Available online at www.sciencedirect.com

ScienceDirect

Journal of Taibah University for Science 9 (2015) 276–287

Journal of Taibah University for Science

www.elsevier.com/locate/jtusci

Elliptic curves over a chain ring of characteristic 3☆

Moulay Hachem Hassib [a,*], Abdelhakim Chillali [b], Mohamed Abdou Elomary [a]

[a] Moulay Ismail University, FSTE, Errachidia, Morocco
[b] USMBA, LSI, FPT, Taza, Morocco

Available online 2 March 2015

Abstract

This paper proposes the generalization of our previous work to the ring $A_n = \mathbb{F}_{3^d}[X]/(X^n)$. All results found before in A_2, A_3 and A_4 [1–3] hold in A_n; but the approach here is clearly different, and has given more interesting results, specially when 3 does not divide $\#E^1_{a_0,b_0}$; the elliptic curve over the ring A_n is a direct sum of the elliptic curve over the field $\mathbb{F}_{3^d}$ and, unexpectedly its own subgroup of elements with the third projective coordinate not invertible, instead of $\mathbb{F}_{3^d}{}^n$ as it was thought in the earlier works. Other results are deduced from, we cite the equivalence of the Discrete Logarithm Problem (DLP) on the elliptic curve over the ring A_n and the field $\mathbb{F}_{3^d}$, which is beneficial for cryptanalysts and cryptographers as well, and we will set the theoretic foundations to build a cryptosystem similar to the one in [4] with more benefits, which will be specified later.
© 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of Taibah University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

MSC: 14H52; 94A60; 11T71

Keywords: Characteristic 3; Elliptic curves; Chain ring; Cryptography; Discrete Logarithm Problem; Short exact sequence

1. Introduction

Let d be a positive integer. We consider the quotient ring $A_n = \mathbb{F}_{3^d}[X]/(X^n)$, where $\mathbb{F}_{3^d}$ is the finite field of order 3^d, and $n \geq 1$. Then the ring A_n is identified to the ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^n = 0$. So we have:

$$A_n = \left\{ \sum_{i=0}^{n-1} x_i \varepsilon^i \mid (x_i)_{0 \leq i \leq n-1} \in \mathbb{F}_{3^d} \right\}.$$

The study of the elliptic curve over the ring of dual numbers was started by Marie Virat in [4]. In her Ph.D. thesis, she has defined the elliptic curve over the ring $\mathbb{F}_p[X]/(X^2)$, where p is a prime number $\neq 2$ and 3, and Chillali [5] has generalized the work of Virat and extended it to the ring $\mathbb{F}_p[X]/(X^n)$.

☆ This work is related to the *International Workshop of Algebra and Applications*, June 18–21, 2014, FST Fez, Morocco.

* Corresponding author. Tel.: +212 650886345.
E-mail address: hachem71@gmail.com (M.H. Hassib).

Peer review under responsibility of Taibah University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jtusci.2015.02.001
1658-3655 © 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of Taibah University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

The authors in their previous works have began the study of the elliptic curve over a chain ring of characteristic 3, and established it for the rings A_2, A_3 and A_4 [1–3].

Generalize our previous work to the ring A_n, is one of the purposes of this article. In Section 2, we will define the ring A_n and establish some useful results which are necessary for the rest of this article, and in Section 3 we will define the elliptic curve over A_n and explicitly the group law over $E^n_{a,b}$. Afterwards, we will classify the elements of the elliptic curve $E^n_{a,b}$ into two parts; where one of them is a subgroup of $(E^n_{a,b}, +)$ and is isomorphic to $(\mathfrak{M}_n, *)$; the maximal ideal of A_n provided with the law *, which is given in Definition 2. This subgroup is namely a direct factor of $E^n_{a,b}$ when 3 does not divide $N = \#E^1_{a,b}$, as it will be shown in Section 3.4.

Other purpose of this article is the application of the results in cryptography. Thereby, Theorem 4 provides the necessary foundations to create a cryptosystem similar to the one given in [4]. The new cryptosystem has the advantage of having a low cost of complexity compared to the first one, since we work in characteristic 3 and, furthermore, may be more secure by managing the choice of the appropriate parameter n; which refers to A_n.

Other cryptographic applications are given in Section 4.

The case 3 divides N is discussed in Section 3.6.

All theoretic results found in [4] hold in A_2; the ring of dual numbers of characteristic 3 and, further more are extended to A_n.

2. The ring A_n

In this section, we will give some results concerning the ring A_n, which are useful for the rest of this article.

Lemma 1. *Let $X = \sum_{i=0}^{n-1} x_i\varepsilon^i \in A_n$.*
X is invertible in A_n if and only if $x_0 \neq 0$.

Lemma 2. *A_n is a local ring, its maximal ideal is $\mathfrak{M}_n = (\varepsilon)$.*

Lemma 3. *A_n is a vector space over $\mathbb{F}_{3^d}$, and have $(1, \varepsilon, \ldots, \varepsilon^{n-1})$ as basis.*

Remark 1. We denote $I_j = (\varepsilon^j)$, where $j = 1, \ldots, n-1$. Then, $(I_j)_{1\leq j\leq n-1}$ is a decreasing sequence of ideals of A_n and $I_1 = \mathfrak{M}_n$.

$$\mathfrak{M}_n = I_1 \supseteq I_2 \cdots \supseteq I_{n-1}$$

Lemma 4. $A_{n-1} \simeq A_n/I_{n-1}$

Proof. Let $A_{n-1} = \left\{\sum_{i=0}^{n-2} x_i\delta^i \mid (x_i)_{0\leq i\leq n-2} \in \mathbb{F}_{3^d} \text{ and } \delta^{n-1} = 0\right\}$ and h the map defined as follows:

$$\begin{array}{ccc} A_{n-1} & \xrightarrow{h} & \dfrac{A_n}{I_{n-1}} \\ \displaystyle\sum_{i=0}^{n-2} x_i\delta^i & \longmapsto & \displaystyle\sum_{i=0}^{n-2} x_i\varepsilon^i + I_{n-1} \end{array}$$

Let prove that h is an isomorphism of rings.

- Let $X = \sum_{i=0}^{n-2} x_i\delta^i \in A_{n-1}$ and $Y = \sum_{i=0}^{n-2} y_i\delta^i \in A_{n-1}$, we have $X + Y = \sum_{i=0}^{n-2}(x_i + y_i)\delta^i \in A_{n-1}$ and $XY = \sum_{i=0}^{n-2} z_i\delta^i \in A_{n-1}$ where, $z_j = \sum_{i=0}^{j} x_i y_{j-i}$ (see Lemma 1.1 in [5, p. 1502]) then, $h(X+Y) = h(X) + h(Y)$ and, $h(XY) = h(X)h(Y)$ and so, h is a homomorphism of rings.
- Let $X = \sum_{i=0}^{n-2} x_i\delta^i \in A_{n-1}$ such that $h(X) = 0 + I_{n-1}$. Then, $\sum_{i=0}^{n-2} x_i\varepsilon^i + I_{n-1} = 0 + I_{n-1}$, so $\sum_{i=0}^{n-2} x_i\varepsilon^i \in I_{n-1}$, this means that $x_i = 0$ for all $i = 0, \ldots, n-2$. So $X = 0$, and $\ker h = 0$, this prove that h is injective. Now let $Y = \sum_{i=0}^{n-1} x_i\varepsilon^i + I_{n-1} \in A_n/I_{n-1}$, then we denote $X = \sum_{i=0}^{n-2} x_i\delta^i$; we have $X \in A_{n-1}$ and $h(X) = Y$, so h is surjective.

Finally h is an isomorphism of rings. □

Download English Version:

https://daneshyari.com/en/article/1263018

Download Persian Version:

https://daneshyari.com/article/1263018

Daneshyari.com