Int. J. Open Problems Compt. Math., Vol. 5, No. 4, December 2012
ISSN 1998-6262; Copyright ©ICSRS Publication, 2012
www.i-csrs.org

The J-invariant over E_{3d}^{n}

Abdelhakim Chillali

FST OF FEZ
chil2007@voila.fr

Abstract

In this work we defined the J-invariant of an elliptic curve over the artinian principal ideal ring R_n of characteristic 3, [1, 2, 3, 4]. More precisely, we establish $\pi(J) = j$, where j is the j-invariant of an elliptic curve over F_q, $q = 3^d$ and π is the canonical projection defined over ring R_n by F_q.

Keywords: *Elliptic Curve Over Ring, The j-invariant, Artinian principal ideal ring.*

1 Introduction

The goal of this article is to study he J-invariant of an elliptic curve over the artinian principal ideal ring R_n.

Let p be an odd prime number and n be an integer such that $n \geq 1$. Consider the quotient ring $R_n = F_q[X]/(X^n)$ where F_q is the finite field of characteristic p and q elements. Then the ring R_n may be identified to the ring $F_q[\epsilon]$ where $\epsilon^n = 0$. In other word [1, 2, 3]

$$R_n = \left\{ \sum_{i=0}^{n-1} a_i \epsilon^i | \ \ (a_i)_{0 \leq i \leq n-1} \in F_q^n \right\}.$$

The following result is easy to prove:

Lemma 1.1 *Let $X = \sum_{i=0}^{n-1} x_i \epsilon^i$ and $Y = \sum_{i=0}^{n-1} y_i \epsilon^i$ be two elements of R_n. Then*

$$XY = \sum_{i=0}^{n-1} z_i \epsilon^i \ \ \texttt{where} \ \ z_j = \sum_{i=0}^{j} x_i y_{j-i}.$$

Remark 1.2 *Let $Y = \sum_{i=0}^{n-1} y_i\epsilon^i$ be the inverse of the element $X = \sum_{i=0}^{n-1} x_i\epsilon^i$. Then*

$$\begin{cases} y_0 = x_0^{-1} \\ y_j = -x_0^{-1}\sum_{i=0}^{j-1} y_i x_{j-i}, \quad \forall j > 0 \end{cases}$$

We consider the canonical projection π defined by:

$$\pi : \left| \begin{array}{rcl} R_n & \longrightarrow & F_q \\ \sum_{i=0}^{n-1} x_i\epsilon^i & \longmapsto & x_0 \end{array} \right.$$

Lemma 1.3 *π is a morphism of rings.*

Proof 1 *Let $X = \sum_{i=0}^{n-1} x_i\epsilon^i$ and $Y = \sum_{i=0}^{n-1} y_i\epsilon^i$, then*

$$X + Y = \sum_{i=0}^{n-1}(x_i + y_i)\epsilon^i$$

$$XY = \sum_{i=0}^{n-1} z_i\epsilon^i \ \ \texttt{where} \ \ z_j = \sum_{i=0}^{j} x_i y_{j-i}.$$

We have:

$$\pi(X + Y) = x_0 + y_0 = \pi(X) + \pi(Y)$$

$$\pi(XY) = z_0 = x_0 y_0 = \pi(X)\pi(Y).$$

So, π is a morphism of rings. ∎

2 Elliptic Curve Over R_n

In this section we suppose $n \geq 1$. An elliptic curve over ring R_n is curve that is given by Weierstrass equation [1, 2, 3, 4]:

$$(\star) : Y^2Z + A_1XYZ + A_3YZ^2 = X^3 + A_2X^2Z + A_4XZ^2 + A_6Z^3$$

with coefficients $A_i \in R_n$.

Notation 2.1 *We denote by:*

- $B_2 = A_1^2 + 4A_2$
- $B_4 = A_1A_3 + 2A_4$
- $B_6 = A_3^3 + 4A_6$
- $B_8 = A_1^2A_6 - A_1A_3A_4 + A_2A_3^2 + 4A_2A_6 - A_4^2$
- $C_4 = B_2^2 - 24B_4$

- $C_6 = -B_2^3 + 36B_2B_4 - 216B_6$

Definition 2.2 *The discriminant of elliptic curve over ring R_n is defined to be:*

$$\Delta_{\epsilon,n} = -B_2^2B_8 - 8B_4^3 - 27B_6^2 + 9B_2B_4B_6.$$

Definition 2.3 *Let $\Delta_{\epsilon,n}$ is inversible in R_n, then we defined the J-invariant of an elliptic curve over R_n by:*

$$J = \frac{C_4^3}{\Delta_{\epsilon,n}}.$$

3 Main Result

In this section the field over which the curve is defined has characteristic 3. An elliptic curve over R_n is the set of all solutions $(X, Y, Z) \in R_n \times R_n \times R_n$, $(X, Y, Z) \neq (0, 0, 0)$ to the equation

$$(\star) : Y^2Z = X^3 + AX^2Z + BZ^3$$

where $A,\ B \in R_n$ and $-A^3B$ is invertible in R_n. [1, 2, 3, 4]
We denote an elliptic curve over R_n by $E^n_{3^d}$.

Definition 3.1 *A Weierstrass equation over R_n is an equation of type*

$$Y^2Z = X^3 + AX^2Z + BZ^3$$

with A and B in R_n. Then the reduction on F_q of such an equation is

$$Y^2Z = X^3 + a_0X^2Z + b_0Z^3$$

with $a_0 = \pi(A)$ and $b_0 = \pi(B)$.

Remark 3.2 *Consider a Weierstrass equation over R_n. It defines a Weierstrass cubic curve over R_n, if and only if $-A^3B$ is invertible in R_n.*

Lemma 3.3 *A Weierstrass equation on R_n defines an elliptic curve on R_n if and only if its reduction on F_q defines an elliptic curve.*

Proof 2 *$-A^3B$ is invertible in R_n if and only if $\pi(-A^3B) \neq 0$ if and only if $-\pi(A)^3\pi(B) \neq 0$ if and only if $Y^2Z = X^3 + \pi(A)X^2Z + \pi(b)Z^3$ defines an elliptic curve on F_q.* ∎

Lemma 3.4 *The J-invariant of $E_{3^d}^n$ can also be written as*

$$J = \frac{-A^3}{B}.$$

Proof 3 *We have*

$$A_1 = A_3 = A_4 = 0,$$

$$A_2 = A$$

and

$$A_6 = B.$$

Then

- $B_2 = A$
- $B_4 = 0$
- $B_6 = B$
- $B_8 = AB$
- $C_4 = A^2$
- $C_6 = -A^3$
- $\Delta_{\epsilon,n} = -A^3 B.$
- $C_4^3 = A^6$

So,

$$J = \frac{A^6}{-A^3 B} = \frac{-A^3}{B}.$$

∎

Lemma 3.5 *Let J the J-invariant of $E_{3^d}^n$ and j the j-invariant of reduction on F_q. Then*

$$\pi(J) = j.$$

Proof 4 *We have*

$$J = \frac{-A^3}{B},$$

and

$$j = \frac{-\pi(A)^3}{\pi(B)}.$$

Let $A = a_0 + \widetilde{A}$ *and* $B = b_0 + \widetilde{B}$, *where* $a_0, b_0 \in F_q$, $\widetilde{A}, \widetilde{B} \in \epsilon R_n$. *We have*

$$\pi(A) = a_0, \pi(B) = b_0$$

$$A^3 = (a_0^3 + X), X \in \epsilon R_n.$$

So,

$$J = -(a_0^3 + X)(b_0 + \widetilde{B})^{-1},$$

i.e

$$J = -\frac{a_0^3}{b_0} + T, T \in \epsilon R_n.$$

We conclude

$$\pi(J) = j.$$

■

Assumption 3.6 *Let* $E^1_{3^d}$ *is reduction of* $E^n_{3^d}$, *and* $N = \sharp E^1_{3^d}$.
If 3 *does not divide* N, *then*

$$E^n_{3^d} \cong E^1_{3^d} \times F^{n-1}_{3^d}.$$

Theorem 3.7 *Let* J *the* J*-invariant of* $E^n_{3^d}$, *and* J' *the* J*-invariant of* ${E'_{3^d}}^n$.
If 3 *does not divide* N, *where* $N = \sharp E^1_{3^d} = \sharp {E'_{3^d}}^1$.
Then $E^n_{3^d}$ *and* ${E'_{3^d}}^n$ *are isomorphic if and only if* $\pi(J) = \pi(J')$.

Proof 5 *Let* j *the* j*-invariant of* $E^1_{3^d}$, *and* j' *the* j*-invariant of* ${E'_{3^d}}^1$. *We have*

$$E^n_{3^d} \cong E^1_{3^d} \times F^{n-1}_{3^d}.$$

and

$${E'_{3^d}}^n \cong E^1_{3^d} \times F^{n-1}_{3^d}.$$

Thus

$$\begin{array}{rcl} E^n_{3^d} \cong {E'_{3^d}}^n & \Leftrightarrow & E^1_{3^d} \times F^{n-1}_{3^d} \cong {E'_{3^d}}^1 \times F^{n-1}_{3^d} \\ & \Leftrightarrow & E^1_{3^d} \cong {E'_{3^d}}^1 \\ & \Leftrightarrow & j = j' \\ & \Leftrightarrow & \pi(J) = \pi(J'). \end{array}$$

■

4 Conclusion

The conclusion in this work we study the elliptic curve over the artinian principal ideal ring $R_n = F_{3^d}[\epsilon], \epsilon^n = 0$. *More precisely, we defined the* J*-invariant of* $E^n_{3^d}$. *More precisely, we establish* $\pi(J) = j$, *where* j *is the* j*-invariant of an elliptic curve over* F_{3^d} *and* π *is the canonical projection defined over ring* R_n *by* F_{3^d}, *and two elliptic curves on* R_n *are isomorphic if and only if they have the same* J*-invariant.*

5 Open Problem

In this section you should present an open problem.

- *Study Elliptic Curve Over Finite Ring Of Characteristic 2.*
- *The J-invariant Over This Curve.*
- *Cryptography Over This Curve.*
- *Discret Logarithm Attack.*

ACKNOWLEDGEMENTS. *I would thank Editors for his helpful comments and suggestions.*

References

[1] *A. Chillali, "Ellipic cuvre over ring",* International Mathematical Forum*, Vol. 6, no . 31, 1501-1505, 2011.*

[2] *A. Chillali, "Identification methods over $E^n_{a,b}$",* In Proceedings of the 2011 international conference on Applied computational mathematics (ICACM'11), Vladimir Vasek, Yuriy Shmaliy, Denis Trcek, Nobuhiko P. Kobayashi, and Ryszard S. Choras (Eds.). World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin*, USA, 133-138.2011.*

[3] *A. Chillali, "Cryptography Over Elliptic Curve Of The Ring $F_q[\epsilon], \epsilon^4 = 0$",* World Academy of Science, Engineering and Technology 78 2011*, pages 847-850, 2011.*

[4] *A. Chillali,"The $J_{\epsilon,n} -$ invariant of $E^n_{A,B}$",* Recent Advances in Computers, Communications, Applied Social Science and Mathematics, *ICANCM'11, Published by WSEAS Press, pages 54-56, 2011.*