Annals of the University of Craiova
Mathematics and Computer Science Series

Vol. LIII, Issue 1, June 2026

Volume Editors: Ionel Rovenţa, Mihaela Sterpu

Layout Editor: Mihai Gabroveanu

ISSN 1223-6934

Online ISSN 2246-9958

Web: http://inf.ucv.ro/∼ami/

Printed in Romania: Editura Universitaria, Craiova, 2026

http://www.editurauniversitaria.ro

Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 53(1), 2026, Pages 1–6, DOI: 10.52846/ami.v53i1.1957
ISSN: 1223-6934

Cryptography on Binary Edwards Curves over the Ring $\mathbb{F}_{2^n}[\varepsilon]$; $\varepsilon^3 = 0$

Moha Ben Taleb El Hamam and Abdelhakim Chillali

Abstract. Let n be a positive integer, in this paper, we study binary Edwards curves defined over the finite local ring $B_3 = \mathbb{F}_{2^n}[\varepsilon]$ with $\varepsilon^3 = 0$ and outline the resulting cryptographic implications.

2020 *Mathematics Subject Classification.* 11G05, 14G50, 94A60.
Key words and phrases. Binary Edwards curves, local rings, elliptic curves, cryptography.

1. Introduction

Edwards curves, introduced by H. Edwards in 2007, offer an elegant and highly symmetric model for elliptic curves with complete and efficient addition laws [1]. Binary Edwards curves, introduced by Bernstein et al [2], provide a parallel construction over fields of characteristic 2, particularly relevant for lightweight and hardware-oriented cryptography.

Several recent works [4, 5, 6, 7, 8, 9, 10, 11, 12] have extended classical elliptic curves to algebraic structures defined over rings such as $\mathbf{F}_q[\varepsilon]$ with relations $\varepsilon^2 = 0$, $\varepsilon^3 = 0$, $\varepsilon^2 = \varepsilon$ or $\varepsilon^3 = \varepsilon^2$.

In this paper, we study the arithmetic of the ring $\mathbb{F}_{2^n}[\varepsilon]$ with $\varepsilon^3 = 0$, and we define binary Edwards curves $E_{B_{a,d}}(B_3)$ over this ring. We then construct the corresponding group extension $E_{B_{a,d}}(B_3)$ of $E_{B_{a_0,d_0}}$, and provide an explicit bijection between the groups $E_{B_{a,d}}(B_3)$ and $E_{B_{a_0,d_0}} \times \mathbb{F}_{2^n}^2$, where $E_{B_{a_0,d_0}}(\mathbb{F}_{2^n})$ denotes the binary Edwards curve over the finite field $\mathbb{F}_{2^n}$.

Finally, we discuss the cryptographic implications of this construction. In particular, we show that the discrete logarithm problem in $E_{B_{a,d}}(B_3)$ is equivalent to the discrete logarithm problem in $E_{B_{a_0,d_0}}(\mathbb{F}_{2^n}) \times \mathbb{F}_{2^n}^2$, and that $\#E_{B_{a,d}}(B_3) = 2^{2n} \#E_{B_{a_0,d_0}}$.

2. Notation and ring arithmetic

Let $B_3 = \frac{\mathbb{F}_{2^n}[X]}{(X^3)}$ be a local ring, where $\mathbb{F}_{2^n}$ is the finite field of order 2^n with n a positive integer. This ring is identified by $\mathbb{F}_{2^n}[\varepsilon]$ where $\varepsilon^3 = 0$. Consequently, B_3 admits the representation: $B_3 = \{x_0 + x_1\varepsilon + x_2\varepsilon^2 \mid (x_0, x_1, x_2) \in (\mathbb{F}_{2^n})^3\}$.

Let X and Y be two elements in B_3, written as

$$X = x_0 + x_1\varepsilon + x_2\varepsilon^2, \quad Y = y_0 + y_1\varepsilon + y_2\varepsilon^2.$$

Received May 19, 2024. Accepted August 9, 2025.

Using the relation $\varepsilon^3 = 0$, their sum and product are given by

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2,$$
$$X \cdot Y = x_0y_0 + (x_0y_1 + x_1y_0)\varepsilon + (x_0y_2 + x_1y_1 + x_2y_0)\varepsilon^2.$$

The following results can easily be verified (see [3]):

- $(B_3, +, \cdot)$ is a finite unitary commutative ring.
- B_3 is an $\mathbb{F}_{2^n}$-vector space of dimension 3 and of basis $\{1, \varepsilon, \varepsilon^2\}$.
- Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 \in B_3$, X is invertible if and only if $x_0 \not\equiv 0 \pmod 2$, in this case:
  - $X^{-1} = x_0^{-1} - x_1x_0^{-2}\varepsilon + (x_1^2x_0^{-3} - x_2x_0^{-2})\varepsilon^2$.
  - X is not invertible if and only if $x_0 \equiv 0 \pmod 2$.
  - B_3 is a local ring, its maximal ideal is $M = (\varepsilon) = \varepsilon\mathbb{F}_{2^n}$.
- We consider the canonical projection τ defined by

$$\begin{array}{rccc} \tau & : & B_3 & \longrightarrow & \mathbb{F}_{2^n} \\ & & x_0 + x_1\varepsilon + x_2\varepsilon^2 & \longmapsto & x_0 \end{array}$$

  is a surjective homomorphism of rings.

3. Binary Edwards curves over B_3

Fix parameters $a = a_0 + a_1\varepsilon + a_2\varepsilon^2$ and $d = d_0 + d_1\varepsilon + d_2\varepsilon^2$ in B_3. We define the binary Edwards curve over B_3 by the affine equation

$$a(X + Y) + d(X^2 + Y^2) = XY + XY(X + Y) + X^2Y^2,$$

such that a and $d + a^2 + a$ are invertible in B_3. We denote it by $E_{B_{a,d}}(B_3)$.

i.e. $E_{B_{a,d}}(B_3) : a(X + Y) + d(X^2 + Y^2) = XY + XY(X + Y) + X^2Y^2$.

Lemma 3.1. *The element $d + a^2 + a$ is invertible in B_3 if and only if*

$$d_0 + a_0^2 + a_0 \neq 0 \quad \text{in } \mathbf{F}_{2^n}.$$

Proof. Compute a^2 in characteristic 2 and $\varepsilon^3 = 0$, we have

$$a^2 = (a_0 + a_1\varepsilon + a_2\varepsilon^2)^2 = a_0^2 + a_1^2\varepsilon^2.$$

Then

$$d + a^2 + a = (d_0 + a_0^2 + a_0) + (d_1 + a_1)\varepsilon + (d_2 + a_2 + a_1^2)\varepsilon^2.$$

By the units characterization in B_3, this element is invertible if and only if its constant term is nonzero, i.e. $d_0 + a_0^2 + a_0 \neq 0$. □

Using Lemma 3.1, if both a and $d+a^2+a$ are invertible in B_3, then $E_{B_{\tau(a),\tau(d)}}(\mathbb{F}_{2^n})$ defines a binary Edwards curve over the finite field $\mathbb{F}_{2^n}$. We denote this curve by $E_{B_{a_0,d_0}}$.

Theorem 3.2. *Let $X = \tilde{x} + x_2\varepsilon^2$, $Y = \tilde{y} + y_2\varepsilon^2$, $a = \tilde{a} + a_2\varepsilon^2$, $d = \tilde{d} + d_2\varepsilon^2$ be elements of B_3 such that*

$$a(X + Y) + d(X^2 + Y^2) = XY + XY(X + Y) + X^2Y^2.$$

Then

$$\tilde{a}(\tilde{x} + \tilde{y}) + \tilde{d}(\tilde{x}^2 + \tilde{y}^2) = \tilde{x}\tilde{y} + \tilde{x}\tilde{y}(\tilde{x} + \tilde{y}) + \tilde{x}^2\tilde{y}^2 + (E + Fx_2 + Gy_2)\varepsilon^2,$$

where

$$E = -a_2(x_0 + y_0) - d_2(x_0^2 + y_0^2), \qquad F = y_0 + y_0^2 - a_0 \qquad \text{and} \qquad G = x_0 + x_0^2 - a_0.$$

Proof. We have

$$\begin{aligned} a(X+Y) &= \tilde{a}(\tilde{x}+\tilde{y}) + \big(\tilde{a}(x_2+y_2) + a_2(\tilde{x}+\tilde{y})\big)\varepsilon^2, \\ d(X^2+Y^2) &= \tilde{d}(\tilde{x}^2+\tilde{y}^2) + d_2(\tilde{x}^2+\tilde{y}^2)\varepsilon^2, \\ XY &= \tilde{x}\tilde{y} + (\tilde{x}y_2 + \tilde{y}x_2)\varepsilon^2, \\ XY(X+Y) &= \tilde{x}\tilde{y}(\tilde{x}+\tilde{y}) + (\tilde{x}^2y_2 + \tilde{y}^2x_2)\varepsilon^2, \\ X^2Y^2 &= \tilde{x}^2\tilde{y}^2. \end{aligned}$$

If $a(X+Y) + d(X^2+Y^2) = XY + XY(X+Y) + X^2Y^2$, then

$$\tilde{a}(\tilde{x}+\tilde{y}) + \tilde{d}(\tilde{x}^2+\tilde{y}^2) = \tilde{x}\tilde{y} + \tilde{x}\tilde{y}(\tilde{x}+\tilde{y}) + \tilde{x}^2\tilde{y}^2 + (E + Fx_2 + Gy_2)\varepsilon^2,$$

where

$$E = -a_2(x_0 + y_0) - d_2(x_0^2 + y_0^2), \qquad F = y_0 + y_0^2 - a_0 \qquad \text{and} \qquad G = x_0 + x_0^2 - a_0.$$

□

Corollary 3.3. *If $(X, Y) \in E_{B_{a,d}}(B_3)$, then $(x_0, y_0) \in E_{B_{a_0,d_0}}$.*

Proof. If $(X, Y) \in E_{B_{a,d}}(B_3)$, then $a(X+Y)+d(X^2+Y^2) = XY+XY(X+Y)+X^2Y^2$. So, by Theorem 3.2 we have

$$a_0(x_0 + y_0) + d_0(x_0^2 + y_0^2) = x_0y_0 + x_0y_0(x_0 + y_0) + x_0^2y_0^2 + A\varepsilon + D\varepsilon^2.$$

Or $(1, \varepsilon, \varepsilon^2)$ is a basis of B_3, then $a_0(x_0+y_0)+d_0(x_0^2+y_0^2) = x_0y_0+x_0y_0(x_0+y_0)+x_0^2y_0^2$. Thus $(x_0, y_0) \in E_{B_{a_0,d_0}}$. □

4. The addition law on the binary Edwards curve $E_{B_{a,d}}(B_3)$

The authors of [2] introduced an explicit addition law for the binary Edwards curve $E_{B,\tau_i(a),\tau_i(d)}(\mathbb{F}_{2^n})$. This addition formula is strongly unified, meaning that it applies both to the addition of two distinct points and to the doubling case where the two inputs coincide.

Given two points (X_1, Y_1) and (X_2, Y_2) on the binary Edwards curve $E_{B_{a,d}}(B_3)$, the sum $(X_3, Y_3) = (X_1, Y_1) + (X_2, Y_2)$, when it is defined, is computed as follows:

$$X_3 = \frac{a(X_1 + X_2) + d(X_1 + Y_1)(X_2 + Y_2) + (X_1 + X_1^2)(X_2(Y_1 + Y_2 + 1) + Y_1Y_2)}{a + (X_1 + X_1^2)(X_2 + Y_2)}, \quad (1)$$

$$Y_3 = \frac{a(Y_1 + Y_2) + d(X_1 + Y_1)(X_2 + Y_2) + (Y_1 + Y_1^2)(Y_2(X_1 + X_2 + 1) + X_1X_2)}{a + (Y_1 + Y_1^2)(X_2 + Y_2)}. \quad (2)$$

If the denominators $\tau(a + (X_1 + X_1^2)(X_2 + Y_2))$ and $\tau(a + (Y_1 + Y_1^2)(X_2 + Y_2))$ are nonzero then the sum (X_3, Y_3) is a point in $E_{B_{a,d}}(B_3)$, with $(0, 0)$ is the neutral element and $-(X_1, Y_1) = (Y_1, X_1)$.

Lemma 4.1. *The projection*

$$\begin{array}{rccc} \tilde{\tau} & : & E_{B_{a,d}}(B_3) & \to & E_{B_{a_0,d_0}}, \\ & & (X,Y) & \mapsto & (\tau(X),\tau(Y)). \end{array}$$

is a surjective morphism of groups.

Proof. Let $(x_0,y_0) \in E_{B_{a_0,d_0}}$. Then there exists a point $(X,Y) \in E_{B_{a,d}}(B_3)$ such that

$$\tilde{\tau}(X,Y) = (x_0,y_0).$$

By Theorem 3.2, we obtain

$$a_0(x_0+y_0) + d_0(x_0^2+y_0^2) = x_0y_0 + x_0y_0(x_0+y_0) + x_0^2y_0^2 + (E + Fx_2 + Gy_2)\,\varepsilon^2,$$

and since $(1,\varepsilon,\varepsilon^2)$ forms a basis of B_3, we necessarily have

$$E = -(Fx_2 + Gy_2).$$

Define

$$f(x,y) = a_0(x+y) + d_0(x^2+y^2) - xy - xy(x+y) - x^2y^2.$$

Then the partial derivatives at (x_0,y_0) satisfy

$$\frac{\partial f}{\partial x}(x_0,y_0) = a_0 - y_0 - y_0^2 = -F, \qquad \frac{\partial f}{\partial y}(x_0,y_0) = a_0 - x_0 - x_0^2 = -G.$$

The coefficients $-F$ and $-G$ are the partial derivatives of f at the point (x_0,y_0), and cannot both vanish simultaneously. Therefore (x_2,y_2) exists, which shows that $\tilde{\tau}$ is surjective. □

Lemma 4.2. *The mapping*

$$\begin{array}{rccc} \vartheta & : & \mathbb{F}_{2^n}^2 & \to & E_{B_{a,d}}(B_3), \\ & & (x_1,x_2) & \mapsto & (x_1\varepsilon + x_2\varepsilon^2, x_1\varepsilon + (a_0^{-1}x_1^2 - x_2)\varepsilon^2) \end{array}$$

is an injective homomorphism.

Proof. Evidently, ϑ is well defined and injective.

Let $x_1,x_2,y_1,y_2 \in \mathbb{F}_{2^n}$, $P = (x_1\varepsilon + x_2\varepsilon^2, x_1\varepsilon + (a_0^{-1}x_1^2 - x_2)\varepsilon^2)$ and $Q = (y_1\varepsilon + y_2\varepsilon^2, y_1\varepsilon + (a_0^{-1}y_1^2 - y_2)\varepsilon^2)$. By (1), (2). We have:

$$P + Q = \left((x_1+y_1)\varepsilon + (x_2+y_2)\varepsilon^2, (x_1+y_1)\varepsilon + (a_0^{-1}(x_1+y_1)^2 - (x_2+y_2))\varepsilon^2\right),$$

then $\vartheta((x_1,x_2)+(y_1,y_2)) = \vartheta(x_1+y_1,x_2+y_2) = \vartheta(x_1,x_2)+\vartheta(y_1,y_2)$, and we conclude that ϑ is injective homomorphism of groups. □

Corollary 4.3. *Let $S = \vartheta(\mathbb{F}_{2^n}^2)$, then $S = \ker(\tilde{\tau})$.*

Proof. Let $(x_1\varepsilon + x_2\varepsilon^2, x_1\varepsilon + (a_0^{-1}x_1^2 - x_2)\varepsilon^2) \in S$, then $\tilde{\tau}(x_1\varepsilon + x_2\varepsilon^2, x_1\varepsilon + x_2\varepsilon^2) = (0,0)$. We conclude that $(x_1\varepsilon + x_2\varepsilon^2, x_1\varepsilon + (a_0^{-1}x_1^2 - x_2)\varepsilon^2) \in \ker(\tilde{\tau})$, thus $S \subset \ker(\tilde{\tau})$. Let $P = (X,Y) \in \ker(\tilde{\tau})$, then $\tilde{\tau}(X,Y) = (0,0)$. So, $X = x_1\varepsilon + x_2\varepsilon^2$ and $Y = y_1\varepsilon + y_2\varepsilon^2$ where $(X,Y) \in E_{B_{a,d}}(B_3)$.

If $(X,Y) \in E_{B_{a,d}}(B_3)$, we have

$$a(X+Y) + d(X^2+Y^2) = a_0(x_1+y_1)\varepsilon + a_0(x_2+y_2)\varepsilon^2 + d_0(x_1+y_1)\varepsilon^2,$$

$$XY + XY(X+Y) + X^2Y^2 = x_1y_1\varepsilon^2.$$

Therefore, $x_1 = y_1$ and $y_2 = a_0^{-1}x_1^2 - x_2$. then $(X, Y) = (x_1\varepsilon + x_2\varepsilon^2, x_1\varepsilon + (a_0^{-1}x_1^2 - x_2)\varepsilon^2)$. Thus $\ker(\tilde{\tau}) \subset S$. Finally, $S = \ker(\tilde{\tau})$. □

Remark 4.1. Since $\vartheta(\mathbb{F}_{2^n}^2)$ is isomorphic to $\mathbb{F}_{2^n}^2$, it follows that $S \cong \mathbb{F}_{2^n}^2$. Hence, S is an abelian 2-group of order 2^{2n}.

Theorem 4.4. *The sequence*

$$0 \longrightarrow S \longrightarrow E_{B_{a,d}}(B_3) \longrightarrow E_{B_{a_0,d_0}} \longrightarrow 0$$

is a short exact sequence which defines the group extension $E_{B_{a,d}}(B_3)$ of $E_{B_{a_0,d_0}}$ by S.

Proof. $\tilde{\tau}$ is a surjective homomorphism of groups, $S = \vartheta(\mathbb{F}_{2^n}^2) = \ker(\tilde{\tau})$ and ϑ is an injective homomorphism. We deduce the sequence

$$0 \longrightarrow S \longrightarrow E_{B_{a,d}}(B_3) \longrightarrow E_{B_{a_0,d_0}} \longrightarrow 0$$

is a short exact sequence which defines the group extension $E_{B_{a,d}}(B_3)$ of $E_{B_{a_0,d_0}}$ by S. □

Corollary 4.5.

$$\#E_{B_{a,d}}(B_3) \;=\; 2^{2n} \cdot \#E_{B_{a_0,d_0}}.$$

Proof. This follows from the exact sequence: $|E_{B_{a,d}}(B_3)| = |\ker(\tilde{\tau})| \cdot |\operatorname{Im}(\tilde{\tau})| = 2^{2n} \cdot |E_{B_{a_0,d_0}}|$. □

Theorem 4.6. *If $\#E_{B_{a_0,d_0}}$ is odd, then the exact sequence splits and*

$$E_{B_{a,d}}(B_3) \cong E_{B_{a_0,d_0}} \times \mathbf{F}_{2^n}^2.$$

Proof. Let $N = \#E_{B_{a_0,d_0}}$. If N is odd then there exists an integer b such that $Nb \equiv 1 \pmod 2$, i.e. $1 - Nb$ is even. Set $t = 1 - Nb = 2c$ for some integer c. Define the endomorphism ψ of $E_{B_{a,d}}(B_3)$ by $\psi(P) = tP$. For any $P \in \ker(\tilde{\tau})$ we have $N\tilde{\tau}(P) = \tilde{\tau}(NP) = \tilde{\tau}(0) = 0$, hence $NP \in \ker(\tilde{\tau})$. But elements of $\ker(\tilde{\tau})$ have 2-power order. Therefore NbP lies in $\ker(\tilde{\tau})$. Thus, there exists a morphism $\sigma : E_{B_{a_0,d_0}} \to E_{B_{a,d}}(B_3)$ with $\tilde{\tau} \circ \sigma = \mathrm{id}$. Concretely one constructs $\sigma(Q) = tP$ for any P with $\tilde{\tau}(P) = Q$ and checks independence of the choice of P. The existence of the section gives the desired splitting and hence the direct product decomposition. □

5. Cryptographic consequences

Theorem 5.1. *The discrete logarithm problem on $E_{B_{a,d}}(B_3)$ reduces to the discrete logarithm problem on $E_{B_{a_0,d_0}}$. More precisely, when the extension splits,*

$$E_{B_{a,d}}(B_3) \cong E_{B_{a_0,d_0}} \times \mathbf{F}_{2^n}^2,$$

and the DLP in $E_{B_{a,d}}(B_3)$ is equivalent to solving the DLP component-wise.

Proof. Given the direct product decomposition, any point $P \in E_{B_{a,d}}(B_3)$ corresponds to $(P_0, U) \in E_{B_{a_0,d_0}} \times \mathbf{F}_{2^n}^2$. A discrete log question $k \mapsto kP$ reduces to computing kP_0 in the base curve and kU in the finite additive group $\mathbf{F}_{2^n}^2$; the latter is trivial to invert since $\mathbf{F}_{2^n}^2$ is an easily solvable additive group, so the hardness is inherited from the base curve $E_{B_{a_0,d_0}}$. □

Key exchange. Use any standard Diffie–Hellman style protocol on $E_{B_{a,d}}(B_3)$: pick generator G, Alice sends aG, Bob sends bG, shared secret is abG. Security essentially reduces to the discrete-log problem on the base curve.

6. Conclusion

We provided full coefficient-level proofs of the structure of binary Edwards curves over the ring $B_3 = \mathbb{F}_{2^n}[\varepsilon]$ with $\varepsilon^3 = 0$. Finally cryptographic consequences follow immediately from the structural decomposition.

Acknowledgment. We would like to thank the unknown referee for his/her several helpful suggestions that helped us to improve our paper.

References

[1] H. Edwards, Normal form for elliptic curves, *Bull. Amer. Math. Soc. (N.S.)* **44** (2007), no. 3, 393-423.

[2] D.J. Bernstein, T. Lange, R. Rezaeian Farashahi, Binary Edwards Curves, In: Oswald E., Rohatgi P. (eds) *Cryptographic Hardware and Embedded Systems - CHES*, Lecture Notes in Computer Science 5154, Springer, Berlin, Heidelberg, 2008. https://doi.org/10.1007/978-3-540-85053-3-16.

[3] A. Chillali, Elliptic curves of the ring $F_q[\epsilon]$, $\epsilon^n = 0$, *Int. Math. Forum* **6** (2011) no. 29-31, 1501-1505.

[4] M.B.T. El Hamam, A. Chillali, L. El Fadil, Public key cryptosystem and binary Edwards curves on the ring $\mathbb{F}_{2^n}[e], e^2 = e$ for data management, In: *2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)* (2022). DOI: 10.1109/IRASET52964.2022.9738249.

[5] M.B.T. El Hamam, A. Chillali, L. El Fadil, Twisted Hessian curves over the ring $\mathbb{F}_q[e], e^2 = e$, *Bol. Soc. Paran. Mat. (3s.)* **40** (2022). DOI: https://doi.org/10.5269/bspm.51867.

[6] M.B.T. El Hamam, A. Chillali, L. El Fadil, A New Addition Law in Twisted Edwards Curves on Non Local Ring, In: Nitaj, A., Zkik, K. (eds) *Cryptography, Codes and Cyber Security. I4CS* (2022), Communications in Computer and Information Science 1747, Springer. https://doi.org/10.1007/978-3-031-23201-5_3.

[7] M.B.T. El Hamam, A. Chillali, L. El Fadil, Twisted Edwards curve over the ring $\mathbb{F}_q[e], e^2 = 0$, *Tatra Mt. Math. Publ.* **83** (2023), 43-50.

[8] M.B.T. El Hamam, A. Grini, A. Chillali, L. El Fadil, El Gamal cryptosystem on a Montgomery curves over non local ring, *WSEAS Trans. Math.* **21** (2022), 85-89.

[9] M.B.T. El Hamam, A. Chillali, L. El Fadil, Classification of the elements of the twisted Hessian curves in the ring $\mathbb{F}_q[e], e^3 = e^2$, *Bol. Soc. Paran. Mat. (3s.)* **42** (2024). DOI: https://doi.10.5269/bspm.62308.

[10] A. Chillali, M.B.T. El Hamam, A. Grini, Twisted Hessian curve over a local ring, *Bol. Soc. Paran. Mat. (3s.)* **42** (2024). DOI: https://doi.10.5269/bspm.62583.

[11] M.B.T. El Hamam, Binary Edwards curves over a local ring, *Palestine Journal of Mathematics* **14**(2025), no. 2, 259-264.

[12] A. Chillali, M.B.T. El Hamam, A. Grini, Huff's form for elliptic curves over a local ring, *Scientific African* **27** (2025), e02597. https://doi.org/10.1016/j.sciaf.2025.e02597

(Moha Ben Taleb El Hamam) Sidi Mohamed Ben Abdellah University, Faculty of Sciences Dhar El Mahraz, Fez, Morocco
E-mail address: mohaelhomam@gmail.com

(Abdelhakim Chillali) Polydisciplinary Faculty of Taza Sidi Mohamed Ben Abdellah University Fez, Morocco
E-mail address: abdelhakim.chillali@usmba.ac.ma

Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 53(1), 2026, Pages 7–31, DOI: 10.52846/ami.v53i1.2001
ISSN: 1223-6934

Study of some Anisotropic Parabolic Problems with Degenerate Coercivity

Aymane El Janathi and Hassane Hjiaj

Abstract. The aim of this paper is the study of the anisotropic parabolic problems described by

$$\begin{cases} \dfrac{\partial u}{\partial t} - \displaystyle\sum_{i=1}^{N} D^i a_i(x,t,u,\nabla u) = f(x,t,u) & \text{in} \quad Q_T = \Omega \times (0,T), \\ u = 0 & \text{on } \Sigma_T = \partial\Omega \times (0,T), \\ u(x,0) = u_0(x) & \text{in } \Omega, \end{cases} \tag{1}$$

where Ω is a bounded open subset of $\mathbb{R}^{\mathbb{N}}$ with $N \geq 2$. We prove the existence of renormalized solutions result for (1). We point out that the function $f(x,t,u)$ satisfies only some growth conditions with respect to u, and the initial data u_0 belongs to $L^1(\Omega)$.

2020 *Mathematics Subject Classification.* 35J75, 35J25.
Key words and phrases. Quasilinear parabolic problem, renormalized solutions, existence of solutions, degenerate coercivity, anisotropic Sobolev spaces.

1. Introduction

Let Ω be a bounded open subset of $\mathbb{R}^N$ $(N \geq 2)$ with Lipschitz boundary $\partial\Omega$. Fan et al. have studied in [16] the nonlinear elliptic Dirichlet problem of the form

$$\begin{cases} -\Delta_{p(\cdot)} u = f(x,u) & \text{in } \Omega, \\ u = 0 & \text{on } \partial\Omega, \end{cases} \tag{1.1}$$

here, the nonlinear term $f(x,u)$ verifying some growth condition with respect to u. They proved the existence of weak solutions for (1.1) in variable exponent Sobolev spaces. In [1], Ahmedatt et al. have studied the existence of renormalized solutions for the following quasilinear elliptic problem

$$\begin{cases} -\displaystyle\sum_{i=1}^{N} D^i a_i(x,u,\nabla u) + |u|^{s(\cdot)-1} u = f(x,u) & \text{in } \Omega, \\ u = 0 & \text{on } \partial\Omega, \end{cases} \tag{1.2}$$

where the Leray-Lions operator $Au = -\displaystyle\sum_{i=1}^{N} D^i a_i(x,u,\nabla u)$ verifying some degenerated coercivity condition, we refer the reader also to [2]. In [10], Boccardo et al. have

Received August 8, 2024. Accepted August 28, 2025.

studied the existence of solutions for the parabolic problem defined by

$$\begin{cases} \dfrac{\partial u}{\partial t} - \Delta_p u + \alpha_0 |u|^{s-1} u = f & \text{in } Q_T = \Omega \times (0,T), \\ u = 0 & \text{on } \Sigma_T = \partial\Omega \times (0,T), \\ u(x,0) = 0 & \text{in } \Omega, \end{cases} \tag{1.3}$$

where f belongs to $L^1(Q_T)$ with α_0 is a strictly positive constant. They also concluded some regularity results. Blanchard el al. in [9] have considered the quasilinear parabolic problem given by

$$\begin{cases} \dfrac{\partial u}{\partial t} - \operatorname{div}(a(x,t,u,\nabla u) + \Phi(u)) = f - \operatorname{div}(g) & \text{in } Q_T, \\ u = 0 & \text{on } \Sigma_T, \\ u(x,0) = u_0 & \text{in } \Omega, \end{cases} \tag{1.4}$$

where the datum $f \in L^1(Q_T)$, the initial data u_0 belongs to $L^1(\Omega)$, with $g \in (L^{p'}(Q_T))^N$ and $\Phi(\cdot)$ is a continuous function. They have established the existence and uniqueness of renormalized solution. In the case where the function a doesn't depend on the solution u, and $\Phi = g = 0$, the authors have proved in [7] the existence and uniqueness of renormalized solution for the quasilinear problem (1.4), we refer the reader also to [8]. In the framework of Sobolev spaces with variable exponents, we refer the reader to [3], [4], [5], and [11].
In the anisotropic parabolic spaces, Chrif et al. have established in [12] the existence of entropy solutions for the quasilinear parabolic problem

$$\begin{cases} \dfrac{\partial u}{\partial t} - \displaystyle\sum_{i=1}^{N} D^i a_i(x,t,\nabla u) + g(x,t,u,\nabla u) + d(x,t)|u|^{p_0-2}u = f - div(\Phi(u)) & \text{in } Q_T, \\ u = 0 & \text{on } \Sigma_T, \\ u(x,0) = u_0 & \text{in } \Omega, \end{cases} \tag{1.5}$$

where the lower order term $g(x,t,s,\xi)$ satisfies the sign and some growth condition, with $f(x,t) \in L^1(Q_T)$, and the initial data $u_0 \in L^1(\Omega)$, we refer the reader also to [13, 14] for more details.
In this paper, we study the degenerated quasilinear parabolic problem

$$\begin{cases} u_t - \displaystyle\sum_{i=1}^{N} D^i(a_i(x,t,u,\nabla u)) = f(x,t,u) & \text{in } Q_T, \\ u = 0 & \text{on } \Sigma_T, \\ u(x,0) = u_0(x) & \text{in } \Omega, \end{cases} \tag{1.6}$$

in anisotropic parabolic Sobolev spaces, where $f(x,t,s)$ verifies some growth condition with respect to s and the initial data u_0 belongs to $L^1(\Omega)$. We are interested on establishing the existence of renormalized solutions for (1.6). However, there are some difficulties connected to our problem, such as the lack of coercivity due to the degenerate coercivity condition, which requires the use of the penalized term $\dfrac{1}{n}|u|^{p_0-2}u$.

This paper is structured as follows : In the section 2 we introduce some definitions and properties concerning the anisotropic Sobolev spaces, then we recall some essentials lemmas. The Section 3 is devoted to presenting the assumptions on the functions

$a_i(x,t,s,\xi)$ and $f(x,t,s)$ under which our problem has at least one renormalized solution. The Section 5, will be devoted to proved our mains result.

2. Notations and preliminaries

This section is devoted to introduce some definitions and basic properties concerning the anisotropic parabolic Sobolev spaces.
Let Ω be an open bounded domain in $I\!R^N$ $(N \geq 2)$ with a Lipschitz boundary $\partial\Omega$.
Let $p_1, p_2, \ldots, p_N$ be N real exponents, such that $1 < p_i < \infty$ for $i = 1, \ldots, N$.
We set $\overrightarrow{p} = (p_1, \ldots, p_N)$, with

$$\underline{p} = \min\{p_1, p_2, \ldots, p_N\} \qquad \text{and} \qquad p_0 = \max\{p_1, p_2, \ldots, p_N\}.$$

Moreover, we denote

$$D^0 u = u \qquad \text{and} \qquad D^i u = \frac{\partial u}{\partial x_i} \qquad \text{for} \qquad i = 1, \ldots, N.$$

The anisotropic Sobolev space $W^{1,\overrightarrow{p}}(\Omega)$ is defined by

$$W^{1,\overrightarrow{p}}(\Omega) = \left\{ u \in L^{p_0}(\Omega) \quad \text{such that} \quad D^i u \in L^{p_i}(\Omega) \quad \text{for} \quad i = 1, 2, \ldots, N \right\},$$

this space is equipped with the norm

$$\|u\|_{1,\overrightarrow{p}} = \sum_{i=0}^{N} \|D^i u\|_{p_i}. \tag{2.1}$$

We set $W_0^{1,\overrightarrow{p}}(\Omega)$ the closure of $\mathcal{C}_0^\infty(\Omega)$ in $W^{1,\overrightarrow{p}}(\Omega)$ for the norm (2.1).
The Sobolev spaces $W^{1,\overrightarrow{p}}(\Omega)$ and $W_0^{1,\overrightarrow{p}}(\Omega)$ are separable and reflexive Banach spaces.

Proposition 2.1. (see [17, 22].) Let $u \in W_0^{1,\vec{p}}(\Omega)$, we have
(i) Poincaré's inequality : there exists a constant $C_p > 0$, such that

$$\|u\|_{L^{p_i}(\Omega)} \leq C_p \, \|D^i u\|_{L^{p_i}(\Omega)} \qquad \text{for any} \quad i = 1, \ldots, N.$$

(ii) Sobolev's inequality : there exists a constant $C_s > 0$, such that

$$\|u\|_{L^q(\Omega)} \leq \frac{C_s}{N} \sum_{i=1}^{N} \|D^i u\|_{L^{p_i}(\Omega)},$$

where

$$\frac{1}{\overline{p}} = \frac{1}{N} \sum_{i=1}^{N} \frac{1}{p_i} \qquad \text{and} \qquad \begin{cases} q = \overline{p}^* = \dfrac{N\overline{p}}{N - \overline{p}} & \text{if} \quad \overline{p} < N, \\ q \in [1, +\infty[& \text{if} \quad \overline{p} \geq N. \end{cases}$$

Lemma 2.1. *Let Ω be a bounded open set in $I\!R^N$ with a Lipschitz boundary. Then, the following embedding are compact.*

- *if $\overline{p} < N$, then $W_0^{1,\overrightarrow{p}}(\Omega) \hookrightarrow\hookrightarrow L^r(\Omega)$ for any $r \in [1, \underline{p}^*[$, where $\dfrac{1}{\underline{p}^*} = \dfrac{1}{\underline{p}} - \dfrac{1}{N}$.*
- *if $\overline{p} = N$, then $W_0^{1,\overrightarrow{p}}(\Omega) \hookrightarrow\hookrightarrow L^r(\Omega)$ for any $r \in [1, +\infty[$,*
- *if $\overline{p} > N$, then $W_0^{1,\overrightarrow{p}}(\Omega) \hookrightarrow\hookrightarrow L^\infty(\Omega) \cap C^0(\overline{\Omega})$.*

The proof is based on the continuous embedding of $W_0^{1,\overrightarrow{p}}(\Omega)$ into $W_0^{1,\underline{p}}(\Omega)$, and the compact embedding theorem for Sobolev spaces.

Definition 2.1. The dual of the anisotropic Sobolev space $W_0^{1,\overrightarrow{p}}(\Omega)$ is denoted by $W^{-1,\overrightarrow{p'}}(\Omega)$, where $\overrightarrow{p'} = (p_1', p_2', \ldots, p_N')$ giving by :

$$\begin{aligned} rW^{-1,\overrightarrow{p'}}(\Omega) &= \Big\{F = F_0 - \sum_{i=1}^{N} D^i F_i \text{ such that } F_0 \in L^{p_0'}(\Omega) \\ &\qquad \text{and} \quad F_i \in L^{p_i'}(\Omega) \quad \text{for} \quad i = 1, 2, \ldots, N\Big\}. \end{aligned}$$

Moreover, for all $u \in W_0^{1,\overrightarrow{p}}(\Omega)$ we have

$$\langle F, u\rangle = \sum_{i=0}^{N} \int_\Omega F_i D^i u \; dx.$$

The norm on the dual space is defined by

$$\begin{aligned} lr\|F\|_{-1,\overrightarrow{p'}} &= \inf\Bigg\{ \sum_{i=0}^{N} \|F_i\|_{p_i'} \text{ with } F = F_0 - \sum_{i=1}^{N} D^i F_i, \\ &\qquad \text{where} \quad F_0 \in L^{p_0'}(\Omega) \text{ and } F_i \in L^{p_i'}(\Omega)\Bigg\}. \end{aligned}$$

Let $T > 0$, we put $Q_T = \Omega \times (0, T)$ and $\sum_T$ the surface $\partial\Omega \times (0, T)$. We introduce the anisotropic parabolic space $L^{\overrightarrow{p}}(0, T; W^{1,\overrightarrow{p}}(\Omega))$ by

$$L^{\overrightarrow{p}}(0, T; W^{1,\overrightarrow{p}}(\Omega)) = \left\{ u \text{ measurable function } / \sum_{i=0}^{N} \int_0^T \left\|D^i u\right\|_{L^{p_i}(\Omega)}^{p_i} dt < \infty \right\}$$

endowed with the norm

$$\|u\|_{L^{\overrightarrow{p}}(0,T;W^{1,\overrightarrow{p}}(\Omega))} = \sum_{i=0}^{N} \left\|D^i u\right\|_{L^{p_i}(Q_T)}.$$

The functional space $L^{\overrightarrow{p}}(0, T; W_0^{1,\overrightarrow{p}}(\Omega))$ is defined by

$$L^{\overrightarrow{p}}(0, T; W_0^{1,\overrightarrow{p}}(\Omega)) = \left\{ u \in L^{\overrightarrow{p}}(0, T; W^{1,\overrightarrow{p}}(\Omega)) / u = 0 \text{ on } \partial\Omega \times [0, T] \right\}.$$

Note that $L^{\overrightarrow{p}}(0, T; W^{1,\overrightarrow{p}}(\Omega))$ and $L^{\overrightarrow{p}}(0, T; W_0^{1,\overrightarrow{p}}(\Omega))$ are separable and reflexive Banach spaces.

Definition 2.2. The dual space of $L^{\overrightarrow{p}}(0, T; W_0^{1,\overrightarrow{p}}(\Omega))$ is defined as follows

$$L^{\overrightarrow{p'}}(0, T; W^{-1,\overrightarrow{p'}}(\Omega)) = \left\{ F = f_0 - \sum_{i=1}^{N} D^i f_i, \text{ with } f_i \in L^{p_i'}(Q_T) \right\}.$$

We define a norm on the dual space by

$$\|F\|_{L^{\overrightarrow{p'}}(0,T;W^{-1,\overrightarrow{p'}}(\Omega))} = \inf\left\{ \sum_{i=0}^{N} \|f_i\|_{L^{p_i'}(Q_T)} / \quad F = f_0 - \sum_{i=1}^{N} D^i f_i \text{ with } f_i \in L^{p_i'}(Q_T) \right\}.$$

The duality of the spaces $L^{\overrightarrow{p}}(0,T;W_0^{1,\overrightarrow{p}}(\Omega))$ and $L^{\overrightarrow{p'}}(0,T;W^{-1,\overrightarrow{p'}}(\Omega))$ is given by the relation

$$\int_0^T \langle F, v\rangle dt = \sum_{i=0}^{N} \int_{Q_T} f_i D^i v \; dxdt \quad \text{for all} \quad v \in L^{\overrightarrow{p}}(0,T;W_0^{1,\overrightarrow{p}}(\Omega)).$$

Lemma 2.2 (see [21].). *Let B_0, B and B_1 be a Banach spaces with $B_0 \subset B \subset B_1$. Let us set*

$$Y = \left\{u \; : \; u \in L^{p_0}(0,T;B_0) \quad \text{and} \quad u' \in L^{p_1}(0,T;B_1)\right\}$$

where $p_0 > 1$ and $p_1 > 1$ are reals numbers.
Assuming that the embedding $B_0 \hookrightarrow\hookrightarrow B$ is compact, then

$$Y \hookrightarrow\hookrightarrow L^{p_0}(0,T;B)$$

and this embedding is compact.

Remark 2.1. Let $\underline{p} > \dfrac{2N}{N+2}$, we set

$$B_0 = W_0^{1,\overrightarrow{p}}(\Omega), \qquad B = L^2(\Omega) \qquad \text{and} \qquad B_1 = W^{-1,\overrightarrow{p'}}(\Omega),$$

with $p_0 = \underline{p}$ and $p_1 = p_0'$. In view of the Lemma 2.2 we obtain

$$\left\{u \; : \; u \in L^{\overrightarrow{p}}(0,T;W_0^{1,\overrightarrow{p}}(\Omega)) \quad \text{and} \quad u' \in L^{\overrightarrow{p'}}(0,T;W^{-1,\overrightarrow{p'}}(\Omega))\right\} \subseteq Y \hookrightarrow\hookrightarrow L^1(Q_T). \tag{2.2}$$

Moreover, in view of [5], we have

$$\left\{u \; : \; u \in L^{\overrightarrow{p}}(0,T;W_0^{1,\overrightarrow{p}}(\Omega)) \quad \text{and} \quad u' \in L^{\overrightarrow{p'}}(0,T;W^{-1,\overrightarrow{p'}}(\Omega))\right\} \subseteq C([0,T];L^1(\Omega)). \tag{2.3}$$

Now, we recall some helpful lemmas for the proof of our main result.

Lemma 2.3 (see [18].). *Let $(u_n)_n$ be a sequence in $L^1(\Omega)$ and $u \in L^1(\Omega)$ such that*
(i): *$u_n \to u$ a.e. in Ω,*
(ii): *$u_n \geq 0$ and $u \geq 0$ a.e. in Ω,*
(iii): $\displaystyle\int_\Omega u_n \, dx \to \int_\Omega u \, dx,$
then u_n converges to u strongly in $L^1(\Omega)$.

Lemma 2.4. *Let $1 < p < \infty$, we assume that $g(x) \in L^p(\Omega)$ and the sequence $(g_n)_n$ is uniformly bounded in $L^p(\Omega)$ with $\|g_n\|_p \leq C$.*
If $g_n(x) \to g(x)$ a.e. in Ω, then $g_n(x) \rightharpoonup g(x)$ weakly in $L^p(\Omega)$.

Definition 2.3. For $k > 0$, we define the truncation function $T_k(\cdot) : \mathbb{R} \longmapsto \mathbb{R}$ by

$$T_k(s) = \max\left\{-k, \min(s,k)\right\}.$$

Proposition 2.5 (see [13]). *Let $\mu > 0$, we define the time mollification of a function u that belongs to $L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$ by*

$$u_\mu(x,t) = \mu \int_{-\infty}^{t} \bar{u}(x,s)\exp(\mu(s-t))ds, \qquad \text{where } \bar{u}(x,s) = u(x,s)\chi_{(0,T)}(s).$$

Thus, we have

(i) *If* $u \in L^q(Q_T)$, *then* u_μ *is measurable in* Q_T. *Moreover,* $(u_\mu)_t = \mu(u - u_\mu)$ *and*

$$\int_{Q_T} |u_\mu|^q \, dx\, dt \leq \int_{Q_T} |u|^q \, dx\, dt.$$

(ii) *If* $u \in L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$, *thus* $u_\mu \to u$ *strongly in* $L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$ *as* $\mu \to +\infty$.

(iii) *If* $u_n \to u$ *strongly in* $L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$, *then* $(u_n)_\mu \to u_\mu$ *strongly in* $L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$.

3. Essential Assumptions

Let Ω be a bounded open subset of $\mathbb{R}^N$ $(N \geq 2)$, with Lipschitz boundary $\partial\Omega$. We consider the operator $Au : L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega)) \mapsto L^{\vec{p'}}(0,T;W^{-1,\vec{p'}}(\Omega))$ defined by

$$Au = -\sum_{i=1}^{N} D^i a_i(x,t,u,\nabla u), \tag{3.1}$$

such that $a_i(x,t,s,\xi) : \Omega \times (0,T) \times \mathbb{R} \times \mathbb{R}^N \mapsto \mathbb{R}$ is a Carathéodory function that verifies the following conditions

$$|a_i(x,t,s,\xi)| \leq \beta(K_i(x,t) + |s|^{p_i - 1} + |\xi_i|^{p_i - 1}), \tag{3.2}$$

where $K_i(.,.)$ is a nonnegative function that belonging to $L^{p_i'}(Q_T)$,

$$(a_i(x,t,s,\xi) - a_i(x,t,s,\xi^*))(\xi_i - \xi_i^*) > 0 \quad \text{for any} \quad \xi_i \neq \xi_i^*, \tag{3.3}$$

and

$$a_i(x,t,s,\xi)\xi_i \geq b(|s|)|\xi_i|^{p_i}, \tag{3.4}$$

such that $b(|\cdot|) : \mathbb{R} \longmapsto \mathbb{R}^+$ is a decreasing positive function, that verifies

$$b(|s|) \geq \frac{b_0}{(1+|s|)^\lambda} \quad \text{with} \quad 0 \leq \lambda < \underline{p} - 1, \tag{3.5}$$

where β and b_0 are two strictly nonnegatives constants.

The Carathéodory function $f(x,t,s)$ having only the growth condition

$$|f(x,t,s)| \leq f_0(x,t) + c(x,t)|s|^{q_0}, \tag{3.6}$$

where $f_0(.,.) \in L^1(Q_T)$ and $0 < q_0 \leq \underline{p} - \lambda - 1$, the positive measurable function $c(.,.)$ belongs to $L^m(Q_T)$ with $\dfrac{\underline{p} - \lambda - 1}{\underline{p} - \lambda - 1 - q_0} < m$.

Lemma 3.1. *Assuming that the conditions* (3.2) − (3.4) *hold true. Let* $(u_n)_n$ *be a sequence in* $L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$ *with* $(u_n)_t \in L^{\vec{p'}}(0,T;W^{-1,\vec{p'}}(\Omega))$, *such that* $u_n \rightharpoonup u$ *weakly in* $L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$ *and*

$$\lim_{n\to\infty} \Big(\sum_{i=1}^{N} \int_{Q_T} (a_i(x,t,T_k(u_n),\nabla u_n) - a_i(x,t,T_k(u_n),\nabla u))(D^i u_n - D^i u)\, dx\, dt + \int_{Q_T} (|u_n|^{p_0 - 2} u_n - |u|^{p_0 - 2} u)(u_n - u)\, dx\, dt \Big) = 0,$$

then $u_n \to u$ *strongly in* $L^{\vec{p}}(0,T;W_0^{1,\vec{p}}(\Omega))$ *for a subsequence.*

The proof of lemma 3.1 follows the same technique used in [13].