# CLASSIFICATION OF ELEMENTS IN ELLIPTIC CURVE OVER THE RING $\mathbb{F}_{q}[\varepsilon]$ 

Bilel Selikh, Douadi Mifoubi<br>AND<br>Nacer Ghadbane<br>Laboratory of Pures and Applied Mathematics<br>Department of Mathematics<br>Mohamed Boudiaf University of M'sila<br>M'sila 28000, Algeria<br>e-mail: bilel.selikh@univ-msila.dz<br>douadi.mihoubi@univ-msila.dz<br>nacer.ghadbane@univ-msila.dz


#### Abstract

Let $\mathbb{F}_{q}[\varepsilon]:=\mathbb{F}_{q}[X] /\left(X^{4}-X^{3}\right)$ be a finite quotient ring where $\varepsilon^{4}=$ $\varepsilon^{3}$, with $\mathbb{F}_{q}$ is a finite field of order $q$ such that $q$ is a power of a prime number $p$ greater than or equal to 5 . In this work, we will study the elliptic curve over $\mathbb{F}_{q}[\varepsilon], \varepsilon^{4}=\varepsilon^{3}$ of characteristic $p \neq 2,3$ given by homogeneous Weierstrass equation of the form $Y^{2} Z=X^{3}+a X Z^{2}+b Z^{3}$ where $a$ and $b$ are parameters taken in $\mathbb{F}_{q}[\varepsilon]$. Firstly, we study the arithmetic operation of this ring. In addition, we define the elliptic curve $E_{a, b}\left(\mathbb{F}_{q}[\varepsilon]\right)$ and we will show that $E_{\pi_{0}(a), \pi_{0}(b)}\left(\mathbb{F}_{q}\right)$ and $E_{\pi_{1}(a), \pi_{1}(b)}\left(\mathbb{F}_{q}\right)$ are two elliptic curves over the finite field $\mathbb{F}_{q}$, such that $\pi_{0}$ is a canonical projection and $\pi_{1}$ is a sum projection of coordinate of element in $\mathbb{F}_{q}[\varepsilon]$. Precisely, we give a classification of elements in elliptic curve over the finite ring $\mathbb{F}_{q}[\varepsilon]$.


Keywords: elliptic curves, finite ring, finite field, projective space.
2010 Mathematics Subject Classification: 14H52, 11T55, 20K30, 20 K 27.

## References

[1] W. Bosma and H.W. Lenstra, Complete System of Two Addition Laws for Elliptic Curves, J. Number Theory 53 (1995) 229-240.
https://doi.org/10.1006/jnth.1995.1088
[2] A. Boulbot, A. Chillali and A. Mouhib, Elliptic curves over the ring $\mathbb{F}_{q}[e], e^{3}=e^{2}$, Gulf J. Math. 4 (2016) 123-129.
[3] A. Boulbot, A. Chillali and A. Mouhib, Elliptic curves over the ring R, Boletim da Sociedade Paranaense de Matematica 38 (2017) 193-201. https://doi.org/10.5269/bspm.v38i3.39868
[4] A. Boulbot, A. Chillali and A. Mouhib, Elliptic curve over a finite ring generated by 1 and an idempotent element $\varepsilon$ with coefficients in the finite field $\mathbb{F}_{3^{d}}$, Boletim da Sociedade Paranaense de Matematica (2018) 1-19.
https://doi.org/10.5269/bspm. 43654
[5] A. Chillali, Elliptic Curves of the Ring $\mathbb{F}_{q}[\varepsilon], \varepsilon^{n}=0$, Internat. Math. 6 (2011) 1501-1505.
[6] H.W. Lenstra, Jr., Elliptic curves and number-theoretic algorithms (Proceedings of the International Congress of Mathematicians, Berkely, California, USA, 1986).
[7] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987) 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5
[8] V. Miller, Use of elliptic curves in cryptography, Advanced cryptology-CRYPTO'85 218 (1986) 417-426.
https://doi.org/10.1007/3-540-39799-X_-31
[9] J.H. Silverman, Advanced topics in the arithmetic of elliptic curves (Springer-Verlag, 1994).
https://doi.org/10.1007/978-1-4612-0851-8
[10] M. Virat, Courbe elliptique sur un anneau et applications cryptographiques, Doctoral thesis (Universite Nice-Sophia Antipolis, Nice, France, 2009).

Received 8 May 2020
Revised 6 September 2020 Accepted 6 September 2020

