hexagon:2611.01015v1

INFINITELY MANY WILSON PRIMES ON THE CURVES $y^2 = x^p - x + a$

DAVID NIEDBALA GIRAUDIN

Abstract. For an odd prime p and $a \in \mathbb{F}_p^\times$ let $A = \mathbb{F}_p[x,y]/(y^2 - x^p + x - a)$, the coordinate ring of a curve of genus $(p-1)/2$ with one point at infinity. With the notion of Wilson prime of [2], we prove: if $P \in \mathbb{F}_p[y]$ is irreducible and $P(y)$ is a prime element of A, then $P(y)$ is a Wilson prime if and only if $P'' = 0$. We deduce that each of these rings has infinitely many Wilson primes, given explicitly: for $p \geq 5$ the binomials $y^t - c$, with c a primitive root modulo p and t running through the powers of a suitable prime divisor of $p-1$ that are congruent to 1 modulo p. The proof rests on the criterion of [2] and on the fact that, on any curve $y^2 = f(x)$ in odd characteristic, the correction term of that criterion vanishes for the prime elements that are polynomials in y.

1. Statements

We use the setting and notation of [2]. Let $k = \mathbb{F}_q$ of odd characteristic p, $f \in k[x]$ monic of odd degree $\gamma = 2g+1 \geq 3$ such that the affine curve $y^2 = f(x)$ is smooth, and $A = k[x,y]/(y^2 - f)$. Then $\deg x = 2$, $\deg y = \gamma$ for $\deg = -\operatorname{ord}_\infty$; $S = \{0, 2, 4, \dots\} \cup \{\gamma, \gamma+2, \dots\}$; the monomials m_j ($j \in S$), $m_j = x^{j/2}$ or $x^{(j-\gamma)/2}y$, form a k-basis of A with $\deg m_j = j$; for $d \in S$, $d \geq 2$, V_d is the span of the m_j with $j \in S$, $j - d \notin S$ and W_d is the product of the non-zero elements of V_d. A prime element π of degree d is a *Wilson prime* if $W_d \equiv -1 \pmod{\pi^2}$. Let D be the derivation of A with $Dx = 2y$, $Dy = f'(x)$. By [2, Theorem 3] (here $h = 0$, so $E = \frac{1}{2}D^2$),

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

where $K_\pi = -\mu(\varkappa)$ and $\varkappa$ is defined by the decomposition $R_0 = R + \pi_1\varkappa$, $R \in V_d \otimes A$, of the element $R_0 \in A \otimes A$ such that $(x_1 - x_2)R_0 = (\pi_1 - \pi_2)(y_1 + y_2)$. Here $a_1 = a \otimes 1$, $a_2 = 1 \otimes a$ and μ is the multiplication.

Proposition 1. *Let $P \in k[T]$ be of degree $n \geq 1$ and such that $\pi = P(y)$ is a prime element of A. Then $R_0 \in V_d \otimes A$, where $d = \gamma n$; hence $\varkappa = 0$ and $K_\pi = 0$.*

Corollary 2. *With the same hypotheses,*

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

So $P(y)$ is a Wilson prime if and only if $P(y)$ divides $P''(y)f'(x)^2 + 2y\, f''(x)P'(y)$.

Theorem 3. *Assume that f' is a non-zero constant (for instance $f = x^p - x + a$). 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 $P'' = 0$.*

Date: 24 November 2026.

Note that $y^2 = f(x)$ is automatically smooth when f' is a non-zero constant. In particular every prime element of the form $y - c$ is then a Wilson prime. For some f with constant derivative no $P(y)$ is a prime element (for instance $f = x^9 - x + a$ over $\mathbb{F}_3$), and the theorem is then empty.

Theorem 4. *Let $p \geq 5$ be a prime, $a \in \mathbb{F}_p^\times$ and $A = \mathbb{F}_p[x,y]/(y^2 - x^p + x - a)$. 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 let c be a primitive root modulo p. Then for every $j \geq 1$, with $t = r^{oj}$,*

$$y^t - c$$

is a Wilson prime of A, of degree pt. In particular A has infinitely many Wilson primes.

Such an r exists: if $p \equiv 3 \pmod 4$ then $(p-1)/2$ is odd and at least 3.

Theorem 5. *Let $p = 3$, $a \in \{1, 2\}$ and $A = \mathbb{F}_3[x,y]/(y^2 - x^3 + x - a)$. For every $j \geq 0$, $y^{4 \cdot 25^j} + y^{25^j} - 1$ is a Wilson prime of A of degree $12 \cdot 25^j$.*

For $a = 2$ this is [1, Theorem 5]. So for every odd prime p and every $a \in \mathbb{F}_p^\times$ the ring $\mathbb{F}_p[x,y]/(y^2 - x^p + x - a)$, of genus $(p-1)/2$, has infinitely many Wilson primes. For $\mathbb{F}_q[t]$, infinitely many Wilson primes were exhibited for many q by Sauerberg, Shu, Thakur and Todd [4], and for every q by Thakur [5, Theorem 2.10]. Theorem 3 is the exact analogue, with y in the role of t, of Thakur's criterion for $\mathbb{F}_q[t]$ [5, Theorem 2.9], and the families of Theorems 4, 5 are built with the classical irreducibility theorems that are also used in [4, 5]. The question of generalising these phenomena to other function fields is [6, §7.5, Question (2)].

2. Proofs

Proof of Proposition 1. Write $P(T_1) - P(T_2) = (T_1 - T_2)Q(T_1, T_2)$ and $f(X_1) - f(X_2) = (X_1 - X_2)\Phi(X_1, X_2)$; Q has degree $n-1$ in T_1 and Φ has degree $\gamma - 1$ in X_1. Then

$$(\pi_1 - \pi_2)(y_1 + y_2) = Q(y_1, y_2)\,(y_1^2 - y_2^2) = Q(y_1, y_2)\,(x_1 - x_2)\,\Phi(x_1, x_2),$$

so $R_0 = Q(y_1, y_2)\Phi(x_1, x_2)$, as $A \otimes A$ is a domain. In the first variable R_0 is a combination, with coefficients in A, of the elements $y^i x^j$ with $0 \leq i \leq n-1$, $0 \leq j \leq \gamma - 1$. It suffices to show that these elements lie in V_d. Now $y^i x^j = y^\epsilon f^{\lfloor i/2 \rfloor} x^j$ with $\epsilon \in \{0, 1\}$, $\epsilon \equiv i \pmod 2$; this is a combination of monomials m_l with $l \equiv i \pmod 2$ (because γ is odd, $\deg x^b y^\epsilon = 2b + \epsilon\gamma \equiv \epsilon$) and $l \leq \gamma i + 2j$.

If $i \leq n-2$, then $l \leq \gamma(n-2) + 2(\gamma - 1) = d - 2$, so $l - d < 0$ and $m_l \in V_d$.

If $i = n-1$, then $l - d \equiv (n-1) - \gamma n \equiv 1 \pmod 2$ and $l - d \leq \gamma(n-1) + 2(\gamma - 1) - \gamma n = \gamma - 2$. An odd integer smaller than γ is not in S, so $m_l \in V_d$.

Hence $R_0 \in V_d \otimes A$, and by uniqueness of the decomposition, $R = R_0$, $\varkappa = 0$. □

Proof of Corollary 2. $D\pi = P'(y)f'(x)$ and $D^2\pi = P''(y)f'(x)^2 + P'(y)\,f''(x)\,2y$. Insert this and $K_\pi = 0$ in (1). □

Proof of Theorem 3. Here $f'' = 0$ and $f' = c \in k^\times$, so by Corollary 2, $\pi = P(y)$ is a Wilson prime if and only if π divides $P''(y)$. But $\deg P''(y) \leq \gamma(n-2) < \gamma n = \deg \pi$, so this means $P''(y) = 0$ in A, i.e. $P'' = 0$, as $k[y] \subset A$ is a polynomial ring. □

Lemma 6. *Let $f = x^p - x + a$, $a \in k$, and let $P \in k[T]$ be irreducible with a root θ. Then $P(y)$ is a prime element of A if and only if $\mathrm{Tr}_{k(\theta)/\mathbb{F}_p}(\theta^2 - a) \neq 0$.*

Proof. $A = k[y][x]/(x^p - x - (y^2 - a))$, so $A/P(y) \cong k(\theta)[x]/(x^p - x - (\theta^2 - a))$. A polynomial $x^p - x - \beta$ over a finite field F of characteristic p is irreducible if and only if $\mathrm{Tr}_{F/\mathbb{F}_p}(\beta) \neq 0$ [3, Corollary 3.79]. □

Proof of Theorem 4. Let $P = T^t - c$. As $r^o \equiv 1 \pmod p$, we have $t \equiv 1 \pmod p$ and $t > p$. *Irreducibility.* By [3, 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, which divides $p-1$, and $4 \mid t$ only if $r = 2$, in which case $p \equiv 1 \pmod 4$ by the choice of r. *Primality.* As P is irreducible of degree t, $\mathrm{Tr}_{\mathbb{F}_p(\theta)/\mathbb{F}_p}(\theta^2)$ is the sum of the squares of the roots of P, which is $e_1^2 - 2e_2 = 0$ because $t \geq 3$; so $\mathrm{Tr}_{\mathbb{F}_p(\theta)/\mathbb{F}_p}(\theta^2 - a) = -ta = -a \neq 0$, and $P(y)$ is a prime element by Lemma 6, of degree $\gamma t = pt$. *Wilson property.* $P'' = t(t-1)T^{t-2} = 0$ since $p \mid t - 1$; apply Theorem 3. □

Proof of Theorem 5. Let $P_j = T^{4 \cdot 25^j} + T^{25^j} - 1$. It is irreducible over $\mathbb{F}_3$: for $j = 0$ directly, and for $j \geq 1$ by [3, Theorem 3.35], as in [1] (the roots of P_0 have order 80, and 5 divides 80 but not $(3^4 - 1)/80$). Its degree is $n \equiv 1 \pmod 3$, the coefficients of T^{n-1} and T^{n-2} vanish, so the sum of the squares of its roots is 0 and $\mathrm{Tr}(\theta^2 - a) = -na = -a \neq 0$ and $P_j(y)$ is a prime element; and $P_j'' = 0$ because all exponents are congruent to 0 or 1 modulo 3. Apply Theorem 3. □

3. Numerical verification

The ancillary script `verify_wilson_artin_schreier.py` (pure Python) works with $f = x^p - x + a$ over $\mathbb{F}_p$ only; the general statements of Proposition 1 and Corollary 2 (other f, other fields) are not tested by it.

Part 1. For $(p, a) = (3,1), (3,2), (5,1), (5,3), (7,2), (11,1)$ and all monic irreducible P of degree at most $5, 5, 3, 3, 2, 1$ respectively (309 polynomials), it decides whether $P(y)$ is a prime element by Lemma 6; for the 227 prime elements it computes W_d modulo π^2 from the definition, checks $W_d \equiv -1 \pmod \pi$, checks that $R_0 \in V_d \otimes A$, and compares the Wilson property with the condition $P'' = 0$. There is no discrepancy; 38 of these prime elements are Wilson primes.

Part 2. For $y^4 + y - 1$ ($p = 3$, $a = 1, 2$, degree 12) and for $y^{16} - 2$, $y^{16} - 3$, $y^{16} - 2$ ($p = 5$, $a = 1, 2, 4$, degree 80) it checks the irreducibility of P, the primality of $P(y)$, and the Wilson property from the definition.

With a second program (FLINT library) the Wilson property was also verified from the definition for $y^{27} - 2$ and $y^{27} - 6$ on $y^2 = x^{13} - x + a$, $a = 1, 5$ (genus 6, degree 351), and 88 further prime elements $P(y)$ with $P'' = 0$, for $p = 3, 5, 7$ and of degree up to 56, were found to be Wilson primes from the definition.

4. Status and questions

Proposition 1, Corollary 2 and Theorems 3, 4, 5 are proved above, on the basis of [2, Theorem 3]. Nothing in this note has been checked by a third party, and [2] has not been either. For $p = 7$, 11, 17 the smallest member of the family of Theorem 4 has degree $7 \cdot 3^6$, $11 \cdot 5^5$, $17 \cdot 2^8$; for these W_d was not computed. Open: the case $a = 0$; the Wilson primes of these rings that are not polynomials in y; and the infinitude of Wilson primes for other curves, in particular in characteristic 2 and for ordinary elliptic curves.

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 coordinate rings of hyperelliptic curves with one point at infinity, Hexagon 2611.01011 (2026).

[3] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, 1997.
[4] J. Sauerberg, L. Shu, D. S. Thakur, G. Todd, Infinitude of Wilson primes for $\mathbb{F}_q[t]$, Acta Arith. **157** (2013), 91–100.
[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