BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP. HỒ CHÍ MINH

Trần Nguyễn Toàn Vinh

ĐƯỜNG CONG ELLIPTIC DẠNG HESSE

Chuyên Ngành: Hình Học Và Tôpô
Mã Số: 60 46 10

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. PHAN DÂN

Thành phố Hồ Chí Minh – 2010

LỜI CẢM ƠN

Luận văn được hoàn thành nhờ sự hướng dẫn khoa học của TS Phan Dân. Tôi xin bày tỏ lòng biết ơn sâu sắc đến Thầy, vì Thầy đã trang bị cho tôi tài liệu, tạo cơ hội cho tôi làm quen với đường cong elliptic và một số ứng dụng của đường cong elliptic, biết được sự tương đương tuyến tính giữa đường cong elliptic dạng Hesse và dạng Weierstrass, ứng dụng của đường cong elliptic dạng Hesse trong Lý thuyết mã hoá thông tin.

Tôi xin chân thành cảm ơn quý Thầy trong tổ Hình học khoa Toán – Tin Trường Đại học Sư phạm Tp.Hồ Chí Minh đã giúp đỡ cho tôi những kiến thức chuyên môn và phương pháp làm việc trong suốt quá trình học Cao học.

Chân thành cảm ơn Ban giám hiệu, phòng Tổ chức hành chính, phòng Khoa học Công nghệ và Sau đại học, phòng Kế hoạch – Tài chính Trường Đại học Sư phạm Tp.Hồ Chí Minh, Ban giám hiệu Trường trung học cơ sở và trung học phổ thông Nguyễn Khuyến cùng toàn thể các đồng nghiệp, các bạn học viên và gia đình đã động viên giúp đỡ, tạo điều kiện thuận lợi cho tôi hoàn thành luận văn này.

Tp.Hồ Chí Minh, tháng 07 năm 2010

Tác giả

Trần Nguyễn Toàn Vinh

BẢNG CHỈ DẪN CÁC KÝ HIỆU

$\sqrt{I}$	Căn của iđêan I
$\deg(f)$	Bậc của đa thức f
$E_H(\mathbb{F}_q)$	Đường cong elliptic dạng Hesse trên trường $\mathbb{F}_q$
$E_W(\mathbb{F}_q)$	Đường cong elliptic dạng Weierstrass trên trường $\mathbb{F}_q$
$E(k)$	Đường cong elliptic trên trường k
#E(K)	Cấp của E(K)
$G(k)$	Nhóm các điểm hữu tỉ
$A \oplus B$	Tổng trực tiếp của các nhóm A và B
k[X]	Trường các hàm hữu tỉ trên X
$\overline{\mathbb{F}}_q$	Trường đóng đại số của $\mathbb{F}_q$
$\mathcal{I}(X)$	Iđêan triệt tiêu của X
$\mathcal{O}$(X)	Vành các hàm chính quy trên X
X(k)	Tập tất cả các điểm k-hữu tỷ trên X
X($\mathbb{Q}$)	Tập hợp các điểm hữu tỷ của đường cong X
$\mathbb{A}^n$	Không gian afin n-chiều
$\mathbb{P}^n$	Không gian xạ ảnh n-chiều trên trường k đóng đại số
$\mathbb{F}_q$	Trường hữu hạn gồm q phần tử
g	Cơ sở Gröbner **g**

$\mathbb{G}_m$	Nhóm nhân
$\mathbb{G}_a$	Nhóm cộng tính
$\mathbb{G}_m^{(a)}$	Nhóm xoắn
$\boldsymbol{G}(k)$	Nhóm các điểm hữu tỉ
gdc(a, b, c)	Ước chung lớn nhất của a, b, c
$k[x_1, \ldots, x_n]$	Vành đa thức trên k với n biến
T(A)	Nhóm con xoắn của nhóm aben A

I. MỞ ĐẦU

I.1 Lý do chọn đề tài

Việc nghiên cứu các đường cong elliptic, các tích phân elliptic và các hàm elliptic đã từng là một trong những chủ đề được quan tâm nhiều nhất trong các lĩnh vực nghiên cứu của các nhà Toán học thế kỷ 19, trong đó có thể kể đến những nhà Toán học có tên tuổi như Abel, Gauss, Jacobi và Legendre. Nói riêng về các đường cong elliptic – thuộc một trong các đối tượng nghiên cứu của Hình học Đại số cũng là một đề tài mang tính thời sự. Tuy nhiên cùng với sự phát triển mạnh mẽ gần đây của Lý thuyết mã hoá thông tin gắn liền với các kết quả nghiên cứu trên các đường cong đã đặt ra một yêu cầu rất tự nhiên là tìm kiếm các dạng mô tả khác nhau đối với đường cong elliptic để từ đó có thể lựa chọn thuật toán ngày càng tốt hơn cho việc tính toán xác định các đặc trưng trên chúng. Phần lớn các kết quả nghiên cứu thuộc lĩnh vực này đều xuất phát từ hai dạng biểu diễn phổ biến nhất là dạng Weierstrass và dạng Hesse của đường cong elliptic.

Trong phạm vi đề tài, chúng tôi sẽ xét dạng Hesse của đường cong elliptic và cũng đề cập tới một số thông tin về mối liên hệ tới dạng Weierstrass của chúng để có được một cách nhìn tổng quát hơn khi nghiên cứu các đối tượng này.

Vì vậy, đề tài có tên gọi là "Đường cong elliptic dạng Hesse".

I.2 Lịch sử của vấn đề

Hướng nghiên cứu mà đề tài tiếp cận dựa trên các kết quả sau đây:

a) Một là kết quả rất thú vị trên các nhóm aben hữu hạn sinh (các Z-mođun hữu hạn sinh): "Mỗi nhóm aben hữu hạn sinh là tổng trực tiếp của các nhóm con cyclic", mà về thực chất thì các hạng tử trong sự biểu diễn này đều có thể mô tả tường minh thông qua 2 phần xoắn và không xoắn.
b) Hai là sử dụng Định lý Bézout về số giao điểm của các đường cong xạ ảnh phức.
c) Ba là Hệ quả của Định lý Riemann-Roch khẳng định về cấu trúc nhóm của tập các điểm trên đường cong elliptic.

Luận văn của chúng tôi tập trung giải quyết một số vấn đề về: mô tả luật nhóm trên các đường cong dạng Hesse, các j-bất biến, thuật toán xác định các điểm n-xoắn, khảo sát sự tương đương tuyến tính của các đường cong elliptic dưới các dạng Hesse và Weierstrass.

I.3 **Đối tượng và phạm vi nghiên cứu**

- Nghiên cứu các đường cong elliptic dưới dạng Hesse trên trường hữu hạn và trường số phức.

- Đề tài chỉ giới hạn trong phạm vi xét luật nhóm trên các đường cong dạng Hesse, đặc trưng j-bất biến và các điểm n-xoắn trên họ đường cong này.

- Xác lập sự tương đương tuyến tính giữa hai cách biểu diễn Weierstrass và Hesse.

- Một số ứng dụng của sự tương đương tuyến tính.

I.4 **Mục đích nghiên cứu**

- Mô tả chi tiết cách tiếp cận, phương pháp xây dựng thuật toán xác định luật nhóm trên đường cong elliptic dạng Hesse.

- Nghiên cứu tính đối xứng của các đường cong dạng Hesse, xác định j-bất biến của các đường cong dạng này
- Tính toán xác định các điểm n-xoắn trên một số lớp đường cong dạng Hesse.
- Mối liên hệ giữa hai dạng Weierstrass và Hesse. Tương đương tuyến tính.

Hoàn chỉnh việc chứng minh một số Định lý mô tả tính chất của các đường cong dạng Hesse thuộc về các chủ đề vừa nêu.

I.5 **Phương pháp nghiên cứu**

Sử dụng phương pháp mô tả các đường cong elliptic dạng Hesse, thực hiện việc xây dựng luật nhóm trên các đường cong này và xác định các điểm xoắn trên một số họ đường cong cụ thể. Phần thứ hai sẽ sử dụng phương pháp tạo lập ánh xạ tuyến tính giữa hai dạng Weierstrass và Hesse của các đường cong elliptic (bảo toàn j-bất biến và tập hợp các điểm). Đây là một số hướng nghiên cứu và kỹ thuật được dùng khá phổ biến trong việc nghiên cứu các đường cong elliptic. Các hướng nghiên cứu này đã và đang được sử dụng và phát triển bởi nhiều tác giả trong hơn nửa thế kỷ qua trên thế giới. Các phương pháp nghiên cứu được dùng trong Luận văn này dựa trên những công cụ nghiên cứu đã được sử dụng trong [Fri], [Ful1], [Sil3].

II. NỘI DUNG

Chương 1. KIẾN THỨC CƠ BẢN

1.1. Các nhóm aben hữu hạn sinh

Định nghĩa 1.1.1:

Một nhóm aben A là hữu hạn sinh nếu có các phần tử hữu hạn $a_1, a_2, ..., a_n \in A$ sao cho với bất kỳ $x \in A$, có các số nguyên $k_1, k_2, \dots, k_n$ sao cho $x = \sum_{i=1}^{n} k_i a_i$.

Định nghĩa 1.1.2:

Cho A là một nhóm aben. Nhóm con xoắn của A, ký hiệu T(A), là tập:

$$T(A) = \{a \in A \mid \exists n \in \mathbb{N} : na = 0\}.$$

Định nghĩa 1.1.3:

Một nhóm aben A được gọi là không xoắn nếu $T(A) = \{0\}$.

Bổ đề 1.1.4:

Cho A là một nhóm aben. Khi đó A/T(A) là không xoắn.

Định nghĩa 1.1.5:

$\mathbb{Z}^n = \mathbb{Z} \oplus ... \oplus \mathbb{Z}$ (n hạng tử) được gọi là nhóm aben tự do hạng n.

Định lý 1.1.6:

Nếu A là một nhóm aben không xoắn hữu hạn sinh mà có một tập hợp các phần tử sinh nhỏ nhất với n phần tử, khi đó A đẳng cấu với nhóm aben tự do hạng n.

Chứng minh:

Lý luận bằng phương pháp quy nạp trên số các phần tử sinh cực tiểu của A. Nếu A là cyclic (đó là được sinh bởi phần tử khác 0), khi đó $A \cong \mathbb{Z}$. Giả sử rằng kết quả cho thấy tất cả các nhóm aben không xoắn hữu hạn sinh với một tập hợp các phần tử sinh nhỏ nhất có ít hơn n phần tử. Giả sử A là

không xoắn và $\{a_1, a_2, ..., a_n\}$ là một tập các phần tử sinh cực tiểu của A. Nếu T(A/<a_1>)={0} khi đó A/<a_1> là không xoắn và được sinh bởi n-1 phần tử, suy ra <a_1> $\cong \mathbb{Z}$. Nếu T(A/<a_1>) không là nhóm tầm thường thì có một nhóm con $B \subset A$ sao cho T(A/<a_1>) $\cong$ B/<a_1>. Như thế với bất kỳ phần tử $0 \neq b \in B$ có một số nguyên $0 \neq i \in \mathbb{Z}$ sao cho $ib \in$<a_1>. Nhưng sau đó thì $ib = ja_1$ với $j \in \mathbb{Z}$. Định nghĩa một ánh xạ :

$$f : B \to \mathbb{Q}$$
$$b \mapsto f(b) = j/i \quad \text{(và f(0) = 0).}$$

Đọc giả có thể kiểm tra ánh xạ này là một phép đồng cấu được định nghĩa tốt trong các nhóm aben và cũng có thể kiểm tra rằng ánh xạ này có hạt nhân tầm thường, do đó là đơn ánh để : $B \cong f(B)$. Bây giờ, nếu B là hữu hạn sinh (vì $\mathbb{Z}$ là một vành Noether) thì B là cyclic.

Để thấy điều này giả sử b = <b_1, …, b_m>. Khi đó:

$f(B) = < f(b_1), \ldots, f(b_m) > = <j_1/i_1, \ldots, j_m/i_m>$ là một nhóm con của nhóm cyclic <$1/i_1 \ldots i_m$>, do đó là cyclic.

Nếu B = A thì A tự do trên một phần tử sinh. Ngược lại thì:

$$A / B = <\overline{a_1}, ..., \overline{a_n}> = <\overline{a_2}, ..., \overline{a_n}>$$

$$A / B \cong (A/ < a_1 >) / (B/ < a_1 >) \cong (A/ < a_1 >) / T(A/ < a_1 >).$$

Do đó, A/B là không xoắn và được sinh bởi ít nhất n – 1 phần tử, do đó là aben tự do hạng m < n.

Suy ra: $A \cong B \oplus \mathbb{Z}^m$ sao cho $B \cong A / \mathbb{Z}^m$ và hữu hạn sinh.

Do B là cyclic nên ta có điều phải chứng minh.

***Chú ý*:** m = n – 1 vì n là cực tiểu.

Định nghĩa 1.1.7:

Cho A là một nhóm aben, và cho B và C là các nhóm con của A. Ta nói rằng A là tổng trực tiếp của B và C, ký hiệu $A = B \oplus C$, nếu A = B + C và $B \bigcap C = \{0\}$, ở đây B + C = { b + c | b∈B và c∈C}.

Định nghĩa 1.1.8:

Cho $\mathfrak{P}$ là một phạm trù và cho X và Y là các vật của $\mathfrak{P}$. Một cấu xạ f: X $\rightarrow$ Y được gọi là đơn xạ khi với bất kỳ vật Z của $\mathfrak{P}$ và bất kỳ cặp cấu xạ: i, j: Z $\rightarrow$ X, nếu $f \circ i = f \circ j$ thì i = j.

Định nghĩa 1.1.9:

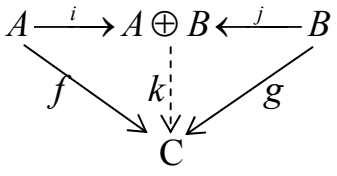
Cho $\mathfrak{P}$ là một phạm trù và cho X và Y là các vật của $\mathfrak{P}$. Một cấu xạ f: X $\rightarrow$ Y được gọi là toàn xạ khi với bất kỳ vật Z của $\mathfrak{P}$ và bất kỳ cặp cấu xạ: i, j: Y $\rightarrow$ Z, nếu $i \circ f = j \circ f$ thì $i = j$.

Định nghĩa 1.1.10:

Cho A và B là các nhóm aben. Tổng trực tiếp của A và B trong phạm trù các nhóm aben, ký hiệu $A \oplus B$ là một nhóm aben, $A \oplus B$ cùng với các phép đồng cấu chính tắc

i: A $\rightarrow$ $A \oplus B$ và j: B $\rightarrow$ $A \oplus B$ với nhóm aben bất kỳ C và các cấu xạ

f: A $\rightarrow$ C và g: B $\rightarrow$ C, có một ánh xạ duy nhất k: $A \oplus B$ $\rightarrow$ C làm cho biểu đồ sau giao hoán:



Suy ra i, j là các phép đơn ánh.

***Chú ý*:** Định nghĩa 1.1.10 là một ví dụ về định nghĩa tính chất phổ dụng. Chú ý rằng, định nghĩa này có ý nghĩa trong phạm trù bất kỳ, nhưng do một vật

không không nhất thiết tồn tại trong mỗi phạm trù; ta vật phải đưa ra một cấu trúc của một vật và chứng minh rằng nó thỏa mãn tính chất phổ dụng.

Định lý 1.1.11:

Cho A là một nhóm aben được hữu hạn sinh. Khi đó có một phép đẳng cấu:

$$f : A \cong T(A) \oplus A / T(A).$$

Chứng minh:

Giả sử $A =< a_1,....,a_n >$. Khi đó $A / T(A) =< \overline{a_1},...,\overline{a_n} >$ sao cho A/T(A) là hữu hạn sinh.

Cho $< \overline{x_1},...,\overline{x_m} >$ là một tập hợp các phần tử sinh cực tiểu cho A/T(A).

Nếu $\overline{a} \in A / T(A)$ thì $\overline{a} = \sum_{i=1}^{m} k_1 x_i$ với các số nguyên $k_i \in \mathbb{Z}$, suy ra $a - \sum_{i=1}^{m} k_1 x_i \in T(A)$.

Do đó, A = $< x_1,...,x_m > + T(A)$.

Hơn nữa, vì A/T(A) là không xoắn, suy ra $< x_1,...,x_m > \bigcap T(A) = \{0\}$, và do đó:

$$\text{A} =< x_1,...,x_m > \oplus T(A).$$

Chú ý: Nếu: $\pi : A \to A / T(A)$ là đồng cấu thương và $\tau : A / T(a) \to A$ được cho bởi $\tau(\overline{x_i}) = x_i$ khi đó $\pi \circ \tau$ là một đồng cấu đồng nhất của A/T(A) và τ là một đơn ánh.

Hệ quả 1.1.12:

Mỗi nhóm aben hữu hạn sinh là tổng trực tiếp của một nhóm hữu hạn và một nhóm aben tự do hạng n với n $\in \mathbb{Z}$.

Chứng minh:

Đọc giả có thể kiểm tra rằng T(A) là một nhóm hữu hạn. A/T(A) được sinh hữu hạn và không xoắn, vì thế, theo định lý 1.1.6, nó là một nhóm aben tự do hạng n với n $\in \mathbb{Z}$.

1.2. Các đa tạp afin và đa tạp xạ ảnh.

1.2.1. Các đa tạp afin.

Chúng ta nghiên cứu trên trường k. Nếu không có giải thích gì thêm thì trường k luôn là đóng đại số.

Định nghĩa 1.2.1.1.

Không gian afin n-chiều $\mathbb{A}^n$ (hoặc $\mathbb{A}^n(k)$) trên trường k là tập hợp các bộ n-thành phần là các phần tử của k. Một phần tử $p = (p_1, p_2, ..., p_n) \in \mathbb{A}^n$ được gọi là một điểm, các p_i là các tọa độ afin của p.

Ta ký hiệu $k[x_1, ..., x_n]$ là vành đa thức trên k với n biến. Các phần tử của $k[x_1, ..., x_n]$ thường thể hiện như các hàm $k^n \to k$.

Định nghĩa 1.2.1.2:

Một tập con $X \subseteq \mathbb{A}^n$ là một đa tạp đại số afin, nếu nó là một tập zero của một tập hữu hạn của các đa thức trong $k[x_1, ..., x_n]$:

Cho $f_1, ..., f_k \in k[x_1, ..., x_n]$ thì: $= Z(f_1, ..., f_k) = \{p \in A^n \mid f_i(p) = 0, \forall i\}$.

Định nghĩa 1.2.1.3.

Một đa tạp $X \subseteq \mathbb{A}^n$ là bất khả quy nếu nó không là hợp hữu hạn của các đa tạp con thực sự, nghĩa là nếu với mỗi đa tạp $X_1, X_2 \subseteq \mathbb{A}^n$ sao cho $X = X_1 \cup X_2$ thỏa mãn thì $X = X_1$ hoặc $X = X_2$.

Mệnh đề 1.2.1.4.

Bất kỳ đa tạp X có thể được phân tích như một hợp hữu hạn của các đa tạp con bất khả quy

$$X = X_1 \cup X_2 \cup ...X_m$$

ở đây, $X_i \not\subseteq X_j$ với mọi $i \neq j$. Vì thế phép phân tích trên là duy nhất sai khác một phép hoán vị.

Ví dụ 1:

Một đa tạp tuyến tính là một tập nghiệm của một hệ tuyến tính $l_1, \ldots, l_k$. Nếu $X = Z(l_1,\ldots, l_k)$ khác rỗng và các phương trình tuyến tính xác định là độc lập, khi đó số chiều của X là n – k và số đối chiều của X là:

$$\text{codim}X = \text{dim}A^n - \text{dim } X = k.$$

Việc định nghĩa về số chiều của các đa tạp tuyến tính có thể được tham khảo từ đại số tuyến tính. Trong trường hợp các đa tạp không tuyến tính ta dựa vào một khái niệm trực giác về số chiều.

Ví dụ 2:

Một siêu mặt $X \subseteq \mathbb{A}^n$ là một đa tạp được cho bởi phương trình, $X = Z(f)$. Nó là một đa tạp có đối chiều 1. Nếu n = 3, siêu mặt được gọi là một mặt.

Cho $f = (x^2 + y^2 - z^2)(z - 1) \in k[x, y, z]$. Khi đó, $Z(f) \in \mathbb{A}^3$ là khả quy bao gồm hai thành phần: một hình nón qua O và một mặt phẳng.

Đối với một siêu mặt, dễ dàng tìm được sự phân tích thành các thành phần bất khả quy: người ta chỉ cần tìm thừa số trong phương trình định nghĩa. Nhìn chung, đối với các đa tạp có đối chiều cao hơn, nó là một bài toán khó. Có các thuật toán giải quyết bài toán này dựa trên việc tìm một cơ sở Gröbner, chúng đòi hỏi một sự tính toán mất nhiều thời gian.

Ví dụ 3:

Một siêu mặt trong $\mathbb{A}^2$ là một đường cong đại số phẳng. Một parabol có thể được cho bởi tham số hóa $t \mapsto (t,t^2)$ hoặc hoàn toàn bởi $y - x^2 \in k[x;y]$.

Ví dụ 4:

Cubic xoắn là một đường cong trong $\mathbb{A}^3$ được cho bởi tham số hóa $t \mapsto (t,t^2,t^3)$. Nó hoàn toàn được cho bởi hai phương trình $f_1 = y - x^2$ và $f_2 = z - xy \in k[x;y;z]$.

Ví dụ 5:

Hợp và giao hữu hạn các đa tạp afin lại là một đa tạp afin.

Nếu $X, Y \subseteq \mathbb{A}^n$ trong đó: $X = Z(f_1, \ldots, f_k)$ và $Y = Z(g_1, \ldots, g_l)$,

thì $X \cap Y = Z(f_1,\ldots,f_k,g_1,\ldots,g_l)$ và $X \cup Y = Z(f_i g_j \mid i = 1,\ldots,k; j = i,\ldots,l)$.

Ví dụ 6:

Cho $X \subseteq \mathbb{A}^n$ được xác định bởi $f_1, \ldots, f_k \in k[x_1,\ldots,x_n]$ và $Y \subseteq \mathbb{A}^m$ cho bởi $g_1,\ldots,g_l \in k[y_1,\ldots,y_m]$. Khi đó tích của X và Y là một đa tạp trong $\mathbb{A}^{m+n}$ và là một tập zero của $f_1, \ldots, f_k, g_1, \ldots, g_l$ với f_i, g_j được hiểu như các đa thức trong $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

1.2. 2. Định lý cơ bản của Hilbert:

Chú ý rằng, nếu một đa tạp afin $X \subseteq \mathbb{A}^n$ được xác định như sau $X = Z(f_1, \ldots, f_k), f_i \in k[x_1,\ldots,x_n]$, thì với mỗi f từ iđêan $I = (f_1, \ldots, f_k)$ ta có $f(p) = 0$ với mọi $p \in X$.

Hơn nữa, nếu hai tập hợp của các phương trình sinh ra cùng iđêan, $(f_1, \ldots, f_k) = (g_1, \ldots, g_l)$ thì dễ dàng chứng minh rằng $Z(f_1, \ldots, f_k) = Z(g_1, \ldots, g_l)$. Do đó ta có thể thay đổi định nghĩa của một đa tạp afin sao cho thay vì nói

các phương trình định nghĩa ta nói iđêan định nghĩa: $X \subseteq \mathbb{A}^n$ là một đa tạp afin nếu nó là một tập zero của một iđêan hữu hạn sinh trong $k[x_1, \ldots, x_n]$.

Cho R là một vành giao hoán với 1. (Trường hợp được xét: R là một trường hoặc một vành đa thức trên một trường).

Định nghĩa 1.2.2.1.

Vành R là vành Noether nếu mọi iđêan của R đều hữu hạn sinh.

Định lý 1.2.2.2. (Định lý cơ bản của Hilbert).

Nếu R là một vành Noether thì R[x] cũng là vành Noether .

Hệ quả 1.2.2.3.

Mọi iđêan trong $k[x_1, \ldots, x_n]$ là hữu hạn sinh.

Từ định lý cơ bản Hilbert ta có giao của các đa tạp đại số lại là một đa tạp, vì nó là một tập zero của một iđêan được sinh bởi tất cả các phần tử sinh của các iđêan định nghĩa.

Hơn thế nữa, tập rỗng $\varnothing$ và toàn bộ $\mathbb{A}^n$ cũng là các đa tạp trong $\mathbb{A}^n$. Do đó ta có định nghĩa sau:

Định nghĩa 1.2.2.4.

Trong tôpô *Zariski* các tập mở là các phần bù đối với các đa tạp đại số.

Các tập mở trong tôpô *Zariski* là rất lớn. Mỗi tập mở khác rỗng là trù mật trong $\mathbb{A}^n$. Hơn nữa bất kỳ hai tập mở khác rỗng đều giao nhau, vì thế nó không phải là tôpô Hausdorff.

1.2.3. Nullstellensatz của Hilbert.

Ví dụ 7:

Iđêan định nghĩa của một đa tạp là không duy nhất. Trong $k[x, y]$ ta xét:

$$f_1 = x^2 - y^2 \qquad I_1 = (f_1).$$

$$f_2 = (x - y)^2(x + y) \qquad I_2 = (f_2).$$

Rõ ràng, $I_1 \neq I_2$ nhưng $Z(I_1) = Z(I_2)$.

Định nghĩa 1.2.3.1.

Cho $I \subseteq k[x_1,...,x_n]$ là một iđêan. Căn của I là:

$$\sqrt{I} = \{f \in k[x_1,...,x_n] \mid f^m \in I, m \in \mathbb{N}\}.$$

Nếu $\sqrt{I} = I$, thì iđêan I được gọi là một iđêan căn.

Một số tính chất về căn của một iđêan:

(i) Với mỗi iđêan I, $\sqrt{I}$ cũng là một iđêan.

(ii) $\sqrt{\sqrt{I}} = \sqrt{I}$.

Từ ví dụ 7 trên ta có: $\sqrt{I_1} = \sqrt{I_2} = (x^2 - y^2)$.

Định nghĩa 1.2.3.2.

Cho $X \subseteq \mathbb{A}^n$ là một tập bất kỳ. Iđêan triệt tiêu của X là:

$$\mathcal{I}(X) = \{f \in k[x_1,...,x_n] \mid f(p) = 0, \forall p \in X\}.$$

Bổ đề 1.2.3.3.

Với mỗi $X \subseteq \mathbb{A}^n$, $\mathcal{I}(X)$ là một iđêan căn.

Định lý 1.2.3.4. (Hilbert's Nullstellensatz, HNS)

Cho $\mathbb{A}^n$ là một không gian afin trên một trường k đóng đại số. Khi đó với bất kỳ iđêan $I \in k[x_1,...,x_n]$ ta có: $\mathcal{I}(Z(I)) = \sqrt{I}$.

Do đó, có một song ánh $X \mapsto \mathcal{I}(X)$ của tập các đa tạp đại số trong $\mathbb{A}^n$ và tập của các iđêan căn trong $k[x_1, ..., x_n]$

Định lý 1.2.3.5. (HNS, phiên bản 2)

Cho $\mathbb{A}^n$ là một không gian afin trên một trường k đóng đại số và cho I là một iđêan trong $k[x_1,...,x_n]$. Nếu $I \neq k[x_1,...,x_n]$(nghĩa là, nếu $1 \notin I$), thì $Z(I) \neq \varnothing$.

Giả thiết k là bao đóng đại số được minh họa trong các ví dụ sau:

Ví dụ 8:

Cho k = **C.** Nếu $I = (x^2 + y^2 + 1) \subset k[x, y]$ thì $I = \sqrt{I}, I \neq k[x, y]$, nhưng $Z(I) = \varnothing$.

Ví dụ 9:

Cho k = **C.** Trong $k[x, y]$ lấy $I_1 = (x^2 + y^2)$ và $I_2 = (x, y)$. Khi đó cả hai iđêan là iđêan căn. $I_1 \neq I_2$, nhưng $Z(I_1) = Z(I_2)$.

Nhờ định lý Hilbert's Nullstellensatz, ta có thể tạo được một loại "từ điển" giữa các khái niệm đại số và hình học như sau:

X	$\mathcal{I}(X)$
$X_1 \subset X_2$	$\mathcal{I}(X_1) \supset \mathcal{I}(X_2)$
X bất khả quy	$\mathcal{I}(X)$ là nguyên tố
$X = X_1 \cup ... \cup X_m$ là một phép phân tích thành các đa tạp con bất khả quy.	$\mathcal{I}(X) = I_1 \cap .... \cap I_m$ là một phép giao của các iđêan nguyên tố, ở đây $I_i = \mathcal{I}(X_i)$

Nhìn chung, nó không thể phân tích một iđêan đã cho như một phép giao của các iđêan nguyên tố (ví dụ: $I \subset k[x]$ được sinh bởi x^2), trừ khi iđêan đã cho là một iđêan căn.

1.2.4. Các đa tạp xạ ảnh.

Định nghĩa 1.2.4.1.

Không gian xạ ảnh n-chiều $\mathbb{P}^n$ (hoặc $\mathbb{P}^n$ (k)) trên k là tập hợp các lớp tương đương của các bộ (n + 1)-phần tử của k, không đồng thời bằng 0, với mối quan hệ tương đương $\sim$, trong đó $(a_0,...,a_n) \sim (b_0,...,b_n)$ nếu có một hằng số khác 0, $\lambda \in k$ sao cho $b_i = \lambda a_i$, $\forall$i = 0, ..., n.

Một phần tử $p = (p_0 : ... : p_n) \in \mathbb{P}^n$ được gọi là một điểm. Các p_i là các tọa độ thuần nhất của p.

Một tập zero trong $\mathbb{P}^n$ của một đa thức bất kỳ $f \in k[x_0,...,x_n]$ nhìn chung không được định nghĩa tốt. Nhưng nó được định nghĩa tốt nếu f là một đa thức thuần nhất, vì khi đó $f(\lambda p_0,...,\lambda p_n) = \lambda^d f(a_0,...,a_n)$, d là bậc của f.

Định nghĩa 1.2.4.2.

Iđêan $I \subseteq k[x_0,...,x_n]$ là thuần nhất, nếu nó được sinh ra bởi các đa thức thuần nhất.

Định nghĩa 1.2.4.3.

Một tập con $X \subseteq \mathbb{P}^n$ là một đa tạp đại số xạ ảnh, nếu nó là một tập zero của một iđêan thuần nhất trong $k[x_0,...,x_n]$.

Tổng, tích và giao của các iđêan thuần nhất cũng là một iđêan thuần nhất, giống như căn của một iđêan. Hơn thế nữa, nếu một iđêan thuần nhất I không là nguyên tố thì có các đa thức thuần nhất f, g sao cho $fg \in I$ nhưng $f, g \notin I$. Do đó tương tự như trong trường hợp afin, ta có tôpô Zariski trên $\mathbb{P}^n$.

Ta luôn có thể nhúng một không gian afin vào không gian xạ ảnh có cùng số chiều như ví dụ sau:

$$\mathbb{A}^n \hookrightarrow \mathbb{P}^n \ , \ (p_1,...,p_n) \mapsto (1 : p_1 : ... : p_n).$$

Nói một cách khác, một không gian xạ ảnh có số chiều n có thể bị phủ bởi n + 1 biểu đồ afin.

$$\mathbb{P}^n = U_0 \cup ... \cup U_n \quad \text{với} \quad U_i = \{p = (p_0 : ... : p_n) \in \mathrm{P}^n \mid p_i \neq 0\}.$$

Khi đó, một phép đẳng cấu $U_i \to \mathbb{A}^n$ được mô tả như sau:

$$(p_0 : ... : p_n) \mapsto \left(\frac{p_0}{p_i} : ... : \frac{p_{i-1}}{p_i} : \frac{p_{i+1}}{p_i} : ... : \frac{p_n}{p_i} \right).$$

Có một iđêan thuần nhất đặc biệt trong $k[x_0,...,x_n]$. $I_+ = (x_0, x_1, ..., x_n)$ được gọi là một iđêan không thích hợp. Nó là một iđêan căn không tầm thường, nhưng không có đa tạp trong $\mathbb{P}^n$ tương ứng với nó, vì $Z(I_+) = (0,...,0)$, nhưng nó không là một điểm bất kỳ trong $\mathbb{P}^n$. Vì thế, với không gian xạ ảnh thì Nullstellensatz của Hilbert cần phải có một cải tiến.

Định lý 1.2.4.4. (HNS, phiên bản 1)

Cho $\mathbb{P}^n$ là một không gian xạ ảnh trên trường k đóng đại số. Khi đó: có một song ánh $X \mapsto \mathcal{I}(X)$ giữa tập hợp các đa tạp đại số trong $\mathbb{P}^n$ và tập hợp các iđêan căn thuần nhất trong $k[x_0,...,x_n]$, ngoại trừ I_+.

Định lý 1.2.4.5. (HNS, phiên bản 2)

Cho $\mathbb{P}^n$ là một không gian xạ ảnh trên trường k đóng đại số và I là một iđêan thuần nhất trong $k[x_0,...,x_n]$. Nếu $Z(I) \subseteq \mathbb{P}^n$ là tập rỗng thì I chứa I_+^m với một giá trị $m \in N$.

Ví dụ 10:

Một đa tạp tuyến tính trong $\mathbb{P}^n$ của số đối chiều k là tập zero của k dạng tuyến tính độc lập.

Ví dụ 11:

Cubic xoắn trong $\mathbb{P}^3$ được cho bởi tham số hóa: $(s:t) \mapsto (s^3 : s^2t : st^2 : t^3)$ và được biểu diễn bằng ba đa thức:

$$x_0x_2 - x_1^2,\ x_1x_3 - x_2^2,\ x_0x_3 - x_1x_2 \ .$$

Nếu ta bỏ một trong ba phương trình thì tập zero sẽ bao gồm cubic xoắn và một đường thẳng cắt cubic tại hai điểm. Các cubic xoắn có thể được tìm thấy trong [Har].

Trong trường hợp siêu mặt, ta có thể dễ dàng tìm được bao đóng xạ ảnh của đa tạp: ta phải thuần nhất phương trình định nghĩa: Nếu $X = Z(f) \subseteq \mathbb{A}^n$, trong đó: $f = f_0 + f_1 + ... + f_d$ với $f_i \in k[x_1,...,x_n]$ có bậc là i, thì bao đóng của nó trong $\mathbb{P}^n$ là $Z(x_0^d f_0 + x_0^{d-1} f_1 + ... + f_d)$.

Ví dụ minh họa của cubic xoắn trong đa tạp afin của số đối chiều cao hơn thì không dễ tìm được các phương trình của bao đóng xạ ảnh. Trong trường hợp này ta có thể thực hiện như sau:

(i) chọn một số hạng có bậc thích hợp được sắp thứ tự trong $k[x_0,...,x_n]$.

(ii) tìm cơ sở Gröbner **g** của iđêan định nghĩa X.

(iii) thuần nhất mỗi đa thức trong **g**.

Iđêan thuần nhất thu được bằng cách này là iđêan định nghĩa của bao đóng xạ ảnh $\overline{X} \subseteq \mathbb{P}^n$ của X.

Ví dụ 12:

Đường cong chuẩn tắc hữu tỉ bậc d, $C \subset \mathbb{P}^d$ là tham số hóa cho bởi:

$$(s:t) \mapsto (s^d : s^{d-1}t : \ldots : t^d)$$

Ta có thể mô tả nó bằng một tập hợp các phương trình bậc hai sao cho ma trận:

$$\begin{pmatrix} x_0 & x_1 & x_2 & \ldots & x_{d-1} \\ x_1 & x_2 & x_3 & \ldots & x_d \end{pmatrix}$$

có hạng là 1. Nghĩa là đường cong là tập zero của các đa thức:

$$x_0x_2 - x_1^2,\ x_0x_3 - x_1x_2, \ldots$$

Ví dụ 13:

Hình chiếu của một đa tạp xạ ảnh từ một điểm nằm ngoài đa tạp cũng là một đa tạp xạ ảnh. Để chứng minh điều đó, ta phải dựa trên các kết quả đã biết và dùng lý thuyết loại trừ. Nhưng ta không thể làm được điều đó với các đa tạp afin.

1.3. Các hàm và các ánh xạ.

1.3.1. Các hàm chính quy trên các đa tạp afin.

Cho X $\subseteq \mathbb{A}^n$ là một đa tạp afin trên trường k đóng đại số, cho $\mathcal{I}(X)$ là iđêan triệt tiêu của X.

Định nghĩa 1.3.1.1.

Vành tọa độ (afin) của X là vành thương

$$k[X] = k[x_1, \ldots, x_n] / \mathcal{I}(X)$$

Nếu ta xem các phần tử của $k[x_1, \ldots, x_n]$ và $k[X]$ như là các hàm thì trong cách xây dựng này ta đồng nhất tất cả các đa thức trong $k[x_1, \ldots, x_n]$ vào

trong X: với $F,G \in k[x_1,...,x_n]$ ta có $F \sim G \pmod{\mathcal{I}(X)}$, chính xác là nếu: $F(x) = G(x)$ với mọi $x \in X$.

Mệnh đề 1.3.1.2.

Một đại số giao hoán A trên trường k đẳng cấu với vành tọa độ k[X] của một đa tạp X nếu và chỉ nếu A không có lũy linh và là hữu hạn sinh như một đại số trên k.

Định nghĩa 1.3.1.3.

Một hàm số $f : X \to k$ là chính quy, nếu có một đa thức $F \in k[x_1,..,x_n]$ sao cho $f(x) = F(x), \forall x \in X$. Vành các hàm chính quy trên X được ký hiệu là $\mathcal{O}$(X).

Từ định nghĩa này ta có: $\mathcal{O}$(X) $\cong$ k[X].

Ví dụ 14:

Nếu X= $\mathbb{A}^n$ thì $k[X] = k[x_1,...,x_n]$, vì: $\mathcal{I}(X) = 0$.

Ví dụ 15:

Nếu X là điểm đơn thì $k[X] \cong k$.

Định lý cơ bản của Hilbert đối với k[X] được "thừa hưởng" từ vành đa thức $k[x_1,...,x_n]$: với một iđêan $I \subseteq k[X]$ thì $\pi^{-1}(I) \subseteq k[x_1,...,x_n]$ cũng là iđêan, trong đó: $\pi : k[x_1,...,x_n] \to k[X]$ là phép chiếu tự nhiên.

Nếu $\pi^{-1}(I)$ được sinh bởi $F_1,...,F_k$ thì I được sinh bởi $\pi(F_1),...,\pi(F_k)$.

Do đó, ta có thể định nghĩa tôpô Zariski trên X bằng cách lấy đa tạp con của X như là các tập đóng (các tập zero của các iđêan trong k[X]).

Tương tự, Nullstellensatz's Hilbert cũng thỏa mãn trong k[X], do đó ta có song ánh Y $\to \mathcal{I}$(Y) giữa các đa tạp con của X và các iđêan căn trong k[X].

Bổ đề 1.3.1.4

Các phát biểu sau là tương đương:

(i) X$\subseteq \mathbb{A}^n$ là bất khả quy,

(ii) một tập con mở khác rỗng là trù mật trong X,

(iii) nếu U_1, U_2 là các tập con mở khác rỗng của X thì $U_1 \cap U_2 \neq \varnothing$.

1.3.2. Các ánh xạ chính quy của các đa tạp afin.

Định nghĩa 1.4.2.1.

Một ánh xạ $\varphi: X \to Y$ là chính quy (một cấu xạ), nếu có m hàm chính quy $f_1,...,f_m \in \mathcal{O}$(X) sao cho $\varphi(x) = (f_1(x),...,f_m(x))$.

Định nghĩa 1.3.2.2.

Ánh xạ chính quy $\phi: X \to Y$ là phép đẳng cấu, nếu nó có một nghịch đảo chính quy. Khi đó các đa tạp X, Y được gọi là đẳng cấu.

Ví dụ 16:

Parabol P $= Z(y - x^2)$ đẳng cấu với đường thẳng afin:

φ: $\mathbb{A}^1 \to$ P có ánh xạ ngược: ψ: P $\to \mathbb{A}^1$

t $\mapsto$ (t, t^2) (x, y) $\mapsto$ x

Khi đó, $\varphi \circ \psi$ là ánh xạ đồng nhất trên P và $\psi \circ \varphi$ là ánh xạ đồng nhất trên $\mathbb{A}^1$.

Một cấu xạ của các đa tạp $\varphi: X \to Y$ cảm sinh một đồng cấu của các k-đại số $k[Y] \to k[X]$ chuyển $f \in f[Y]$ thành $f \circ \varphi$. Thật vậy, nếu f là một hàm chính quy thì nó được mô tả bởi đa thức $F \in k[y_1,...,y_m]$. Vì φ là một

cấu xạ nên có $F_1,...,F_m \in k[x_1,...,x_n]$ sao cho $\varphi = (F_1,...,F_m)$. Do đó: với $f \circ \varphi : X \to k$ thì ta có: $f \circ \varphi(x) = F(F_1(x),...,F_m(x))$ và nó thật sự là một hàm chính quy trên X.

Ánh xạ $\varphi^* : k[Y] \to k[X]$ chuyển f đến $f \circ \varphi$ được gọi là cái níu lại của φ. Dễ dàng chỉ ra rằng φ^* là đồng cấu k-đại số.

Mặt khác, với mỗi đồng cấu k-đại số $\phi : k[Y] \to k[X]$ thì tồn tại một cấu xạ $\varphi : X \to Y$ sao cho $\varphi^* = \phi$.

Định lý 1.3.2.3.

Các đa tạp afin X và Y là đẳng cấu nhau nếu và chỉ nếu k[X] và k[Y] là đẳng cấu như các k-đại số.

1.3.3. Các hàm hữu tỉ trên các đa tạp afin.

Cho $X \subseteq \mathbb{A}^n$ là một đa tạp bất khả quy. Thì vành tọa độ của nó k[X] không có ước của 0 và do đó có thể được nhúng vào trường các thương của nó mà ta ký hiệu là k[X]. Nói cách khác, k[X] là tập các lớp tương đương $\left\{ G/H \,|\, G,H \in k[x_1,..,x_n], H \notin I(X) \right\} |\sim$,

Trong đó, $G/H \sim G'/H'$ nếu $GH' - HG' \in I(X)$ và phép "+","." được định nghĩa theo nghĩa thông thường.

Định nghĩa 1.3.3.1.

Trường k[X] được gọi là trường các hàm hữu tỉ trên X hay là trường hàm của X.

Định nghĩa 1.3.3.2.

Hàm $f \in k[X]$ được gọi là chính quy tại $x \in X$ nếu có $G,H \in k[x_1,...,x_n]$ sao cho $f = \frac{G}{H}$ và $H(x) \neq 0$.

Định lý 1.3.3.3.

Nếu một hàm hữu tỉ $f \in k[X]$ là chính quy tại mọi điểm $x \in X$ thì nó chính quy (theo Định nghĩa 1.3.3.1).

1.3.4. Các ánh xạ hữu tỉ của các đa tạp afin.

Cho $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$ là các đa tạp afin bất khả quy.

Định nghĩa 1.3.4.1.

Một ánh xạ hữu tỉ $\varphi : X \to Y$ là một m-bộ các hàm hữu tỉ $f_1,...,f_m \in k[X]$ sao cho $\varphi = (f_1,...,f_m)$. Nếu f_i là chính quy tại x với mọi $x \in X$ thì ánh xạ φ là chính quy tại x.

Định nghĩa 1.3.4.2.

Một ánh xạ hữu tỉ $\varphi : X \to Y$ được gọi là trội, nếu ảnh của X qua φ là trù mật trong Y.

Định nghĩa 1.3.4.3.

Một ánh xạ hữu tỉ $\varphi : X \to Y$ là song hữu tỉ (tương đương song hữu tỉ) nếu nó có ánh xạ ngược hữu tỉ, nghĩa là nếu có $\psi : Y \to X$ sao cho:

- Cả φ và ψ đều trội,
- $\varphi \circ \psi = 1_Y$ và $\psi \circ \varphi = 1_X$, tại mọi nơi các phép hợp thành là xác định.

Khi đó, X và Y được gọi là tương đương song hữu tỉ (song hữu tỉ).

Ví dụ 17:

Cubic lùi $C = Z(y^2 - x^3)$ là song hữu tỉ vào trong $\mathbb{A}^1$:

ánh xạ

$$\varphi : A^1 \to C$$
$$t \mapsto (t^2, t^3)$$

có ánh xạ ngược hữu tỉ

$$\psi : C \to A^1$$
$$(x, y) \mapsto y / x$$

Nếu ánh xạ hữu tỉ $\varphi : X \to Y$ là trội thì cái níu lại $\varphi^* : k[Y] \to k[X]$ được xác định.

Khi đó: với mỗi $f \in k[Y]$ ta có: $\varphi^*(f) \in k[X]$. Ánh xạ này được mở rộng một cách duy nhất đến $k[Y]$. Tương tự như trường hợp các ánh xạ chính quy, φ^* là một song ánh giữa các ánh xạ hữu tỉ trội $X \to Y$ và các phép nhúng k-đại số $k(Y) \hookrightarrow k(X)$.

Định lý 1.3.4.4.

Các đa tạp X và Y là song hữu tỉ nếu và chỉ nếu $k(X) \cong k(Y)$.

1.3.5. Các hàm trên các đa tạp tựa xạ ảnh.

Với mỗi đa tạp xạ ảnh $X \subseteq \mathbb{P}^n$, vành tọa độ của X được xác định tương tự như trong trường hợp afin:

$$k[X] = k[x_0, ..., x_n] / I(X),$$

nhưng bây giờ nó có một cấu trúc cộng của một vành phân bậc, nghĩa là nó là tổng trực tiếp của các không gian vectơ

$$k[X] = R_0 \oplus R_1 \oplus R_2 \oplus ...,$$

trong đó, $R_i R_j \subseteq R_{i+j}$. Các phần tử của R_i là các lớp tương đương của các dạng $x_0, ..., x_n$ có bậc là i.

Ví dụ 18:

Cho $X = Z(x_1^2 + x_2^2 - x_0^2) \subseteq P^2$ là đường tròn đơn vị. Thì k[X] là tổng trực tiếp của các không gian vectơ:

$$R_0 = \langle 1 \rangle_k,$$
$$R_1 = \langle x_0, x_1, x_2 \rangle_k,$$
$$R_2 = \langle x_0^2, x_0x_1, x_0x_2, x_1^2, x_1x_2 \rangle_k, \ (x_2^2 = x_0^2 - x_1^2)$$
$$\dots$$

Định nghĩa 1.3.5.1.

Một đa tạp tựa xạ ảnh $X \subseteq \mathbb{P}^n$ là một tập con mở của một đa tạp xạ ảnh.

Sau đây ta chỉ xét các đa tạp tựa xạ ảnh.

Định nghĩa 1.3.5.2.

Đối với một đa tạp bất khả quy $X \subseteq \mathbb{P}^n$, trường của những hàm hữu tỷ trên X (trường hàm của X) là một tập hợp các lớp tương đương:

$$\{g/h \,\big|\, g,h \in R_d \text{ đối với một d nào đó, } h \neq 0(\mathrm{mod}\, I(X))\}\big|\sim,$$

với $g/h \sim g'/h'$ khi gh’ – hg’ = 0 (modI(X)) .

Các phần tử trên k(X) được gọi là các hàm hữu tỷ trên X .

Định nghĩa 1.3.5.3.

Hàm hữu tỷ $f : X \to k$ là chính quy tại $x \in X$ nếu tồn tại một tập mở $U \subseteq X$ chứa x và với $g,h \in k[X]$ thuần nhất cùng bậc sao cho h không triệt tiêu trên U và f = g/h.

Hàm $f : X \to k$ là chính quy nếu nó chính quy tại mọi điểm $x \in X$. Vành các hàm chính quy trên X được ký hiệu là $\mathcal{O}(X)$.

Định lý 1.3.5.4.

Nếu $X \subseteq \mathbb{P}^n$ là đóng (nghĩa là nó là một đa tạp xạ ảnh) thì $\mathcal{O}(X) \cong k$.

1.3.6. Các ánh xạ của những đa tạp tựa xạ ảnh.

Cho $X \subseteq \mathbb{P}^n$ và $Y \subseteq \mathbb{P}^m$ là những đa tạp tựa xạ ảnh.

Định nghĩa 1.3.6.1.

Một ánh xạ $\varphi : X \to Y$ của những đa tạp tựa xạ ảnh là chính quy (một cấu xạ) nếu với mọi tập con mở $V \subseteq Y$ và với mỗi hàm số $f : V \to k$ chính quy trên V thì hàm số: $f \circ \varphi : \varphi^{-1}(V) \to k$ cũng chính quy.

Sự giải thích sau đây có thể là hữu ích hơn. Ánh xạ $\varphi : X \to Y$ là chính quy nếu với mỗi $x \in X$ thì tồn tại các dạng $f_0,...,f_m \in k\left[x_0,...,x_n\right]$ có cùng bậc sao cho:

- $\varphi = \left(f_0 :....: f_m\right)$ xác định trên một tập mở chứa x và
- $f_i(x) \neq 0$ tại ít nhất một giá trị i.

Định nghĩa 1.3.6.2.

Một cấu xạ $\varphi : X \to Y$ là một phép đẳng cấu nếu nó có ánh xạ ngược chính quy. Khi đó X và Y được gọi là đẳng cấu. Một ánh xạ $\varphi : X \to Y$ được gọi là phép nhúng nếu nó là một đẳng cấu của X và ảnh của nó là $\varphi(X)$.

Ví dụ 19:

Một conic $C = Z\left(x_0x_2 - x_1^2\right)$ trong $\mathbb{P}^2$ đẳng cấu với đường thẳng xạ ảnh. Nếu $(s:t)$ là tọa độ thuần nhất trên $\mathbb{P}^1$ và $\left(x_0 : x_1 : x_2\right)$ là tọa độ thuần nhất trên $\mathbb{P}^2$ thì ánh xạ chính quy $\varphi : \mathbb{P}^1 \to C$

$$(s:t) \mapsto \left(s^2 : st : t^2\right)$$

có ánh xạ ngược chính quy $\psi : C \to \mathbb{P}^1$

$$\left(x_0 : x_1 : x_2\right) \mapsto \left(x_0 : x_1\right) \text{ trên } U_0\ (x_0 \neq 0)$$

$$\left(x_1 : x_2\right) \text{ trên } U_2\ (x_2 \neq 0)$$

Khi đó $C = \left(C \cap U_0\right) \cup \left(C \cap U_2\right)$, ta có thể mô tả ánh xạ ψ tại mọi điểm.

Định nghĩa ψ là một định nghĩa tốt kể cả trong trường hợp $x_i \neq 0 \ \forall i$ thì ta luôn có $\left(x_0 : x_1\right) = \left(x_0 x_1 : x_1^2\right) = \left(x_0 x_1 : x_0 x_2\right) = \left(x_1 : x_2\right)$.

Lưu ý rằng vành tọa độ của các đa tạp xạ ảnh chứa nhiều thông tin hơn vành afin tương ứng. Trong Ví dụ 19, conic C là một đẳng cấu của $\mathbb{P}^1$, tuy nhiên các vành tọa độ của chúng không đẳng cấu, vì $k[C]$ được sinh ra bởi 2 phần tử. Vành $k[X]$ không những phụ thuộc vào lớp các phép đẳng cấu của các đa tạp mà còn phụ thuộc vào phép nhúng của X vào không gian xạ ảnh. Trên thực tế, nếu các vành tọa độ của hai đa tạp là đẳng cấu thì những đa tạp này là tương đương xạ ảnh, có nghĩa là tồn tại phép biến đổi tuyến tính của không gian xạ ảnh ambient biến đa tạp này thành đa tạp khác.

Định nghĩa 1.3.6.3.

Ánh xạ $\varphi : X \to Y$ là hữu tỷ nếu nó được xác định ít nhất trên một tập con mở trù mật của X và nó chính quy trên miền xác định của nó. Hơn nữa, ánh xạ đó còn là song hữu tỷ nếu nó có ánh xạ ngược hữu tỷ, khi đó X và Y được gọi là tương đương song hữu tỷ.

Định nghĩa 1.3.6.4.

Một đa tạp X được gọi là hữu tỷ nếu nó tương đương song hữu tỷ với $\mathbb{P}^d$. Sự tương đương song hữu tỷ này được gọi là một tham số hóa của X. Đa tạp X được gọi là đơn hữu tỷ nếu nó là ảnh hữu tỷ của một $\mathbb{P}^d$.

Một ánh xạ hữu tỉ trội $\varphi : X \to Y$ cảm sinh một đồng cấu k-đại số $\varphi^* : k(Y) \hookrightarrow k(X)$, được gọi là cái níu lại.

Định lý 1.3.6.5.

Các đa tạp X và Y là song hữu tỷ khi và chỉ khi $k(X) \cong k(Y)$.

Định lý 1.3.6.6.

Mọi đa tạp đại số đều là song hữu tỷ với một siêu mặt trong $\mathbb{P}^m$, với m nào đó.

1.3.7. Một số ví dụ.

Ví dụ 20:

Chúng ta hay gọi " đa tạp afin " với ý nghĩa là một đa tạp tựa xạ ảnh đẳng cấu với một đa tạp afin. Một " tập con mở chính " trên $\mathbb{A}^n$ được hiểu là phần bù của một siêu mặt, nghĩa là tập hợp $\{p \in \mathbb{A}^n \mid f(p) \neq 0\}$ với một đa thức đơn $f \in k\left[x_1,....x_n\right]$. Ta thấy rằng một tập con mở chính là một đa tạp afin.

Cho $\varphi : (\mathbb{A}^n \backslash Z(f)) \to \mathbb{A}^{n+1}$ xác định bởi $\left(p_1,....p_n\right) \mapsto \left(p_1,...,p_n,1/f(p)\right)$ thì φ là chính quy với ảnh Y = Z(g) với g = $fx_{n+1} - 1 \in k\left[x_1,....,x_{n+1}\right]$. Ánh xạ ngược là phép chiếu $\psi : \left(p_1,....,p_{n+1}\right) \mapsto \left(p_1,....,p_n\right)$.

Ví dụ 21:

Chúng ta hay gọi " một đa tạp xạ ảnh " là một vật mà có thể được nhúng vào trong một không gian xạ ảnh như là một đa tạp xạ ảnh. Trên thực tế, tích $\mathbb{P}^n \times \mathbb{P}^m$ là một đa tạp xạ ảnh vì nó có thể được nhúng vào $\mathbb{P}^N$ với N= (n+1)(m+1) -1 như sau:

$$\left(x_0 : .... : x_n ; y_0 : ... y_m\right) \mapsto \left(x_0 y_0 : x_0 y_1 : .... x_n y_m\right) = \left(z_{00} : z_{01} : .... z_{nm}\right)$$

Ảnh là tập zero của các đa thức

$$z_{ij} z_{kl} - z_{il} z_{kj},\ i,k = 0,...,n;\ j,l = 0,...,m$$

Ánh xạ nói trên được gọi là phép nhúng Segre.

1.4. Các đường cong elliptic

1.4.1. Các đường cong phẳng.

Cho k là một trường. Chẳng hạn, k có thể là trường các số hữu tỷ $\mathbb{Q}$, trường các số thực $\mathbb{R}$, trường các số phức $\mathbb{C}$, trường các số p-adic $\mathbb{Q}_p$, hoặc trường hữu hạn $\mathbb{F}_q$ của q phần tử. Cho $\bar{k}$ là một bao đóng đại số của k (Xem [Kob], [Ser1]).

Một đường cong phẳng X trên k được định nghĩa bởi phương trình $f(x,y) = 0$, ở đây $f(x,y) = \sum a_{ij} x^i y^j \in k[x,y]$ là bất khả quy trên $\bar{k}$. Ta định nghĩa bậc của X và f như sau: deg X = deg f $= \max\{ i + j : a_{ij} \neq 0\}$.

Một điểm k-hữu tỷ (hoặc đơn giản là k-điểm) trên X là một điểm (a,b) với tọa độ thuộc k sao cho $f(x,y) = 0$. Tập tất cả các điểm k-hữu tỷ trên X được ký hiệu $X(k)$.

Ví dụ 22: Phương trình $x^2 y - 6y^2 - 11 = 0$ xác định một đường cong phẳng X trên $\mathbb{Q}$ bậc 3 và (5, ½) ∈ X($\mathbb{Q}$).

Tại điểm này ta có thể phát biểu một bài toán mở, mà trên nhiều thế kỷ đã được dùng như một động lực thúc đẩy cho sự phát triển của các ngành toán học, đó là:

Câu hỏi: Liệu có hay không một thuật toán, mà khi cho một đường cong phẳng X trên $\mathbb{Q}$ thì xác định được $X(\mathbb{Q})$ có khác rỗng hay không?

Mặc dù $X(\mathbb{Q})$ không nhất thiết hữu hạn, nhưng ta sẽ thấy rằng, nó luôn luôn thừa nhận một sự mô tả hữu hạn, vì thế vấn đề xác định $X(\mathbb{Q})$ có thể được chính xác hóa sự mô tả bằng cách sử dụng khái niệm của máy Turing; xem [HU] để tiếp cận định nghĩa. Mối quan hệ của câu hỏi này với bài toán thứ 10 của Hilbert, xin xem tổng quan trong [Po2].

Hiện tại có sự tồn tại các phương pháp tính toán trả lời câu hỏi cho một X đặc biệt, mặc dù nó chưa bao giờ được chứng minh là các phương pháp này làm việc trong trường hợp chung. Thậm chí các vấn đề sau còn bỏ ngỏ:

(1) Liệu có một thuật toán mà khi cho một đa thức bậc bốn f(x) $\in \mathbb{Q}$[x], thì có xác định được $y^2 = f(x)$ có một điểm hữu tỷ hay không?

(2) Liệu có một thuật toán mà khi cho một đa thức $f(x,y) \in \mathbb{Q}[x,y]$ bậc ba, thì có xác định được f(x)=0 có một điểm hữu tỷ hay không?

Thực ra, các vấn đề (1) và (2) là tương đương.

1.4.2. Hình học xạ ảnh.

Mặt phẳng xạ ảnh: Mặt phẳng afin $\mathbb{A}^2$ là mặt phẳng thông thường, với $\mathbb{A}^2$(k) = $\{(a,b) : a,b \in k\}$ với trường k bất kỳ. ‘‘Compact hóa’’ $\mathbb{A}^2$ bằng cách nối một số điểm “tại vô cùng” để sinh ra mặt phẳng xạ ảnh $\mathbb{P}^2$. Một trong những lý do chính cho việc làm điều này là làm cho lý thuyết tương giao tốt hơn: xem định lý của Bézout trong phần dưới đây.

Tập hợp của các k-điểm trên mặt phẳng xạ ảnh $\mathbb{P}^2$ có thể được định nghĩa một cách trực tiếp như sau: $\mathbb{P}^2$ (k) := $(k^3 - 0)/ k^*$. Nói cách khác, một điểm k-hữu tỷ trên $\mathbb{P}^2$ là một lớp tương đương của bộ ba (a,b,c) với $a,b,c \in k$ và không đồng thời bằng 0, qua mối quan hệ tương đương ~ , ở đây $(a,b,c) \sim (\lambda a, \lambda b, \lambda c), \ \forall \lambda \in k^*$. Lớp tương đương của (a,b,c) được ký hiệu $(a:b:c)$. Ta cũng có thể đồng nhất $\mathbb{P}^2$ (k) với tập hợp của các đường qua 0 trong không gian (x,y,z).

Đơn ánh $\mathbb{A}^2$(k) ↪ $\mathbb{P}^2$ (k) ánh xạ (a,b) vào $(a:b:1)$ gần như là một song ánh: các điểm của $\mathbb{P}^2$ (k) không có tạo ảnh, có dạng $(a:b:0)$ hình thành một đường xạ ảnh $\mathbb{P}^1$(k) của " các điểm tại vô cùng". Xem $\mathbb{P}^2$(k) như đường qua 0 trong không gian (x,y,z), $\mathbb{A}^2$(k) là tập hợp các đường như thế đi qua $(a,b,1)$ với $a,b \in k$, và phần bù $\mathbb{P}^1$(k) là tập hợp các đường qua 0 trong mặt phẳng (x,y).

$\mathbb{P}^2$ cũng có thể được bao phủ bởi 3 bản sao của $\mathbb{A}^2$, là:

$$\{(x:y:z) \mid x \neq 0\}, \ \{(x:y:z) \mid y \neq 0\}, \text{ và } \{(x:y:z) \mid z \neq 0\}.$$

Bao đóng xạ ảnh của các đường cong: Hàm thuần nhất của một đa thức thuần nhất $f(x,y)$ bậc d là $F(X,Y,Z) := Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$. Bằng cách

thay x bởi X, y bởi Y, và thêm đầy đủ các thành phần của Z để mỗi đơn thức mang bậc tổng của của mỗi đơn thức là d. Ta có: $f(x,y) = F(x,y,1)$.

Nếu $f(x,y) = 0$ là một đường cong phẳng C trong $\mathbb{A}^2$, bao đóng xạ ảnh của nó là đường cong $\tilde{C}$ trong $\mathbb{P}^2$ được định nghĩa bởi phương trình thuần nhất $F(X,Y,Z) = 0$. Đường cong $\tilde{C}$ bằng với C cộng với một số điểm "tại vô cực".

Ví dụ 23: Nếu $f(x,y) = y^2 - x^3 + x - 7$, thì:

$$F(X, Y, Z) = Y^2Z - X^3 + XZ^2 - 7Z^3$$

Và $$\tilde{C}(\mathbb{Q}) = \frac{\{zeros\ of\ F\}}{\mathbb{Q}^*}$$

$$= \{zeros\ of\ F(X, Y, 1)\} \cup \frac{\{zeros\ of\ F(X, Y, Z)\} - 0}{\mathbb{Q}^*}$$

$$= C(\mathbb{Q}) \cup \{P\},$$

ở đây P là điểm (0 : 1: 0) "tại vô cực".

Định lý Bézout:

Một trong những lý do chủ yếu sớm được đề cập đến việc nghiên cứu trong mặt phẳng xạ ảnh là thu được một lý thuyết tương giao tốt. Cho $F(X,Y,Z) = 0$ và $G(X,Y,Z) = 0$ là những đường cong trong $\mathbb{P}^2$ trên k, có bậc tương ứng là m và n. Định lý Bézout chứng tỏ chúng giao nhau tại mn điểm của $\mathbb{P}^2$, với điều kiện là:

(1) F và G không có các thừa số chung không tầm thường.

(2) Nghiên cứu trên một trường đại số đóng, và

(3) Đếm các điểm tương giao với bội (trong trường hợp kỳ dị, hoặc các điểm tiếp xúc).

1.4.3. Cách xác định X(ℚ): sự chia nhỏ theo bậc.

Ta trở lại vấn đề xác định tập hợp các điểm hữu tỷ $X(\mathbb{Q})$ ở đây X là một đường cong phẳng afin $f(x,y)=0$ trên $\mathbb{Q}$ hoặc bao đóng xạ ảnh của nó. Cho $d=\deg f$. Ta sẽ quan sát bài toán theo việc tăng dần giá trị của d.

. d = 1: là các đường thẳng. Ta biết tham số hóa các điểm hữu tỷ trên đường thẳng $ax+by+c=0$ như thế nào!

. d = 2: là các đường conic. Legendre đã chứng minh rằng các đường conic thỏa mãn nguyên lý Hasse. Điều này nghĩa là: X có một $\mathbb{Q}$-điểm nếu và chỉ nếu X có $\mathbb{R}$ điểm và một $\mathbb{Q}_p$ –điểm với mỗi số nguyên tố p. Vì một đường conic xạ ảnh được mô tả bằng một dạng bậc hai có 3 biến, kết quả của Legendre có thể được xem như một trường hợp đặc biệt của định lý *Hasse-Minkowsk I* [Ser1, chương IV].

Định lý của Legendre dẫn đến một thuật toán để xác định sự tồn tại của một $\mathbb{Q}$-điểm trên conic X. Đây là một thuật toán như vậy: bổ sung bình phương, nhân với một hằng số, để cảm sinh trường hợp $aX^2+bY^2+cZ^2=0$ trong $\mathbb{P}^2$, ở đây $a,b,c\neq 0$, không chính phương**,** đôi một nguyên tố. Khi đó ta có thể chứng minh rằng tồn tại một $\mathbb{Q}$-điểm nếu và chỉ nếu a,b,c không cùng dấu và các phương trình đồng dư:

$$ax^2+b\equiv 0 \pmod{c}$$
$$by^2+c\equiv 0 \pmod{a}$$
$$cy^2+a\equiv 0 \pmod{b}$$

giải được trong tập số nguyên. Hơn nữa, trong trường hợp này, $aX^2 + bY^2 + cZ^2 = 0$ có một nghiệm không tầm thường trong tập số nguyên X, Y, Z thỏa mãn $|X| \leq |bc|^{1/2}$, $|Y| \leq |ac|^{1/2}$, và $|Z| \leq |ab|^{1/2}$, xem [Mo2].

Trong trường hợp đường conic X có một $\mathbb{Q}$-điểm P_0, vấn đề còn lại là việc mô tả tập hợp tất cả các $\mathbb{Q}$-điểm. Đối với điều này có một cách làm hợp lý là: với mỗi điểm $P \in X(\mathbb{Q})$ vẽ một đường qua P_0 và P, và giả sử t là độ dốc của nó, trong $\mathbb{Q}$ (hoặc có thể là ∞). Ngược lại, cho $t \in \mathbb{Q}$, định lý Bézout bảo đảm rằng đường qua P_0 với độ dốc t sẽ cắt đường conic tại một điểm khác (miễn là đường này không tiếp xúc với conic tại P_0), và đây sẽ là một điểm hữu tỷ.

Ví dụ 24: nếu X là đường tròn $x^2 + y^2 = 1$ và $P_0(-1, 0)$, thì :

$$t \quad \rightarrow \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

$$\frac{y}{x+1} \leftarrow (x, y)$$

Định nghĩa các ánh xạ song hữu tỷ từ $\mathbb{A}^1$ đến X và ngược lại, nghĩa là bỏ qua một số hữu hạn các tập con có số chiều nhỏ hơn (một vài điểm), chúng là các ánh xạ được cho bởi các hàm hữu tỷ của các biến mà cảm sinh một song ánh giữa các $\overline{\mathbb{Q}}$-điểm. Những ánh xạ song hữu tỷ này được định nghĩa trên $\mathbb{Q}$; các hệ số của các hàm hữu tỷ thuộc $\mathbb{Q}$, vì thế chúng cũng cảm sinh

một song ánh giữa các $\mathbb{Q}$-điểm (bỏ qua các tập con như trước). Đặc biệt, tập hợp đầy đủ các nghiệm hữu tỉ của phương trình: $x^2 + y^2 = 1$ là

$$\left\{\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) : t \in \mathbb{Q}\right\} \cup \{(-1,0)\}.$$

. d = 3: các đường bậc 3 phẳng. Lind [Lin] và Reichardt [Rei] đã phát hiện ra rằng nguyên lý *Hasse* có thể không đúng với các đường cong phẳng bậc ba. Ở đây là một ví dụ thuộc về Selmer [Sel]: đường cong $3X^3 + 4Y^3 + 5Z^3 = 0$ trong $\mathbb{P}^2$ có một R-điểm $(((-4/3)^{1/3}:1:0)$ là một) và một $\mathbb{Q}_p$ -điểm với mỗi số nguyên tố p, nhưng nó không có $\mathbb{Q}$-điểm .(Đối với p > 5, sự tồn tại các $\mathbb{Q}_p$-điểm có thể được chứng minh bằng cách dùng bổ đề Hensel [Kob, định lý 3] với một biến thiên để chứng minh sự tồn tại của các nghiệm modulo p. Vì p = 2, 3, 5, một dạng tổng quát hơn của bổ đề Hensel có thể được sử dụng [Kob, chương I, bài tập 6]. Sự không tồn tại của các $\mathbb{Q}$-điểm khó thiết lập hơn).

1.4.4. Đường cong elliptic

1.4.4.1. Các định nghĩa tương đương:

Cho k là một trường hoàn chỉnh. Một đường cong elliptic trên k có thể được định nghĩa theo một trong ba hình thức phát biểu như sau:

(1) Bao đóng xạ ảnh của một đường cong không kỳ dị được định nghĩa bởi một "phương trình Weierstrass"

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Với $a_{1,}a_2, a_3, a_4, a_6 \in k$. Nếu đặc số của k khác 2 hoặc 3, người ta có thể hạn chế sự xét tới các bao đóng xạ ảnh của các đường cong $y^3 = x^3 + Ax + B$.

Ta có thể chứng minh rằng đường cong không kỳ dị nếu và chỉ nếu: $x^3 + Ax + B$ có các nghiệm khác biệt trong $\bar{k}$, và điều này tồn tại nếu và chỉ nếu $\Delta := -16(4A^3 + 27B^2) \neq 0$.

(2) Một đường cong giống một xạ ảnh không kỳ dị trên k được liên kết với một điểm k-hữu tỷ 0.

(3) Một đa tạp nhóm xạ ảnh một chiều trên k.

1.4.4.2. Các điểm kỳ dị:

Nếu (0, 0) là một điểm trên đường cong afin $f(x, y) = 0$ trên k, khi đó (0, 0) là một điểm kỳ dị nếu cả hai $\partial f / \partial x$ và $\partial f / \partial y$ triệt tiêu tại (0, 0). Một cách tương đương, (0, 0) là điểm kỳ dị nếu $f = f_2 + f_3 + \ldots + f_d$, ở đây mỗi $f_i \in k[x, y]$ là một đa thức thuần nhất bậc i. Chẳng hạn (0, 0) là điểm kỳ dị trên $y^2 = x^3$ và trên $y^2 = x^3 + x^2$, nhưng không là điểm kỳ dị trên đường $y^2 = x^3 - x$. Một cách tổng quát hơn, (a, b) là kỳ dị trên $f(x, y) = 0$ nếu và chỉ nếu (0, 0) là kỳ dị trên $f(X + a, Y + b) = 0$.

Một đường cong afin là không kỳ dị nếu nó không có các điểm kỳ dị. Một đường cong xạ ảnh $F(X, Y, Z) = 0$ là không kỳ dị nếu " các mảnh afin" của nó $F(x, y, 1) = 0$, $F(x, 1, z) = 0$, $F(1, y, z) = 0$ là không kỳ dị.

Thuật ngữ " trơn" là một từ đồng nghĩa với không kỳ dị, ít nhất là đối vối các đường cong trên một trường hoàn chỉnh k.

1.4.4.3. Giống (Loại):

Cho X là đường cong xạ ảnh không kỳ dị trên một trường hoàn chỉnh k. Giống của X là một số nguyên không âm g để đo sự phức tạp hình học của X. Nó có các định nghĩa tương đương sau:

(A) $g = \dim_k \Omega$, ở đây Ω là không gian véctơ của các vi phân chính qui trên X. (Chính quy mang nghĩa: "không cực điểm". Nếu k = ℂ, thì chính quy tương đương với chỉnh hình).

(B) g là giống tôpô (số các quai) của mặt Riemann compact X(ℂ). (Định nghĩa này chỉ có nghĩa nếu k có thể được nhúng vào ℂ.)

(C) $g = \dfrac{(d-1)(d-2)}{2}$ - (các số hạng của các kỳ dị) ở đây Y là một đường cong phẳng bậc d song hữu tỷ với X (có thể là một điểm kỳ dị). Ví dụ, đường cong phẳng bậc 3 không kỳ dị có giống là 1.

1.4.4.4. Luật nhóm: **Định nghĩa**

Để nói rằng một đường cong elliptic E trên k là một đa tạp nhóm nghĩa đại thể là có một ánh xạ "phép cộng" $E \times E \to E$ được cho bởi các hàm hữu tỷ, cảm sinh ra một cấu trúc nhóm trên $E(L)$ đối với trường mở rộng bất kỳ L của k.

Luật nhóm được đặc trưng bởi hai quy tắc sau:

(1) Điểm O = (0 : 1 : 0) tại vô cực là đơn vị của nhóm .

(2) Nếu một đường L cắt E tại 3 k-điểm P, Q, R $\in E(k)$, thì P + Q + R = 0 trong luật nhóm.

Từ những điều này ta suy ra:

a) Cho P $\in E(k)$, P ≠ O, đường thẳng đứng qua P cắt E tại P, O và một điểm thứ 3 là - P.

b) Cho P, Q $\in E(k)$ khác O, đường qua P và Q (lấy tiếp tuyến với E tại P nếu P = Q) cắt E tại P, Q và R $\in E(k)$. Nếu R = O, thì P + Q = O , trái lại P + Q = -R, ở đây - R có thể được xây dựng như trong a).

Chú ý : $E(k)$ là một nhóm aben.

1.4.4.5. Luật nhóm: Các công thức

Một cách tổng quát, tọa độ của P + Q có thể được biểu diễn như các hàm hữu tỷ theo tọa độ của P và Q. Ở đây ta trình bày các công thức chi tiết cho một thuật toán để tính P + Q.

Sự tồn tại của các công thức này trở nên quan trọng trong phần 1.5.8.5 khi ta thực hiện phương pháp phân tích đường cong elliptic.

Để tính tổng R của các điểm $P, Q \in E(k)$ trên $y^2 = x^3 + Ax + B$ trên k:

1. Nếu P = O, đặt R = Q và dừng lại.
2. Nếu Q = O, đặt R = P và dừng lại.
3. Trường hợp khác, giả sử $P = (x_1 : y_1 : 1)$ và $Q = (x_2 : y_2 : 0)$. Nếu $x_1 \neq x_2$, đặt:

$$\lambda = (y_1 - y_2)(x_1 - x_2)^{-1}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$R = (x_3 : y_3 : 1)$$

và dừng lại.

4. Nếu $x_1 = x_2$ và $y_1 = -y_2$, đặt R = O và dừng lại.
5. Nếu $x_1 = x_2$ và $y_1 \neq -y_2$ (như vậy P = Q), đặt

$$\lambda = (3x_1^2 + A)(y_1 + y_2)^{-1,}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$R = (x_3 : y_3 : 1)$$

và dừng lại.

1.4.4.6. Luật nhóm: Các ví dụ

Giả sử E là đường cong elliptic $y^2 = x^3 - 25x$. (Từ nay, khi ta đưa ra một phương trình không thuần nhất cho đường cong elliptic E thì nó được hiểu rằng nghĩa thật sự là ta cho E được định nghĩa như bao đóng xạ ảnh của đường cong afin này).

Vì $x^3 - 25x$ có các nghiệm khác nhau, E không kỳ dị, vì thế E thật sự là một đường cong elliptic.

Đường thẳng L đi qua P := (-4, 6) và Q := (0, 0) có phương trình $y = (-3/2)x$. Ta tính $L \cap E$ bởi sự thay thế:

$$((-3/2)x)^2 = x^3 - 25x$$

$$\Leftrightarrow 0 = (x + 4)\, x\, (x - 25/4)$$

và tìm $L \cap E = \{P, Q, R\}$, trong đó: R := (25/4, - 75/8).

Do đó P + Q + R = O theo luật nhóm, và P + Q = - R = (25/4, 75/8).

Giao của đường X = 0 trong $\mathbb{P}^2$ với E: $Y^2Z = X^3 - 25XZ^2$ là $X = 0 = Y^2Z$, mà (0 : 1 : 0) = O và (0 : 0 : 1) = Q, có bội 2. (Về mặt hình học, điều này tương ứng với đường $x = 0$ tiếp xúc với E tại Q).

Do đó Q + Q + O = O, và 2Q = O; nghĩa là, Q là một điểm có cấp là 2 và là một điểm 2-xoắn. (Tổng quát, các điểm 2-xoắn khác không trên $y^2 = x^3 + Ax + B$ là $(\alpha, 0)$ ở đây α là một nghiệm của $x^3 + Ax + B$: chúng lập thành một nhóm con của $E(\bar{k})$ đẳng cấu với $\mathbb{Z}/2 \times \mathbb{Z}/2$).

1.4.5. Đường cong elliptic trên trường số phức.

Một mặt E(ℂ) là một đa tạp phức nhưng ở một khía cạnh khác thì nó là một nhóm, và các tọa độ của P+Q là các hàm hữu tỉ theo tọa độ của P và Q vì luật nhóm này là chỉnh hình. Do đó, E(ℂ) là một nhóm Lie 1-chiều trên ℂ. Hơn nữa, E(ℂ) là đóng trong $P^2(C)$ compact nên E(ℂ) là compact, liên thông. Theo sự phân lớp của nhóm Lie compact liên thông 1-chiều trên ℂ ta có:

$E(C) \simeq C/\Lambda$ như là các nhóm Lie trên $\mathbb{C}$, với dàn: $\Lambda = Z\omega_1 + Z\omega_2$, trong đó ω_1, ω_2 là một R-cơ sở của $\mathbb{C}$. Các ω_i được gọi là các chu kỳ. Vì có một hàm phân hình $p(z)$ trên $\mathbb{C}$ được xác định sau đây sao cho: $p(z+\omega) = p(z)\ \forall \omega \in \Lambda$.

Ngược lại giả sử rằng, ta bắt đầu xét trên $\mathbb{C}$ một dàn Λ rời rạc có hạng là 2: $\Lambda = Z\omega_1 + Z\omega_2$ với là R-cơ sở trên $\mathbb{C}$, ta cần chỉ ra là làm thế nào để tìm ngược lại một đường cong tương ứng trên $\mathbb{C}$.

Tập $g_2 = 60\sum'_{\omega\in\Lambda} \omega^{-4}$ và

$$g_3 = 140\sum'_{\omega\in\Lambda} \omega^{-6}$$

trong đó, " ' " nghĩa là bỏ đi số hạng $\omega = 0$.

Đặt: $p(z) = z^{-2} + \sum'_{\omega\in\Lambda}((z-\omega)^{-2} - \omega^{-2})$

Khi đó, ta có thể chứng minh các kết luận sau :

+ $p(z)$ là phân hình trên $\mathbb{C}$ với cực điểm trên Λ.

+ $p(z+\omega) = p(z)\ \forall \omega \in \Lambda$ và $z \mapsto (p(z), p'(z))$ xác định một phép đẳng cấu giải tích $C/\Lambda \to E(C)$ với E là đường cong elliptic trên $\mathbb{C}$: $y^2 = 4x^3 - g_2 x - g_3$ (cực điểm của $p(z)$ qua đẳng cấu tương ứng với điểm $O \in E(C)$).

Vi phân $\dfrac{dx}{y}$ trên E níu tới dz trên C/Λ,

do đó, ánh xạ ngược : $C(E) \to C/\Lambda$ được xác định bởi:

$$(a;b) \mapsto \int_0^{(a;b)} \frac{dx}{y} = \int_\infty^a \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}}$$

Tổng quát hơn, Riemann đã chứng minh rằng: một mặt Riemann compact bất kỳ đẳng cấu với $X(C)$ đối với một đường cong xạ ảnh không kỳ dị X nào đó trên C.

1.4.6. Đường cong elliptic trên trường hữu hạn.

Cho E là một đường cong elliptic trên trường hữu hạn $\mathbb{F}_q$ có q phần tử. Vì $E(\mathbb{F}_q)$ là một tập con của $\mathbb{P}^2(\mathbb{F}_q)$, nên $E(\mathbb{F}_q)$ là một nhóm aben hữu hạn. Hass đã chứng minh được: $\#E(\mathbb{F}_q)$ = q +1-a, trong đó, $|a| \le 2\sqrt{q}$. Đây là trường hợp đặc biệt của "giả thuyết Wiel". Hơn nữa, thuật toán của Schoof [Sch] đã tính $\#E(\mathbb{F}_q)$ với độ phức tạp $(\log q)^{0(1)}$ như sau: ta sẽ không giải thích sự xác định $\#E(\mathbb{F}_q)$ theo modun l với mỗi l nguyên tố ta có xấp xỉ $\log q$, định lý số dư Trung hoa đã xét xong $\#E(\mathbb{F}_q)$.

Ví dụ 25: Cho E là đường cong elliptic $y^2 = x^3 - x + 1$ trên trường $\mathbb{F}_3$. Định lý Hass chỉ ra: $1 \le \#E(\mathbb{F}_3) \le 7$.

Thật ra: $E(\mathbb{F}_3)$ ={(0;1),(0;-1),(1;1),(1;-1),(2;1),(2;-1),O} và $E(\mathbb{F}_3) \cong \mathbb{Z}/7$.

Ví dụ 26: Cho E là đường cong elliptic $y^2 = x^3 - x$ trên trường $\mathbb{F}_3$ thì

$E(\mathbb{F}_3)$ = {(0;0),(1;0),(2;0),O} và $E(\mathbb{F}_3) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

1.4.7. Đường cong elliptic trên trường hữu tỉ.

1.4.7.1. Định lý Mordell:

Cho E là đường cong elliptic trên trường $\mathbb{Q}$. Mordell đã chứng minh rằng: $E(\mathbb{Q})$ là một nhóm aben hữu hạn sinh: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times T$ với $r \in \mathbb{Z}_{\ge 0}$, được gọi là hạng, và $T = E(\mathbb{Q})_{tors}$ là nhóm aben hữu hạn được gọi là nhóm con xoắn. (Định lý Mordell còn được gọi là định lý Mordell-Weil, vì Weil đã tổng quát hoá đối với các đa tạp aben trên các trường số. Đa tạp aben là đa tạp nhóm xạ ảnh có số chiều tùy ý).

Ví dụ 27: Cho E là đường cong elliptic $y^2 = x^3 - x^2$ trên trường $\mathbb{Q}$. Ta có thể chỉ ra rằng:

$E(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}/2$. Trong đó: $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ được sinh bởi (-4;6).

Ví dụ 28: Cho E là đường cong elliptic $y^2 + y = x^3 - x^2$ trên trường $\mathbb{Q}$, được xem như là đường cong môđula $X_1(11)$".

Khi đó, $E(\mathbb{Q})=\{(0;0),(0;-1),(1;0),(1;-1),O\} \cong \mathbb{Z}/5$.

Ví dụ 29: Cho E là đường cong elliptic trên trường $\mathbb{Q}$: $1063y^2 = x^3 - x$ (không phải dạng Weierstrass nhưng nó đẳng cấu với $y^2 = x^3 - 1063^2 x$). Sử dụng "các điểm Heegner trên các đường cong môđula", Elkies [Elk] đã tính được $E(\mathbb{Q}) \simeq \mathbb{Z}\times\mathbb{Z}/2\times\mathbb{Z}/2$.

Trong đó, $E(\mathbb{Q})/\ E(\mathbb{Q})_{tors}$ được sinh bởi 1 điểm với hoành độ $x = \frac{q^2}{1063}$.

với $q = \frac{1109186374182976967504702163571228176738233966743464 5}{3173426575447721807352079773209000125228079367788 7}$

Ví dụ 30: Cho E là đường cong eliptic: $y^2 + xy + y = x^3 + ax + b$

Trong đó: $a = -120039822036992245303534619191166796374$

Và

$b = 5042249924849106700108017991680827267594437562229114151 16$

Martin và McMillen [MM] đã chỉ ra rằng $E(\mathbb{Q}) \simeq \mathbb{Z}^r$ trong đó $r \geq 24$.

1.4.7.2. Các đatạp nhóm afin 1-chiều trên k.

Các đa tạp nhóm afin 1-chiều G trên k có thể được phân lớp. Một cách đơn giản, ta có thể giả sử k là 1 trường hoàn chỉnh có đặc số khác 2.

Ta có bảng:

G	Đa tạp	Luật nhóm	$G(k)$
$\mathbb{G}_a$	$\mathbb{A}^1$	$x_1, x_2 \mapsto x_1 + x_2$	k, với phép +
$\mathbb{G}_m$	$xy = 1$	$(x_1, y_1),(x_2, y_2) \mapsto (x_1x_2, y_1y_2)$	k^*, với phép .
$\mathbb{G}_m^{(a)}$	$x^2 - ay^2 = 1$	$(x_1, y_1),(x_2, y_2) \mapsto$ $(x_1x_2 + ay_1y_2, x_1y_2 + x_2y_1)$	$\ker(k(\sqrt{a})^* \xrightarrow{\text{chuẩn}} k^*)$

Cột 1: Đa tạp nhóm G, là nhóm cộng tính $\mathbb{G}_a$ hoặc nhóm nhân $\mathbb{G}_m$ hoặc nhóm xoắn $\mathbb{G}_m^{(a)}$ với $a \in k^*$.

+ Loại đẳng cấu của $\mathbb{G}_m^{(a)}$ xem như là một đa tạp nhóm được xác định bởi ảnh của a trong k^*/k^{*2}, và nếu $a \in k^*$ thì $\mathbb{G}_m^{(a)} \cong \mathbb{G}_m$.

Cột 2: Mô tả G như là một đa tạp, ở mỗi trường hợp G cũng là $\mathbb{A}^1$ hoặc là một đường cong phẳng trong $\mathbb{A}^2$.

Cột 3: Biểu diễn cấu xạ luật nhóm: $G \times G \to G$ theo các tọa độ.

Cột 4: Mô tả nhóm các điểm hữu tỉ $G(k)$.

1.4.7.3. Các cubic Weierstrass kỳ dị.

Nếu E là một đường cong kỳ dị được xác định như là bao đóng xạ ảnh của: $y^2 = x^3 + ax^2 + bx + c$ thì E có nhiều nhất một điểm kỳ dị.

Giả sử P_0 là điểm kỳ dị. Bằng cách đổi biến số ta có thể giả sử: $P_0 = (0;0)$, ta có phương trình dạng: $(y^2 - ax^2) - x^3 = 0$.

Các đường thẳng tiếp xúc với các nhánh tại $(0;0)$ là: $y = \pm\sqrt{a}x$.

Các điểm kỳ dị được gọi là điểm nút hoặc điểm lùi tùy theo $a \neq 0$ hoặc $a = 0$.

Trong mỗi trường hợp, $E_{ns} := E - \{P_0\}$ trở thành đa tạp nhóm afin 1-chiều sử dụng cách xây dựng hình học giống như trường hợp không kỳ dị. (Một đường thẳng L đi qua hai điểm không kỳ dị không thể xuyên qua P_0, vì sẽ trái với kết quả của định lý Bézout)

Thật vậy: $E_{ns} \cong \begin{cases} G_a \ \ khi \ \ a = 0 & (\textit{điểm lùi}) \\ G_m \ \ khi \ \ a \in k^{*2} & (\textit{điểm nút}) \\ G_m^{(a)} \ \ khi \ \ a \ \textit{không chính phương} & (\textit{điểm nút}) \end{cases}$

Ví dụ 31: Nếu E là bao đóng xạ ảnh của: $y^2 = x^3$, E có điểm lùi tại $(0;0)$, và phép đẳng cấu được cho bởi:

$$\begin{array}{lll} E_{ns} & \leftrightarrow & G_a \\ (x,y) & \rightarrow & x/y \\ (t:1:t^3) = (t^{-2},t^{-3}) & \leftarrow & t \end{array}$$

Ta có thể kiểm tra được rằng $(t:1:t^3),(u:1:u^3),(v:1:v^3)$ là cộng tuyến trong $\mathbb{P}^2$ với: $t+u+v=0$.

1.4.7.4. Sự rút gọn theo mod p.

Với bất kỳ $u \in \mathbb{Q}^*$, đường cong elliptic E: $y^2 = x^3 + Ax + B$ trên $\mathbb{Q}$ đẳng cấu với: $Y^2 = X^3 + u^4AX + u^6B$ (nhân phương trình với u^6, Đặt : $Y = u^3y$; $X = u^2x$).

Do đó ta có thể giả sử: $A, B \in \mathbb{Z}$.

Khi đó: ta có thể rút gọn phương trình theo mod p (nguyên tố) để nhận được đường cong bậc ba $\overline{E}$ trên $\mathbb{F}_p$. Nhưng $\overline{E}$ có thể kỳ dị. Điều này xảy ra nếu và chỉ p là ước của Δ.

Ta nói rằng E có rút gọn tốt tại p nếu có một phương trình Weierstrass cho E (thu được bằng cách đổi tọa độ) mà sự rút gọn theo mod p là không kỳ dị. Tương tự, nếu có một phương trình Weierstrass cho E mà sự rút gọn theo mod p là một đường cong bậc ba có một điểm nút thì ta nói rằng E có sự rút gọn nhân tại p. Khi đó: ta nói rằng E có sự rút gọn nhân tách hoặc rút gọn nhân không tách tùy theo $\overline{E}_{ns}$ là $\mathbb{G}_m$ hoặc là một xoắn.

Trái lại: nếu E không có rút gọn tốt hoặc rút gọn nhân thì tất cả các phương trình Weierstrass đối với E rút gọn theo mod p tới một đường cong bậc ba với một điểm lùi và ta nói E có sự rút gọn cộng. Ta có bảng tóm tắt:

Điểm kỳ dị	$\overline{E}_{ns}$	Thuật ngữ .
Không có điểm nào	$\overline{E}$	Rút gọn tốt .
Điểm lùi	$\mathbb{G}_a$	Rút gọn cộng .
Điểm nút	$\mathbb{G}_m$ hoặc $\mathbb{G}_m^{(d)}$	Rút gọn nhân .

1.4.7.5. Sự hữu hạn của nhóm xoắn $T := E(\mathbb{Q})_{tors}$

Giả sử một đường cong elliptic E trên $\mathbb{Q}$ có rút gọn tốt tại p. Bất kỳ một điểm trên $E(\mathbb{Q})$ có thể được viết dưới dạng $(a:b:c)$ với $a;b;c \in \mathbb{Z}$ sao cho: $gdc(a,b,c)=1$ thì a,b,c có thể được rút gọn theo mod p cho ta một điểm trên $\overline{E}(\mathbb{F}_p)$.Điều này xác định một phép đồng cấu: $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$. Ký hiệu $gdc(a,b,c)$ để chỉ ước chung lớn nhất của a,b,c.

Định lý 1.4.7.5.1:

Nếu E có rút gọn tốt tại $p>2$ thì nhóm con xoắn T của $E(\mathbb{Q})$ nhúng được vào $\overline{E}(\mathbb{F}_p)$

Hệ quả 1.4.7.5.2:

T là hữu hạn.

Ví dụ 32: Cho đường cong elliptic $E: y^2 = x^3 - 4x + 4$ trên $\mathbb{Q}$

thì: $\Delta = -16(4(-4)^3 + 27.4^2) = -2^8.11$

nên E có rút gọn tốt tại p ít nhất là với $p \neq 2,11$.

Ta tính được: $\#\overline{E}(\mathbb{F}_3)$=7 và $\#\overline{E}(\mathbb{F}_5)$=9.

Nhóm duy nhất được nhúng đơn ánh vào các nhóm cấp 7 và 9 là nhóm tầm thường.

Vậy $T=\{0\}$. Đặc biệt: $(0;2) \in E(\mathbb{Q})$ có cấp vô hạn và $E(\mathbb{Q})$ có hạng dương.

1.4.7.6. Các định lý khác về nhóm con xoắn T**.**

Định lý Luzt_Nagell: Cho $A,B\in\mathbb{Z}$ và E: $y^2=x^3+Ax+B$ là một đường cong elliptic. Nếu $P\in T$ và $P\neq O$ thì $P=(x_0,y_0)$ trong đó: $x_0,y_0\in\mathbb{Z}$ và $y^2 \setminus (4A^3+27B^2)$.

Điều này cho ta một phương pháp để xác định T.

Định lý Mazur: Nếu E là 1 đường cong elliptic trên $\mathbb{Q}$ thì: $T\simeq\mathbb{Z}/\mathrm{N}$ với $\mathrm{N}\leq 12$, $\mathrm{N}\neq 11$

hoặc $T\simeq \mathbb{Z}/2\times \mathbb{Z}/2\mathrm{N}\mathbb{Z}$ với $\mathrm{N}\leq 4$. Đặc biệt: $\#T\leq 16$.

Với mỗi $m\geq 1$, ta có thể sử dụng luật nhóm để tính các đa thức $\Phi_m(x)\in\mathbb{Q}[x]$ mà các nghiệm của đa thức là hoành độ x của các điểm có cấp là m trong $E(\overline{Q})$. Việc xác định các điểm có cấp m trong E(Q) là tìm các nghiệm hữu tỉ của Φ_m và kiểm tra lại để có tung độ y hữu tỉ.

Theo định lý Mazur chỉ có hữu hạn m được xét từ đó cho ta thuật toán thời gian đa thức để tính T.

1.4.7.7. Các hàm độ cao.

Ta mô tả các bước để chứng minh định lý Mordell:

Nếu $P=(a:b:c)\in\mathbb{P}^2(\mathbb{Q})$, ta có thể giả sử: $a,b,c\in\mathbb{Z}$ và $gdc(a,b,c)=1$.

Khi đó ta định nghĩa: $H(P):=\max(|a|,|b|,|c|)$ và $h(P):=\log H(P)$

Ta gọi $h(P)$ là độ cao (logarit) của P.

Dễ thấy: với bất kỳ $B>0$, $\#\{P\in\mathbb{P}^2(\mathbb{Q})\colon H(P)\leq B\}\leq(2B+1)^3$

Vì vậy:

(1): $\{P\in\mathbb{P}^2(\mathbb{Q})\colon h(P)\leq B\}$ là hữu hạn.

Đây là trường hợp đặc biệt của định lý Northcott [Ser2, bài 2.4]. Nếu $E\subset\mathbb{P}^2$ là 1 đường cong elliptic trên $\mathbb{Q}$ thì ta có thể chỉ ra rằng với $P,Q\in E(\mathbb{Q})$, có

(2): h(P+Q)+h(P - Q)=2h(P)+2h(Q)+O(1)

Định nghĩa độ cao chính tắc hay độ cao Néron_Tate của $P \in E(\mathbb{Q})$ bởi $\hat{h}(P) := \lim_{n\to\infty} h(2^n P)/4^n$. Sau đây là các hệ quả của (1) và (2) với $P,Q \in E(\mathbb{Q})$ và $n \in Z$,

(a) $h(2P) = 4h(P) + 0(1)$

(b) Định nghĩa giới hạn $\hat{h}(P)$ là tồn tại.

(c) $\hat{h}(P) = h(P) + 0(1)$.

(d) $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.

(e) $\hat{h}(nP) = n^2 \hat{h}(P)$.

(f) $\hat{h}(P) \geq 0$. Dấu "=" xảy ra khi và chỉ khi : $P \in E(\mathbb{Q})_{tors}$.

(Với O(1) phụ thuộc E, không phụ thuộc P và Q).

Đặc biệt : $\hat{h}$ là dạng toàn phương bậc 2 trên $E(\mathbb{Q})/\ E(\mathbb{Q})_{tors}$.

Hơn nữa, (1) và (2) với định lý Mordell-Weil yếu khẳng định sự hữu hạn của $E(\mathbb{Q})/2E(\mathbb{Q})$ thì $E(\mathbb{Q})$ là hữu hạn sinh.

Nếu các phần tử sinh của $E(\mathbb{Q})/2E(\mathbb{Q})$ được tìm một cách hiệu quả thì hạng của $E(\mathbb{Q})$ và các phần tử sinh của $E(\mathbb{Q})$ cũng tìm được một cách hiệu quả.

1.4.8. Phương pháp phân tích đường cong elliptic.

1.4.8.1. Một sự giải thích về sự phân tích.

Giả sử: p,q là hai số nguyên tố lớn chưa biết và $N = p.q$. Ta tìm cách để xác định một số nguyên m sao cho m là $m \equiv 0 \pmod{p}$ nhưng m không đồng dư $0 \pmod{q}$.

Khi đó: $gdc(m,N)$ có thể được tính toán một cách nhanh chóng.

1.4.8.2. Một số phương pháp phân tích.

Ta có thể tìm ra các phương pháp phân tích khác nhau từ quan điểm vừa trình bày ở mục trước (xem $\mathbb{Z}/N$ như là cách viết gọn của vành thương $\mathbb{Z}/N\mathbb{Z}$).

Thử chia với: $m=2, m=3, m=5...$

Pollard p: Cho hàm: $f: \mathbb{Z}/N \to \mathbb{Z}/N$

Xét dãy các phần tử của $\mathbb{Z}/N$: $x_1, x_2, x_3...$ sao cho: $x_{i+1}=f(x_i)$ và thử với: $m=x_i-x_j \ (i\neq j)$

Sàng toàn phương, sàng trường số: tìm nghiệm không tầm thường: $x^2 \equiv y^2 (\mathrm{mod}\, n)$ và thử với $m=x+y$.

Pollard $p-1$: Chọn ngẫu nhiên một số $a \bmod N$. Lấy $K=k!$ với $k\geq 1$ và thử: $m=a^K-1$.

Phương pháp đường cong elliptic của Lenstra: thay cho a^K với $a\in (Z/N)^*$. Xét $K.P$

với $P\in E(\mathbb{Z}/N)$, với đường cong elliptic E nào đó.

Trong đó: $K.P=\underbrace{P+P+...+P}_{K\ lần}$ trong một nhóm aben $E(\mathbb{Z}/N)$ đã được xác định.

1.4.8.3. Phương pháp Pollard $p-1$

Phương pháp đường cong elliptic có thể được xem tương tự như phương pháp Pollard $p-1$. Với phương pháp đường cong elliptic ở đây người ta mô tả phương pháp $p-1$ một cách đầy đủ hơn nhưng vẫn bỏ qua chi tiết và sự cải tiến hữu ích.

Để phân tích N:

1) Chọn một số nguyên $K>1$ với nhiều nhân tử, chẳng hạn ta có: $K=k!$ với $k\geq 1$.

2) Chọn tùy ý số nguyên a sao cho : 1<a<N-1.

3) Nếu $gdc(a,N)>1$. Khi đó ta dừng lại. Nếu ngược lại thì tiếp tục.

4) Sử dụng phép khai triển nhị phân của K để tính $a^K \bmod N$.

5) Tính $g=\gcd(a^K-1,N)$.

+ Nếu: $1<g<N$ thì ta dừng lại. Khi đó: g là một nhân tử không tầm thường của N.

+ Nếu: $g=N$, ta thử lại với một giá trị khác với a hoặc với K được thay thế bằng một ước số .

+ Nếu: $g=1$ thì thử lại với K lớn hơn,…

Nếu K là bội của $p-1$ (với p nguyên tố) chia hết N thì trong bước 4 ($a^K \bmod p$) là một lũy thừa của ($a^{p-1} \bmod p$), nó là ($1 \bmod p$), do định lý nhỏ Fermat. Khi đó trong bước 5, a^K-1 chia hết cho p. Vì vậy: $g=p$.

Điều khó khăn trong phương pháp này là: không dễ để sắp xếp K là bội của $p-1$. Vì ta không biết được p.

Cách tốt nhất là ta có thể chọn K có nhiều nhân tử và hy vọng có chứa nhân tử $p-1$. Ví dụ, ta chọn $K=k!$

1.4.8.4. Các phương án của phương pháp $p-1$.

Thay vì dùng định lý Fermat nhỏ trên F_p^*, ta có thể nhận thấy rằng mọi phần tử của $F_{p^2}^* / F_P^*$ có bậc chia hết p + 1, có thể phát triển một phương pháp p+1 bởi việc thực hiện trên $A^* / (Z/N)^*$ mà $A=(Z/N)[t]/(t^2-b)$ với giá trị nào đó $b \in Z/N$.

Bằng cách tương tự ta có thể dùng nhóm con của $F_{p^r}^*$ cho số r đủ nhỏ để phát triển phương pháp đang được thực hiện tốt khi $p^2 + p + 1$ là trơn, khi $p^2 + 1$ là trơn, khi $\Phi_r(p)$ là trơn với $\Phi_r(z)$ là đa thức chia vòng tròn bậc r. Điều đó nhanh chóng trở nên không còn tác dụng bởi vì $p^2 + p + 1$ là quá lớn hơn p – 1 và do đó trở nên khó trơn.

Tư tưởng của Lenstra: thay thế F_p^* bởi nhóm $E(F_p)$ mà E là đường cong elliptic. Có nhiều E khác nhau để thực hiện.

1.4.8.5. Đường cong elliptic trên Z/N :

Cho N là số nguyên dương. Để cho việc giải thích đơn giản, ta xem như $\gcd(N,6)=1$. Định nghĩa :

$$P^2(Z/N) := \frac{\{(a:b:c) \mid a,b,c \in Z/N, \gcd(a,b,c,N)=1\}}{(Z/N)^*}$$

Một đường cong elliptic E trên Z/N được cho bởi một phương trình thuần nhất: $Y^2Z = X^3 + AXZ^2 + BZ^3$ với $A,B \in Z/N$ sao cho $\Delta := -16(4A^3 + 27B^2)$ thuộc $(Z/N)^*$. Thế thì $E(Z/N)$ là tập con của những điểm (a:b:c) $\in P^2(Z/N)$ thỏa mãn phương trình bậc ba. Với bất kỳ số nguyên tố p chia hết N, $E(Z/p)$ là tập hợp những điểm trong $P^2(Z/p)$ thỏa mãn phương trình quy gọn theo mod p.

Để đơn giản, giả sử N= pq với p, q là những số nguyên tố phân biệt lớn hơn 3. Định lý số dư Trung Hoa dẫn đến

$$\frac{Z}{N} \simeq \frac{Z}{p} \times \frac{Z}{q}$$ (như là những vành)

$$\left(\frac{Z}{N}\right)^{*} \simeq \left(\frac{Z}{p}\right)^{*} \times \left(\frac{Z}{q}\right)^{*} \qquad \text{(như là những nhóm)}$$

$$P^2\left(\frac{Z}{N}\right) \simeq P^2\left(\frac{Z}{p}\right) \times P^2\left(\frac{Z}{q}\right) \qquad \text{(như là những tập hợp)}$$

$$E\left(\frac{Z}{N}\right) \simeq E\left(\frac{Z}{p}\right) \times E\left(\frac{Z}{q}\right) \qquad \text{(như là những nhóm)}$$

Do đó tập hợp $E\left(Z/N\right)$ thừa hưởng cấu trúc của một nhóm aben. Phần lớn những cặp điểm trên $E\left(Z/N\right)$ có thể có thể được cộng bởi việc sử dụng công thức của phần 1.4.4.5. Thực tế, những công thức đó chỉ sai nếu có một vài phép tính trên Z/N là 0(mod p) và khác không (mod q) hay ngược lại. Khi đó N được phân tích.

1.4.8.6. Phương pháp đường cong elliptic:

Giả sử rằng số nguyên N thỏa mãn $\gcd(N,6) = 1$ và $N \neq n^r$ với mọi số nguyên n, $r \geq 2$. Để tìm ra những thừa số của N nhỏ hơn P ta thực hiện như sau:

1. Cố định một giới hạn trơn y nhỏ hơn P và cho K là LCM của tất cả các số nguyên y-smooth nhỏ hơn hay bằng P
2. Chọn các số nguyên ngẫu nhiên A, x_1 ; $y_1 \in [1;N]$
3. Đặt $B = y_1^2 - x_1^3 - Ax_1 \in Z/N$ và giả sử E là $y^2 = x^3 + Ax + B$ sao cho $P_1 := (x_1;y_1) \in E\left(Z/N\right)$. Nếu gcd($4A^3 + 27B^2$, N) $\neq 1$, trở lại bước 2.
4. Dùng sự mở rộng nhị nguyên của những nhân tử của K để tìm ra K. $P_1 \in E\left(Z/N\right)$ dùng công thức của luật nhóm.

5. Nếu tại một vài điểm mà không thỏa công thức, thì chúng ta tìm ra một thừa số của N. Trái lại, trở lại bước 2 và thực hiện trên một đường elliptic khác.

Chú ý rằng trong bước 2 và bước 3 ta chọn điểm đầu tiên và tìm đường cong elliptic đi qua điểm đó. Do những phức tạp về mặt thuật toán để tìm ra một điểm ngẫu nhiên trên đường cong elliptic, ta sẽ thực hiện bằng cách đơn giản hơn: trước tiên chọn tọa độ x, lấy căn bậc hai của một phần tử của Z/N.

1.4.8.7. Những phân tích đặc trưng của phương pháp đường cong elliptic:

Nếu $\#E\left(Z/p\right)$ chia hết K, thì $K.P_1$ sẽ rút gọn thành 0 mod p. Trong trường hợp đó có thể $K.P_1$ có thể không phải là O mod N, hay tối thiểu tại một vài điểm của việc tính $K.P_1$, thu được K' sao cho $K'.P_1$ là 0 mod N. Do đó điều cần thiết của sự phân tích thành thừa số N đòi hỏi một chút may mắn để chọn E sao cho $\#E\left(Z/p\right)$ chia hết K.

Giả sử rằng N có một thừa số nguyên tố p sao cho $p+1+2\sqrt{p} \le P$. Chọn s là xác suất cho việc xây dựng nên E ngẫu nhiên bởi thuật toán, cấp của $E\left(Z/p\right)$ là y-smooth. Nếu $E\left(Z/p\right)$ là y-smooth, thì $E\left(Z/p\right)\backslash K$, do định nghĩa của K và do định lý Hasse rằng $\#E\left(Z/p\right) \le p+1+2\sqrt{p}$. Do đó, số đường cong elliptic cần thiết phải thử trong suốt thuật toán là $O\left(1/s\right)$. Mỗi phép thử dẫn đến O(logN) phép toán luật nhóm, đòi hỏi $(\log N)^{0(1)}$ toán tử bit, cần thời gian tổng cộng là $R = 0\left(s^{-1}(\log K)(\log N)^{0(1)}\right)$

Giả sử $L(x) = \exp\left(\sqrt{(\log x)(\log\log x)}\right)$, sao cho $\log x << L(x) << x$ khi $x \to \infty$. Đặt $y = L(P)^a$ với $a > 0$. Để diễn tả thời gian chạy R trong giới hạn những tham số của thuật toán, gọi tên là N, P, và a, trước tiên ta tính K:

$$K \le \prod_{l \le y} l^{\left[\log_l P\right]} \le \prod_{l \le y} P \le P^y$$

$$\log K \le y \log P = L(P)^{a+0(1)}$$

Tiếp theo ta cần ước lượng về xác suất trơn s. Định lý của Canfield, Erdos, và Pomerance [CEP] chỉ ra rằng xác suất để một số nguyên ngẫu nhiên thuộc $[1, x]$ để $L(x)^a$ – trơn là $L(x)^{-1/(2a)+0(1)}$ khi $x \to \infty$. Dùng thuật toán Deuring số đường cong elliptic trơn được cho trên Z/p, ta có thể chỉ ra rằng $\#E\left(Z/p\right)$ là gần với phân bố đều trên hầu hết các khoảng biến thiên Hasse $\left[p+1-2\sqrt{p}; p+1+2\sqrt{p}\right]$.

Để tiếp tục, ta giả sử rằng kết quả của định lý Canfield – Erdos – Pomerance thỏa mãn với số nguyên ngẫu nhiên là nhỏ hơn nhiều. Thì $s = L(P)^{-1/(2a)+0(1)}$.

Theo giả thiết, tổng thời gian cần thiết của phương pháp đường cong elliptic là

$$R = L(P)^{a+1/(2a)+0(1)} (\log N)^{0(1)}.$$

Đẳng thức đó sẽ đạt tối ưu hóa khi $a = \frac{1}{\sqrt{2}}$, $y = L(P)^{\frac{1}{\sqrt{2}}}$ và

$R = L(P)^{\sqrt{2}+0(1)} (\log N)^{0(1)}$.

Để hoàn thành phân tích N, ta đặt $P = \sqrt{N}$, và tính thời gian chạy của $L(N)^{1+0(1)}$.

Một thuận lợi của phương pháp đường cong elliptic so với phần lớn các phương pháp phân tích thành thừa số khác là thời gian thực hiện chỉ phụ thuộc vào kích cỡ của phần tử được tìm thấy, nó có khả năng tìm thấy những phân tử nhỏ mà nhanh hơn.

Trong thực tế, vì tối ưu hóa cách chọn y và do đó K phụ thuộc vào P nên việc thực hiện phương pháp đường cong elliptic là hợp lý. Hơn nữa, nếu không tìm được thừa số ta có thể thực hiện lại bằng cách tăng dãy các giá trị của P. Cuối cùng, nếu không tìm được những phần tử nào đủ nhỏ thì ta nên chuyển sang sàng trường số, nó sẽ tiệm cận nhanh hơn nếu những nhân tử là lớn.

1.4.8.8. Những kết quả của phương pháp đường cong elliptic:

Thừa số lớn nhất được tìm thấy bởi phương pháp đường cong elliptic là một nhân tử nguyên tố gồm 54 chữ số :

484061254276878368125726870789180231995964870094916937

của $\left(6^{43}-1\right)^{42}+1$.

Chương 2. CÁC ĐƯỜNG CONG ELLIPTIC DẠNG HESSE

2.1. Tổng quan

Đường cong elliptic dạng Hesse được thừa nhận thích hợp với số học hơn đường cong dạng Weierstrass. Nhưng các hệ thống mật mã đường cong elliptic thường sử dụng dạng Weierstrass. Ta biết rằng cả hai dạng trên là tương đương song hữu tỉ. Sự tương đương song hữu tỉ là tương đối khó tính toán. Chúng ta sẽ chứng minh rằng các đường cong elliptic dạng Hesse và dạng Weierstrass là tương đương tuyến tính trên trường ban đầu hoặc trên sự mở rộng của chính nó và sự tương đương này là dễ dàng để chứng minh được. Nếu lực lượng của trường hữu hạn $q \equiv 2(\mathrm{mod}\,3)$ và vết Frobenius $T \equiv 0(\mathrm{mod}\,3)$, thì sự tương đương được xác định trên trường hữu hạn ban đầu. Sự tương đương tuyến tính này cho phép nhân một điểm trên đường cong elliptic dạng Weierstrass bằng cách chuyển qua đường cong Hesse, tính các điểm nhân trên đường cong này sau đó chuyển ngược lại. Tốc độ của phép nhân điểm tăng khoảng 1,37 lần.

2.1.1. Tương đương tuyến tính giữa đường cong elliptic dạng Weierstrass và đường cong elliptic dạng Hesse

2.1.1.1. Lời giới thiệu

Cho $\mathbb{F}_q$ là trường gồm $q = p^n$ phần tử đối với số nguyên tố p và $\overline{\mathbb{F}}_q$ là bao đóng đại số của nó. Mặt phẳng xạ ảnh là tập các điểm được cho bởi bộ ba $(X,Y,Z) \setminus (0,0,0)$ với quan hệ tương đương: $(X,Y,Z) \sim (uX,uY,uZ)\ \forall u \in \overline{\mathbb{F}}_q^*$. Những điểm với $Z = 0$ là những điểm tại vô cực.

Đường cong đại số xạ ảnh là tập con của mặt phẳng xạ ảnh, trong đó $f(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ nhận giá trị 0. Đường cong đại số afin là tập con của đường cong xạ ảnh với $Z \neq 0$.

Nếu $\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = L \begin{pmatrix} U \\ V \\ W \end{pmatrix}$, trong đó L là ma trận khả nghịch, và $f(X,Y,Z) = g(U,V,W)$, thì các đường cong được cho bởi đa thức f, g là tương đương tuyến tính và $\deg(f) = \deg(g)$.

Nếu giữa hai đa thức f, g tồn tại các ánh xạ hữu tỉ φ, ψ sao cho: $f = \varphi(g), g = \psi(f)$, và $\varphi\psi$, $\psi\varphi$ là các ánh xạ đồng nhất (nếu các ánh xạ trên là xác định) trên các đường cong tương ứng, thì các đường cong được cho bởi các đa thức f, g là tương đương song hữu tỉ.

Tương đương song hữu tỉ có thể được xác định một cách riêng và nó có thể làm thay đổi bậc của đa thức. Nếu các ánh xạ φ, ψ giữa các đường cong afin là đa thức thì các đường cong là đẳng cấu với nhau. Sự tương đương tuyến tính này ánh xạ các điểm tại vô cực tới các điểm tại vô cực xác định phép đẳng cấu giữa các đường cong đại số.

Đường cong elliptic là đường cong xạ ảnh trơn bậc ba. Các đường cong elliptic trên trường hữu hạn được sử dụng một cách rộng rãi trong khóa mật mã. Các đường cong có thể được cho bởi các đa thức khác nhau. Hầu hết các đa thức trong dạng Weierstrass thường có dạng:

$$E_W(\mathbb{F}_q): Y^2Z - X^3 - AXZ^2 - BZ^3 \quad \text{nếu } p \geq 5. \quad (1)$$

Đường cong này có điểm uốn tại vô cực $P_\infty = (0,1,0)$.

Đường cong elliptic dạng Hesse được cho bởi đa thức:

$$E_H(\mathbb{F}_q): U^3 + V^3 + W^3 - 3mUVW \quad (2),$$

trong đó $p \neq 3$ và $m^3 \neq 1$.

Đường cong này có 3 điểm uốn tại vô cực

$P_\infty = (1,-1,0),(1,-\rho,0),(1,-\rho^2,0), \rho = \frac{-1+\sqrt{-3}}{2}$(nếu -3 là một bình phương), hoặc chỉ có một điểm uốn tại P_∞ (nếu -3 không là một bình phương).

Đường cong elliptic sai khác đẳng cấu (trên $\mathbb{F}_q$ hoặc là mở rộng hữu hạn của nó) thì được xác định bởi j-bất biến của nó, $j = \frac{2^8 3^3 A^3}{4A^3 + 27B^2}$ đối với đường cong dạng (1) và $j = \left(\frac{3m(8+m^3)}{-1+m^3} \right)^3$ đối với đường cong dạng (2).

Các điểm của các đường cong elliptic lập nên nhóm aben qua phép cộng:

$$(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3).$$

Đối với đường cong dạng (1) thì phần tử đối của (X,Y,Z) là $(X,-Y,Z)$, phần tử 0 là P_∞ và tổng của hai điểm xác định bởi các đa thức bậc 6:

$$X_3 \equiv 2Y_1Z_1((3X_1^2 + AZ_1^2)^2 - 8X_1Y_1^2Z_1),$$

$$Y_3 \equiv 4Y_1^2Z_1(3X_1(3X_1^2 + AZ_1^2) - 2Y_1^2Z_1) - (3X_1^2 + AZ_1^2)^3,$$

$$Z_3 \equiv 8Y_1^3Z_1^3,$$

nếu $(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$ và bởi các đa thức bậc 8:

$$X_3 \equiv (X_2Z_1 - X_1Z_2)(Z_1Z_2(Y_2Z_1 - Y_1Z_2)^2 - (X_2Z_1 + X_1Z_2)(X_2Z_1 - X_1Z_2)^2),$$

$$Y_3 \equiv (X_2Z_1 - X_1Z_2)^2(Y_2Z_1(X_2Z_1 + 2X_1Z_2) - Y_1Z_2(X_1Z_2 + 2X_2Z_1)) - Z_1Z_2(Y_2Z_1 - Y_1Z_2)^3,$$

$$Z_3 \equiv Z_1Z_2(X_2Z_1 - X_1Z_2)^3,$$

nếu $(X_1, Y_1, Z_1) \neq (X_2, Y_2, Z_2)$

Ta có thể ước lượng tính phức tạp của số học đường cong elliptic như là số lượng các phép nhân trên trường.

Điểm kép lấy 13 phép nhân trên trường (12 đối với $A = \pm 1$). Nếu một điểm là cố định với $Z = 1$, thì cần lấy 12 phép nhân trường.

Đối với đường cong dạng (2) thì phần tử đối của (U,V,W) là (V,U,W), phần tử 0 là P_∞. Tổng của các điểm được cho bởi các đa thức bậc 4

Nếu $(U_1,V_1,W_1)=(U_2,V_2,W_2)$:

$$U_3 = V_1(W_1^3 - U_1^3),$$
$$V_3 = U_1(V_1^3 - W_1^3), ,$$
$$W_3 = W_1(U_1^3 - V_1^3)$$

Nếu $(U_1,V_1,W_1)\neq(U_2,V_2,W_2)$:

$$U_3 = U_1W_1V_2^2 - U_2W_2V_1^2$$
$$V_3 = V_1W_1U_2^2 - V_2W_2U_1^2$$
$$W_3 = U_1V_1W_2^2 - U_2V_2W_1^2$$

Điểm kép lấy 9 phép nhân trường. Nếu một trong hai điểm được cố định và có $W=1$, thì điểm cộng lấy 10 phép nhân trường.

Đường cong cải tiến dạng Hesse thừa nhận tính toán số học nhanh hơn dạng Weierstrass [HWCD]. Thuật toán chữ ký số đường cong elliptic [FIPS] dùng đường cong dạng Weierstrass (1).

M.Ciet, G.Piret và J-J. Quisquater trong [CPQ], M.Joyee và J-J. Quisquater trong [JQ] chỉ ra rằng tồn tại phép đẳng cấu song hữu tỉ giữa dạng Weierstrass và dạng Hesse. Ánh xạ này thì không dùng chung để tính toán. Mục đích của mục này là để chỉ ra rằng có sự tồn tại tương đương tuyến tính chung giữa đường cong elliptic (1) và (2) và sự tương đương này được xác định trên trường ban đầu hoặc trên sự mở rộng hữu hạn của chính nó, và để nhận diện xem liệu có hay không tồn tại sự tương đương trên trường hữu hạn ban đầu. Sự tương đương này có thể làm tăng tốc độ xử lý số học của đường cong elliptic dạng Weierstrass. Bên cạnh đó là đưa ra các công thức đơn giản cho phép nhân phức trên đường cong elliptic dạng Hesse.

2.1.1.2. Đường cong elliptic tương đương tuyến tính

Định lý 1:

Cho trường đặc số khác 2, 3. Các đường cong elliptic $E(\mathbb{F}_q)$ cho bởi các đa thức (1) và (2) là tương đương tuyến tính trên $\overline{\mathbb{F}_q}$. Trên $\mathbb{F}_q$ tồn tại ánh xạ tuyến tính từ (2) vào (1). Trên $\mathbb{F}_q$ tồn tại ánh xạ tuyến tính từ (1) vào (2) hoặc là sự mở rộng của nó có bậc 2, 3, 4 ,6.

Chứng minh: Ánh xạ tuyến tính từ (2) vào (1) được xác định bởi ma trận

$$L = \begin{pmatrix} m & 1 & \dfrac{4-m^3}{3} \\ m & -1 & \dfrac{4-m^3}{3} \\ -2 & 0 & -2m^2 \end{pmatrix}$$

Định thức của ma trận bằng $\dfrac{16(-1+m^3)}{3}$. Nó là khả nghịch nếu $p \neq 2,3$ và được xác định trên trường ban đầu. Ánh xạ tuyến tính nghịch đảo từ (1) vào (2) được xác định bởi ma trận

$$M = \begin{pmatrix} m^2 & m^2 & \dfrac{4-m^3}{3} \\ \dfrac{-4+4m^3}{3} & \dfrac{4-4m^3}{3} & 0 \\ -1 & -1 & -m \end{pmatrix}$$

(để đơn giản M là tích của L^{-1} với ma trận vô hướng).

j_bất biến là một lập phương trong trường ban đầu [5]. Giả sử $j = \gamma_2{}^3$. Phương trình $\gamma_2 = \dfrac{3m(8+m^3)}{-1+m^3}$ có thể có 0, 1, 2 hoặc 4 nghiệm trong $\mathbb{F}_q$. Trên $\mathbb{F}_q$ thì trường phân rã k có bậc tương ứng là 4, 3, 2, 1.

Phương trình $j = \left(\frac{3m(8+m^3)}{-1+m^3} \right)^3$ tương đương với phương trình

$$(\gamma_2(-1+m^3))^3 = (3m(8+m^3))^3 \qquad (3)$$

Các nghiệm của nó trong k hoặc trong dạng mở rộng bậc hai của k nếu $\sqrt{-3} \notin k$. Chú ý rằng nếu bậc của k trên $\mathbb{F}_q$ là chẵn thì $\sqrt{-3} \in k$. Vì vậy trường phân rã của phương trình (3) có bậc trên $\mathbb{F}_q$ là 1, 2, 3, 4, 6.

Ảnh của đường cong Hesse là:

$$Y^2Z - X^3 + \frac{m(8+m^3)XZ^2}{3} - \frac{2(-8-20m^3+m^6)Z^3}{27} \qquad (4)$$

Sự tương đương tuyến tính không làm thay đổi j-bất biến.

Định lý 2:

Cho $E_2 = \varphi(E_1)$ là ánh xạ tuyến tính khả nghịch của các đường cong elliptic và $\psi : E_1 \to E_1$ là ánh xạ khả nghịch được cho bởi đa thức đa thức thuần nhất bậc d. Khi đó phép tương đương tuyến tính xác định ánh xạ khả nghịch $\varphi\psi\varphi^{-1}$ của đường cong E_2 được cho bởi các đa thức thuần nhất bậc d.

Chứng minh:

Ánh xạ $\varphi\psi\varphi^{-1}$ tác động lên E_2 và khả nghịch như là tích của các ánh xạ khả nghịch. Vì φ là ánh xạ tuyến tính, nên ánh xạ $\varphi\psi\varphi^{-1}$ được cho bởi đa thức có bậc $\le d$. Giả thiết rằng bậc bé hơn d dẫn đến mâu thuẫn, vì ánh xạ tương ứng $\psi = \varphi^{-1}(\varphi\psi\varphi^{-1})\varphi$ trên E_1 sẽ được cho bởi các đa thức có bậc bé hơn d.

Hệ quả 3:

Nếu cấp của nhóm là số nguyên lẻ, thì tồn tại các đa thức thuần nhất bậc 4 cho phép lấy điểm kép và cộng điểm trên đường cong elliptic dạng Weierstrass.

Chứng minh:

Nếu cấp của nhóm là lẻ, thì phép lấy điểm kép là ánh xạ khả nghịch. Phép lấy điểm kép và điểm cộng trên đường cong elliptic dạng Hesse được xác định bởi đa thức bậc 4. Áp dụng các định lý 1 và 2 ta có điều phải chứng minh.

2.1.1.3. Tương đương tuyến tính trên trường ban đầu

Ta xét xem liệu có hay không ánh xạ tuyến tính $E_w(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ được xác định trên $\mathbb{F}_q$. Sự tồn tại của ánh xạ tuyến tính tương đương với sự tồn tại của đường cong elliptic dạng Hesse với cùng số lượng các điểm và j-bất biến như đường cong elliptic dạng Weierstrass.

Cho $q \equiv 2(\mathrm{mod}\,3)$, thì mỗi phần tử của $\mathbb{F}_q$ là một lũy thừa bậc ba, vì thế ánh xạ $\gamma_2 \to \gamma_2^3 = j$ là song ánh. Phương trình

$$\gamma_2(-1+m^3) = 3m(8+m^3) \quad (5) \quad \text{có 4 nghiệm trên } \overline{\mathbb{F}}_q:$$

$$\frac{1}{12}\left(\gamma_2 \pm \sqrt{(6+\gamma_2)^2+108} \pm \sqrt{2(12-\gamma_2)(-6-\gamma_2 \pm \sqrt{(6+\gamma_2)^2+108})}\right),$$

Trong đó dấu của $\sqrt{(6+\gamma_2)^2+108}$ thay đổi đồng thời trong cả hai vị trí.

Phương trình (5) tương đương tuyến tính với phương trình trùng phương $x^4 + 2ax^2 + b = 0$ nếu

$$a = \frac{6\gamma_2 + \alpha - 12\sqrt{\alpha} - \gamma_2\sqrt{\alpha}}{18},\ b = \frac{-\gamma_2 - 6\sqrt{\alpha} + \gamma_2\sqrt{\alpha}}{36},\ \alpha = (6+\gamma_2)^2 + 108.$$

Các nghiệm của nó là $\pm\sqrt{-a \pm \sqrt{a^2-b}}$. Do đó $\alpha = (6+\gamma_2)^2 + 108$ là một bình phương trong $\mathbb{F}_q$.

Phương trình (5) có nghiệm trong $\mathbb{F}_q$ nếu các số hạng

$\sqrt{(6+\gamma_2)^2+108}$ và $\sqrt{2(12-\gamma_2)\left(-6-\gamma_2 \pm \sqrt{(6+\gamma_2)^2+108}\right)}$ đều thuộc trong $\mathbb{F}_q$. Trong trường hợp này có hai nghiệm. Tương đương tuyến tính giữa phương trình (5) và phương trình trùng phương có nghĩa là nếu có một số

hạng trong $\mathbb{F}_q$, thì cũng có một số hạng khác cũng ở trong $\mathbb{F}_q$. Xác suất của nó là $\approx 0,5$. Tồn tại đường cong elliptic như đã nêu, nếu $(6+\gamma_2)^2+108$ là một bình phương. Hai nghiệm tương ứng với các đường cong elliptic xoắn chúng có cùng j nhưng ngược vết của tự đồng cấu Frobenius.

Định lý 4:

Nếu $q \equiv 2(\mathrm{mod}\,3)$, thì đường cong elliptic Hesse có vết của tự đồng cấu Frobenius $T \equiv 0(\mathrm{mod}\,3)$.

Chứng minh:

Đường cong elliptic trên trường tùy ý có điểm uốn afin $(0,-1,1)$ cấp 3. Do đó số lượng các điểm trên trường hữu hạn $N \equiv 0(\mathrm{mod}\,3)$. Vết của tự đồng đồng cấu Frobenius được xác định là $T = q+1-N$. Thay $q \equiv 2(\mathrm{mod}\,3)$, nhận được $T \equiv 0(\mathrm{mod}\,3)$.

Ánh xạ tuyến tính $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ được xác định trên $\mathbb{F}_q$ nếu các đẳng thức nhận được trong định lý 1 thỏa mãn đồng thời

$$A = -\frac{m(8+m^3)}{3}, B = \frac{2(-8-20m^3+m^6)}{27}$$

Khi xác suất gần với 1 thì không có nhiều m như vậy. Nhưng tham số m ta có thể tìm được nhờ phép đẳng cấu đường cong elliptic Weierstrass

$$(X,Y,Z,A,B) \to (u^2X, u^3Y, Z, u^4A, u^6B) \text{ với } u \neq 0 \text{ tùy ý.}$$

Vậy thì các phương trình trở thành

$$u^4A = -\frac{m(8+m^3)}{3}, u^6B = \frac{2(-8-20m^3+m^6)}{27} \qquad (6)$$

Nếu $q \equiv 5(\mathrm{mod}\,6)$ và đường cong elliptic Weierstrass $E_W(\mathbb{F}_q)$ có $T \equiv 0(\mathrm{mod}\,3)$, thì tồn tại đường cong elliptic Hesse $E_H(\mathbb{F}_q)$ tương đương tuyến tính. Phương trình (6) có nghiệm $(m, \pm u)$ trong $\mathbb{F}_q$ nếu và chỉ nếu

phương trình (5) có nghiệm trong $\mathbb{F}_q$. Như đã chỉ ra ở trên rằng $(6+\gamma_2)^2+108$ là một bình phương trong $\mathbb{F}_q$ và phương trình (5) có nghiệm như yêu cầu. Do đó phương trình (6) cũng có nghiệm trong $\mathbb{F}_q$. Sự tương đương tuyến tính giữa đường cong elliptic dạng Weierstrass và dạng Hesse được xác định trong $\mathbb{F}_q$ và được xác định bởi các phương trình:

$$\begin{aligned} U &= u^2 mX + u^3 Y + \frac{4-m^3}{3} Z, \\ V &= u^2 mX - u^3 Y + \frac{4-m^3}{3} Z, \qquad (7) \\ W &= -2u^2 X - 2m^2 Z, \end{aligned}$$

$$\begin{aligned} X &= u^{-2}(m^2(U+V) + \frac{4-m^3}{3} W), \\ Y &= u^{-3}\frac{4-m^3}{3}(-U+V), \qquad (8) \\ Z &= -U-V-mW. \end{aligned}$$

Nếu $q \equiv 1 (\mathrm{mod}\, 3)$, thì cubing không song ánh. Tồn tại $\rho = \frac{-1+\sqrt{3}}{2} \in \mathbb{F}_q$, và đường cong elliptic Hesse có 9 điểm cấp 3. Nhóm các điểm cấp 3 là tổng trực tiếp của hai nhóm cyclic cấp 3. Do đó số các điểm thỏa mãn phương trình đồng dư $N \equiv 0 (\mathrm{mod}\, 9)$. Ánh xạ tuyến tính $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ có thể được xác định trên sự mở rộng của trường ban đầu. Chú ý rằng đường cong elliptic Hesse $E_H(\mathbb{F}_q)$ có thể chỉ tương ứng với 1 trong 2 đường cong Weierstrass xoắn. Vì thế trong trường hợp $q \equiv 1 (\mathrm{mod}\, 3)$ ít được quan tâm hơn trường hợp $q \equiv 2 (\mathrm{mod}\, 3)$.

2.1.1.4. Sự ứng dụng của tương đương tuyến tính

Sự tương đương tuyến tính có thể được sử dụng một cách trực tiếp (cả trong phép biến đổi từ đường cong Weierstrass sang đường cong Hesse, phép

nhân một điểm với một số và biến đổi ngược lại) và để xác định các công thức nhân phức tạp, các công thức cho phép chúng ta tính toán nhanh hơn. Ta xét một số ví dụ sau:

Ví dụ 33: Đường cong elliptic có $j=0$ và đẳng cấu với đường cong $Y^2Z-X^3-BZ^3$ nếu $m=0,-2$. Đường cong cuối cùng ở trên có phép nhân phức bởi $\frac{1+\sqrt{-3}}{2}$:

$$\frac{1+\sqrt{-3}}{2}(X,Y,Z)=(\rho X,-Y,Z),\rho=\frac{-1+\sqrt{-3}}{2}.$$

Nếu $m=0$ thì ánh xạ tuyến tính và ánh xạ ngược của nó được cho bởi các ma trận:

$$\begin{pmatrix} 0 & 1 & \frac{4}{3} \\ 0 & -1 & \frac{4}{3} \\ -2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 4 \\ -4 & 4 & 0 \\ -3 & -3 & 0 \end{pmatrix}.$$

Ảnh đẳng cấu của đường cong Hesse có hệ số $B=-\frac{16}{27}$. Tương ứng với phép nhân phức của đường cong Hesse là ánh xạ

$$\frac{1+\sqrt{-3}}{2}(X,Y,Z)=(Y,X,\rho Z).$$

Ví dụ 34: Đường cong elliptic dạng Hesse có $j=1728$ và đẳng cấu với đường cong $Y^2Z=X^3-AXZ^2$ nếu $m=1+\sqrt{3}$. Đường cong cuối cùng ở trên có phép nhân phức bởi $\sqrt{-1}:\sqrt{-1}(X,Y,Z)=(-X,\sqrt{-1}Y,Z)$. Ảnh đẳng cấu của đường cong dạng Hesse có hệ số $A=-4(3+2\sqrt{3})$. Phép nhân phức tương ứng của đường cong Hesse là ánh xạ tuyến tính

$$\sqrt{-1}(X,Y,Z) = (\rho X + \rho^2 Y + Z, \rho^2 X + \rho Y + Z, X + Y + Z).$$

Ví dụ 35: Đường cong elliptic dạng Hesse có $j = 8000$ và đẳng cấu với đường cong $Y^2Z = (X^3 - 4tX^2Z + 2t^2XZ^2)$ nếu $m = \frac{-2-\sqrt{-2}}{3}$. Đường cong sau ở trên có phép nhân phức được xác định bởi:

$$\sqrt{-2}(X,Y,Z) = \left(-Y^2Z, \frac{Y(X^2 - 2t^2Z^2)}{\sqrt{-2}}, 2X^2Z \right).$$

Điểm $(0,0)$ có cấp là 2. Đường cong này có thể được chuyển thành dạng (1) bởi phép thế $X \leftarrow X + \frac{4t}{3}Z,$ thì đa thức (1) có các hệ số $A = -\frac{10}{3}t^2, B = -\frac{56}{27}t^3$. Giá trị m cần thiết đạt được nếu $t = \frac{-2+5\sqrt{-2}}{9}$. Phép nhân phức tương ứng trên đường cong Hesse được xác định bởi các đa thức thuần nhất bậc 3.

Ví dụ 36: Phép nhân một điểm của đường cong eliptic Weierstrass với một số.

Trong các ứng dụng mật mã cấp của nhóm là các số nguyên tố lớn. Theo Hệ quả 3, phép lấy đúp điểm và cộng điểm trên đường cong elliptic Weierstrass có thể được xác định bởi đa thức thuần nhất bậc 4 thay cho các đa thức bậc 6, 8 đã biết. Nó đủ điều kiện để chuyển từ đường cong Weierstrass thành đường cong dạng Hesse, phép lấy đúp điểm hoặc cộng điểm và làm phép biến đổi ngược lại.

Tính toán tương đương tuyến tính và nghịch đảo dùng tới 9 phép nhân trên trường.

Ánh xạ tuyến tính $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ theo (7) lấy 5 phép nhân trường:

$$u^2mX, -2u^2X, u^3Y, \frac{4-m^3}{3}Z, -2m^2Z.$$

Ánh xạ tuyến tính nghịch đảo $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ theo (8) lấy 4 phép nhân trường: $u^{-2}m^2(U+V), \frac{4-m^3}{3u^2}W, \frac{4-4m^3}{3u^3}(-U+V), mZ$.

Nếu cấp của nhóm cỡ $n = 160$ bit, tính phức tạp của việc tính toán các ánh xạ tuyến tính là không đáng kể so với tính phức tạp của phép nhân điểm.

2.1.2. Thực hiện hệ thống mã hóa đường cong elliptic bằng cách sử dụng đường cong Hesse trên các trường số nguyên tố

2.1.2.1. Tổng quan

Ta xét kết quả của các thí nghiệm so sánh hệ thống mật mã đường cong elliptic sử dụng đường cong Hesse với các hệ thống sử dụng đường cong Weierstrass truyền thống. Đường cong elliptic dạng Hesse được tin tưởng sẽ cho hiệu quả cao hơn các dạng hiện nay đang được sử dụng trong việc thực hiện. Để thực hiện các thí nghiệm này, chúng ta thực hiện các tác động điểm trên các đường cong trong C++. Kết quả của thí nghiệm này chỉ ra rằng sử dụng đường cong dạng Hesse để triển khai thì nhanh hơn đường cong Weierstrass 20%-30%. Dạng Hesse làm cho việc mã hóa đường cong elliptic hấp dẫn hơn khi có thể xem như là một sự thay thế cho RSA trong ứng dụng thực tiễn, rất thích hợp cho các thiết bị tính toán hạn chế như là card thông minh.

2.1.2.2. Giới thiệu

Khi Koblizt và Miller đề nghị nghiên cứu một cách độc lập sử dụng các đường cong elliptic trong sự mã hóa khóa cộng vào năm 1985, việc làm tăng hiệu quả của hệ thống mật mã đường cong elliptic (ECC) đã được phát triển. Ngày nay, hệ thống này nhanh như hệ thống dựa trên nền nhân tử hóa các số nguyên với độ dài khóa giống nhau, xem [Ros].

Vì các hệ thống mật mã đường cong elliptic có sự an toàn như nhau như là RSA, nhưng có khóa ngắn hơn, hiệu quả hơn, và thường có thể thay thế

RSA. ECC đặc biệt thích hợp để dùng cho card thông minh, điện thoại tế bào và các thiết bị tính toán ràng buộc khác.

Các điểm trên đường cong lập thành một nhóm cộng aben có phép cộng như là phép toán nhóm.

Phép nhân một điểm trên đường cong elliptic với một số nguyên, đó chính là phép cộng nhiều lần một điểm với chính nó, là cơ sở nền móng cho việc sử dụng đường cong elliptic trong lý thuyết mật mã. Chúng ta sử dụng ký hiệu $[n]P = P + P + ... + P$ (n hạng tử), trong đó P là một điểm trên đường cong elliptic, và n là một số nguyên. Một thuật toán đơn giản và hiệu quả cho việc tính $[n]P$ là sử dụng một tổ hợp các đúp điểm và các phép cộng điểm. Số lượng các phép đúp điểm sẽ bằng hoặc nhiều hơn số lượng các phép cộng điểm. Cũng bằng cách sử dụng các phép trừ điểm, số lượng các phép cộng điểm có thể được rút gọn lại. Cho nên quan trọng nhất là sử dụng các đúp điểm thì thuật toán sẽ nhanh.

Tất cả các đường cong elliptic có thể được viết dưới dạng *Weierstrass dài*:

$$y^2 + a_i xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (1)$$

Với một số điều kiện xác định phương trình của đường cong elliptic có thể được rút gọn thành *dạng Weierstrass ngắn*:

$$E_{a,b} : y^2 = x^3 + ax + b \qquad (2)$$

Với một số điều kiện khác chúng có thể được viết dưới *dạng Hesse*:

$$E_D : x^3 + y^3 + 1 = Dxy \qquad (3)$$

Sự lựa chọn dạng ảnh hưởng đến hiệu suất của các phép toán trong các hệ thống mã hóa, bởi vì các biểu diễn khác nhau thì có các công thức khác nhau đối với việc nhân điểm.

Các nghiên cứu gần đây chỉ ra rằng đường cong trên dạng Hesse có một số tính chất làm cho chúng được dùng thích hợp hơn trong lý thuyết mật mã, không chỉ vì làm tăng hiệu suất, mà chúng còn có thể được dùng để bảo vệ để chống lại một số loại kênh tấn công. Chúng ta sẽ tập trung vào so sánh hiệu suất thực nghiệm giữa *dạng Weierstrass ngắn* và *dạng Hesse*.

Có hai loại thiết lập ECC chính, trên $\mathbb{F}_{2^r}$ và trên $\mathbb{F}_p$.

Trong phần này chúng ta sẽ mô tả các thí nghiệm mà chúng ta đã thực hiện với các đường cong elliptic dạng Hesse trên trường hữu hạn K=$\mathbb{F}_p$. Một mô tả của ECC sử dụng dạng Hesse trên $\mathbb{F}_{2^r}$ có thể xem trong [Sma].

Phần còn lại sẽ được trình bày trong phần 2.2 chúng ta sẽ xem lại luật nhóm đối với các điểm trên đường cong elliptic.

2.2. Luật nhóm: Xét trên đường cong dạng Hesse

Các điểm trên đường cong elliptic tạo thành một nhóm aben cùng với phép cộng điểm.

Nếu **P** và **Q** là hai điểm trên đường cong elliptic **E**, thì có một luật nhóm sao cho **P+Q** là một điểm hoàn toàn được xác định trên **E**.

2.2.1 Tọa độ xạ ảnh

Trong tọa độ xạ ảnh, hai điểm (x_1, y_1, z_1) và (x_2, y_2, z_2) (trong đó chúng ta giả thiết rằng $z_1, z_2 \neq 0$) được xem như tương đương nếu có $\lambda \neq 0$ sao cho $\lambda(x_1, y_1, z_1) = (x_2, y_2, z_2)$. Nếu (x, y, z) biểu diễn tọa độ một điểm trong tọa độ xạ ảnh, tương ứng với phép biểu diễn afin thì thu được là $\left(\frac{x}{z}, \frac{y}{z}\right)$.

Bằng cách sử dụng tọa độ xạ ảnh, ta có thể thực hiện cộng và nhân đôi các điểm mà không có phép chia. Phép chia trên trường hữu hạn thường là chậm hơn nhiều so với phép nhân, vì vậy nó thường có lợi khi sử dụng trong

tọa độ xạ ảnh, thậm chí nếu nhiều phép cộng và phép nhân thì tốt hơn với tọa độ afin.

Có vài loại tọa độ xạ ảnh. Thông thường thì sử dụng tọa độ xạ ảnh Jacobi đối với dạng Weierstrass, xem [BSS], và dùng tọa độ xạ ảnh chuẩn tắc đối với dạng Hesse.

2.2.2 Luật nhóm đối với các điểm trên đường cong dạng Hesse.

Sự thiết lập cơ bản trên các đường cong Weierstrass là tài liệu và phép thử tốt, và thường được sử dụng nhất trong thiết lập của ECC ngày nay, xem [IEEE]. Đường cong được khuyên dùng là đường cong Weierstrass. Có hướng dẫn và phương pháp tốt cho sự lựa chọn đường cong mạnh trong lý thuyết mật mã. Chúng ta sẽ không đi vào chi tiết việc sử dụng dạng Weierstrass, vì có nhiều sự mô tả tốt hơn điều đó, ví dụ như [BSS], [Ros] và [MOC].

Cho $P=(x_1,y_1,z_1)$ và $Q=(x_2,y_2,z_2)$ là hai điểm khác nhau trong hệ tọa độ xạ ảnh chuẩn tắc trên một đường cong elliptic E_D, $P+Q,-P$ và $[2]P$ có thể được biểu diễn như sau:

$$(P+Q)=(y_1^2x_2z_2-y_2^2x_1z_1,x_1^2y_2z_2-x_2^2y_1z_1,z_1^2x_2y_2-z_2^2x_1y_1) \quad (4)$$

$$-P=(y_1,x_1,z_1) \quad (5)$$

$$[2]P=(y_1(x_1^3-z_1^3),x_1(z_1^3-y_1^3),z_1(y_1^3-x_1^3)) \quad (6)$$

Một thuận lợi lớn bởi việc dùng dạng Hesse là các phép toán điểm có thể được thực hiện một cách đồng thời, xem [Sma].

Tổng của hai điểm $P+Q=R$

trong đó $P=(x_1,y_1,z_1),Q=(x_2,y_2,z_2),R=(x_3,y_3,z_3)$ và $P,Q,R\in E_D(K)$ có thể thực hiện một cách đồng thời theo cách sau:

$$\begin{cases} \lambda_1 = y_1 x_2 \quad \lambda_2 = x_1 y_2 \quad \lambda_3 = x_1 z_2 \\ \lambda_4 = z_1 x_2 \quad \lambda_5 = z_1 y_2 \quad \lambda_6 = z_2 y_1 \\ s_1 = \lambda_1 \lambda_6 \quad s_2 = \lambda_2 \lambda_3 \quad s_3 = \lambda_5 \lambda_4 \\ t_1 = \lambda_2 \lambda_5 \quad t_2 = \lambda_1 \lambda_4 \quad t_3 = \lambda_6 \lambda_3 \\ x_3 = s_1 - t_1 \quad y_3 = s_2 - t_2 \quad z_3 = s_3 - t_3 \end{cases} \qquad (7)$$

Các công thức đúp có thể thực hiện một cách đồng thời theo cách tương tự, xem [Sma]. Bảng 2 bao gồm khái quát các phép toán cơ bản cần để thực hiện cộng điểm và đúp điểm của các điểm trong dạng Weierstrass và Hesse.

2.2.3. Tác động kênh biên

Tất cả các phép toán điểm trong dạng Hesse có thể được tính toán chỉ bằng công thức cộng.

Bảng 1. Định thời đối với các phép toán trên trường các phần tử với độ dài 160bit và 240bit.

	Thời gian(p_{160})	Thời gian(p_{240})	Viết tắt
Phép cộng (c, a, b)	0.46 μs	0.51 μs	A
Phép trừ (c, a, b)	0.44 μs	0.51 μs	SU
Phủ định (c, a)	0.52 μs	0.57 μs	
Phép nhân với 2()	0.47 μs	0.52 μs	M2
Phép chia cho 2()	23.76 μs	28.34 μs	I2
Phép nhân(c, a, b)	2.57 μs	5.50 μs	M
Phép chia(c, a, b)	39.72 μs	63.08 μs	
Nghịch đảo (c, a)	33.39 μs	53.64 μs	I
Bình phương (c, a)	2.33 μs	4.84 μs	SQ
Lũy thừa (c, a, 3)	1.46 μs	16.80 μs	-

Hệ thống bị nứt với sự trợ giúp của thông tin kênh biên (như là năng lượng, thời gian, …) mà có thể được dùng để tính toán số lượng các phép cộng và

nhân đôi, điều đó được thực hiện bằng một phép nhân. Trong một vài trường hợp điều này có thể đã từng quen với việc tìm thấy các số nguyên bí mật mà các điểm được nhân.

Trong [JQ] mô tả đúp điểm và trừ điểm có thể được thực hiện như thế nào bởi việc đổi tọa độ, và sử dụng công thức cho cộng điểm. Kỹ thuật này được yêu cầu trong [JQ] thì nhanh hơn ít nhất 33% so với các phương pháp khác đối với việc bảo vệ chống lại tác động kênh biên.

Cho điểm $P=(x,y,z)$ là một điểm trên đường cong Hesse, thì $[2]P$ có thể được tính toán bởi việc cộng các điểm (z,x,y)và (y,z,x) với phương trình 4, xem [JQ] trang 6.

Chúng ta không sử dụng phương pháp này trong các phép thử của chúng ta.

2.2.4. Cách cài đặt các thí nghiệm

Tất cả các kết quả trong phần này là trung bình của 100 phép thử (các điểm được chọn một cách ngẫu nhiên).

Chúng ta đo thời gian thực hiện các phép toán trên các phần tử của trường hữu hạn từ LiDIA, các kết quả từ các phép thử này được thể hiện trong Bảng 1. Điều này là nền móng cho việc xem xét khoảng thời gian tiêu tốn của các công thức cho phép toán cộng và nhân đôi (phép đúp điểm).

Phép thử của các phép toán trên trường cơ bản được thực hiện trên cùng một trường hữu hạn như các phép toán điểm, vì thế các kết quả từ các phép thử khác nhau là so sánh được.

Các phép thử được thực hiện trên hai trường hữu hạn khác nhau $\mathbb{F}_p$ trong đó p là một số nguyên tố p_{160} có độ dài 160bit, và số nguyên tố khác p_{240} có độ dài 240bit, đây là kích thước thực tế trong việc sử dụng lý thuyết mật mã.

Bảng 2: Các phép toán cơ bản trong phép cộng và nhân đôi trên đường cong elliptic qua một trường hữu hạn (Viết gọn như trong Bảng 1).

Op.		Các phép toán cơ bản
Add.	Afin LiDIA	2 . M + SQ + I +6 . SU
	Xạ ảnh LiDIA	12 . M + 4 . SQ + A + 7 . SU + 2 . M2 +I2
	Weierstrass	12 . M + 4 . SQ + 2 . A + 5 . SU + 6 . M2
	Hesse	12 . M + 3 .SU
Add. mix.	Xạ ảnh LiDIA	8 . M + 3 . SQ + A + 7 . SU + M2 + I2
	Weierstrass	8 . M + 3 . SQ + A + 5 . SU + 7 . M2
	Hesse	10 . M + 3 . SU
Dbl.	Afin LiDIA	3 . M + 2 . SQ + I + A + 3 . SU + 2 . M2
	Xạ ảnh LiDIA	4 . M + 6 . SQ + 4 . A + 3 . SU + 6 . M2
	Weierstrass	4 . M + 6 . SQ + 4 . A + 3 . SU + 6 . M2
	Hesse	6 . M + 3 . SQ + 3 . SU

Chúng ta đã tìm được hai đường cong mà chúng ta đã sử dụng trong các phép thử. Đường cong đầu tiên được định rõ bởi các số liệu sau:

P_{160}=1224753567915253525600877180059052116597297173971

D=155084242162794225825732878535100753203309402 42

a=180890127234310861440619063553097796467445303876

b=6387231065610304706782316703719324216503513898 55

Dạng Hesse được cho bởi dạng D,và đường cong Weierstrass tương ứng được cho bởi a và b.

Đường cong thứ hai thì được cho một cách tương tự bởi:

p_{240}=16920716211102866991413418964116700961959871317136245022362607751814061 03

D=70249723857389687569279996011413629722731041382076985034755825112097874 9

a=43164347410179053180950770507349714338925522818022387686039349453284925 0

b=9938907497500547973745707026183472285859717797758236024775615986918871 83

- Cấp (số lượng các điểm) của đường cong là:

#E(K)=3.4082511893050845085336258395399575189669561010 71 và #E(K)=3.5640238737034288997137806321372233658182706401750080706837978319881127 11 tương ứng.

Đối với cả hai đường cong, cấp #E(K) là một số nguyên tố được nhân với 3. Chú ý rằng cấp của một đường cong Hesse thì luôn được chia hết bởi 3 (là ước của 3).

Bảng 2 chỉ ra số lượng phép toán của trường cơ bản đã sử dụng trong các phép toán điểm. Afin LiDIA và xạ ảnh LiDIA, hướng theo sự thiết lập được cung cấp bởi LiDIA. Weierstrass và Hesse hướng tới sự cài đặt của chúng ta.

Xạ ảnh LiDIA và Weierstrass đều là sự cài đặt các phép toán điểm sử dụng tọa độ xạ ảnh Jacobi, nhưng chúng ta đã thực hiện một vài sự cải tiến.

Nếu z-tọa độ của một trong các điểm bằng 1, thì công thức đối với phép cộng có thể đã được đơn giản, điều này được gọi là các tọa độ trộn. Nếu điểm được nhân đã được biết trước, thì tất cả các sự nhân đôi có thể đã được tính toán trước, và kết quả là các điểm được tính toán trước có thể đã được chuẩn hóa với $z = 1$. Chúng ta đã thực hiện điều này, và tham khảo nó như là add.mix. trong các bảng 2 và 3.

Bảng 3 cho ta một sự khác biệt lớn giữa thời gian tiêu chuẩn và thời gian ước lượng đối với các phép toán điểm của LiDIA. Ta nghĩ rằng có ba lí do chính cho điều đó; các phép toán của LiDIA bao gồm các sự mô tả các biến số địa phương trong các hàm thao tác điểm, nhiều phép thử hơn được thực hiện, và người ta sử dụng hàm các con trỏ để làm các hàm tổng quát hơn.

Bảng 3: Định thời cho phép cộng và nhân đôi điểm trên đường cong elliptic qua trường hữu hạn với các đặc số p_{160} và p_{240} .

Op.		160bit		240bit	
		Đo được	Ước lượng	Đo được	Ước lượng
Add.	Afin LiDIA	83.91 μs	43.5 μs	114.37 μs	72.54 μs
	Xạ ảnh LiDIA	91.88 μs	68.4 μs	143.02 μs	118.2 μs
	Weierstrass	52.32 μs	46.1 μs	98.71 μs	92.05 μs
	Hesse	36.31 μs	32.16 μs	72.27 μs	67.53 μs
Add. mix.	Xạ ảnh LiDIA	79.07 μs	55.32 μs	116.24 μs	91.46 μs
	Weierstrass	38.55 μs	33.50 μs	70.78 μs	64.18 μs
	Hesse	31.58 μs	27.02 μs	61.58 μs	56.53 μs
Dbl.	Afin LiDIA	73.36 μs	48.48 μs	105.31 μs	82.90 μs
	Xạ ảnh LiDIA	5.26 μs	30.24 μs	83.34 μs	57.73 μs
	Weierstrass	37.18 μs	30.24 μs	65.08 μs	57.73 μs
	Hesse	26.1 μs	23.73 μs	51.75 μs	47.97 μs

Phép nhân điểm: Phép nhân điểm có thể được thực hiện bởi các phép nhân đôi được lặp lại và phép cộng, một phép nhân đôi là cần thiết cho mỗi bit trong biểu diễn số điểm được nhân. Nếu sử dụng phép trừ trong phép cộng để nhân đôi và cộng, thì phép nhân có tốc độ nhanh, bằng cách sử dụng cái gọi là sự biểu diễn SD2 (Signed Digit base 2). Trong biểu diễn SD2, số được nhân thì được biểu diễn bởi{-1, 0, 1} thay thế cho chỉ 0 và 1, sao cho số chữ số 0 là ít nhất. Điều này dẫn đến một số rút gọn của các phép cộng. SD2 là thuật toán được sử dụng trong sự thiết lập điểm nhân của chúng ta.

Bảng 4. Thời lượng đối với phép nhân điểm trên đường cong elliptic trên trường hữu hạn với các đặc tuyến p_{160} và p_{240}.

	160bit		240bit	
Phép nhân	Đo được	Ước lượng	Đo được	Ước lượng
Affin LiDIA	16.35ms	16.14ms	34.81ms	34.32ms
Jacobi LiDIA	14.58ms	13.69ms	32.14ms	31.44ms
Jacobi Weierstrass	8.91ms	8.70ms	23.72ms	23.40ms
Hesse	6.24ms	6.09ms	18.39ms	18.17ms

Phép toán quan trọng trong suốt sự mã hóa và sự giải mã là phép nhân điểm, $[k]P$. Trong phép tính này, k là một giá trị ngẫu nhiên có kích thước giống nhau như là bậc của đường cong. Trong các phép thử, chúng ta chọn k là giá trị ngẫu nhiên giữa 0 và số các điểm trên đường cong. Các kết quả được cho trong Bảng 4.

Trong các sự thiết lập của chúng ta, hai dạng chứng tỏ rằng dạng Hesse nhanh hơn 30% so với dạng Weierstrass ngắn đối với 160bit và nhanh hơn 20% đối với 240bit. Chúng ta tin rằng các kết quả đó chỉ ra một cách rõ ràng rằng các hệ thống mật mã sử dụng đường cong Hesse sẽ thực hiện tốt hơn các hệ thống sử dụng đường cong Weierstrass.

Lí do chính để giảm sự khác nhau giữa thời gian thực hiện 240bit và 160bit, đó là thời gian thực hiện đối với phép nhân của các phần tử trong một trường hữu hạn tăng nhanh hơn nhiều so với các phép toán cơ bản khác. Do đó sự khác nhau của số các phép nhân trở thành quan trọng nhất trong kết quả.

Chú ý rằng trong tất cả các ước lượng, chúng ta tính toán tất cả các phép toán trường cơ sở, và không chỉ là phép nhân (phép bình phương) như thường thấy trong bài thuyết trình. Đối với 160bit, một sự ước lượng chỉ dựa trên đếm các phép nhân (và bình phương) (Bảng 2) thực tế dự đoán một hiệu

suất nhỏ hơn tăng thêm khoảng 15%, so với các kết quả và các ước lượng khoảng 30%.

2.2.5. Kết luận

Các thí nghiệm của chúng ta chứng tỏ rằng hệ thống mật mã sử dụng đường cong Hesse thực hiện tốt hơn hệ thống sử dụng đường cong Weierstrass. Hơn thế nữa, hiệu suất tăng thêm thì lớn hơn cái mà chúng ta kỳ vọng từ việc đếm các phép nhân trên trường như thường thấy trong các bài thuyết trình, bởi vì các công thức đối với các phép toán điểm trong dạng Hesse thì đơn giản hơn dạng Weierstrass.

Dựa trên điều này, chúng ta kết luận rằng các hệ thống mật mã đường cong elliptic sử dụng dạng Hesse nên được xem xét sử dụng nhiều hơn, đặc biệt trong các thiết bị tính toán ràng buộc như là thẻ thông minh.

Cuối cùng chúng ta tin rằng với các kết quả trên chứng tỏ rằng dạng Hesse có thể thiết lập mật mã đường cong elliptic hay hơn thậm chí có khả năng thay thế RSA để ứng dụng trong thực tiễn.

III. KẾT LUẬN

Trong luận văn đã đưa ra các kết luận về:

- Phương pháp xây dựng thuật toán xác định luật nhóm trên đường cong elliptic dạng Hesse.
- Tính đối xứng của các đường cong dạng Hesse, j-bất biến của các đường cong dạng này.
- Tính toán các điểm n-xoắn trên một số họ đường cong dạng Hesse.
- Tương đương tuyến tính giữa đường cong elliptic dạng Weierstrass và đường cong elliptic dạng Hesse.
- Thực hiện hệ thống mã hóa đường cong elliptic bằng cách sử dụng đường cong Hesse trên các trường số nguyên tố.
- Một số thí nghiệm chứng tỏ rằng hệ thống mật mã sử dụng đường cong Hesse thực hiện hiệu quả hơn hệ thống sử dụng đường cong Weierstrass.

Chứng minh một số Định lý mô tả tính chất của các đường cong dạng Hesse thuộc về các chủ đề đã nêu trong phần mở đầu của Đề cương Luận văn.

BẢNG THUẬT NGỮ

Trang

A

B

C

D , Đ

G

H

I

J

K

L

M

N

P

Q

S

T

V

X

Xạ ảnh LiDIA	70
Xạ ảnh không kì dị	33

TÀI LIỆU THAM KHẢO

[BSS] Blake, Seroussi, and Smart, *Elliptic Curves in Cryptography*. Cambridge university press, 1999.

[CEP] E. R. Canfield, P. Erdos, and C. Pomerance, On a problem of Oppenheim concerning "factorisatio numerorum", J. Number Theory 17 (1983), no. 1, 1-28.

[CPQ] M. Ciet, G. Piret and J. –J Quisquater, *Several optimizations for elliptic curve implementation on smart card.* Universite Catholique de Louvain, Technical report CG-2001/1

[Elk] N. D. Elkies, Heegner point computations, Algorithmic number theory (Ithaca, NY, 1994), 122-133, Lecture Notes in Comput. Sci. 877, Spinger, Berlin, 1994.

[FIPS] FIPS 186-2, *Digital signature standard* (DSS), National Institute of Standards and Technology, USA, 2000.

[Fri] Frium H. R. *The Group Law on Elliptic Curvers on Hesse form.* Proc. of the Sixth Int. Conf. on Finite Fields and Applications. Mehico (2001).

[Ful1] Fulton W. *Algebraic Curves., An Introduction to Algebraic Geometry*. Mathematic Lecture Notes Series. (1974).

[Ful2] W. Fulton, Algebraic curves. An introduction to algebraic geometry. Notes written with the collabora-tion of Richard Weiss. Reprint of 1969 original. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[Har] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Tests in Mathematics*. Spinger-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[HU] J. E. Hopecroft and J. D. Ullman, Formal languages and their relation to automata. Addition-Wesley Publishing Co., Reading, Mass.-London-Don Mills,.Ont. 1969.

[HWCD] H. Hisil, K. Wong, G. Carter, E. Dawson, *Faster group operations on elliptic curves.* International Association for Crytologic Research, Cryptology ePrint Archive, 2007/441.

[IEEE] *IEEE 1363-2000: Standard Specifications for Public Key Cryptography.*

[JQ] M. Joye and J. –J Quisquater, *Hessian elliptic curves and side channel attacks,* Proceedings of CGES 2001, LNCS, v.2162, springer-Verlag, 2001, pp. 402-410.

[Kob] N. Koblitz, *p-adic* numbers, *p-adic* analysis, and zeta-funtions. Second edition. Graduate Texts in Mathematics 58, Springer-Verlag, New York-Berlin, 1984.

[Lin] C.-E. Lind Untersuchungen uber die rationalen Punkte der ebenen kubischen Kurven vom geschlecht Eins, Thesis, University of Uppsala, 1940.

[MM] R. Martin and W. McMillen, An elliptic curve over Q with rank at least 24, Janury 2000, electronic announcement on the NMBRTHRY list server (posted May 2, 2000),

[Mo1] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Cambrige Phil. Soc. 21 (1922), 179-192.

[Mo2] L. J. Mordell, On the magnitude of the integer solutions of the equation $ax^2 + by^2 + cz^2 = 0$ J. Number Theory 1 (1969),1-3.

[MOC] A. Miyaji, T. Ono, and II. Cohen, "Efficient elliptic curve exponentiaion," in *Ad-vances in Cryptology-Proceedings of ICICS'97.* Springer-Verlag LNCS1334, 1997, pp. 282-290.

[Po1] B. Poonen Computational aspects of curves of genus at least 2, pp. 283-306 in: Cohen, H. (ed.), Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings, Lecture Notes in Computer Science 1122, Springer-Verlag, Berlin.

[Po2] B. Poonen, Computing rational points on cuvers, to appear in the Proceedings of the Millennial Conference on Number Theory, May 21-26, 2000, held at the University of Illinois at Urbana_Champaign.

[Rei] H. Reichardt, Einige im Kleinen uberall losbare, im Grossen unlosbare diophantische Gleichungen, J. Reine Angew. Math. 184 (1942), 12-18.

[Ros] M. Rosing, *Implementing Elliptic Curve Cryptography*. Manning, 1990.

[Sch] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44 (1945), no. 170, 483-494.

[Sel] E. Selmer, The diophantine equation $ax^3+by^3+cz^3=0$, Acta Math. 85 (1951), 203-362 and 92 (1954), 191-197.

[Ser1] J. P. Serre, A course in arithmetic. Translated from the French. Graduate Texts in Mathematics 7, Springer-Verlag, New York-Heidelberg, 1973.

[Ser2] J. P. Serre, Lectures on the Mordell-Weil theorem. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Aspects of Mathematics, E15 Friedr. Vieweg & Sohn, Braunschweig, 1989.

[Sha1] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles reid.

[Sha2] I. R. Shafarevich, Basic algebraic geometry. 1. Varieties in projective space. Second edition. Translated from the 1988 Russian edition and with notes by Miles Reid. Springer-Verlag, Berlin 1994.

[Sha3] I.R. Shafarevich, Basic algebraic geometry. 2. Schemes and complex manifolds. Second edition. Translated from the 1988 Russian edition by Miles Reid. Sptinger-Verlag, Berlin, 1994.

[Sil1] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106, Springer-Verlag, New York-Berlin, 1986.

[Sil2] J. Silverman, *Advanses topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, New York, 1994.

[Sil3] Silverman J. H. and . Tate J. *Rational Points on Elliptic Curves.* Springer (1992).

[Sma] N. P. Smart, "The Hessian form of an elliptic curve," in CHES 2001, Koc, Nacache, and Paar, Eds. Springer-Verlag LNCS 2162, May 2001,pp. 118-125.

[ST] J. H Silverman and J. Tate, Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.