THÔNG TIN VỀ LUẬN VĂN THẠC SĨ

1. Họ và tên học viên: **Võ Tùng Linh** 2. Giới tính: Nam

3. Ngày sinh: 01/09/1983 4. Nơi sinh: Thanh Hóa

5. Quyết định công nhận học viên số: , ngày tháng năm

6. Các thay đổi trong quá trình đào tạo: Không

7. Tên đề tài luận văn:

"Về dạng chuẩn Edwards và một vài ứng dụng"

8. Chuyên ngành: Đại số và lý thuyết số 9. Mã số: 60.46.01.04

10. Cán bộ hướng dẫn khoa học: ***TS.Phó Đức Tài*** - Đại học Khoa học Tự nhiên - Đại học Quốc Gia Hà Nội

11. Tóm tắt các kết quả của luận văn:

Luận văn được trình bày theo bố cục gồm 3 chương.

Chương 1: Kiến thức chuẩn bị

Trong chương này, chúng tôi nhắc lại một số định nghĩa cơ bản và kết quả quan trọng của lý thuyết đường cong elliptic tổng quát như là phép cộng điểm, định lý Hasse. Ngoài ra chúng tôi cũng trình bày về dạng Montgomery cho đường cong elliptic và sự biến đổi qua lại giữa nó với dạng Weierstrass.

Định lý 1.10 *Cho* K *là một trường với* $\text{char}\left(K\right) \neq 2,3$. *Một đường cong elliptic dạng Weierstrass ngắn* $E: y^2 = x^3 + ax + b$ *biến đổi được về dạng Montgomery nếu và chỉ nếu các điều kiện sau được thỏa mãn:*

1. *Phương trình* $x^3 + ax + b = 0$ *có ít nhất một nghiệm trong* K.
2. *Phần tử* $3\alpha^2 + a$ *là chính phương trong* K, *ở đây* α *là một nghiệm của phương trình* $x^3 + ax + b = 0$ *trong* K.

Chương 2: Dạng chuẩn Edwards cho đường cong elliptic

Trong chương này, chúng tôi trình bày định nghĩa đường cong Edwards và đường cong Edwards cuộn. Chúng tôi chỉ ra mọi đường cong elliptic có một điểm cấp 4 là

tương đương song hữu tỉ với một đường cong Edwards trên trường k có đặc số khác 2. Tiếp theo chúng tôi trình bày công thức cộng điểm trên đường cong Edwards cuộn. Cuối cùng, chúng tôi chỉ ra tập các điểm trên đường cong Edwards cuộn lập thành một nhóm aben dưới phép cộng điểm đó.

Định lý 2.15 *Cho* $E_{E,a,d}$ *là một đường cong Edwards cuộn xác định trên* k *với* $\text{char}\left(k\right) \neq 2$. *Giả sử rằng* $P_1, P_2 \in \overline{E}_{E,a,d}\left(k\right)$. *Viết* $P_1 = \left(\left(X_1 : Z_1\right), \left(Y_1 : T_1\right)\right)$, $P_2 = \left(\left(X_2 : Z_2\right), \left(Y_2 : T_2\right)\right)$. *Định nghĩa*

$$\begin{aligned} X_3 &= X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2, \\ Z_3 &= Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2, \\ Y_3 &= Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2, \\ T_3 &= Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2, \end{aligned}$$

và

$$\begin{aligned} X_3' &= X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1, \\ Z_3' &= aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2, \\ Y_3' &= X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1, \\ T_3' &= X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2. \end{aligned}$$

Khi đó $X_3Z_3' = X_3'Z_3$ *và* $Y_3T_3' = Y_3'T_3$. *Hơn nữa, ít nhất một trong các trường hợp dưới đây được thỏa mãn:*

- $\left(X_3, Z_3\right) \neq \left(0,0\right)$ *và* $\left(Y_3, T_3\right) \neq \left(0,0\right)$. *Khi đó* $P_1 + P_2 = \left(\left(X_3 : Z_3\right), \left(Y_3 : T_3\right)\right)$.
- $\left(X_3', Z_3'\right) \neq \left(0,0\right)$ *và* $\left(Y_3', Z_3'\right) \neq \left(0,0\right)$. *Khi đó* $P_1 + P_2 = \left(\left(X_3' : Z_3'\right), \left(Y_3' : T_3'\right)\right)$.

Nếu $P_1 = P_2$ *thì trường hợp thứ nhất xảy ra.*

Chương 3: Một số ứng dụng của đường cong dạng chuẩn Edwards

Trước tiên, chúng tôi tính các điểm có cấp nhỏ trên một đường cong Edwards cuộn. Tiếp theo chúng tôi trình bày cách xây dựng các đường cong Edwards với nhóm xoắn cho trước. Sau đó chúng tôi áp dụng những cách xây dựng này cho đường cong elliptic dạng Weierstrass. Cuối cùng chúng tôi đưa ra một số ví dụ về các đường cong elliptic dạng Weierstrass với nhóm xoắn đã biết và ứng dụng của đường cong Edwards trong mật mã.

Hệ quả 3.12 *Giả sử* $d \in \mathbb{Q} \setminus \{0,1\}$. *Khi đó đường cong elliptic xác định trên* $\mathbb{Q}$

$$\mathcal{E} : Y^2 = X^3 + \frac{1+d}{2} X^2 + \frac{\left(1-d\right)^2}{16} X$$

có nhóm xoắn $\mathcal{E}_{\text{tor}}\left(\mathbb{Q}\right)$ *đẳng cấu với*

$$\begin{cases} \mathbb{Z}/12\mathbb{Z}, \text{ nếu } \ d = \frac{\left(1+t^2\right)^3\left(1-4t+t^2\right)}{\left(1-t\right)^6\left(1+t\right)^2} \text{ với } t \in \mathbb{Q} \setminus \{0,\pm 1\}; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \ \text{ nếu } \ d = \frac{\left(t^2-2\right)^2\left(t^2+4t+2\right)^2}{\left(t^2+2t+2\right)^4} \ \text{ với } \ t \in \mathbb{Q} \setminus \{-2,-1,0\}; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \ \text{ nếu } \ d \in \mathbb{Q}^2 \ \text{ và } \ \left(dx^4 - 2x^2 + 1\right)\left(dx^4 - 2dx^2 + 1\right) \neq 0, \forall x \in \mathbb{Q}; \\ \mathbb{Z}/8\mathbb{Z}, \quad \text{nếu } \ d \notin \mathbb{Q}^2 \ \text{ và } \ d = \frac{2t^2-1}{t^4} \ \text{ với } \ t \in \mathbb{Q} \setminus \{0,\pm 1\} \\ \mathbb{Z}/4\mathbb{Z}, \quad \text{các trường hợp còn lại,} \end{cases}$$

ở đây ký hiệu $\mathbb{Q}^2 = \{a^2 \mid a \in \mathbb{Q}\}$..

Ngày 03 tháng 12 năm 2014

Học viên

(Kí và ghi rõ họ tên)

Võ Tùng Linh

INFORMATION ON MASTER'S THESIS

1. Full name: **Võ Tùng Linh** 2. Sex: male

3. Date of birth:01/09/1983 4. Place of birth: Thanh Hóa

5. Admission decision number: Dated

6. Changes in academic process: no

7. Official thesis title:

"On the Edwards form and some applications"

8. Major: Algebra and number theory 9. Code: 60.46.01.04

10. Supervisors: ***Dr. Phó Đức Tài***

11. Summary of the thesis:

The thesis includes 3 chapters.

Chapter 1: Background

In this chapter, the firrst we repeat some basic definitions and important results of general elliptic curve theory included addition law and Hasse's theorem. Furthermore, we also present the Montgomery form of the elliptic curves and study transformabilities from the Weierstrass-form to the Montgomery form.

Theorem 1.10 *Let* K *be a field with* $\text{char}\left(K\right) \neq 2,3$. *A short Weierstrass-form elliptic curve* $E: y^2 = x^3 + ax + b$ *is transformable to the Montgomery-form if and only if it satisfies two conditions as follows:*

3. *The equation* $x^3 + ax + b = 0$ *has at least one root in* K.
4. *The element* $3\alpha^2 + a$ *is square in* K, *where* α *is a root of the equation* $x^3 + ax + b = 0$ *in* K.

Chapter 2: Edwards form of the elliptic curves

In this chapter, we present the definition of a Edwards curve and a twisted Edwards cuvres. We show that every elliptic curves which has a point of order 4 is

birationally equivalent to an Edwards curve over field k with $\text{char}\left(k\right) \neq 2$. Next we present formula for addition of points on the twisted Edwards curve. Finally, we show that set of points on an twisted Edwards curve forms a abelian group under that addition law.

Theorem 2.15 *Let $E_{E,a,d}$ be a twisted Edwards cuve difined in k with* $\text{char}\left(k\right) \neq 2$. *Assume that $P_1, P_2 \in \bar{E}_{E,a,d}\left(k\right)$. Write $P_1 = \left(\left(X_1 : Z_1\right), \left(Y_1 : T_1\right)\right)$, $P_2 = \left(\left(X_2 : Z_2\right), \left(Y_2 : T_2\right)\right)$. Define*

$$\begin{aligned} X_3 &= X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2, \\ Z_3 &= Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2, \\ Y_3 &= Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2, \\ T_3 &= Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2, \end{aligned}$$

and

$$\begin{aligned} X_3' &= X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1, \\ Z_3' &= aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2, \\ Y_3' &= X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1, \\ T_3' &= X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2. \end{aligned}$$

Then $X_3Z_3' = X_3'Z_3$ and $Y_3T_3' = Y_3'T_3$. Furthermore, at least one of the following cases occurs:

- $\left(X_3, Z_3\right) \neq \left(0,0\right)$ *and* $\left(Y_3, T_3\right) \neq \left(0,0\right)$. *Then* $P_1 + P_2 = \left(\left(X_3 : Z_3\right), \left(Y_3 : T_3\right)\right)$.
- $\left(X_3', Z_3'\right) \neq \left(0,0\right)$ *and* $\left(Y_3', Z_3'\right) \neq \left(0,0\right)$. *Then* $P_1 + P_2 = \left(\left(X_3' : Z_3'\right), \left(Y_3' : T_3'\right)\right)$.

If $P_1 = P_2$ then the first case occurs.

Chapter 3: Some application of the Edwards curve

The first, we compute the points of small order on a twisted Edwards curve. The we present constructions the Edwards curves with given torsion group. Then we apply these contructions for the Weierstrass-form elliptic curves. Finally, we give some examples of the Weierstrass elliptic curves with given torsion group and the application of Edwards curve in cryptogrpahy.

Corollary 3.12 *Let* $d \in \mathbb{Q} \setminus \{0,1\}$. *Then the elliptic curve difined in* $\mathbb{Q}$

$$\mathcal{E} : Y^2 = X^3 + \frac{1+d}{2} X^2 + \frac{\left(1-d\right)^2}{16} X$$

has torsion group $\mathcal{E}_{\text{tor}}\left(\mathbb{Q}\right)$ *that isomorphic to*

$$\begin{cases} \mathbb{Z}/12\mathbb{Z}, \ if \quad d = \frac{\left(1+t^2\right)^3\left(1-4t+t^2\right)}{\left(1-t\right)^6\left(1+t\right)^2} \ with \ t \in \mathbb{Q} \setminus \{0, \pm 1\}; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \quad if \quad d = \frac{\left(t^2-2\right)^2\left(t^2+4t+2\right)^2}{\left(t^2+2t+2\right)^4} \quad with \quad t \in \mathbb{Q} \setminus \{-2,-1,0\}; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad if \quad d \in \mathbb{Q}^2 \quad and \quad \left(dx^4 - 2x^2 + 1\right)\left(dx^4 - 2dx^2 + 1\right) \neq 0, \forall x \in \mathbb{Q}; \\ \mathbb{Z}/8\mathbb{Z}, \quad if \quad d \notin \mathbb{Q}^2 \quad and \quad d = \frac{2t^2-1}{t^4} \quad with \quad t \in \mathbb{Q} \setminus \{0, \pm 1\} \\ \mathbb{Z}/4\mathbb{Z}, \quad otherwise. \end{cases}$$

where $\mathbb{Q}^2 = \{a^2 \mid a \in \mathbb{Q}\}$.

Date:03/12/2014

Signature:

Full name: ***Võ Tùng Linh***