hexagon:2611.01053v1

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

DAVID NIEDBALA GIRAUDIN

Abstract. Let $A = \mathbb{F}_q[x,y]/(F)$ be the coordinate ring of a smooth affine plane curve $F = y^a - \alpha x^b + \sum_{ai+bj<ab} c_{ij} x^i y^j$ with $\gcd(a,b) = 1$; such a curve has one point at infinity. With the Wilson product W_d attached to the monomial basis, we prove for every prime element π of degree d the congruence $W_d \equiv -1 + \pi\,(E(\pi) + K_\pi D\pi)/(D\pi)^2 \pmod{\pi^2}$, where D is the invariant derivation, E an explicit second order operator and K_π a correction term defined by a canonical decomposition involving at most g monomials. This extends to all these curves the theorem proved for hyperelliptic curves in [3]. For the curves $y^a = f(x)$ and the prime elements $P(y)$ the correction vanishes; when f' is a non-zero constant and the second Hasse derivative of f is zero, $P(y)$ is a Wilson prime if and only if the second Hasse derivative of P is zero, which is Thakur's criterion for $\mathbb{F}_q[t]$ with y in the role of t. We deduce infinitely many Wilson primes on $y^a = x^p - x + \alpha$ over $\mathbb{F}_p$ for every odd p and every $a \geq 2$ prime to p, and on $y^a = x^4 + x + 1$ over $\mathbb{F}_2$ for every odd $a \geq 3$.

1. Setting and statements

Let $k = \mathbb{F}_q$ of characteristic p, and let $a, b \geq 2$ be coprime integers. Let

$$F(x,y) = y^a - \alpha x^b + \sum_{ai+bj<ab} c_{ij}\, x^i y^j \in k[x,y], \qquad \alpha \in k^\times,$$

and assume that the affine curve $C\colon F = 0$ is smooth over $\bar{k}$. Put $A = k[x,y]/(F)$. In coding theory these are the C_{ab} curves of Miura [7]; the case $a = 2$ is the imaginary hyperelliptic model of [3].

Lemma 1. *F is absolutely irreducible. The smooth projective model of C has exactly one point ∞ outside C; it is k-rational, and $\deg := -\operatorname{ord}_\infty$ satisfies $\deg x = a$, $\deg y = b$. The ring A is the ring of functions regular outside ∞, a Dedekind domain with $A^\times = k^\times$. The monomials $x^i y^j$, $i \geq 0$, $0 \leq j < a$, form a k-basis of A, their degrees $ai + bj$ are pairwise distinct and fill the semigroup $S = a\mathbb{N} + b\mathbb{N}$, whose complement in $\mathbb{N}$ has $g = (a-1)(b-1)/2$ elements, the genus of C. Moreover $F_y := \partial F/\partial y$ is not zero in A.*

For $s \in S$ let m_s be the monomial $x^i y^j$ $(0 \leq j < a)$ of degree s; note $x\, m_s = m_{s+a}$. We write $u = \sum_s u_s m_s$ for $u \in A$. A *prime element* is a $\pi \in A$ such that A/π is a field; its degree is $d = \dim_k A/\pi = \deg \pi \in S$. We do not assume that A is principal.

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

Lemma 3. *If $u \in A$ has degree $d \geq 1$ (so $d \in S$), then $A = V_d \oplus uA$. In particular, for a prime element π of degree d the map $V_d \to A/\pi$ is bijective and $W_d \equiv -1 \pmod{\pi}$.*

Proof. The degree of a non-zero element of V_d lies in $S \setminus (d + S)$, the degree of a non-zero multiple of u lies in $d + S$, so $V_d \cap uA = 0$. The set $S \setminus (d + S)$ contains exactly one element in

Date: 25 November 2026.

each class modulo d (the least element of S in that class; here $d \in S$ is used), so $\dim V_d = d$. On the other hand $\dim_k A/uA = \sum_P \operatorname{ord}_P(u) \deg P = -\operatorname{ord}_\infty(u) = d$, the sum being over the closed points of C, because ∞ is rational. □

The space V_d, hence the notion of Wilson prime, depends on the model. For $a = 2$ this is the definition of [1, 2, 3]; in $\mathbb{F}_q[t]$ the analogous product is Thakur's F_d [9, 10], and the generalisation to other function fields is asked for in [10, Section 7, Question (2)].

The operators D and E. Write F_x, F_y, F_{xy} for the partial derivatives of F and $F^{(2)}_{xx}, F^{(2)}_{yy}$ for its second Hasse partial derivatives (the coefficients of s^2 in $F(x+s, y)$ and $F(x, y+s)$), all read in A. As C is smooth, $\Omega_{A/k}$ is free on the differential ω with $dx = F_y\,\omega$, $dy = -F_x\,\omega$, which has neither zero nor pole on C, and there is a unique k-derivation D of A with $du = D(u)\,\omega$:

$$Dx = F_y, \qquad Dy = -F_x.$$

For a prime element π the zeros of π are simple, so $D\pi$ is a unit modulo π. Let K be the fraction field of A. As $F_y \neq 0$, x is a separating element of K; let $\partial = \partial^{(1)}$, $\partial^{(2)}$ be the first two Hasse derivatives of K with respect to x, i.e. the coefficients of the k-algebra homomorphism $K \to K[[t]]$, $u \mapsto \sum_n \partial^{(n)}u\, t^n$, which extends $x \mapsto x + t$ [5]. Then $D = F_y\,\partial$. Define

$$E(u) = F_y^2\,\partial^{(2)}u + \left(F_yF_{xy} - F^{(2)}_{yy}F_x\right)\partial u. \tag{1}$$

By Lemma 15, E maps A into A, and it is the unique k-linear map $A \to A$ such that

$$E(uv) = uE(v) + vE(u) + D(u)D(v), \qquad E(x) = F_yF_{xy} - F^{(2)}_{yy}F_x, \qquad E(y) = -F_yF^{(2)}_{xx}. \tag{2}$$

If p is odd, $E = \frac{1}{2}(D^2 + F_{xy}D)$. For $F = y^2 + h(x)y - f(x)$ these are the operators of [3].

The element K_π. In $A \otimes_k A$ write $u_1 = u \otimes 1$, $u_2 = 1 \otimes u$, and let $\mu\colon A \otimes A \to A$ be the multiplication. Let $G \in A \otimes A$ be the image of the polynomial $(F(x_1, y_1) - F(x_1, y_2))/(y_1 - y_2)$. By Lemma 13 there is, for a prime element π, a unique $R_0 \in A \otimes A$ with

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

By Lemma 3, $A \otimes A = (V_d \otimes A) \oplus (\pi A \otimes A)$, so there are unique $R \in V_d \otimes A$ and $\varkappa \in A \otimes A$ with

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

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

Theorem 4. *Let π 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 π is a Wilson prime if and only if π divides $E(\pi) + K_\pi\,D\pi$.

Proposition 5. *$\varkappa = \sum_{s \in S,\ s<2g} m_s \otimes c_s$ with $c_s \in A$; so $K_\pi = -\sum_{s \in S,\, s<2g} m_s\, c_s$ involves at most g terms. If $R_0 \in V_d \otimes A$, then $K_\pi = 0$.*

The curves $y^a = f(x)$. Let now $F = y^a - f(x)$ with $\deg f = b$, and write $f^{[2]}$, $P^{[2]}$ for second Hasse derivatives of polynomials in one variable.

Proposition 6. *Let $P \in k[T]$ be of degree $n \geq 1$ and $\pi = P(y)$. Then the element R_0 defined by (3) lies in $V_d \otimes A$, where $d = bn$. If π is a prime element, then $K_\pi = 0$ and*

$$W_d \equiv -1 + \pi \, \frac{f'(x)^2 \, P^{[2]}(y) + a \, y^{a-1} f^{[2]}(x) \, P'(y)}{P'(y)^2 f'(x)^2} \pmod{\pi^2}.$$

Theorem 7. *Assume that f' is a non-zero constant and that $f^{[2]} = 0$ (the second condition follows from the first if p is odd; for $p = 2$ the two conditions mean $f \in cx + k[x^4]$, $c \neq 0$). Let $P \in k[T]$ be such that $P(y)$ is a prime element of A. Then $P(y)$ is a Wilson prime if and only if $P^{[2]} = 0$, i.e. if and only if all the exponents of P are congruent to 0 or 1 modulo p when p is odd, modulo 4 when $p = 2$.*

The curve is automatically smooth under these hypotheses, and p divides b, so $p \nmid a$. The criterion is the one of Thakur for the primes of $\mathbb{F}_q[t]$ [9, Theorem 2.9], with y in the role of t. For $a = 2$ and p odd, Proposition 6 and Theorem 7 are in [4].

Theorem 8. *Let p be an odd prime, $a \geq 2$ an integer prime to p, $\alpha \in \mathbb{F}_p^\times$ and $A = \mathbb{F}_p[x, y]/(y^a - x^p + x - \alpha)$, of genus $(a-1)(p-1)/2$.*

1. *If $p \geq 5$, let r be a prime divisor of $p-1$, chosen odd if $p \equiv 3 \pmod 4$, let o be the order of r modulo p and c a primitive root modulo p. For every $j \geq 1$ such that $t = r^{oj} > a$, the element $y^t - c$ is a Wilson prime of A, of degree pt.*
2. *If $p = 3$, then for every $j \geq 0$ such that $3 \cdot 25^j > a$, the element $y^{4 \cdot 25^j} + y^{25^j} - 1$ is a Wilson prime of A, of degree $12 \cdot 25^j$.*

In particular A has infinitely many Wilson primes.

Theorem 9. *Let $a \geq 3$ be odd and $A = \mathbb{F}_2[x, y]/(y^a - x^4 - x - 1)$, of genus $3(a-1)/2$. For every $j \geq 0$ such that $8 \cdot 73^j > a$, the element $y^{9 \cdot 73^j} + y^{73^j} + 1$ is a Wilson prime of A, of degree $36 \cdot 73^j$. In particular A has infinitely many Wilson primes.*

For $a = 2$, Theorem 8 is [4]. Theorem 9 gives the first infinite families in characteristic 2 outside $\mathbb{F}_q[t]$ that we know of; for $\mathbb{F}_q[t]$ see [8] and [9, Theorem 2.10].

2. Proof of Lemma 1

Let F_1 be an irreducible factor of F over $\bar{k}$ and L the function field of $F_1 = 0$. As F is monic in y, F_1 is not in $\bar{k}[x]$, so x is not constant in L; let v be a pole of x, $v(x) = -m < 0$. If $v(y) \geq 0$, the term αx^b of F would have valuation $-bm$, strictly smaller than all the others (the term y^a has valuation ≥ 0 and the others have $i < b$), which is impossible; so $v(y) = -n < 0$. The terms of F have valuations $-an$, $-bm$ and $-(im + jn)$ with $ai + bj < ab$. If $an \geq bm$, then $im + jn = \frac{m}{a}(ai + bj) + j\big(n - \frac{bm}{a}\big) < bm + (an - bm) = an$ (use $ai + bj < ab$ and $0 \leq j < a$); so if $an > bm$ the term y^a alone has least valuation, impossible. Symmetrically, if $an < bm$ then $im + jn = \frac{n}{b}(ai + bj) + i\big(m - \frac{an}{b}\big) < bm$ and the term αx^b alone has least valuation, impossible. Hence $an = bm$, and as $\gcd(a, b) = 1$, $m = ae$, $n = be$ with $e \geq 1$. The ramification index of v over the pole of x in $\bar{k}(x)$ is $m \geq a$, while $[L : \bar{k}(x)] = \deg_y F_1 \leq a$. So $F_1 = F$, v is the only pole of x, $e = 1$, $v(x) = -a$, $v(y) = -b$. Being unique, this place is defined over k. As C is smooth, A is integrally closed, hence it is the integral closure of $k[x]$ in its fraction field, i.e. the ring of functions regular outside ∞; so $A^\times = k^\times$. The basis is clear (F is monic in y), the degrees $ai + bj$ with $0 \leq j < a$ are distinct since $\gcd(a, b) = 1$, and the number of gaps of S is the genus by the Weierstrass gap theorem; it equals $(a-1)(b-1)/2$.

Finally suppose $F_y = 0$ in A. Its degree in y is less than a, so $F_y = 0$ as a polynomial, $F \in k[x, y^p]$ and $p \mid a$, hence $p \nmid b$ and $F_x = -b\alpha x^{b-1} + \cdots$, which is written in the monomial basis, is an element of A of degree $a(b-1) > 0$ (recall $b \geq 2$). It has a zero on C, which is then a singular point. So $F_y \neq 0$ in A. □

3. Reduction to a linear coefficient

Fix a prime element π of degree d, $\mathbf{F}_\pi = A/\pi$, $\rho_\pi \colon V_d \to \mathbf{F}_\pi$ the bijection of Lemma 3, 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 λ_0 be the coefficient of z for δ_π.

Proposition 10. $W_d \equiv -1 + \pi\lambda_0/D\pi \pmod{\pi^2}$.

Lemma 11. $\mathrm{tr}_k(M_u \circ \delta_\pi) = \mathrm{Tr}_{\mathbf{F}_\pi/k}(u\lambda_0)$ *for* $u \in \mathbf{F}_\pi$, *where* M_u *is multiplication by* u.

The proofs are those of [3, Proposition 8 and Lemma 9]: they use only that A is a Dedekind domain whose module of differentials is free on ω, and Lemma 3. We recall them. *Lemma 11.* Let ϕ be the q-Frobenius of $\mathbf{F}_\pi$. For $0 < j < d$ the trace $\mathrm{tr}_k(M_b\phi^j)$ is k-linear in b, hence equal to $\mathrm{Tr}(c_j b)$ for some c_j; conjugation by M_ζ gives $\mathrm{Tr}(c_j b) = \mathrm{Tr}(c_j b \zeta^{q^j-1})$ for all b, so $c_j(1 - \zeta^{q^j-1}) = 0$, and $c_j = 0$ on taking ζ a generator of $\mathbf{F}_\pi^\times$; finally $\mathrm{tr}_k(M_b) = \mathrm{Tr}_{\mathbf{F}_\pi/k}(b)$. *Proposition 10.* The completion of A at π is $\mathbf{F}_\pi[[\pi]]$; writing $u \equiv \bar{u} + \delta(u)\pi \pmod{\pi^2}$, δ is a k-derivation with $\delta(\pi) = 1$, so $\delta = \overline{D(\cdot)}/\overline{D\pi}$. The polynomial $e(z) = \prod_{v \in V_d}(z - v)$ is k-linear with coefficient of z equal to W_d, and $e(z) \equiv z^{q^d} - z + \pi g(z) \pmod{\pi^2}$ with g k-linear of degree less than 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 $g = \delta_\pi/\overline{D\pi}$, and one compares the coefficients of z.

4. The pairing and the kernel

For $u, v \in A$ put $\langle u, v \rangle = -\operatorname{Res}_\infty(uv\,\omega/\pi)$.

Lemma 12. $\langle u, v \rangle = \mathrm{Tr}_{\mathbf{F}_\pi/k}\big(\bar{u}\bar{v}/\overline{D\pi}\big)$. *It induces a non-degenerate symmetric* k*-bilinear form on* $\mathbf{F}_\pi$ *with* $\langle uv, z \rangle = \langle u, vz \rangle$.

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

Lemma 13. *For every* $u \in A$ *there is a unique* $R_0(u) \in A \otimes A$ *with* $(x_1 - x_2)R_0(u) = (u_1 - u_2)G$.

Proof. $A \otimes A$ is a domain because C is geometrically integral; uniqueness follows. We have $A \otimes A/(x_1 - x_2) \cong A[Y]/(F(x, Y))$, with Y the image of y_2. Writing $u = \sum_j c_j(x) y^j$, the image of $u_1 - u_2$ is $\sum_j c_j(x)(y^j - Y^j) = (y - Y)\,c(Y)$ with $c \in A[Y]$, and the image of $(y_1 - y_2)G$ is $F(x, y) - F(x, Y) = -F(x, Y)$. So the image of $(u_1 - u_2)G$ is $-c(Y)F(x, Y) = 0$. □

Lemma 14. *Write* $R_0 = R_0(\pi) = \sum_i r_i \otimes s_i$. *Then* $\sum_i \langle u, s_i \rangle\, r_i \equiv u \pmod{\pi}$ *for every* $u \in A$.

Proof. As π generates a radical ideal, it suffices to evaluate at a zero $P = (x_P, y_P) \in C(\bar{k})$ of π, 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 $C_P = \gamma(y)/(x_P - x)$, where $\gamma(Y) = F(x_P, Y)/(Y - y_P) \in \bar{k}[Y]$. So the left side is $\operatorname{Res}_\infty(u\,C_P\,\omega)$, and we must show that $u\,C_P\,\omega$ has, on C, a single pole, simple, at P, with residue $-u(P)$.

Let $Q = (x_P, y_Q)$ be a point of C on the line $x = x_P$ and e_Q the multiplicity of y_Q as a root of $F(x_P, Y)$, so $F(x_P, Y) = (Y - y_Q)^{e_Q} U_Q(Y)$ with $U_Q(y_Q) \neq 0$. If $F_y(Q) \neq 0$, then $e_Q = 1$ and $x - x_P$ is a uniformiser at Q. If $F_y(Q) = 0$, then $F_x(Q) \neq 0$, $s = y - y_Q$ is a uniformiser at

Q, and expanding $F(x_P+\xi, y_Q+s)=0$ gives $\xi = x-x_P = -U_Q(y_Q)\,s^{e_Q}/F_x(Q) + O(s^{e_Q+1})$. In both cases $\operatorname{ord}_Q(x-x_P) = e_Q \le \operatorname{ord}_Q\big((y-y_Q)^{e_Q}\big)$.

For $Q \neq P$, $\gamma(Y)$ is divisible by $(Y-y_Q)^{e_Q}$, so C_P is regular at Q. At P: if $F_y(P)\neq 0$, then $\gamma(y_P) = F_y(P)$ and $u\,C_P\,dx/F_y$ has a simple pole with residue $-u(P)$. If $F_y(P)=0$, then $\gamma(y) = s^{e_P-1}U_P(y)$ and, with $\omega = -dy/F_x$ and the expansion of ξ, $C_P = F_x(P)\,s^{-1}(1+O(s))$ and $u\,C_P\,\omega = -u(P)\,s^{-1}ds\,(1+O(s))$. The residue theorem gives $\operatorname{Res}_\infty(u\,C_P\,\omega) = u(P)$. □

Lemma 15. *Let $\tau\colon A\otimes A \to K[[t]]$ be the ring homomorphism $\tau(u\otimes v) = v\sum_n \partial^{(n)}u\,t^n$, 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 $\mu(D_1\Phi) = F_y\,\Phi_1$. Consequently, for every $u\in A$,*

$$\mu(R_0(u)) = D(u), \qquad \mu(D_1R_0(u)) = E(u),$$

so $E(A)\subset A$, and (2) holds.

Proof. $\mu(\Phi)=\Phi_0$ is clear. The maps $\tau\circ D_1$ and $\tau\big((F_y)_1\big)\frac{d}{dt}\circ\tau$ are derivations of $A\otimes A$ into $K[[t]]$ over τ; both vanish on $1\otimes A$ and both send x_1 to $\tau((F_y)_1)$. The relation $\tau((F_y)_1)\,\vartheta(y_1) = -\tau((F_x)_1)\,\vartheta(x_1)$, valid for both derivations ϑ because $F(x_1,y_1)=0$, and the fact that $\tau((F_y)_1)$ has constant term $F_y\neq 0$, show that they agree on y_1; so they are equal, and taking constant terms gives $\mu(D_1\Phi) = F_y\Phi_1$.

Now $\tau(x_1-x_2) = t$ and $\tau(u_1-u_2) = \partial u\,t + \partial^{(2)}u\,t^2+\cdots$. In $k[x_1,y_1,y_2]$ we have $G = \sum_{n\ge1} F_y^{(n)}(x_1,y_2)(y_1-y_2)^{n-1}$, with $F_y^{(n)}$ the Hasse derivatives in y; as $\tau(y_1-y_2) = \partial y\,t+\cdots$, we get $\tau(G) = F_y + (F_{xy} + F_{yy}^{(2)}\,\partial y)t + \cdots$. Hence $\tau(R_0(u)) = F_y\,\partial u + (F_y\,\partial^{(2)}u + (F_{xy} + F_{yy}^{(2)}\partial y)\,\partial u)t + \cdots$, which gives $\mu(R_0(u)) = D(u)$ and, since $F_y\,\partial y = Dy = -F_x$, $\mu(D_1R_0(u)) = E(u)$ with E as in (1).

The product rule in (2) follows from (1) and $\partial^{(2)}(uv) = u\partial^{(2)}v + \partial u\,\partial v + v\partial^{(2)}u$; $E(x)$ is read on (1). For $E(y)$: $(y_1-y_2)G = F(x_1,y_1) - F(x_1,y_2) = -\big(F(x_1,y_2)-F(x_2,y_2)\big)$, so $R_0(y) = -\sum_{n\ge1} F_x^{(n)}(x_2,y_2)(x_1-x_2)^{n-1}$, $\tau(R_0(y)) = -F_x - F_{xx}^{(2)}t - \cdots$ and $E(y) = -F_yF_{xx}^{(2)}$. A k-linear map satisfying (2) is determined by its values on x and y. For p odd, $D^2 = F_y\partial(F_y\partial) = 2F_y^2\partial^{(2)} + F_y(F_{xy}+2F_{yy}^{(2)}\partial y)\partial$, whence $E = \frac12(D^2 + F_{xy}D)$. □

5. Proof of Theorem 4 and of Proposition 5

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 14 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 3. So $\operatorname{tr}_k(T) = \sum_j \langle T\bar m_j, \bar t_j\rangle$ for every endomorphism T of $\mathbf{F}_\pi$, and with Lemma 12

$$\operatorname{tr}_k(M_u\circ\delta_\pi) = \sum_j \langle u\,D(m_j), t_j\rangle = \langle u, \Theta\rangle, \qquad \Theta := \sum_j D(m_j)\,t_j = \mu(D_1R).$$

By (4) and Lemma 15,

$$\Theta = \mu(D_1R_0) - \mu\big(D_1(\pi_1\varkappa)\big) = E(\pi) - D\pi\cdot\mu(\varkappa) - \pi\,\mu(D_1\varkappa) \equiv E(\pi) + K_\pi D\pi \pmod\pi.$$

By Lemmas 11 and 12, $\operatorname{Tr}(u\lambda_0) = \langle u,\Theta\rangle = \operatorname{Tr}(u\,\Theta/D\pi)$ for all $u\in\mathbf{F}_\pi$, so $\lambda_0 = \Theta/D\pi$ in $\mathbf{F}_\pi$, and Proposition 10 gives the theorem.

For Proposition 5, grade $A\otimes A$ by the degree in the first variable. The monomials occurring in G in the first variable are y^l, $l\le a-1$, and x^iy^l with $ai+b(l+1)<ab$; so G has first degree $b(a-1)$, and $(\pi_1-\pi_2)G$ has first degree at most $d+ab-b$. Multiplication by x_1-x_2 raises the first degree by exactly a, so R_0 has first degree at most $d+ab-a-b = d+2g-1$. The decomposition (4) is obtained by removing, in decreasing order, the components $m_{d+s}\otimes r$ with

$s \in S$ by subtracting a multiple of $\pi_1(m_s \otimes r)$, which has first degree $d+s$; so only $s \leq 2g-1$ occur. If $R_0 \in V_d \otimes A$ then $\varkappa = 0$ by uniqueness. □

6. The curves $y^a = f(x)$

Proof of Proposition 6. Here $G = (y_1^a - y_2^a)/(y_1 - y_2)$. Write $P(T_1) - P(T_2) = (T_1 - T_2)Q(T_1, T_2)$ and $f(X_1) - f(X_2) = (X_1 - X_2)\Phi(X_1, X_2)$. Then $(\pi_1 - \pi_2)G = Q(y_1, y_2)(y_1^a - y_2^a) = Q(y_1, y_2)(x_1 - x_2)\Phi(x_1, x_2)$, so $R_0 = Q(y_1, y_2)\Phi(x_1, x_2)$. In the first variable R_0 is a combination, with coefficients in A, of the elements $y^l x^i$ with $0 \leq l \leq n-1$, $0 \leq i \leq b-1$. Write $l = J + ae$ with $0 \leq J < a$; then $y^l x^i = y^J f^e x^i$ is a combination of monomials $x^I y^J$ with $I \leq be + b - 1$. Let $J' \in [0, a)$ be congruent to $J - n$ modulo a and $m = (n - J + J')/a$. Then $\deg(x^I y^J) - d = aI + bJ - bn = a(I - bm) + bJ'$, which belongs to S if and only if $I \geq bm$. But $n \geq l + 1 = J + ae + 1$ gives $m > e$, so $bm \geq be + b > I$. Hence all these monomials are in V_d and $R_0 \in V_d \otimes A$; by Proposition 5, $K_\pi = 0$ when π is prime. By (2) and induction, $E(y^n) = ny^{n-1}E(y) + \binom{n}{2} y^{n-2} D(y)^2$, so $E(P(y)) = P'(y)E(y) + P^{[2]}(y)D(y)^2$, with $D(y) = f'(x)$, $E(y) = a\, y^{a-1} f^{[2]}(x)$ and $D(P(y)) = P'(y)f'(x)$. Insert in Theorem 4. □

Proof of Theorem 7. With $f' = c \in k^\times$ and $f^{[2]} = 0$, Proposition 6 shows that $\pi = P(y)$ is a Wilson prime if and only if π divides $P^{[2]}(y)$. As $\deg P^{[2]}(y) \leq b(n-2) < bn$, this means $P^{[2]}(y) = 0$ in A, i.e. $P^{[2]} = 0$. The description by exponents follows from Lucas' theorem. □

Lemma 16. *Let $P \in k[T]$ be irreducible with a root θ, and $F = y^a - f(x)$.*

1. *If $f = x^p - x + \alpha$, then $P(y)$ is a prime element of A if and only if $\mathrm{Tr}_{k(\theta)/\mathbb{F}_p}(\theta^a - \alpha) \neq 0$.*
2. *If $p = 2$ and $f = x^4 + x + \alpha$, then $P(y)$ is a prime element of A if and only if $[k(\theta) : \mathbb{F}_2]$ is odd and $\mathrm{Tr}_{k(\theta)/\mathbb{F}_2}(\theta^a + \alpha) = 1$.*

Proof. $A/P(y) \cong L[x]/(f(x) - \theta^a)$ with $L = k(\theta)$. (1) $x^p - x - \beta$ is irreducible over a finite field L of characteristic p if and only if $\mathrm{Tr}_{L/\mathbb{F}_p}(\beta) \neq 0$ [6, Corollary 3.79]. (2) Let $\beta = \theta^a + \alpha$ and ρ a root of $x^4 + x + \beta$; its roots are $\rho + c$, $c \in \mathbb{F}_4$. If $[L : \mathbb{F}_2]$ is even, $\mathbb{F}_4 \subset L$ and the Frobenius of L maps ρ to $\rho + c$ with $2c = 0$, so ρ has degree at most 2 over L. If it is odd, put $u = \rho^2 + \rho$, so $u^2 + u = \beta$: $[L(u) : L] = 2$ if and only if $\mathrm{Tr}_{L/\mathbb{F}_2}(\beta) = 1$, and then $x^2 + x - u$ is irreducible over $L(u)$ because $\mathrm{Tr}_{L(u)/\mathbb{F}_2}(u) = \mathrm{Tr}_{L/\mathbb{F}_2}(1) = 1$, the conjugates of u over L having sum 1. □

Lemma 17. *Let $g \in k[T]$ be monic of degree n_0 with $g(0) \neq 0$, $n_1 < n_0$ the degree of $g - T^{n_0}$, $N \geq 1$, and $\theta_1, \ldots, \theta_n$ the roots of $g(T^N)$ counted with multiplicity, $n = n_0 N$. Then $\sum_i \theta_i^a = 0$ for $1 \leq a < (n_0 - n_1)N$.*

Proof. The elementary symmetric functions $e_1, \ldots, e_a$ of the roots vanish, and Newton's identities express $\sum_i \theta_i^a$ as an integral combination of products involving $e_1, \ldots, e_a$. □

Proof of Theorem 8. (1) Let $P = T^t - c$. As $r^o \equiv 1 \pmod p$, $t \equiv 1 \pmod p$. By [6, Theorem 3.75], $T^t - c$ is irreducible over $\mathbb{F}_p$ if every prime factor of t divides the order e of c in $\mathbb{F}_p^\times$ but not $(p-1)/e$, and $p \equiv 1 \pmod 4$ if $4 \mid t$; here $e = p - 1$, the only prime factor of t is r, and $4 \mid t$ only if $r = 2$, in which case $p \equiv 1 \pmod 4$. By Lemma 17 ($n_0 = 1$, $n_1 = 0$, $N = t > a$), $\mathrm{Tr}_{\mathbb{F}_p(\theta)/\mathbb{F}_p}(\theta^a) = 0$, so $\mathrm{Tr}(\theta^a - \alpha) = -t\alpha = -\alpha \neq 0$ and $P(y)$ is a prime element by Lemma 16. Finally $P^{[2]} = \binom{t}{2} T^{t-2} = 0$ since $p \mid t - 1$; apply Theorem 7.

(2) Let $g = T^4 + T - 1$ and $P_j = g(T^{25^j})$. The polynomial g is irreducible over $\mathbb{F}_3$ and its roots have order 80 (machine verification); as 5 divides 80 but not $(3^4 - 1)/80$, and 25^j is odd, P_j is irreducible by [6, Theorem 3.35] for $j \geq 1$. Its degree $n = 4 \cdot 25^j$ is 1 modulo 3, and by Lemma 17

($n_0 = 4$, $n_1 = 1$) the trace of θ^a vanishes for $a < 3 \cdot 25^j$; so $\mathrm{Tr}(\theta^a - \alpha) = -n\alpha = -\alpha \neq 0$ and $P_j(y)$ is a prime element. Its exponents are 0 or 1 modulo 3; apply Theorem 7. □

Proof of Theorem 9. Here $f = x^4 + x + 1$ satisfies $f' = 1$, $f^{[2]} = 0$, and $\gcd(a, 4) = 1$. Let $g = T^9 + T + 1$ and $P_j = g(T^{73^j})$. The polynomial g is irreducible over $\mathbb{F}_2$ and its roots have order 73 (machine verification); 73 does not divide $(2^9 - 1)/73 = 7$, and 73^j is odd, so P_j is irreducible by [6, Theorem 3.35] for $j \geq 1$. Its degree $n = 9 \cdot 73^j$ is odd, and by Lemma 17 ($n_0 = 9$, $n_1 = 1$) the trace of θ^a vanishes for $a < 8 \cdot 73^j$, so $\mathrm{Tr}_{\mathbb{F}_2(\theta)/\mathbb{F}_2}(\theta^a + 1) = n = 1$ and $P_j(y)$ is a prime element by Lemma 16(2), of degree $4n$. As $73 \equiv 1 \pmod 4$, the exponents $9 \cdot 73^j$, 73^j, 0 are 0 or 1 modulo 4; apply Theorem 7. □

7. Numerical verification

The ancillary script `verify_wilson_plane_curves.py` (pure Python, no argument, about one minute and a half) works over prime fields. For a prime element π of degree d it computes W_d modulo π^2 from Definition 2 (as a plain product when $p^d \leq 4000$, otherwise through the k-linear polynomial $\prod_{v \in V_d}(z - v)$ built one basis vector at a time), builds R_0, R, $\varkappa$, and checks $W_d \equiv -1 \pmod \pi$, $\mu(R_0) = D\pi$, $\mu(D_1 R_0) = E(\pi)$ with E computed from (2), the support of $\varkappa$ (Proposition 5) and the congruence of Theorem 4. Smoothness of each curve is checked by verifying that F_x and F_y generate the unit ideal of A.

- *Theorem 4*: all prime elements, up to units, of degree at most the bound indicated, on the 17 curves of the table: 1124 prime elements, of which 39 are Wilson primes, no failure. The first curve is one of those of [3], and the counts agree with the table given there.
- *Proposition 6, Theorem 7, Lemma 16*: on ten curves $y^a = f(x)$ ($p = 2, 3, 5, 7$; $a = 2, 3, 4, 5$), all irreducible P of small degree: the primality criteria of Lemma 16 on the seven curves where they apply, and, for the 109 prime elements $P(y)$ found, $K_\pi = 0$, the formula for $E(P(y))$, and Theorem 7 on the seven curves satisfying its hypotheses.
- *Families*: the Wilson property is checked from the definition for $y^9 + y + 1$ on $y^3 = x^4 + x + 1$ and on $y^5 = x^4 + x + 1$ over $\mathbb{F}_2$ (degree 36; these are the cases $j = 0$, $a = 3, 5$ of Theorem 9), for $y^4 + y - 1$ on $y^2 = x^3 - x + 1$ over $\mathbb{F}_3$ (degree 12; the case $j = 0$, $a = 2$ of Theorem 8(2)), and for two instances of Theorem 7 not covered by Theorem 8: $y^4 + y - 1$ on $y^5 = x^3 - x + 1$ over $\mathbb{F}_3$ (degree 12) and $y^6 + 3y^5 + y + 1$ on $y^3 = x^5 - x + 1$ over $\mathbb{F}_5$ (degree 30). No member of the family of Theorem 8(1) is checked by the script. The two machine facts used in the proofs of Theorems 8(2) and 9 are checked as well.

p	curve	g	$d \leq$	primes	Wilson (degrees)
3	$y^2 = x^3 + 2x + 2$	1	6	212	15 $(3, 5, 6)$
2	$y^2 + y = x^3 + x + 1$	1	9	120	5 $(2, 5)$
2	$y^2 + xy = x^5 + x^2 + 1$	2	9	65	0
2	$y^3 = x^4 + x + 1$	3	13	61	1 (4)
2	$y^3 + xy + y = x^4 + x^2 + 1$	3	11	48	0
2	$y^3 + y^2 + xy = x^4 + 1$	3	12	203	2 $(4, 12)$
3	$y^3 + y = x^4$	3	9	53	0
3	$y^3 + y^2 = x^4 + 2x + 2$	3	8	74	5 $(4, 6, 7)$
5	$y^3 + xy = x^4 + x + 2$	3	6	24	0
7	$y^3 = x^4 + x + 1$	3	4	7	1 (4)
5	$y^3 = x^2 + 1$	1	4	29	0
3	$y^4 = x^3 - x + 1$	3	9	54	3 $(3, 9)$
3	$y^4 + xy = x^3 + x^2 + 2$	3	8	72	5 $(4, 7)$
2	$y^3 + xy + y = x^5 + 1$	4	11	35	0
2	$y^5 = x^4 + x + 1$	6	14	11	1 (4)
2	$y^4 + y = x^3 + 1$	3	12	31	1 (4)
2	$y^5 + y^2 + xy = x^3 + x + 1$	4	11	25	0

These computations cover prime fields and the listed cases only. The members of the infinite families other than those listed above are not verified numerically; their Wilson property rests on the proofs.

8. Status

Lemma 1, Theorem 4, Propositions 5, 6 and Theorems 7, 8, 9 are proved above; two facts (irreducibility and order of T^4+T-1 over $\mathbb{F}_3$ and of T^9+T+1 over $\mathbb{F}_2$) are machine verifications. Nothing in this note has been checked by a third party, and [1, 2, 3, 4] have not been either. We found no earlier work on Wilson primes outside $\mathbb{F}_q[t]$ in the literature we consulted; we do not claim that this search is exhaustive. Open: the prime ideals that are not principal; an explicit expression of K_π in terms of the leading coefficients of π beyond the hyperelliptic case [3]; infinitely many Wilson primes on the four rings of class number one in characteristic 2 and 3 other than the families of [1].

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

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

[3] D. Niedbala Giraudin, Wilson primes for coordinate rings of hyperelliptic curves with one point at infinity, Hexagon 2611.01011 (2026).

[4] D. Niedbala Giraudin, Infinitely many Wilson primes on the curves $y^2 = x^p - x + a$, Hexagon 2611.01015 (2026).

[5] 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.

[6] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, 1997.

[7] S. Miura, Algebraic geometric codes on certain plane curves, Electron. Comm. Japan Part III **76** (1993), no. 12, 1–13.

[8] J. Sauerberg, L. Shu, D. S. Thakur, G. Todd, Infinitude of Wilson primes for $\mathbb{F}_q[t]$, Acta Arith. **157** (2013), no. 1, 91–100.

[9] D. S. Thakur, Differential characterization of Wilson primes for $\mathbb{F}_q[t]$, Algebra Number Theory **7** (2013), no. 8, 1841–1848.
[10] 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