primes for the coordinate rings of class number one in characteristic two, Hexagon 2611.01009 (2026).

[4] H. Hasse, F. K. Schmidt, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten, J. reine angew. Math. **177** (1937), 215–237.

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

[6] 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