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

TRẦN THẾ PHỤC

CÁC ĐIỂM HỮU TỶ TRÊN CÁC ĐƯỜNG CONG ELLIPTIC TRÊN TRƯỜNG HỮU TỶ

Chuyên ngành : Hình học Tôpô
Mã số : 60.46.10

Người hướng dẫn khoa học :
TS. PHAN DÂN

Thành phố Hồ Chí Minh – 2010

LỜI CÁM 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 giúp đỡ tạo điều kiện cho tôi tiếp xúc với các nguồn tài liệu quý, tài liệu nước ngoài , giảng giải và chỉ bảo tận tình cho tôi trong suốt quá trình làm luận văn . Hơn nữa thầy đã dành nhiều công sức , thời gian để đọc và chỉnh sửa luận văn .

Tôi xin chân thành cám ơn Quý Thầy Cô khoa Toán – Tin trường Đại Học Sư Phạm Tp Hồ Chí Minh , đặc biệt là Quý Thầy tổ Hình học đã cung cấp những kiến thức chuyên môn cần thiết cho tôi để làm nền tảng cho việc hoàn thành luận văn này

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 PTTH Phú Nhuận 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.

Tôi xin chân thành cám ơn

Tp.Hồ Chí Minh, tháng 07 năm 2010

Tác giả

Trần Thế Phục

LỜI GIỚI THIỆU

1 - MỞ ĐẦU

1.1 Lý do chọn đề tài

Một trong những vấn đề thời sự của Toán học trong suốt ba thế kỷ qua là việc nghiên cứu tìm lời giải cho Bài toán Fermat (còn được gọi là Định lý lớn Fermat hay Định lý Fermat-Wiles). Đây là một bài toán thuộc về lĩnh vực Lý thuyết số nhưng đã thu hút được sự quan tâm nghiên cứu của rất nhiều nhà khoa học. Điều thú vị nhất là trong quá trình tìm kiếm lời giải cho giả thuyết Fermat, người ta đã phải sử dụng tới rất nhiều kiến thức và kỹ thuật cũng như phương pháp nghiên cứu của rất nhiều ngành khác nhau như Lý thuyết số, Đại số giao hoán, Giải tích, Hình học, Lý thuyết Galois, …, và đặc biệt trong số đó có sự đóng góp rất quan trọng của ngành Hình học Đại số. Lý thuyết về các đa tạp, các đường cong đại số và các điểm hữu tỷ trên chúng, các hàm elliptic, các dạng modular, … là các khái niệm rất quan trọng và các kết quả nghiên cứu liên quan là những tiệm cận của lời giải định lý Fermat. Chúng tôi lựa chọn đề tài này thuộc lĩnh vực Hình học Đại số với ý tưởng tìm hiểu và giới thiệu một số kiến thức chuyên môn về "Lý thuyết về các đường cong Elliptic" cùng với việc xét tính chất của một số họ đường cong trên trường số hữu tỷ và mô tả sự phân bố của nhóm các điểm hữu tỷ trên chúng.

Trong phạm vi đề tài , chúng tôi sẽ xét các đường cong Elliptic trên trường các số hữu tỷ được mô tả dưới dạng Weierstrass.

Vì vậy, Luận văn được đặt tên là :

"Các điểm hữu tỷ trên các đường cong elliptic trên trường hữu tỷ"

1.2 Lịch sử của vấn đề

Cơ sở lý thuyết và công cụ nghiên cứu cũng như phương pháp giải quyết vấn đề trong Luận văn dựa trên một số kết quả sau đây:

a) Một là kết quả rất thú vị về tính chất tách trực tiếp của các nhóm aben hữu hạn sinh (các Z-mođun hữu hạn sinh) thành phần xoắn và không có xoắn, và cuối cùng là sự tách trực tiếp thành tổng các hạng tử không thể tách được mà mỗi một trong chúng là nhóm cyclic.

b) Định lý Nagell-Lutz về sự mô tả các điểm hữu tỷ, Định lý Mordell-Weil khẳng định rằng tập các điểm hữu tỷ trên một đường cong elliptic là một nhóm abel hữu hạn sinh và Định lý Mazur mô tả tập các điểm có cấp hữu hạn trong tập các điểm hữu tỷ.

c) Các kết quả và phương pháp mô tả luật nhóm trên nhóm các điểm hữu tỷ trên các đường cong Elliptic.

Luận văn của chúng tôi tập trung giải quyết một số vấn đề về: xác định nhóm các điểm hữu tỷ trên một số họ đường cong trên Q được cho dưới dạng Weierstrass: $y^2 = x^3 + Ax + B$, với $A, B \in Z$. Một số kết quả nghiên cứu thuộc hướng này đã và đang được tiếp tục phát triển trong thời gian gần đây bởi nhiều tác giả.

1.3 Đối tượng và phạm vi nghiên cứu

- Nghiên cứu cấu trúc của nhóm các điểm hữu tỷ trên một số họ đường cong elliptic dưới dạng Weierstrass trên trường các số hữu tỷ.
- Xét một số họ các đường cong với mục đích là mô tả nhóm các điểm hữu tỷ dựa theo luật nhóm xác định trên chúng.
- Phân loại nhóm con xoắn của các điểm hữu tỷ trên một số họ đường cong (các điểm cấp 2, cấp 3 ..)
- Đề tài chỉ giới hạn trong phạm vi xét các đường cong Elliptic E không kỳ dị trên Q với ý tưởng là mô tả cấu trúc nhóm của tập các điểm hữu tỷ E(Q).

1.4 Mục đích nghiên cứu

- Mô tả cấu trúc nhóm của tập các điểm hữu tỷ E(Q) của đường cong Elliptic không kỳ dị E trên Q.
- Mô tả các điểm xoắn trên một số lớp đường cong Elliptic
- Mô tả thuật toán xác định các điểm xoắn hữu tỷ trên đường cong elliptic

1.5 Phương pháp nghiên cứu.

Sử dụng các phương pháp, công cụ của Đại số và Lý thuyết số để giải quyết bài toán mô tả cấu trúc của các nhóm abel hữu hạn sinh. Kết hợp các kết quả này với các Định lý Nagell-Lutz (mô tả các điểm hữu tỷ) và Định lý Mazur (mô tả các điểm có cấp hữu hạn) để xác định các điểm xoắn trên một số họ đường cong được xét. Cuối cùng, tập các điểm hữu tỷ trong những trường hợp cụ thể có thể xác định nhờ Định lý Mordell -Weil. Đây là một số hướng nghiên cứu và các phương pháp được dùng khá phổ biến trong việc xét các đường

cong elliptic. Các hướng nghiên cứu này đã và đang được sử dụng và phát triển bởi nhiều tác giả trong nhiều năm gần đây. Các phương pháp nghiên cứu và các kỹ thuật cũng như các thuật toán được dùng trong Luận văn này dựa trên những công cụ nghiên cứu đã được sử dụng trong [Ful 74] ,[Har 77] , [Was 03]

2 - NỘI DUNG

2 .1 **Luận văn bao gồm 2 chương**

Chương 1: **Kiến thức cơ bản**.

Chương này trình bày một số khái niệm và các kết quả nghiên cứu đã được công bố trong nhiều tài liệu về các chuyên ngành Toán:

- Các định lý cơ bản về sự tách trực tiếp các nhóm aben hữu hạn sinh.
- Một số kết quả quen biết về lĩnh vực Lý thuyết số.
- Các đa tạp xạ ảnh, afin.
- Một số kiến thức cơ bản và kỹ thuật, thuật toán liên quan thuộc về Hình học Đại số, trích dẫn từ [Fri 01] , [Mil 06] , [Sil 86] , [Sil 92] ,[Was 30]
- Các khái niệm, các kết quả nghiên cứu về đường cong elliptic. Các đường cong trên trường số hữu tỷ. Các định lý cơ bản mô tả về cấu trúc của nhóm các điểm hữu tỷ trên các đường cong elliptic.

Chương 2: **Các đường cong Elliptic dạng Weierstrass trên Q.**

- Tổng quan về các đường cong dạng Weirstrass trên Q.
- Các điểm hữu tỷ trên đường cong Elliptic trên Q .

Nhóm Mordell – Weil

- Mối liên hệ giữa đường cong elliptic với phép nhân tử hóa
- Điểm xoắn hữu tỷ trên đường cong elliptic
- Mô tả thuật toán xác định điểm xoắn hữu tỷ trên đường cong Elliptic

BẢNG CÁC KÝ HIỆU

$T(A)$	Nhóm con xoắn của nhóm abel A
$A \oplus B$	Tổng trực tiếp của A và B
$\overline{K}$	Bao đóng đại số của K
$X(K)$	Tập hợp các điểm K- hữu tỷ trên đường cong X
$X(\mathbb{Q})$	Tập hợp các điểm hữu tỷ của đường cong X xác định trên $\mathbb{Q}$
$\mathbb{P}^2$	Mặt phẳng xạ ảnh
$E(k)$	Đường cong E xác định trên trường k , với $k \in \left\{\mathbb{Q}, \mathbb{R}, \mathbb{C}, F_q\right\}$
$C(\mathbb{Q})_{tors}$	Tập hợp các điểm hữu tỷ xoắn của đường cong C xác định trên $\mathbb{Q}$
$h(P)$	Hàm chiều cao của P
$\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus ..... \oplus \mathbb{Z}}_{n \text{ lân}}$	Nhóm abel tự do hạng n , không xoắn
$k\left[x_1, ...x_n\right]$	Vành đa thức trên trường k với n biến
$\mathbb{A}^n$	Không gian affine n chiều trên trường k
$k[X]$	Vành tọa độ của X
$\mathcal{O}(X)$	Vành các hàm chính quy trên X
$\sqrt{I}$	Căn của ideal I
$k(X)$	Trường các hàm hữu tỷ trên X
$Div\left(X_{\overline{k}}\right)$	Nhóm các k – số chia là tập hợp của những tổng tự nhiên của các điểm trên $X\left(\overline{k}\right)$
$Div^0\left(X_{\overline{k}}\right)$	Nhóm của những $\overline{k}$ - số chia có bậc 0
$Pic(X)$	Nhóm Picard hay nhóm lớp các số chia của X
$Spec0_F$	Vành của những số nguyên của F
O	Điểm tại vô cực

$\Delta(f_m)$	Biệt thức của f_m của m - đa thức chia
Δ	Biệt thức của đường cong elliptic

BẢNG CHÚ GIẢI THUẬT NGỮ KHOA HỌC

Thuật ngữ	Trang
Nhóm abel	7
Nhóm con xoắn	7
Không gian affine $\mathbb{A}^n$	10
Đa tạp đại số affine	10
Đa tạp bất khả quy	10
Vành Noether	11
Không gian xạ ảnh n-chiều $\mathbb{P}^n$ (hoặc $\mathbb{P}^n(k)$) trên k	13
Đa tạp đại số xạ ảnh	13
Vành tọa độ (affine)	15
Hàm số chính quy	15
Ánh xạ chính quy	16
Đa tạp tựa xạ ảnh	18
Đa tạp không khả quy	18
Hàm hữu tỷ chính quy	18
Ánh xạ đẳng cấu	18
Ánh xạ hữu tỷ	19
Đa tạp hữu tỷ	19
Điểm kỳ dị	24
Đường cong elliptic	40
Luật nhóm	42
Đường cong phẳng	19
Điểm K - hữu tỷ	19
Ideal thuần nhất	13
Hàm chiều cao	31
Định lý Nagell – Lutz về điểm hữu tỷ trên đường cong	39

Chương 1
CÁC KIẾN THỨC CHUẨN BỊ

1.1 CÁC NHÓM ABEL HỮU HẠN SINH.

Định nghĩa 1 : Một nhóm abel A được gọi là hữu hạn sinh nếu tồn tại hữu hạn phần tử $a_1, a_2, ..., a_n \in A$ sao cho với bất kỳ $x \in A$, tồn tại các số nguyên

$k_1, k_2, \ldots, k_n$ thỏa $x = \sum_{i=1}^{n} k_i a_i$.

Định nghĩa 2: Cho A là một nhóm abel. Nhóm con xoắn của A, ký hiệu T(A), là tập: $T(A) = \{a \in A \mid \exists n \in N \text{ sao cho } na = 0\}$.

Định nghĩa 3: Một nhóm abel A được gọi là không có xoắn nếu
$T(A) = \{0\}$.

Bổ đề 4: Cho A là một nhóm abel. Khi đó A/T(A) là không có xoắn.

Định nghĩa 5: $\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus ..... \oplus \mathbb{Z}}_{n \text{ lần}}$ được gọi là nhóm abel tự do hạng n.

Định lý 6 : Nếu A là một nhóm abel không có xoắn hữu hạn sinh mà có một tập hợp nhỏ nhất các phần tử sinh gồm n phần tử, thì A đẳng cấu với nhóm abel tự do hạng n.

Chứng minh: Áp dụng phương pháp quy nạp trên số phần tử sinh nhỏ nhất của A. Nếu A là cyclic (nghĩa là được sinh bởi một phần tử khác 0), khi đó $A \cong \mathbb{Z}$. Giả sử rằng kết quả trên đúng với tất cả các nhóm abel không có hữu hạn sinh với một tập hợp các phần tử sinh nhỏ nhất có số phần tử ít hơn n phần tử. Giả sử rằng A là không có xoắn và giả sử rằng $\{a_1, a_2, ..., a_n\}$ là một tập nhỏ nhất các phần tử sinh của A. Nếu $T(A/<a_1>)=\{0\}$ khi đó $A/<a_1>$ là không có xoắn và được sinh bởi n -1 phần tử nên $<a_1> \cong \mathbb{Z}$. 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 ta lại có $ib = ja_1$ với số nguyên $j \in \mathbb{Z}$. Khi đó , ta định nghĩa một ánh xạ :

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

Ánh xạ này là một phép đồng cấu được xác định trên các nhóm abel. Ánh xạ này có hạt nhân tầm thường, và do dó là một đơn ánh nên $B \cong f(B)$. Bây giờ, nếu B được sinh hữu hạn (vì $\mathbb{Z}$ là một vành Noether) thì B là cyclic.

Để thấy điều này giả sử $B = <b_1, \ldots, b_m>$. 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. Nếu không, khi đó:

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

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

Do đó, A/B là không có xoắn và được sinh bởi nhiều nhất n – 1 phần tử, do đó A/B là nhóm abel tự do có hạng m < n do quy nạp . Điều đó dẫn đến $A \cong B \oplus \mathbb{Z}^m$ và $B \cong A/\mathbb{Z}^m$ và là hữu hạn sinh. Khi đó , B là cyclic nên ta có điều phải chứng minh.Chú ý rằng m = n – 1 vì n là cực tiểu.

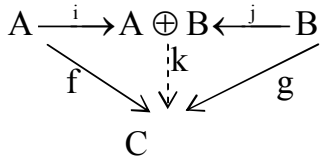
Định nghĩa 7: Cho A là một nhóm abel, và cho B và C là các nhóm con của A. Ta nói rằng A là tổng trực tiếp trong của B và C, ký hiệu $A = B \oplus C$, nếu
$A = B + C$ và $B \cap C = \{0\}$, ở đây $B + C = \{ b + c \mid b \in B \text{ và } c \in C\}$.

Định nghĩa 8*:* Cho $\mathfrak{P}$ là một phạm trù và cho X và Y là các vật của $\mathfrak{P}$. Một cấu xạ $f : X \to Y$ được gọi là đơn xạ khi với bất kỳ vật Z của $\mathfrak{P}$ và bất kỳ cặp cấu xạ: $i, j : Z \to X$, nếu $f \circ i = f \circ j$ thì i = j.

Định nghĩa 9: Cho $\mathfrak{P}$ là một phạm trù và cho X và Y là các vật của $\mathfrak{P}$. Một cấu xạ $f : X \to Y$ được gọi là toàn xạ khi với bất kỳ vật Z của $\mathfrak{P}$ và bất kỳ cặp cấu xạ: $i, j : Y \to Z$, nếu $i \circ f = j \circ f$ thì i = j.

Định nghĩa 10: Cho A và B là các nhóm abel. Tổng trực tiếp ngoài của A và B trong phạm trù của các nhóm abel, ký hiệu $A \oplus B$ là một nhóm abel $A \oplus B$ với các phép đồng

cấu chính tắc $i : A \to A \oplus B$ và $j : B \to A \oplus B$ với tính chất rằng cho bất kỳ nhóm abel C và các cấu xạ $f : A \to C$ và $g : B \to C$, có một ánh xạ duy nhất $k : A \oplus B \to C$ làm cho biểu đồ sau giao hoán:



Suy ra i, j là các phép đơn cấu .

Như vậy : Định nghĩa 10 là một ví dụ về đối tượng được biết đến khi định nghĩa bởi tính chất phổ dụng. Chú ý rằng, định nghĩa này có ý nghĩa trong phạm trù bất kỳ, nhưng do một vật không nhất thiết tồn tại trong mỗi phạm trù; vật phải đưa một cấu trúc và chứng minh rằng nó thỏa mãn tính chất phổ dụng.

Định lý 11*:* Cho A là một nhóm abel được sinh hữu hạn. 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 . Chọn $< \overline{x_1},...,\overline{x_m} >$ là một tập hợp tối thiểu các phần tử sinh cho A/T(A). Nếu $\bar{a} \in A/T(A)$ thì $\bar{a} = \sum_{i=1}^{m} k_i \overline{x_i}$ với các số nguyên $k_i \in \mathbb{Z}$, suy ra $a - \sum_{i=1}^{m} k_i x_i \in T(A)$. Do đó, $A = < x_1,...,x_m > + T(A)$.

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

<u>*Chú ý*</u> 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 đồng cấu đồng nhất của A/T(A) và τ là một đơn cấu

Hệ quả 12: Mỗi nhóm abel hữu hạn sinh là tổng trực tiếp của một nhóm hữu hạn và một nhóm abel tự do hạng n với số nguyên $n \in \mathbb{Z}$.

Chứng minh: Ta có T(A) là một nhóm hữu hạn. A/T(A) là hữu hạn sinh và không có xoắn, vì thế, do định lý 6, nó là một nhóm abel tự do hạng n với số nguyên $n \in \mathbb{Z}$.

1.2 CÁC ĐA TẠP XẠ ẢNH – ĐA TẠP AFFINE

1.2.1 Các khái niệm cơ bản

1.2.1.1 Các đa tạp affine

Chúng ta nghiên cứu trên trường k , và nếu không ghi chú gì thêm thì k là trường đóng đại số.

Định nghĩa 13: Không gian affine n-chiều $\mathbb{A}^n$ (hoặc $\mathbb{A}^n$ (k)) trên trường k là tập hợp các n – bộ của các phần tử của k. Một phần tử $p = (p_1, p_2, \ldots, p_n) \in \mathbb{A}^n$ được gọi là một điểm, các p_i là các tọa độ affine của p.

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

Định nghĩa 14: Một tập con $X \subseteq \mathbb{A}^n$ là một đa tạp đại số affine , nếu nó là một tập zero của một tập hữu hạn của các đa thức trong $k[x_1, \ldots, x_n]$. Cho $f_1, \ldots, f_k \in k[x_1, \ldots, x_n]$ thì: $X = Z(f_1, \ldots, f_k) = \{p \in A^n \mid f_i(p) = 0, \forall i\}$.

Định nghĩa 15: 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 đối với các đa tạp $X_1, X_2 \subseteq \mathbb{A}^n$ sao cho $X = X_1 \cup X_2$ dẫn đến $X = X_1$ hoặc $X = X_2$.

Mệnh đề 16: Bất kỳ đa tạp X có thể được phân tích như là hợp hữu hạn của các đa tạp con bất khả quy $X = X_1 \cup X_2 \cup \ldots X_m$ với $X_i \not\subseteq X_j$ với mọi $i \neq j$. Phép phân tích trên là duy nhất sai khác phép hoán vị

Ví dụ 1: Một đa tạp tuyến tính là 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:

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

Việc định nghĩa về số chiều của các đa tạp tuyến tính có thể được lấy 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 của đối chiều 1. Nếu n = 3, siêu diện 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.

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 đơn giản là $y - x^2 \in k[x;y]$

Ví dụ 4: Một cubic xoắn là một đường cong trong $\mathbb{A}^3$ được cho bởi tham số hóa $t \mapsto (t,t^2,t^3)$ hay 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 của hữu hạn các đa tạp affine là một đa tạp affine. Nếu $X,Y \subseteq \mathbb{A}^n$ với X = Z(f_1, …, f_k) và Y = Z(g_1, …, g_l), thì

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

Ví dụ 6: Cho $X \subseteq \mathbb{A}^n$ được xác định bởi $f_1, \ldots, f_k \in k[x_1,...,x_n]$ và $Y \subseteq \mathbb{A}^m$ cho bởi $g_1,...,g_l \in k[y_1,...,y_m]$. Khi đó tích của X và Y là một đa tạp trong $\mathbb{A}^{m+n}$ 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 $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

1.2.1.2 Định lý cơ bản của Hilbert

Chú ý rằng, nếu một đa tạp affine $X \subseteq \mathbb{A}^n$ được xác định bởi

X = Z(f_1, …, f_k), $f_i \in k[x_1,...,x_n]$, thì với mỗi f thuộc ideal I = (f_1, …, 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 ideal,
(f_1, …, f_k) = (g_1, …, g_l) thì ta luôn có Z(f_1, …, f_k) = Z(g_1, …, g_l). Do đó ta có thể thay đổi định nghĩa của một đa tạp affine bằng cách thay vì định nghĩa các phương trình định nghĩa

thì ta sẽ định nghĩa bằng các ideal định nghĩa : $X \subseteq \mathbb{A}^n$ là một đa tạp affine nếu nó là một tập zero của một ideal hữu hạn sinh trong $k[x_1, \ldots, x_n]$.

Ta xét R là một vành giao hoán (nó cũng có thể là một trường hoặc một vành đa thức trên một trường) , có đơn vị 1

Định nghĩa 17: Vành R là Noether nếu bất kỳ ideal của R có hữu hạn phần tử sinh

.

Định lý 18: (Định lý cơ bản của Hilbert) Nếu R là một vành Noether thì R[x] cũng là vành Noether .

Hệ quả 19 : Mọi ideal trong $k[x_1, \ldots, x_n]$ là hữu hạn sinh.

Từ định lý cơ bản Hilbert dẫn đến giao của các đa tạp đại số là một đa tạp, vì nó là một tập zero của một ideal được sinh bởi tất cả các phần tử sinh của các ideal 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 đây:

Định nghĩa 20: Trong tôpô Zariski , các tập mở là 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.

1.2.1.3 Hilbert's Nullstellensatz(Định lý về các không điểm của Hilbert)

Ví dụ 7: Ideal định nghĩa của một đa tạp là không duy nhất. Trong $k[x, y]$ ta xét:

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

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

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

Định nghĩa 21: Cho $I \subseteq k[x_1,...,x_n]$ là một ideal. Căn của I là:

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

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

Một số tính chất về căn của một ideal:

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

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

Từ VD7 trên ta có: $\sqrt{I_1} = \sqrt{I_2} = (x^2 - y^2)$.

Định nghĩa 22: Cho $X \subseteq \mathbb{A}^n$ là một tập bất kỳ. Ideal 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 23: Với mỗi $X \subseteq A^n$, $\mathcal{I}(X)$ là một ideal căn .

Định lý 24 (Định lý không điểm của Hilbert 1): Cho $\mathbb{A}^n$ là một không gian affine trên một trường k đóng đại số. Khi đó với bất kỳ ideal $I \in k[x_1,...,x_n]$ 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 A^n và tập của các ideal căn trong $k[x_1, ..., x_n]$

Định lý 25 (Định lý không điểm của Hilbert 2): Cho $\mathbb{A}^n$ là một không gian affine trên một trường k đóng đại số và cho I là một ideal trong $k[x_1, \ldots, x_n]$. Nếu $I \neq k[x_1, \ldots, x_n]$ thì Z(I) là khác rỗng.

Giả thiết k là đóng đại số là cốt yếu , như kết quả 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 ideal là ideal căn. $I_1 \neq I_2$, nhưng $Z(I_1) = Z(I_2)$.

Ta có mối liên quan 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	$\mathcal{I}(X) = I_1 \cap .... \cap I_m$ là một phép giao của các

thành các đa tạp con bất khả quy.	ideal nguyên tố, ở đây $I_i = \mathcal{I}(X_i)$

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

1.2.1.4 Các đa tạp xạ ảnh

Định nghĩa 26: Không gian xạ ảnh n-chiều $\mathbb{P}^n$ (hoặc $\mathbb{P}^n(k)$) trên k là tập hợp các lớp tương đương của (n + 1) - bộ của các phần tử của k, không bằng 0, với quan hệ tương đương $\sim$, ở đây $(a_0,...,a_n) \sim (b_1,...,b_n)$ nếu có một hằng số $\lambda \in k$ 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 P^n của một đa thức bất kỳ $f \in k[x_0,...,x_n]$ 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 27: Ideal $I \subseteq k[x_0,...,x_n]$ là thuần nhất, nếu nó được sinh ra bởi các đa thức thuần nhất.

Định nghĩa 28: Một tập con $X \subseteq \mathbb{P}^n$ là một đa tạp đại số xạ ảnh, nếu nó là một tập zero của một ideal thuần nhất trong $k[x_0,...,x_n]$.

Tổng tích và giao của các ideal thuần nhất lại là một ideal thuần nhất, cũng tương tự như căn của một ideal. Hơn thế nữa, nếu một ideal 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 affine, ta có tôpô Zariski trong trên P^n.

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

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

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

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

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

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

Định lý 29 (Định lý không điểm Hilbert 1) : Cho $\mathbb{P}^n$ là một không gian xạ ảnh trên trường đóng đại số k. Khi đó , tồn tại một song ánh từ: $X \to I(X)$, giữa tập hợp các đa tạp đại số trong P^n và tập hợp các ideal thuần nhất trong $k[x_0,...,x_n]$, ngoại trừ I_+.

Định lý 30 (Định lý không điểm Hilbert 2): Cho $\mathbb{P}^n$ là một không gian xạ ảnh trên trường đại số đóng k và I là một ideal thuần nhất trong $k[x_0,...,x_n]$. Nếu $Z(I) \subseteq P^n$ là tập rỗng thì tồn tại một giá trị $m \in N$ sao cho I chứa I_+^m

Ví dụ 10: Một đa tạp tuyến tính trong $\mathbb{P}^n$ với đối chiều k là tập zero của k dạng độc lập tuyến tính .

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 định nghĩa thì tập zero sẽ bao gồm cubic xoắn và một đường thẳng cắt cubic tại hai điểm , điều đó có thể tìm thấy trong [Har95]

Trong trường hợp siêu diện, ta có thể dễ dàng tìm được bao đóng xạ ảnh của đa tạp bằng cách ta thuần nhất phương trình định nghĩa: Nếu $X = Z(f) \subseteq A^n$, 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 12: Đường cong chuẩn tắc hữu tỉ bậc d, $C \subset P^d$ là tham số hóa cho bởi: $(s:t) \mapsto (s^d : s^{d-1}t : ... : t^d)$. Ta có thể mô tả nó bằng một tập hợp các phương trình bậc hai sao cho ma trận: $\begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{d-1} \\ x_1 & x_2 & x_3 & \cdots & x_d \end{pmatrix}$

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

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

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.

1.**2.2 Các hàm và các ánh xạ**

1.2.2.1 Các hàm chính quy trên các đa tạp affine.

Cho $X \subseteq A^n$ là một đa tạp affine trên trường đại số đóng k, cho $I(X)$ là ideal triệt tiêu của X.

Định nghĩa 31: Vành tọa độ (affine) của X là vành thương.

$$k[X] = k[x_1, ..., x_n] / I(X)$$

Mệnh đề 32: Một đại số giao hoán A trên trường k đẳng cấu với vành tọa độ $k[X]$ của một đa tạp X nào đó nếu và chỉ nếu A không có lũy linh và là hữu hạn sinh như một đại số trên k.

Định nghĩa 33: 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, ký hiệu là $O(X)$.

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

Ví dụ 14: Nếu $X = A^n$ thì $k[X] = k[x_1, ..., x_n]$, bởi vì $I(X) = 0$.

Ví dụ 15: Giả sử X là parabole , $\mathrm{X}=\mathrm{Z}\left(\mathrm{y}-\mathrm{x}^2\right)\subset A^2$, thế thì $\mathrm{k}[\mathrm{X}]=\mathrm{k}[\mathrm{x},\mathrm{y}]\Big/\left(\mathrm{y}-\mathrm{x}^2\right)\cong\mathrm{k}[\mathrm{x}]$. Do đó , ta có $k[X]\cong k\left[A^1\right]$.

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

Nếu π^{-1} 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 các đa tạp con của X như là các tập đóng (các tập zero của các iđêan trong $k[X]$).

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

Bổ đề 34: Các phát biểu sau là tương đương:

(i) $X\subseteq A^n$ 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 $U_1\cap U_2\neq\varnothing$.

1.2.2.2 Các ánh xạ chính quy của các đa tạp affine.

Định nghĩa 35: Một ánh xạ $\varphi: X\to Y$ là chính quy (một cấu xạ), nếu có m hàm chính quy $f_1,...,f_m\in O(X)$ sao cho $\varphi(x)=(f_1(x),...,f_m(x))$.

Định nghĩa 36: Ánh xạ chính quy $\phi: X\to Y$ là phép đẳng cấu, nếu nó có một chính quy nghịch đảo . 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: $\begin{array}{l}\varphi: A^1\to P\\ t\ \mapsto(t,t^2)\end{array}$ có ánh xạ ngược: $\begin{array}{l}\psi: P\to A^1\\ (x,y)\mapsto x\end{array}$

Rõ ràng, $\varphi\circ\psi$ là ánh xạ đồng nhất trên P và $\psi\circ\varphi$ là ánh xạ đồng nhất trên 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 một 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 đối 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 thành $f \circ \varphi$ được gọi là cái níu lại của φ và dễ thấy 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 37: Các đa tạp affine X và Y là đẳng cấu nếu và chỉ nếu $k[X]$ và $k[Y]$ là đẳng cấu như các k-đại số.

1.2.2.3 Các hàm hữu tỉ trên các đa tạp affine

Cho $X \subseteq A^n$ là một đa tạp bất khả quy. Vành tọa độ của nó $k[X]$ không có ước của 0 và do đó có thể được nhúng vào trường các thương mà ta ký hiệu là $k(X)$. Nói cách khác, $k(X)$ là tập các lớp tương đương $\left\{G/H \mid G,H \in k[x_1,..,x_n], H \notin I(X)\right\}|\sim$,trong đó , $G/H \sim G'/H'$ nếu $GH' - HG' \in I(X)$ và phép "+","." được định nghĩa theo nghĩa thông thường.

Định nghĩa 38: Trường $k(X)$ được gọi là trường các hàm hữu tỉ trên X hay là trường hàm của X.

Định nghĩa 39: Hàm $f \in k(X)$ 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 40: Nếu một hàm hữu tỉ $f \in k[X]$ là chính quy tại mọi điểm $x \in X$ thì nó chính quy .

1.2.2.4 Các ánh xạ hữu tỉ của các đa tạp affine.

Cho $X \subseteq A^n, Y \subseteq A^m$ là các đa tạp affine bất khả quy.

Định nghĩa 41: 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 42: 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 43: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 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: Một cubic lùi $C = Z(y^2 - x^3)$ là song hữu tỉ tới A^1:

ánh xạ $\begin{array}{l} \varphi: A^1 \to C \\ t \mapsto (t^2, t^3) \end{array}$ có ánh xạ ngược hữu tỉ $\begin{array}{l} \psi: C \to A^1 \\ (x,y) \mapsto \dfrac{y}{x} \end{array}$

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 duy nhất $k(Y)$. 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 $k(Y) \to k(X)$.

Định lý 44: Các đa tạp X và Y là song hữu tỉ nếu và chỉ nếu $k(X) \cong k(Y)$.

1.2.2.5 Các hàm trên các đa tạp tựa xạ ảnh.

Với mỗi đa tạp xạ ảnh $X \subseteq P^n$, vành tọa độ của X được xác định tương tự như trong trường hợp affine: $k[X] = k[x_0,...,x_n]/I(X)$,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 , $R_i R_j \subseteq R_{i+j}$.

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:

$R_0 = \langle 1 \rangle_k$,

$R_1 = \langle x_0, x_1, x_2 \rangle_k$,

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

Định nghĩa 45 : Một đa tạp tựa xạ ảnh $X \subseteq \mathbb{P}^n$ là một tập con mở của một đa tạp xạ ảnh

Định nghĩa 46 : 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

$$\left\{ g/h \middle| g,h \in R_d \text{ mà } d,\ h \neq 0 (\mathrm{mod} I(X)) \right\} \Big| \sim$$

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 47 : Một hàm hữu tỷ $f : X \to k$ là chính quy tại $x \in X$ nếu tồn tại một tập con mở $U \subseteq X$ chứa x và với $g,h \in k[X]$ thuần nhất cùng bậc sao cho h không bị triệt tiêu trên X 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 48 : Nếu $X \subseteq \mathbb{P}^n$ là đóng nghĩa là X là đa tạp xạ ảnh thì $\mathcal{O}(X) \cong k$

1.2.2.6 Ánh xạ trên 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 49: 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 $V \subseteq X$ và với mỗi hàm $f : V \to k$ chính quy trên V thì hàm số $f \circ \varphi : \varphi^{-1}(V) \to k$ cũng là 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 $U \subseteq X$ chứa x

+ $f_i(x) \neq 0$ đối với ít nhất một giá trị I .

Định nghĩa 50 : 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 $\mathbb{P}^2$ là một đẳng cấu với một 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 $\psi : C \to \mathbb{P}^1$ được xác định như sau :

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

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

Vì $C = \left(C \cap U_0\right) \cup \left(C \cap U_2\right)$, 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 $\left(x_0 : x_1\right) = \left(x_0x_1 : x_1^2\right) = \left(x_0x_1 : x_0x_2\right) = \left(x_1 : x_2\right)$

Lưu ý rằng vành tọa độ của một đa tạp xạ ảnh chứa nhiều thông tin hơn vành tọa độ affine tương ứng . Trong ví dụ trên , conic C là đẳng cấu với $\mathbb{P}^1$, tuy nhiên những vành tọa độ của chúng không đẳng cấu , vì khi $k[C]$ được sinh bởi 2 phần tử . Vành $k[X]$ không

những phụ thuộc vào lớp đẳng cấu của đa tạp mà còn phụ thuộc vào phép nhúng của X vào không gian xạ ảnh .

Định nghĩa 51 :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 . Hơn nữa ,ánh xạ đó còn là song hữu tỷ nếu nó có ánh xạ ngược hữu tỉ , khi đó X và Y được gọi là tương đương song hữu tỷ

Định nghĩa 52 :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 $\mathbb{P}^d$.

Định lý 53 : Các đa tạp X và Y là song hữu tỷ khi và chỉ khi $k(X) \cong k(Y)$

Định lý 54 : Mọi đa tạp đại số đều là song hữu tỷ với một siêu diện trong $\mathbb{P}^m$, với một $m \in \mathbb{N}$

Chứng minh : Vì k(X) là mở rộng hữu hạn sinh của một trường đóng đại số , do đó $k(X) = k\left(y_1,.....,y_{m-1}\right)\left(y_m\right)$ với $y_1,...y_m$ là độc lập siêu việt trên k và y_m là đại số trên $k(y_1,....,y_{m-1})$ . . Gọi $p' \in k\left(y_1,.....,y_{m-1}\right)[x]$ là đa thức nhỏ tối thiểu của y_m .Bằng các phép biến đổi đa thức , ta xác định được một phần tử $p \in k\left[y_1,.....,y_{m-1},x\right]$. Khi đó , X là song hữu tỷ với bao đóng xạ ảnh của $Z(p)$ mà đây là một siêu mặt trong $\mathbb{P}^m$.

1.2.2.7 Một vài ví dụ

Ví dụ 20 : Chúng ta hay gọi " đa tạp affine " với ý nghĩa là một đa tạp tựa xạ ảnh đẳng cấu với một đa tạp affine . Một " tập con mở chính " của $\mathbb{A}^n$ được hiểu là phần bù của một siêu diện , là tập hợp $\{ p \in \mathbb{A}^n \mid f(p) \neq 0 \}$ với các đa thức đơn $f \in k\left[x_1,....x_{n+1}\right]$. Ta thấy rằng một tập con mở chính của $\mathbb{A}^n$ là một đa tạp affine

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

Ví dụ 21 : Chúng ta hay gọi " một đa tạp xạ ảnh " là một vật thể 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 :

$$(x_0 :....: x_n ; y_0 :...y_m) \mapsto (x_0y_0 : x_0y_1 :....x_ny_m) = (z_{00} : z_{01} :....z_{nm})$$

Ánh xạ nói trên được gọi là phép nhúng Segre

1.3 ĐƯỜNG CONG ELLIPTIC

1.3.1 Các đường cong phẳng

Cho K là một trường. Ví dụ chẳng hạn, K có thể là trường $\mathbb{Q}$ của các số hữu tỷ, trường $\mathbb{R}$ của các số thực, trường $\mathbb{C}$ của các số phức, trường $\mathbb{Q}_p$ của số p – adic (xem [Kob]) , hoặc trường hữu hạn $\mathbb{F}_q$ của q phần tử (xem chương 1 , của [Ser1]) . Cho $\overline{K}$ là một bao đóng đại số của K.

Một đường cong phẳng X trên K được xác định bởi phương trình $f(x,y) = 0$, với $f(x,y) = \sum a_{ij} x^i y^j \in K[x,y]$ là bất khả quy trên $\overline{K}$. 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 $x^2y - 6y^2 - 11 = 0$ xác định một đường cong phẳng X trên $\mathbb{Q}$ bậc 3 và $\left(5, \frac{1}{2}\right) \in X(\mathbb{Q})$

Vấn đề đặt ra là : Liệu có tồn tại một thuật toán mà khi ta cho một đường cong phẳng X trên $\mathbb{Q}$ thì ta có thể xác định $X(\mathbb{Q})$, hoặc ít nhất xác định được $X(\mathbb{Q})$ có khác rỗng hay không?

Mặc dù $X(\mathbb{Q})$ không nhất thiết phải hữu hạn, nhưng ta thấy rằng, nó luôn luôn tồn tại một sự mô tả hữu hạn, vì thế vấn đề về sự xác định $X(\mathbb{Q})$ có thể được xác định rõ ràng bằng cách sử dụng máy Turing (xem [HU]) về mối quan hệ giữa câu hỏi trên và bài toán số của Hilbert , xem [Po2]

Bài tóan hiện tại là liệu rằng có tồn tại các phương pháp xác định $X(\mathbb{Q})$ khi ta cho một đường cong X cụ thể , mặc dù hiện tại ta chưa chứng minh được những phương pháp đó có thể dùng trong trường hợp tổng quát . Chính vì vậy , có những vấn đề mà chưa tìm ra câu trả lời

(1) Có tồn tại thuật toán mà khi cho một đa thức bậc bốn : $f(x) \in \mathbb{Q}[x]$ thì ta có thể xác định những điểm $y^2 = f(x)$ là điểm hữu tỷ hay không?

(2) Có tồn tại thuật toán mà khi cho một đa thức bậc ba : $f(x,y) \in \mathbb{Q}[x,y]$ thì ta có thể xác định những điểm $f(x,y) = 0$ là điểm hữu tỷ hay không?

1.3.2 Hình học xạ ảnh

1.3.2.1 Mặt phẳng xạ ảnh

Mặt phẳng affine $\mathbb{A}^2$ là mặt phẳng thông thường, với

$\mathbb{A}^2(K) = \{(a,b) : a,b \in K\}$ với mọi trường K. Compact hóa $\mathbb{A}^2$ bằng cách nối một số điểm " tại vô cực " để sinh ra mặt phẳng xạ ảnh $\mathbb{P}^2$.

Tập hợp những K - điểm trên mặt phẳng xạ ảnh P^2 có thể được định nghĩa một cách trực tiếp như: $P^2(k) := (k^3 - 0)/ k^*$. Nói cách khác, một điểm K- hữu tỷ trên P^2 là một lớp tương đương của bộ ba (a,b,c) với $0 \neq a,b,c \in K$, với quan hệ tương đương $\sim$, ở đây

$(a,b,c) \sim (\lambda a, \lambda b, \lambda c)$, $\lambda \in K^*$. Lớp tương đương của (a,b,c) được ký hiệu $(a:b:c)$. Ta cũng có thể đồng nhất $P^2(K)$ với tập hợp của các đường qua 0 trong không gian (x,y,z).

Đơn ánh $A^2(k) \hookrightarrow P^2(k)$ ánh xạ (a,b) vào $(a:b:1)$ hầu như là một song ánh: các điểm của $P^2(K)$ không thuộc trong ảnh, có dạng $(a:b:0)$ hình thành một đường xạ ảnh $P^1(K)$ của " các điểm tại vô cực ". Xem $P^2(K)$ như đường qua 0 trong không gian (x,y,z), $A^2(K)$ là tập hợp các đường như thế đi qua $(a,b,1)$ với $a,b \in K$, và phần bù $P^1(K)$ là tập hợp các đường qua 0 trong mặt phẳng (x,y). P^2 cũng có thể được bao phủ bởi ba bản sao của A^2, là: $\{(x:y:z) \mid x \neq 0\}$, $\{(x:y:z) \mid y \neq 0\}$, và $\{(x:y:z) \mid z \neq 0\}$.

1.3.2.2 Bao đóng xạ ảnh của các đường cong:

Phép thuần nhất của một đa thức $f(x,y)$ bậc d là $F(X,Y,Z) := Z^d f\left(\frac{X}{Z}, \frac{Y}{z}\right)$. Nói cách khác, ta thay đổi x bởi X , y bởi Y, và thêm vào đủ các thừa số của Z để mỗi đơn thức mang bậc tổng như nhau bằng d. Ta có thể thu lại f như sau: $f(x,y) = F(x,y,1)$.

Nếu $f(x,y) = 0$ là một đường cong phẳng C trong A^2, bao đóng xạ ảnh của nó là đường cong $\overline{C}$ trong 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 $$\tilde{C}(Q) = \frac{\{\text{zeros of } F\}}{Q^*}$$

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

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

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

1.3.2.3 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 P^2 trên K, bậc m và n, tương ứng. Định lý Bézout chỉ ra một cách chính xác rằng chúng giao nhau tại mn điểm trong P^2, và thỏa :

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

(2) Chúng cắt nhau trên một trường đóng đại số

(3) Những điểm tương giao là vô số trong trường hợp chúng là những điểm kì dị hay là những tiếp điểm

1.3.3 Xác định X(ℚ): sự phân chia bằng bậc

Ta trở lại vấn đề xác định tập hợp các điểm hữu tỷ X(ℚ) với X là một đường cong affine phẳng $f(x, y) = 0$ trên ℚ hoặc trên bao đóng xạ ảnh của nó . Cho d = deg *f* . Ta sẽ xem xét bài toán bằng việc cho tăng dần giá trị của d.

3.3.1- Khi d = 1: X là đường thẳng. Ta đã biết cách tham số hóa các điểm hữu tỷ trên đường thẳng $ax + by + c = 0$

3.3.2 - Khi d = 2: X là đường conic. Legendre đã chứng minh rằng các đường conic thỏa mãn Nguyên lý Hasse . Điều này nghĩa là: X có một ℚ - điểm nếu và chỉ nếu X có một ℝ - điểm và một điểm $\mathbb{Q}_p$ - điểm với mỗi số nguyên tố p. Vì một đường conic xạ ảnh được mô tả bởi một dạng bậc hai 3 ẩn số , do đó kết quả của Legendre có thể được xem như một trường hợp đặc biệt của định lý Hasse-Minkowski [Ser1] , khẳng định rằng một dạng toàn phương n biến trên ℚ biểu diễn 0 nếu và chỉ nếu nó biểu diễn 0 trên ℝ và $\mathbb{Q}_p$ với mọi p.

Định lý của Legendre dẫn đến một thuật toán để xác định sự tồn tại của một ℚ - điểm trên đường conic X. Thuật toán: bổ sung chính phương , nhân một hằng số, và thu về các biến, để rút gọn thành $aX^2 + bY^2 + cZ^2 = 0$ trong $\mathbb{P}^2$, với $a, b, c \neq 0$,không chính phương có quan hệ từng đôi nguyên tố với nhau . Khi đó ta có thể chứng minh rằng tồn tại

một $\mathbb{Q}$ - điểm nếu và chỉ nếu a,b,c đều không cùng dấu và: $\begin{cases} ax^2 + b \equiv 0 \pmod{c} \\ by^2 + c \equiv 0 \pmod{a} \\ cz^2 + a \equiv 0 \pmod{b} \end{cases}$ là giải được trong tập $\mathbb{Z}$

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

Trong trường hợp đường conic X có một $\mathbb{Q}$ - điểm P_0, vấn đề còn lại là làm thế nào để mô tả tập hợp tất cả các $\mathbb{Q}$ -điểm . Khi đó , ta sẽ dùng một thủ thuật quen thuộc : với mỗi điểm $P \in X(\mathbb{Q})$ vẽ một đường qua P_0 và P , và gọi t là hệ số góc của đường thẳng sao cho $t \in \mathbb{Q}$ (hoặc có thể là ∞). Ngược lại, cho $t \in \mathbb{Q}$, định lý Bézout bảo đảm rằng đường qua P_0 với hệ số góc 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:

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

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

xác định các ánh xạ song hữu tỷ từ A^1 đến X và ánh xạ ngược :điều đó có nghĩa là khi ta bỏ đi một số hữu hạn các tập con có chiều nhỏ hơn (có thể chỉ là một vài điểm), thì 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 trên mỗi chiều. Những ánh xạ song hữu tỷ 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 . Đặc biệt, tập hợp những nghiệm hữu tỷ của đường tròn $x^2 + y^2 = 1$ là $\left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\} \cup \{(-1,0)\}$.

3.3 Khi d = 3: X là các đường phẳng bậc 3 . Lind [Lin] và Reichardt [Rei] đã nhận thấy rằng những Nguyên lý Hasse có thể không đúng với các đường cong phẳng bậc ba. Xét một phản ví dụ : theo Selmer [Sel] thì đường cong

$3X^3 + 4Y^3 + 5Z^3 = 0$ trong P^2 có một $\mathbb{R}$- điểm $\left(\left(-\frac{4}{3}\right)^{1/3} : 1 : 0\right)$ và một $\mathbb{Q}_p$ - điểm với mỗi số nguyên tố p, nhưng nó không có $\mathbb{Q}$ - điểm (Vì p > 5, sự tồn tại các $\mathbb{Q}_p$ - điểm có thể được chứng minh bằng cách sử dụng bổ đề Hensel [Kob] để chứng minh sự tồn tại của các nghiệm đồng dư modulo p**.** Với p = 2, 3, 5, dạng tổng quát hơn của của bổ đề Hensel [Kob] có thể được sử dụng . Sự không tồn tại của các $\mathbb{Q}$- điểm khó thiết lập hơn .)

Bài tóan liệu một đường cong phẳng bậc ba có điểm hữu tỷ hay không hiện tại là một bài toán chưa được giải quyết. Do đó ta sẽ chú ý đến những đường cong phẳng bậc ba mà có một điểm hữu tỷ. Những đường này được gọi là các đường cong elliptic

1.3.4 Các đường cong elliptic

1.3.4.1 Các định nghĩa tương đương

Cho K là một trường hoàn chỉnh. Một đường cong elliptic trên K có thể được định nghĩa bằng một trong những cách 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 không là 2 hoặc 3, người ta có thể hạn chế sự chú ý tới các bao đóng xạ ảnh của các đường cong $y^3 = x^3 + Ax + B$.

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

(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

1.3.4.2 Các điểm kỳ dị

Nếu (0, 0) là một điểm trên đường cong affine $f(x,y)=0$ 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 đồng nhất bậc i. Chẳng hạn (0, 0) là kỳ dị trên $y^2 = x^3$ và trên $y^2 = x^3 + x^2$, nhưng không là điểm kỳ dị trên đường $y^2 = x^3 - x$. 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 affine 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 affine" 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 cho các đường cong trên một trường hoàn chỉnh K .

1.3.4.3 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 độ 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 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 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).

1.3.4.4 Luật nhóm - Định nghĩa

Một đường cong elliptic E trên K là một đa tạp nhóm nghĩa là có một ánh xạ "phép cộng" E x E $\rightarrow$ E được cho bởi các hàm hữu tỷ, mà cảm sinh ra một cấu trúc nhóm trên E(L) cho bất kỳ sự mở rộng trường L của K. Luật nhóm được đặc trưng bởi hai quy luật 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 là P, Q, R $\in$ E(K) thì khi đó: P + Q + R = O trong luật nhóm.

Từ những điều này ta suy ra:

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

b) Cho P, Q $\in$ E(K) khác O, đường thẳng qua P và Q (lấy tiếp tuyến với E tại P nếu P = Q) cắt E tại P, Q và điểm thứ 3 là R $\in$ E(k). Nếu R = O, thì P + Q = O , mặt khác P + Q = -R, ở đây - R có thể được xây dựng như trong a).

Chú ý rằng E(K) là một nhóm abel.

1.3.4.5 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 nhằm tìm ra một thuật toán cho phép tính P + Q. Sự tồn tại của các công thức này sẽ là quan trọng khi ta phát triển 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 ngừng.

2) Nếu Q = O, đặt R = P và ngừng.

3) Mặt khác cho 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 ngừng.

4) Nếu $x_1 = x_2$ và $y_1 = -y_2$, đặt R = O và ngừng.

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 ngừng.

1.3. 4.6 Luật nhóm - các ví dụ

Cho E là đường cong elliptic $y^2 = x^3 - 25x$. (Từ bây giờ, khi ta đưa ra một phương trình không thuần nhất cho đường cong elliptic E, nó được hiểu rằng ta cho E được định nghĩa như bao đóng xạ ảnh của đường cong affine 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: $((-3/2)x)^2 = x^3 - 25x$

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

và tìm $L \cap E = \{P, Q, R\}$ ở đây R := (25/4, - 75/8). Do đó P + Q + R = 0 trong luật nhóm, và P + Q = - R = (25/4, 75/8).

Sự tương 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. (điều này tương ứng với đường $x = 0$ đang tiếp xúc với E tại Q). Do đó Q + Q + O = O, và

2Q = O ; nghĩa là Q là một điểm có cấp 2 , 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 hình thành một nhóm con của $E(\overline{K})$ đẳng cấu với $\mathbb{Z}/2 \times \mathbb{Z}/2$.)

1.3.5 Cấu trúc E(K) đối với các trường K khác nhau

1.3.5.1 Đường cong Elliptic trên trường số phức

Trên một phương diện nào đó $E(\mathbb{C})$ là một đa tạp phức nhưng trên một phương diện khác thì nó là một nhóm và tọa độ của P + Q là hàm hữu tỉ theo tọa độ của P và Q. Do đó , $E(\mathbb{C})$ là một nhóm Lie 1- chiều trên $\mathbb{C}$. Hơn nữa , $E(\mathbb{C})$ là đóng trong $P^2(C)$ compact nên $E(\mathbb{C})$ là compact , liên thông . Theo sự phân lớp của nhóm Lie compact liên thông 1- chiều trên $\mathbb{C}$, ta xem $E(\mathbb{C}) \simeq C/\Lambda$ như là nhóm Lie trên $\mathbb{C}$, với dàn $\Lambda = Z\omega_1 + Z\omega_2$, trong đó ω_1, ω_2 là một $\mathbb{R}$- cơ sở của $\mathbb{C}$. Các ω_i được gọi là các chu kỳ vì tồn tại một hàm phân hình $p(z)$ trên $\mathbb{C}$ được xác định sao cho : $p(z + \omega) = p(z)\ \forall \omega \in \Lambda$.

Gỉa sử , ta bắt đầu xét trên $\mathbb{C}$ một dàn Λ rời rạc có hạng là 2 : $\Lambda = Z\omega_1 + Z\omega_2$ với ω_1, ω_2 là $\mathbb{R}$- cơ sở của $\mathbb{C}$, ta cần chỉ ra là làm thế nào để tìm ra một đường cong tương ứng trên $\mathbb{C}$.

Tập $g_2 = 60\Sigma'_{\omega \in \Lambda}\omega^{-4}$ và $g_3 = 140\Sigma'_{\omega \in \Lambda}\omega^{-6}$ trong đó ,ký hiệu ' nghĩa là bỏ đi số hạng $\omega = 0$.

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

Khi đó : ta có thể chứng minh như sau :

+ $p(z)$ là phân hình trên 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 $C/\Lambda \to E(\mathbb{C})$ với E là đường cong elliptic trên $\mathbb{C}$ có phương trình : $y^2 = 4x^3 - g_2 x - g_3$ (cực điểm của $p(z)$ qua đẳng cấu tương ứng là gốc tọa độ $O \in E(\mathbb{C})$).

- Vi phân $\frac{dx}{y}$ trên E cái níu với 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 $X(\mathbb{C})$ đối với một đường cong xạ ảnh không kỳ dị X trên $\mathbb{C}$.

1.3.5.2 Đường cong Elliptic trên trường số thực

Cho đường cong elliptic $E: y^2 = f(x)$ trên $\mathbb{R}$. Trong đó : $f(x) = x^3 + Ax + B \in \mathbb{R}[x]$ là không chính phương .

Ta có $E(\mathbb{R})$ nhóm Lie compact giao hoán 1- chiều trên $\mathbb{R}$.

Ta xét các miền mà f là không âm . Khi đó : ta nhận thấy rằng $E(\mathbb{R})$ có 1 hoặc 2 thành phần liên thông , f có 1 hoặc 3 nghiệm thực .Khi đó , nhóm đường tròn : $\mathbb{R}/\mathbb{Z} \simeq \{z \in C : |z| = 1\}$ là một nhóm Lie giao hoán compact 1- chiều liên thông trên $\mathbb{R}$.

với $E(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/\mathbb{Z} & \text{neu f có 1 nghiêm thuc} \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2 & \text{neu f có 3 nghiem thuc} \end{cases}$

Nhóm $E(\mathbb{R})$ có thể được xem như là một nhóm con của $E(\mathbb{C})$ cố định bằng phép liên hợp phức .Nếu E được xác định trên $\mathbb{R}$, ta có thể chọn Λ của mặt cắt trước nhằm ổn định qua phép liên hợp phức và tác động lên các tọa độ thành phần của phép liên hợp phức trên $E(\mathbb{C})$ tương ứng với tác động tự nhiên trên C/Λ . Trong trường hợp này ta định nghĩa chu kỳ thực như là hàm sinh dương của nhóm cyclic vô hạn $\Lambda \cap \mathbb{R}$. Một cách chính xác , Λ được xác định một cách duy nhất bởi một số thực khác 0 ; việc chọn Λ tương đương với việc chọn một vi phân của E trên $\mathbb{R}$ và chu kỳ thì phụ thuộc vào việc lựa chọn trên

1.3.5.3 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 $\mathbb{P}^2(\mathbb{F}_q)$, $E(\mathbb{F}_q)$ 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 Weil" . Hơn nữa , thuật toán của Shoof [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 số nguyên tố l 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 $E(\mathbb{F}_3) \simeq \mathbb{Z}/7$.

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),0} và $E(\mathbb{F}_3) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

1.3.6 Đường cong elliptic trên trường hữu tỷ

1.3.6.1 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 $r \in \mathbb{Z}_{\ge 0}$, r : gọi là hạng và T =: $E(\mathbb{Q})_{tors}$ là nhóm aben hữu hạn sinh gọi là nhóm xoắn . (Định lý Mordell còn được gọi là

định lý Mordell -Weil , vì Weil đã tổng quát hóa đối với các đa tạp aben trên các trường số . Đa tạp aben là đa tạp nhóm xạ ảnh với số chiều tùy ý) .

Ví dụ 27 : Cho E là đường cong elliptic trên trường $\mathbb{Q}$: $y^2 = x^3 - x^2$. Ta có thể chỉ ra rằng : $E(\mathrm{Q}) \simeq \mathrm{Z} \times \mathrm{Z}/2 \times \mathrm{z}/2$ trong đó : $\mathrm{E(Q)}/\ \mathrm{E(Q)}_{tors}$ được sinh bởi
(-4;6) .

Ví dụ 28 : Cho E là đường cong elliptic trên trường $\mathbb{Q}$: $y^2 + y = x^3 - x^2$ còn được gọi là " đường cong modular $X_1(11)$" thì

$$\mathrm{E(Q)}=\{(0,0),(0,-1),(1,0),(1,-1),0\} \simeq \mathrm{Z}/5 \ .$$

Ví dụ 29 : Cho E là đường cong elliptic trên trường $\mathbb{Q}$:$1062y^2 = x^3 - x$ (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 modular" , Elkies [Elk] đã tính được
$\mathrm{E(Q)} \simeq \mathrm{Z} \times \mathrm{Z}/2 \times \mathrm{z}/2$.
Trong đó , $\mathrm{E(Q)}/\ \mathrm{E(Q)}_{tors}$ được sinh bởi 1 điểm với hoành độ $q^2/1063$
và $q = \dfrac{1109186374182976967504702163571228176738233966743464 5}{3173426575447721807352079773209000125228079367788 7}$

Ví dụ 30 : Cho E là đường cong elliptic : $y^2 + xy + y = x^3 + \mathrm{a}x + \mathrm{b}$
Trong đó : $\mathrm{a} = -120039822036992245303534619191166796374$
và $\mathrm{b} = 5042249924849106700108017991680827267594437562229114 15116$
Martin và McMillen [MM] đã chỉ ra rằng $\mathrm{E(Q)} \simeq \mathrm{Z}^r$ trong đó $r \geq 24$.

1.3.6.2 Các đa tạp nhóm affine 1 – chiều trên trường K

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

G	Đa tạp	Luật nhóm	G(K)
G_a	$\mathbb{A}^1$	$\mathrm{x}_1, \mathrm{x}_2 \mapsto \mathrm{x}_1 + \mathrm{x}_2$	K, với phép +
G_m	$xy = 1$	$(\mathrm{x}_1, \mathrm{y}_1), (\mathrm{x}_2, \mathrm{y}_2) \mapsto (\mathrm{x}_1\mathrm{x}_2, \mathrm{y}_1\mathrm{y}_2)$	K^*, với phép .

G_m^a	$x^2 - ay^2 =$	$(x_1, y_1), (x_2, y_2) \mapsto (x_1x_2 + ay_1y_2, x_1y_2 + x_2$	$\ker(k(\sqrt{a})^* \xrightarrow{\text{chuaån}} k^*$

- Cột 1 : Đa tạp nhóm G , cũng là nhóm cộng tính G_a hoặc nhóm nhân G_m hoặc độ xoắn G_m^a với $a \in K^*$.

+ Loại đẳng cấu của G_m^a xem như là 1 đa tạp nhóm được xác định bởi ảnh của a trên K^*/K^{*2} . Nếu $a \in K^*$ thì $G_m^a \simeq G_m$.

- Cột 2 : Mô tả G như là 1 đa tạp , ở mỗi trường hợp G cũng là A^1 hoặc là 1 đường cong phẳng trong A^2.

- Cột 3 : Biểu diễn quy luật nhóm cấu xạ : $G \times G \to G$ trong hệ tọa độ .

- Cột 4 : Mô tả nhóm các điểm hữu tỉ G(K) .

1.3.6.3 Các cubic Weierstrass kỳ dị

Nếu E là một đường cong kỳ dị được định nghĩa như là bao đóng xạ ảnh của : $y^2 = x^3 + ax^2 + bx + c$ thì có tối đa một điểm kì dị .Giả sử P_0 là điểm kỳ dị . Bằng cách đổi biến số ta có thể giả sử : $P_0 = (0;0)$ .Phương trình có dạng : $(y^2 - ax) - x^3 = 0$. Đường thẳng tiếp xúc với các nhánh tại $(0;0)$ là : $y = \pm x\sqrt{a}$. Các điểm kỳ dị được gọi là điểm nút hoặc điểm lùi khi $a \neq 0$ hoặc $a = 0$.

Trong trường hợp còn lại : $E_{ns} := E - \{P_0\}$ trở thành đa tạp nhóm affine 1- chiều có cấu trúc tương tự như cấu trúc hình học trong trường hợp không kỳ dị (Một đường thẳng L đi qua 2 điểm không kỳ dị không thể đi qua P_0, vì sẽ trái với kết quả định lý Bézout)

Thật vậy : $E_{ns} \simeq \begin{cases} G_a & \text{khi } a = 0 \quad (\text{diem lùi}) \\ G_m & \text{khi } a \in K^{*2} \quad (\text{diem nút}) \\ G_m^a & \text{khi } a \text{ không chính phuong (diem nút)} \end{cases}$

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

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

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

1.3.6.4 Sự rút gọn 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 các 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 được đường cong bậc ba $\overline{E}$ trên F_p . Nhưng $\overline{E}$ có thể kỳ dị . Điều này xảy ra nếu và chỉ nếu 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 biến số) 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 với nhân tại p . Khi đó : ta nói rằng E có sự rút gọn nhân tách hoặc rút gọn nhân không tách khi E_{ns} là 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	G_a	Rút gọn cộng .
Điểm nút	G_m hoặc $G_m^{(d)}$	Rút gọn nhân .

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

Giả sử một đường cong elliptic E trên $\mathbb{Q}$ có sự rút gọn tốt tại p . Bất kỳ 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 $\overline{E}(F_p)$. Điều này xác định 1 phép đồng cấu : $E(\mathbb{Q}) \to \overline{E}(F_p)$.

Định lý 55: Nếu E có sự rút gọn tốt tại p > 2 thì nhóm con xoắn T của $E(\mathbb{Q})$ nhúng được vào trong $\overline{E}(F_p)$

Mệnh đề 56*:* T là hữu hạn .

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

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

vì E là rút gọn tốt tại p khi $p \neq 2,11$ .Ta tính được : $\#\overline{E}(F_3)=7$ và $\#\overline{E}(F_5) = 9$.

Nhóm duy nhất được nhúng đơn ánh vào các nhóm cấp 7 và 9 là nhóm tầm thường . Vậy $T = \{0\}$. Đặt biệt : $(0;2) \in E(\mathbb{Q})$: có cấp vô hạn và $E(\mathbb{Q})$ có hạng dương .

1.3.6.6 Các định lý khác về nhóm con xoắn T.

Định lý 57 (định lý Luzt - Nagell):

Cho $A,B \in \mathbb{Z}$ và E: $y^2 = x^3 + Ax + B$ là 1 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 $y_0^2 \mid 4A^3 + 27B^2$

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

Định lý 58 (định lý Mazur) :

Nếu E là một đường cong elliptic trên $\mathbb{Q}$ thì : $T \simeq \mathbb{Z}/N$ với $N \leq 12$, $N \neq 11$ hoặc $T \simeq \mathbb{Z}/2 \times \mathbb{Z}/2N\mathbb{Z}$ với $N \leq 4$. 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 của các điểm có cấp là m trong $E(\overline{\mathbb{Q}})$. Việc tìm những điểm có cấp m trong $E(\mathbb{Q})$ là tìm những nghiệm hữu tỷ của Φ_m và kiểm tra xem chúng có tung độ hữu tỷ .Theo định lý Mazur chỉ có hữu hạn m được xét từ đó cho ta thuật toán thời gian đa thức để tính T .

1.3.6.7 Các hàm độ cao

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

Nếu $P = (a : b : c) \in P^2(\mathbb{Q})$

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 của P .

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

Vì vậy :

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

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

(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 kết quả của (1) và (2) với $P, Q \in E(\mathbb{Q})$ và $n \in \mathbb{Z}$

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

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

Hơn nữa , theo (1) và (2) , định lý Mordell-Weil khẳng định sự hữu hạn của $E(\mathbb{Q})/2 E(\mathbb{Q})$ thì $E(\mathbb{Q})$ là hữu hạn sinh .Nếu các phần tử sinh của $E(\mathbb{Q})/2 E(\mathbb{Q})$ 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 hợp lý .

1.3.7 Phương pháp phân tích đường cong elliptic

1.3.7.1 Giải thích về sự phân tích

- Giả sử p , q là 2 số nguyên tố lớn chưa biết và N= pq . Ta tìm cách xác định một số nguyên n sao cho m $m \equiv 0(\mathrm{mod}\, p)$ nhưng $m \not\equiv 0(\mathrm{mod}\, q)$. Khi đó gdc(m , N) có thể được tính tóan nhanh

1.3.7.2 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 $\mathbb{Z}/N$ với $x_1, x_2, x_3 ...$ sao cho : $x_{i+1} = f(x_i)$ và kiểm tra với : $m = x_i - x_j$ $(i \neq j)$

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

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

Phương pháp đường cong elliptic của Lenstra : Thay a^K với $a \in (\mathbb{Z}/N)^*$, ta xét K.P với $P \in E(\mathbb{Z}/N)$, trên đường cong elliptic E . Ở đây , ta xem $K.P = \underbrace{P + P + ... + P}_{K \text{ lần}}$, trong một nhóm aben $E(\mathbb{Z}/N)$ đã được xác định

1.3.7.3 Phương pháp Pollard p – 1

Phương pháp đường cong elliptic có thể được xem như 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 , nhưng bỏ qua những chi tiết và sự cải tiến hữu ích

Để phân tích N

1) Chọn một số nguyên K > 1 có nhiều ước số , có thể như K = k! với $k \geq 1$

2) Chọn tùy ý một số nguyên a thỏa $1 < a < N - 1$

3) Nếu gdc(a , N) > 1 , khi đó ta dừng lại , ngược lại ta tiếp tục

4) Dùng 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 tiếp tục thực hiện cho tới khi g là ước số không tầm thường của N

+ Nếu $g = N$, thì ta thực hiện quá trình với giá trị a khác , hay ta thay K bởi một ước số khác

+ Nếu $g = 1$, ta thực hiện lại quá trình với K lớn hơn

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

Vấn đề của phương pháp này là sẽ không dễ dàng để tìm K mà chia hết bởi $p - 1$ trong khi ta không biết p là gì .Cách tốt nhất ta có thể làm là chọn một số K có nhiều ước số và hy vọng có chứa nhân tử $p - 1$

1.3.7.4 Các phương án của phương pháp p – 1

Thay vì 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 $A^* / (\mathbb{Z}/N)^*$ mà $A = \dfrac{(\mathbb{Z}/N)[t]}{t^2 - b}$ với bất kỳ $b \in \mathbb{Z}/N$.

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 thực hiện tốt khi $p^2 + p + 1$ là trơn . Khi $p^2 + 1$ là trơn , thì $\Phi_r(p)$ là trơn với $\Phi_r(z)$ là r – đa thức chia vòng tròn bậc r . Điều đó nhanh chóng trở nên vô dụng bởi vì $p^2 + p + 1$ là quá lớn so với $p - 1$ và do đó trở nên khó trơn

Phương pháp của Lenstra là : thay thế F_p^* bởi nhóm $E(F_p)$ mà E là đường cong Elliptic .Khi đó sẽ có nhiều E khác nhau để thực hiện .

1.3.7.5 Đường cong Elliptic trên $\mathbb{Z}/N$

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

$$P^2\left(\mathbb{Z}/N\right) := \frac{\left\{(a:b:c)\middle| a,b,c \in \mathbb{Z}/N, \gcd(a,b,c,N)=1\right\}}{\left(\mathbb{Z}/N\right)^*}$$

Một đường cong elliptic E trên $\mathbb{Z}/N$ được cho bởi một công thức thuần nhất : $Y^2Z = X^3 + AXZ^2 + BZ^3$ với $A,B \in \mathbb{Z}/N$ sao cho $\Delta := -16\left(4A^3 + 27B^2\right)$ thuộc $\left(\mathbb{Z}/N\right)^*$. Khi đó , $E\left(\mathbb{Z}/N\right)$ là tập con của những điểm (a : b : c) $\in P^2\left(\mathbb{Z}/N\right)$ thỏa mãn phương trình bậc ba . Với bất kỳ số nguyên tố p ước số của N , $E\left(\mathbb{Z}/p\right)$ là tập hợp những điểm trong $P^2\left(\mathbb{Z}/p\right)$ 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

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

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

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

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

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

1.3.7.6 Phương pháp đường cong Elliptic

Giả sử rằng số nguyên N là thừa số 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 trơn y nhỏ hơn hay bằng P

2) Chọn bất kỳ những số nguyên A, x_1 ; $y_1 \in [1;N]$

3) Đặt B = $y_1^2 - x_1^3 - Ax_1 \in \mathbb{Z}/N$ và cho E là $y^2 = x^3 + Ax + B$ sao cho $P_1 := (x_1; y_1) \in E\left(\mathbb{Z}/N\right)$. Nếu gcd($4A^3 + 27B^2$, N) $\neq 1$, trở lại bước 2

4) Dùng sự mở rộng nhị nguyên của những thừa số của K để tìm ra K . Dùng công thức của luật nhóm tính $P_1 \in E\left(\mathbb{Z}/N\right)$

5) Nếu tại một vài điểm , công thức không thỏa thì chúng ta tìm 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 phải chọn được những điểm đầu tiên và tìm ra đường cong elliptic đi qua những điểm đó . Do những phức tạp về mặt thuật tóan 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 các phần tử của $\mathbb{Z}/N$.

1.3.7.7 Những phân tích đặc trưng của phương pháp đường cong elliptic

Nếu $\#E\left(\mathbb{Z}/p\right)$ chia hết K , thì $K.P_1$ sẽ rút gọn thành 0 mod p . Trong trường hợp đó , ta có thể giả thiết rằng $K.P_1$ có thể không phải là O mod N , hay tối thiểu tại một vài điểm của phép 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 N đòi hỏi một chút may mắn để chọn E sao cho $\#E\left(\mathbb{Z}/p\right)$ chia K

Giả sử rằng N có một thừa số nguyên tố p sao cho $p+1+2\sqrt{p} \leq P$. Chọn s là xác suất cho viêc xây dựng nên E ngẫu nhiên bởi thuật tóan , cấp của $E\left(\mathbb{Z}/p\right)$ là y – trơn . Nếu $E\left(\mathbb{Z}/p\right)$ là y- trơn , thì $\#E\left(\mathbb{Z}/p\right) \mid K$, do định nghĩa của K và do định lý Hasse rằng $\#E\left(\mathbb{Z}/p\right) \leq p+1+2\sqrt{p}$. Do đó , số đường cong elliptic cần thiết trong suốt thuật tóan là

$O(1/s)$. 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 $R = 0\left(s^{-1}(\log K)(\log N)^{0(1)}\right)$

Đặt 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 , đặt tên là N , P , và a , và trước tiên ta tính K : $K \le \prod_{l \le y} l^{\left[\log_l P\right]} \le \prod_{l \le y} P \le P^y$

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

Kế đó ta cần ước lượng về xác suất trơn s. Đinh lý của Canfield - Erdos - Pomerance chỉ ra rằng xác suất để một số nguyên bất kỳ thuộc $[1,x]$ để $L(x)^a$ – trơn là $L(x)^{-1/(2a)+0(1)}$ khi $x \to \infty$. Dùng thuật tóan Deuring về số đường cong elliptic trơn được cho trên $\mathbb{Z}/p$, ta có thể chỉ ra rằng $\#E\left(\mathbb{Z}/p\right)$ là đóng được phân bố đều trên hầu hết các khỏang 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 cho số nguyên bất kỳ là nhỏ hơn nhiều với biên độ . Thì s = $L(P)^{-1/(2a)+0(1)}$

Theo giả thiết , tổng thời gian 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 chạy chỉ phụ thuộc vào kích cỡ của phần tử được tìm thấy , nó có khả năng tìm thấy những phân tử nhỏ hơn mà nhanh hơn

Trong thực tế , khi tối ưu hóa cách chọn y và do đó K phụ thuộc vào P , việc thực hiện phương pháp đường cong Elliptic là hợp lý với P đủ nhỏ cho trước . Hơn nữa , nếu không tìm được thừa số , ta có thể thực hiện lại bằng cách gia tăng dãy các giá trị của P . Cuối cùng nếu không tìm được những phần tử nào đủ nhỏ thì ta chuyển sang thực hiện trên một miền số khác sao cho tiệm cận nhanh hơn nếu những phần tử là lớn

1.3.7.8 Những kết quả của phương pháp đường cong Elliptic

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

484061254276878368125726870789180231995964870094916937 của

$\left(6^{43}-1\right)^{42}+1.$

Richard Bent đã suy ra rằng những kết quả của phương pháp đường cong Elliptic là một con số gồm D chữ số trong năm $Y(D):=9.3.\sqrt{D}+1932.3$

Ví dụ 33: Như Y(54) = 2000.6 và Y(60) = 2004. 3

1.3.8 Một số loại đường cong

1.3.8.1 Những số chia

Những số chia có thể được dùng để tạo ra những đường cong Elliptic tương tư có cấp cao hơn , kết nối để được những đường cong có cấp cao hơn . Chúng cũng là những chứng minh một cách tự nhiên nhất về tính kết hợp thành từng nhóm của những đường cong Elliptic

Cho X là một đường cong xạ ảnh không suy biến trên một miền hòan hảo k . Nhóm các k – số chia $\mathrm{Div}\left(X_{\bar{k}}\right)$ là tập hợp của những tổng tự nhiên của các điểm trên $X\left(\bar{k}\right)$. Nhóm con của những k – số chia hữu tỷ $\mathrm{Div}(X)$ là nhóm con của $\mathrm{Gal}\left(\bar{k}/k\right)$- số chia ổn định . Bậc của số chia $D=n_1(P_1)+.....+n_r(P_r)$ là số nguyên $n_1+.....+n_r$. Khi đó $\mathrm{Div}^0\left(X_{\bar{k}}\right)$ là nhóm của những $\bar{k}$ - số chia có bậc 0 .Tương tự , là định nghĩa của $\mathrm{Div}^0(X)$

Ví dụ 34: Cho E là đường cong Elliptic $y^2 = x^3 + 17$ trên $\mathbb{Q}$. Những điểm $P\left(1+\sqrt{-7};-2+\sqrt{-7}\right)$; $Q\left(1-\sqrt{-7};-2-\sqrt{-7}\right)$; R(-1 ; 4) nằm trên $E\left(\overline{\mathbb{Q}}\right)$. Số chia D:= 2(P)

+ 2(Q) – 7(R) là ổn định trên $Gal\left(\overline{Q}/Q\right)$ mặc dù P và $\mathbb{Q}$ là không ổn định , và $D \in Div(E)$.

Bậc của D là 2 + 2 – 7 = -3

1.3.8.2 Những số chia chính quy và nhóm Picard :

Nếu f là một hàm hữu tỷ khác 0 trên X và $P \in X\left(\overline{k}\right)$, đặt $ord_P(f)$ biểu thị tất cả các bậc của f triệt tiêu tại P , thì số chia của f là $(f) := \sum_{P \in X\left(\overline{k}\right)} ord_P(f).P \in Div^0\left(X_{\overline{k}}\right)$, và nếu hệ số của f là k , thì $(f) \in Div^0(X)$. Tập hợp những dạng f như thế là tập con Princ(X) của số chia chính quy . Nếu $D; D' \in Div(X)$, ta viết $D \sim D'$ nếu $D - D' \in Princ(X)$. Định nghĩa nhóm Picard hay nhóm lớp các số chia của X là $Pic(X) := \frac{Div(X)}{Princ(X)}$; $Pic^0(X) := \frac{Div^0(X)}{Princ(X)}$

Ví dụ 35 : Nếu E , P , Q , R là các ví dụ phần trước , f = y – x + 3 thì ta có

(f) = (P) + (Q) + (R) – 3(O) , và (P) + (Q) + (R) ~ 3(O) trên Pic(E)

Định lý 59 : Nếu E là đường cong Elliptic trên k , ánh xạ $E(k) \to Pic^0(E)$ biến P thành lớp của (P) – (O) là song ánh

Cấu trúc nhóm trên $Pic^0(E)$ cảm sinh từ cấu trúc nhóm trên E(k)

1.3.8.3 Sự tương đương

Thật hữu ích khi ta tìm hiểu những sự tương tự giữa những trường số đại số và những đường cong hình học

Trường số	Hàm tương ứng
Z	k(t)
$\mathbb{Q}$	k(t)
$\mathbb{Q}_P$	k(t)
Trường số F	Sự mở rộng hữu hạn của k(t)
Spec0_F (0_F là vành của những số nguyên của F)	Đường cong affine trơn X

Sự mở rộng hữu hạn F' của F	Phủ $X' \to X$
Ideal phân thức	Số chia
Ideal chính quy	Số chia chính quy
Nhóm các lớp	Pic(X)
Hàm phân thức $\varsigma(s)$, giả thiết Rieman , giả thiết Rieman tổng quát	Giả thiết Weil

1.3.8.4 Điểm hữu tỷ trên đường cong

Ta sẽ tìm hiểu ngắn gọn về điểm hữu tỷ trên đường cong tùy ý . Một đường cong trên $\mathbb{Q}$ có thể có $X(\mathbb{Q}) = \emptyset$. Trong bảng bên dưới , giả thiết rằng X là một đường cong phẳng trên $\mathbb{Q}$ có $X(\mathbb{Q}) \neq \emptyset$ và ta định nghĩa

$$N_X(B) := \#\{P \in X(\mathbb{Q}) : h(P) \leq B\}$$

Dáng điệu định tính của $X(\mathbb{Q})$ và trong trường hợp cụ thể , tốc độ gia tăng của hàm phân thức $N_X(B)$ được xác định bởi giá trị

Giá trị	X(Q)	$N_X(B)$
0	Vô hạn	$\left(c_1 + o(1)\right)e^{c_2 B}$
1	Nhóm abel hữu hạn	$\left(c_3 + o(1)\right)B^{c_4}$
≥ 2	Hữu hạn	O(1)

Trong cột thứ 3 , c_1 ; c_2 ; $c_3 > 0$; $c_4 \geq 0$ là những hằng số phụ thuộc vào X và sự ước lượng đạt đến khi $B \to \infty$

Thực tế thì $X(\mathbb{Q})$ là hữu hạn khi bậc lớn hơn hay bằng 2 , đã được khẳng định bởi Mordell [Mo1] . Những chứng minh được thực hiện bởi Falting [Fa] và Vojta [Vo] và bản chứng minh thu gọn của Vojta được ghi chép bởi Bombieri [Bo] . Tất cả những chứng minh đã được biết đều không hiệu quả vì đã không chỉ ra được có hay không tồn tại một thuật tóan để xác định $X(\mathbb{Q})$ cho dù thuật tóan đó là duy nhất .

1.3.8.5 Jacobians : Một công cụ để tìm hiểu những đường cong có cấp cao hơn :

Nhắc lại rằng , cho đường cong Elliptic E , ta có một nhóm đẳng cấu $E(k) \simeq Pic^0(k)$. Nhưng nếu X là một đường cong xạ ảnh không suy biến có bậc lớn hơn 1 trên miền k , thì sẽ không có một song ánh giữa X(k) và $Pic^0(X)$ và trên thực tế X không thể được tạo từ một đa tạp nhóm

Một đa tạp abel là một đa tạp nhóm xạ ảnh sao cho mỗi đường cong Elliptic là một đa tạp abel một chiều . Lấy X bất kỳ có bậc g trên đó , có một đa tạp abel J có số chiều g được gọi là Jacobian của X với tính chất $J(k) \simeq Pic^0(X)$. điều đó chỉ có khi X là một đường cong Elliptic sao cho J trùng X.

Nếu $P_0 \in X(k)$ thì có một ánh xạ nhúng đa tạp X vào trong J , biến mỗi điểm P trên X thành lớp số chia của $(P) - (P_0)$ trong $Pic^0(X)$

Ví dụ 36: Bây giờ ta thực hiên một vài phép tính trên một Jacobian của đường cong Fermat . Cho X là một bao đóng xạ ảnh của $x^{13} + y^{13} = 1$ trên Q . Bậc của X là $g = \frac{(13-1)(13-2)}{2} = 66$. Cho P= (1;0) và Q(0;1) trên X(Q) . Gọi J là Jacobian của X thì J là một đa tạp abel 66 chiều . Số chia của đa thức $\frac{y-1}{x-1}$ trên X là 13(Q) – 13(P) , do đó lớp của 13(Q) – 13(P) trên $Pic^0(X)$ là tầm thường . Do đó lớp của (Q) – (P) là một điểm 13 – xoắn trên J(Q)

Giả sử rằng X là một đường cong xạ ảnh không suy biến trên Q có bậc $g \geq 2$ với $X(\mathbb{Q}) := \emptyset$. Do định lý Mordell – Weil , J(Q) là một nhóm abel hữu hạn . Hơn nữa , $\frac{J(Q)}{J(Q)_{tors}}$ có thể được trang bị một hàm $\hat{h}$ tòan phương chính tắc cao hơn . Tính hữu hạn của $X(\mathbb{Q})$ trong chứng minh của Vojta nghiên cứu có bao nhiêu điểm của $X(\mathbb{Q})$ có thể có bên trong mang lưới bởi ứng dụng của kỹ thuật xấp xỉ điophan

Không may , kỹ thuật xấp xỉ điophan không hữu hiệu . Chúng đem lại cho ta số lượng những điểm hữu tỷ nhưng không giới hạn độ cao của chúng (Hạn chế độ cao giúp làm giảm số lượng những bài tóan để thành những phép tính hữu hạn)

Hơn thế , tồn tại những kỹ thuật thường được sử dụng để xác định $X(\mathbb{Q})$ trên phần lớn các đường cong X , được trình bày trong [Po1] và [Po2] . Bên cạnh đó , một số các kết

quả gần đây chỉ ra rằng X($\mathbb{Q}$) có thể được tính trực tiếp trên tất các các đường cong X trên $\mathbb{Q}$, xem phần F.4.2 của [HS]

1.4 CÁC ĐIỂM HỮU TỶ TRÊN ĐƯỜNG CONG ELLIPTIC

1.4.1 Lịch sử

Một phần quan trọng của lý thuyết số là thuật tóan Diophantine . Có những đa thức mà ta hy vọng rằng có thể tìm được tập hợp các nghiệm nguyên hay nghiệm hữu tỷ của đa thức . Chúng được quan tâm sau khi Diophantus of Alexandria , một trong những nhà tóan học nêu ra nhiều vấn đề về điều đó . những câu hỏi thường được đưa ra là :

1) Có tồn tại những nghiệm nguyên không ?

2) Có tồn tại những nghiệm và có thành phần hữu tỷ ?

3) Có bao nhiêu nghiệm nguyên trên đó ?

4) Có bao nhiêu nghiệm hữu tỷ trên đó ?

Với những đa thức bậc hai tuyến tính , ta đã biết câu trả lời cho những câu hỏi ở trên . Với biểu thức tuyến tính ax + by = c , luôn tồn tại vô hạn những nghiệm hữu tỷ . Nếu gcd(a , b) không chia hết cho c , thì có vô hạn nghiệm nguyên . Ngược lại , nếu gcd(a, b) chia hết cho c thì không có nghiệm nguyên . Với một đa thức bậc hai , nếu có thể tìm thấy một nghiệm hữu tỷ thì sẽ có vô hạn các nghiệm hữu tỷ khác . Nhưng với đường cong elliptic $y^2 = x^3 + ax^2 + bx + c$ thì sao ? Những nghiệm nguyên và hữu tỷ của dạng đa thức trên không được biêt chính xác . Viêc mô tả những nghiệm này cần sự phối hợp giữa đại số , lý thuyết số và hình học

1.4.2 Những điểm nguyên và hữu tỷ

Trong thập niên 1920 , Siegel đã chỉ ra rằng , một đường cong elliptic có hữu hạn những nghiệm nguyên . Sau đó , vào 1970 , Baker và Coates đã chỉ ra nhóm các nghiệm lớn nhất dựa trên những hệ số của đường cong elliptic . Tuy nhiên, tập hợp này quá lớn và không thực tiễn .

Vào năm 1901 , về những điểm hữu tỷ trên đường cong eliptic , Poincaré ước đóan tồn tại hữu hạn một tập hợp những điểm mà có thể đại diện cho tất cả những điểm hữu tỷ . Điều này đã được chứng minh vào nămm 1923 bởi Mordell .Hơn nữa , phương pháp

Moredell cho phép tìm ra tập hợp đại diện hữu hạn , nhưng điều đó chưa từng đươc chứng minh bởi các kết quả . Do đó , điều đó vẫn chỉ là sự phỏng đóan

1.4.3 Các điểm hữu tỷ - Sự mô tả định tính

Cho E là 1 đường cong Elliptic trên $\mathbb{Q}$ và

$E(\mathbb{Q}) = \{(x,y) \in E | x,y \in \mathbb{Q}\} \cup \{\infty\}$ được gọi là nhóm cộng tính của những điểm hữu tỷ trên E . Ta sẽ tìm hiểu về nhóm này , về kích cỡ và cấu trúc của nó

Định lý 60 (định lý Nagell – Lutz) : Cho E: $y^2 = f(x) = x^3 + ax^2 + bx + c$ là một đường cong elliptic và cho D là biệt thức của f(x) . Nếu P =(x,y) là 1 điểm hữu tỷ xác định thì x; y là những số nguyên và y = 0 hay $y|D$

Định lý 61 (định lý Mazur): Cho E là một đường cong elliptic trên $\mathbb{Q}$ và giả sử rằng $E(\mathbb{Q})$chứa một điểm có cấp xác định là m thì $1 \le m \le 10$ hay m = 12

Định lý trên sẽ chỉ cho ta một hạn chế trên những nhóm con xác định của $E(\mathbb{Q})$

- Từ đó ta sẽ tiếp tục giới thiêu khái niệm về chiều cao của một số hữu hạn và phương pháp làm giảm . Ta sẽ thảo luận về phương pháp 2- descent and , time and space permitting .và phương pháp chung p – descents

Định lý 62 (định lý Mordell – Weil) : Cho E là một đường cong elliptic thì $E(\mathbb{Q})$ là nhóm aben hữu hạn sinh

Dựa trên định lý Mordell – Weil người ta chú ý đến một số đường cong elliptic và tìm cách tính độ xoắn của nhóm con của E và hạng của E . Một cách tổng quát , việc tính hạng của $E(\mathbb{Q})$ là khó , nhưng ta sẽ xét một số kết quả cụ thể trong chương sau.

Chương 2

CÁC ĐƯỜNG CONG ELLIPTIC DẠNG WEIERSTRASS TRÊN $\mathbb{Q}$

2.1 TÌM ĐIỂM HỮU TỶ TRÊN ĐƯỜNG CONG ELLIPTIC

2.1.1 Đại cương về đường cong elliptic

-Một đường cong elliptic xác định trên một trường K là tập hợp những điểm (x_0, y_0) với $x_0, y_0 \in K$ thỏa phương trình đa thức (dạng Weierstrass dài) :

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

với a_1 , a_2 , a_3 , a_4 , a_6 là hằng số thụôc K

- Bây giờ chúng ta sẽ tìm hiểu những nghiệm trên trường K và chú ý đến những nghiệm hữu tỷ của (1) . Do đó chúng ta thực hiện phép đổi biến nhằm làm cho đơn giản biểu thức của đường cong elliptic , nghĩa là biểu diễn tổng quát của một đường cong elliptic là biểu diễn dạng Weierstrass ngắn $Y^2 = X^3 + a_4X + a_6$ 2) với $a_i \in \mathbb{Z}$

- Một cách đặc biệt , trước tiên ta thực hiên phép đổi biến

$$Z = x$$

$$W = y + \frac{a_1}{2}x + \frac{a_3}{2} \quad (3)$$

- Khi đó (1) trở thành $W^2 = Z^3 + \left(a_2 + \frac{a_1^2}{4}\right)Z^2 + a_4Z + a_6 + \frac{a_3^2}{4}$

Ta có thể viết lại biểu thức cho phù hợp $W^2 = Z^3 + a'_2Z^2 + a_4Z + a'_6$ (4)

Ta thực hiện phép đổi biến số $X = Z + \frac{a'_2}{3}$; Y= W (5)

Ta thu được : $Y^2 = X^3 + a'_4X + a''_6$ (6)

- Bây giờ ta sẽ tiếp tục chú ý đến những điểm trên (2) với tọa độ hữu tỷ . Nếu ta có một đường cong $Y^2 = X^2 + \frac{m}{n}x + \frac{p}{q}$ với m , n, p , q là những số nguyên , thì ta có thể nhân thêm vào biểu thức n^6q^6 để được :

$$\left(n^3q^3y\right)^2 = \left(n^2q^2x\right)^2 + mn^3q^4\left(n^2q^2x\right) + pn^6q^5$$

Và thực hiện phép đổi biến X' = n^2q^2X ; Y' = n^3q^3Y là song tuyến tính hữu tỷ thực hiện trên biểu diễn ngắn Weierstrass với A = mn^3q^4 và B = pn^6q^5

- Một chú ý quan trọng : Những ánh xạ song hữu tỷ thực hiện những phép biến đổi trên không tạo ra và không làm mất đi những điểm có tọa độ hữu tỷ trên đường cong . Một điểm (x , y) với x , y hữu tỷ ánh xạ thành điểm

(f_1(x , y) ; f_2(x, y)) với f_1(x , y) ; f_2(x , y) hữu tỷ và ngược lại , hàm ngược $f_1^{-1}(x,y)$ và $f_2^{-1}(x,y)$ biến những 1 điểm hữu tỷ thành 1 điểm hữu tỷ

- Như vậy ta có thể thực hiện trên phần lớn những biểu diễn tổng quát của đường cong elliptic ở dạng Weierstrass ngắn : $y^2 = x^3 + Ax + B$ với A , B là những số nguyên và nghiệm của phương trình này có các tọa độ hữu tỷ .

2.1.2 Nhóm Mordell – Weil của đường cong elliptic

- Từ rất lâu , đã có những sự quan tâm đặc biệt trong viêc tìm tất cả những nghiệm hữu tỷ của các phương trình (2) . Giả sử rằng ta có hai điểm $P_1(x_1, y_1)$ và $P_2(x_2, y_2)$ mà tất cả các thành phần tọa độ là hữu tỷ thì ta dễ dàng tìm được điểm thứ ba . Lưu ý rằng ,một đường thẳng cắt đồ thị đa thức bậc ba tại 3 vị trí . Đường thẳng qua P_1 và P_2 có phương trình y = mx + b với $m = \frac{y_2 - y_1}{x_2 - x_1}$; và $b = y_1 - mx_1$. Do đó tương giao của đường thẳng với (2) là :

$$y^2 = x^3 + Ax + B$$
$$(mx + b)^2 = x^3 + Ax + B$$
$$0 = x^3 - m^2x^2 + (A - 2mb)x + B - b^2$$

Khi đó , đa thức bậc ba có 3 nghiệm và 2 trong 3 nghiệm là x_1 và x_2 , ta có thể viết

$$0 = (x - x_1)(x - x_2)(x - x_3)$$

$$0 = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3$$

Đồng nhất các hệ số :

$$m^2 = x_1 + x_2 + x_3$$

$$A - 2mb = x_1x_2 + x_2x_3 + x_3x_1$$

$$B - b^2 = -x_1x_2x_3$$

Thực tế : Cho 2 điểm $P_1(x_1, y_1)$ và $P_2(x_2, y_2)$ trên đường cong elliptic :

$y^2 = x^3 + Ax + B$ thì điểm thứ ba là giao giữa đường cong và đường thẳng có tọa độ là :

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_3 - x_1) + y_1$$

Lưu ý : Nếu hai điểm trùng nhau thì ta không thể tính được hệ số góc m bằng cách này thì khi đó ta phải tính hệ số góc từ đường thẳng tiếp xúc . Ta lấy vi phân dạng Weierstrass ngắn $2y(dy) = (3x^2 + A)(dx)\dfrac{dy}{dx} = \dfrac{3x^2 + A}{2y}$

Khi đó hệ số góc m của đường thẳng tiếp xúc đường cong tại $P_1(x_1; y_1)$ là $m = \dfrac{3x_1^2 + A}{2y_1}$ và ta sử dụng giá trị này khi cần tính hệ số góc của đường thẳng .

Khi ta cho một điểm đơn trên đường cong , thì ta có thể tìm nhiều điểm hơn bằng cách sử dụng đường thẳng tiếp xúc để tìm điểm thứ hai và phương pháp dây cung – tiếp tuyến để tìm các điểm cho đến khi ta không thể tìm thêm . Lưu ý rằng , mỗi điểm mà ta tính bằng phương pháp này sẽ có tọa độ hữu tỷ cung cấp cho ta một điểm đơn có toạ độ hữu tỷ để bắt đầu với điểm đơn đó bởi vì tất cả tất cả các phép biến đổi đại số đều khả nghịch hữu tỷ.

2.1.2.1 Điểm tại vô cực

- Có những điểm mà ta phải đặt câu hỏi : Điều gì sẽ xảy ra nếu ta có một điểm hữu tỷ mà đường thẳng tiếp xúc tại đó là một đường thẳng đứng .Khi tìm tập hợp những điểm là nghiệm của phương trình (2) , thì nó sẽ bao gồm cả một điểm đơn tại vô cực O

- Một trong những câu hỏi chính về đường cong elliptic là làm cách nào có thể tìm hết được tất cả những nghiệm hữu tỷ bằng phương pháp dây cung – tiếp tuyến ở trên . Đó chính là nội dung quan trọng nhất của định lý đươc trình bày bởi Louis Mordell : tất cả những điểm hữu tỷ trên đường cong (bao gồm cả điểm tại vô hạn) có thể được tìm thấy bởi việc áp dụng phương pháp dây cung – tiếp tuyến trên một số hữu hạn những điểm sinh và do đó tập hợp những nghiệm hữu tỷ là một nhóm abel hữu hạn sinh , gọi là nhóm Mordell –Weil

Luật nhóm : Tập hợp những điểm hữu tỷ trên một đường cong elliptic kể cả điểm tại vô cực là một nhóm với phép toán " cộng điểm"

1) Đơn vị của nhóm là điểm tại vô cực O

2) Cho một điểm $P_1(x_1 , y_1)$ với $y_1 \neq 0$, phép cộng P_1 với chính nó được thực hiện bằng cách sử dụng công thức tiếp tuyến để xác định điểm (x_3, y_3) như là điểm thứ ba trên đường thẳng tiếp xúc . Phép cộng điểm là $P_1 + P_1 = P_3 = \left(x_3, -y_3\right)$

3) Cho điểm $P_1(x_1 , y_1)$ với $y_1 = 0$, thì tổng của P_1 với chính nó là điểm tại vô cực

4) Cho hai điểm phân biệt $P_1(x_1 , y_1)$ và $P_2(x_2, y_2)$, tổng P_1 và P_2 được hiện bởi việc sử dụng công thức trên (x_3, y_3) như là điểm thứ ba trên đường thẳng nối P_1 và P_2 , phép cộng điểm là $P_1 + P_2 = P_3 = \left(x_3, -y_3\right)$

5) Nghịch đảo của $P_1(x_1 ; y_1)$ là điểm - $P_1(x_1 , -y_1)$

Một quan điểm khác khá đơn giản về luật nhóm là : tổng của ba điểm thẳng hàng là điểm zêrô tại vô cực . Điều này dẫn đến một trường hợp đặc biệt là tổng của điểm (x_1 , y_1) và $(x_1 , - y_1)$ ứng với đường thẳng nối hai điểm là một đường thẳng đứng thì điểm thứ ba là điểm tại vô cực . Với quy ước đó thật dễ dàng để chỉ ra rằng bản chất của phép cộng các điểm trên đường cong elliptic thỏa mãn tất cả các tiêu chuẩn của một nhóm giao hóan với điểm vô hạn là đơn vị

2.1.2.2 Ví dụ

- Cho đường cong $y^2 = x^3 - x + 1$. Có 6 cặp điểm có tọa độ nguyên trên đường cong này là :

Điểm	x	y
P_0	-1	± 1
P_1	0	± 1
P_2	1	± 1
P_3	3	± 5
P_4	5	± 11
P_5	56	± 419

- Liên quan đến những điểm trên ta thu được :

$$P_0 + P_0 + P_3 = O$$
$$P_0 - P_1 - P_4 = O$$
$$P_0 - P_2 - P_2 = O$$
$$P_1 + P_1 + P_2 = O$$
$$P_1 - P_2 - P_3 = O$$
$$P_2 - P_3 - P_4 = O$$
$$P_3 - P_4 - P_5 = O$$

- Và các điều sau đây là chính xác :

$$P_0 + P_0 = -P_3$$
$$P_1 + P_1 = \left(\frac{1}{4}, -\frac{7}{8}\right)$$
$$P_2 + P_2 = P_0$$
$$P_3 + P_3 = \left(\frac{19}{25}, -\frac{103}{125}\right)$$
$$P_4 + P_4 = \left(\frac{159}{121}, -\frac{1861}{1331}\right)$$

2.1.3 Những đường cong elliptic đồng dư số nguyên tố

- Ta xét dạng khai triển Weierstrass ngắn: $y^2 = x^3 + Ax + B$

và những nghiệm hữu tỷ (x, y) của phương trình trên. Nhưng ta cùng xem xét đến những nghiệm hữu tỉ mà tử số và mẫu số tăng rất nhanh , dẫn đến việc tính toán hiệu quả là không

thể. Do đó, ta chỉ quan tâm đến những đường cong elliptic vì ta có thể xem xét những nghiệm đồng dư số nguyên tố p và tổng quát hơn là đồng dư số nguyên m

- Khi xét những đường cong và các điểm hữu tỷ , thực sự ta có thể tìm thấy một điểm hữu tỷ đơn trên đường cong và dùng thuật toán dây cung - tiếp tuyến để tìm ra vô hạn điểm trên đường cong. Trong trường hợp những đường cong đồng dư số nguyên tố p, chắc chắn rằng không có nhiều hơn p^2 điểm trên đường cong

Định lý 63 : Cho $y^2 = x^3 + Ax + B$ là một đường cong elliptic đồng dư số nguyên tố p . Khi đó số điểm trên đường cong là p – 1 + a với $|a| < 2\sqrt{p}$. Hơn nữa với mỗi giá trị thuộc tập bị chặn này , có ít nhất một đường cong đồng dư p với đúng p -1 + a điểm.

Kết quả chính thứ hai là những điểm trên đường cong được lấy theo đồng dư p làm thành một nhóm mà cấu trúc được cảm sinh từ nhóm các điểm hữu tỷ trên đường cong. Nếu ta tiếp tục thực hiện cách cộng điểm vào những số hữu tỷ bằng việc biểu diễn của những mẫu số như là thực hiện phép nghịch đảo đồng dư p, thì tất cả những phần việc số học mà chúng ta tính toán cũng chỉ như là những số hữu tỷ cho đến khi chúng ta có mẫu số sao cho nó là zero đồng dư p tại điểm mà ta áo thể xem như những số hữu tỷ có mẫu số là zero được xem như là điểm tại vô cực

2.1.3.1 Ví dụ

- Xét đường cong $y^2 = x^3 - x + 1$ đồng dư 7. Những điểm nguyên trên đường cong luôn tồn tại, nhưng ta chú ý rằng điểm P_5 biến thành điểm P_1 vì
56 = 0 (mod 7) và 419 =-1 (mod7), và ta lưu ý rằng ta thêm vào điểm quen thuộc được đặt tên là P_6 .

Điểm	x	y
P_0	6	± 1
P_1	0	± 1
P_2	1	± 1
P_3	3	± 2
P_4	5	± 3
P_5	0	± 1
P_6	2	0

Bây giờ , ta có thể khẳng định :

1	$P_1 = (1,1)$	$= (1,1)$
2	$P_1 = (1,1) + (1,1)$	$= (6,1)$
3	$P_1 = (1,1) + (6,1)$	$= (0,-1)$
4	$P_1 = (1,1) + (0,-1)$	$= (3,2)$
5	$P_1 = (1,1) + (3,2)$	$= (5,-3)$
6	$P_1 = (1,1) + (5,-3)$	$= (2,0)$
7	$P_1 = (1,1) + (2,0)$	$= (5,3)$
8	$P_1 = (1,1) + (5,3)$	$= (3,-2)$
9	$P_1 = (1,1) + (3,-2)$	$= (0,1)$
10	$P_1 = (1,1) + (1,1)$	$= (6,-1)$
11	$P_1 = (1,1) + (6,-1)$	$= (1,-1)$
12	$P_1 = (1,1) + (1,-1)$	$= O$

2.1.4 Những đường cong elliptic với mục đích nhân tử hóa

- Ý tưởng chính trong việc sử dụng những đường cong elliptic để nhân tử hóa là ở chỗ những nhóm các đường cong elliptic đồng dư nguyên tố p có thể được dùng tương tự như nhóm đồng dư p được dùng trong phương pháp nhân tử hóa
(p -1) của Polland . Tuy nhiên, không giống như Polland, ta có thể chọn nhiều đường cong khác nhau bằng việc thay đổi các lựa chọn nhằm thu được một nhóm trơn.

- Giả sử rằng, ta cố gắng thực hiện phép phân tích n = pq là tích của hai nguyên tố. Khi đó, cấp của nhóm elliptic đồng dư p là p – 1 + a với a bị chặn, cấp của nhóm là p, cấp của nhóm các nguyên tố đồng dư p là p – 1 gần với p .

- Chọn một đường cong Weierstrass ngắn, chọn một điểm cơ bản

P = (x_0,y_0) trên đường cong và thực hiện nhiều phép tích phức hợp trên bộ phận M . Bây giờ tính tóan M.P trên đường cong đồng dư n. Trên các số đồng dư n , ta sẽ tìm đươc những số nghịch đảo đồng dư n .Ta thực hiên điều này bằng cách dùng định lý số dư Trung Hoa và tính nghịch đảo đồng dư p và đồng dư q nhưng do ta không biết p và q do đó ta cứ thực hiện như thể n là một số nguyên tố và hy vọng điều tốt nhất sẽ đạt được . Nếu chúng ta có một điểm mà chúng ta không thể nghịch đảo các thành phần để đồng dư n , khi đó ta sẽ biết rằng ta sẽ có một mẫu số sao cho zero đồng dư p nhưng trên thực tế thì không phải là zero

- Khi một thuật tóan không thể thưc hiện , điều đó có nghĩa là , ta không có đủ những thông tin cần thiết về hệ số n . Và khi đó gcd của mẫu thức với n và p sẽ không thể có

- Thuật tóan TWEAK :Ta sẽ thưc hiện trên những số hữu tỷ và giũ cho tử số và mẫu số là những biến số độc lập .

- Ý tưởng chính : Có nhiều đường cong elliptic do có nhiều cách chọn A và B . Mỗi đường sẽ có $\alpha_{(A;B)}$ và do đó sẽ có bậc nhóm khác nhau . Chúng ta có thể thực hiện nhiều bước song song và chúng ta cần một trong những đường đó có giá trị $p-1+\alpha_{(A;B)}$ sao cho đường đó là trơn . Điều đó sẽ tốt hơn Pollard vì với Pollard ta chỉ có một cơ hội duy nhất sao cho p – 1 với p chia hết n là trơn . Hơn nữa khi chọn một đường cong , ta có thể cố định B = 1 và cố tính bội số của A . Do đó khi ta có điểm $(0,\pm 1)$ trên đương cong $y^2 = x^3 + Ax + 1$, chúng ta không phải tìm kiếm một điểm cơ bản để bắt đầu

2.1.5 Các đường cong elliptic và vấn đề độ rời rạc

- Trong thập niên 1980, với những phát hiện độc lập của Victor Miller và Neal Kodlitz mà điều then chốt trong bài tóan trao đổi khóa Diffice – Hellman đã có thể cài đặt bằng việc sử dụng nhóm những điểm đồng dư modulo p trên một đường cong elliptic thay thế cho những số nguyên đồng dư một số nguyên tố p lớn.

- Thuận lợi của điều trên là có thể dùng những phương pháp đã biết như là phương pháp thực hiện phép tính trên các chỉ số nhằm giải quyết những vấn đề về độ rời rạc trên đường cong. Do đó, những số nguyên tố dùng cho những đường cong có thể nhỏ hơn những số đươc dùng cho thuật toán sự trao đổi khóa dạng RSA.

2.1.6 Phép tịnh tiến đến tọa độ xạ ảnh

- Xét đường cong dạng Weiertrass ngắn $y^2 = x^3 + Ax + B$ với những nghiệm hữu tỷ của phương trình này . Việc xử lý những số hữu tỷ là vất vả bởi vì phép chia khó khăn. Tốt hơn nếu ta thay bằng tọa độ xạ ảnh bởi vì khi đó ta có thể tách các tử số và mẫu số và tránh thực hiện phép chia.

- Xét dạng xạ ảnh biểu diễn Weierstrass ngắn : $y^2z = x^3 + Axz^2 + Bz^3$ trên đó ta thêm vào ẩn số z nhằm làm cho tất cả các đơn thức đều có cùng tổng số mũ (bậc toàn phần như nhau) . Ta viết lại biểu thức $\left(\frac{y}{z}\right)^2 = \left(\frac{x}{z}\right)^3 + A\left(\frac{x}{z}\right) + B.$

- Và dĩ nhiên khi được viết lại đồng dư p cho một và số nguyên tố thì ta luôn luôn có thể bắt đầu bằng một cặp nghiệm (x;y) và biến nó thành nghiệm (x;y;z) với z = 1

- Hệ số góc $m = \frac{\Delta y}{\Delta x}$ của đường thẳng nối 2 điểm $(x_1; y_1)$ và $(x_2; y_2)$ là

$$m = \frac{\frac{y_2}{z_2} - \frac{y_1}{z_1}}{\frac{x_2}{z_2} - \frac{x_1}{z_1}} = \frac{y_2z_1 - y_1z_2}{x_2z_1 - x_1z_2} = \frac{u}{v}$$

- Do đó , ta cần $\frac{x_3}{z_3} = \left(\frac{u}{v}\right)^2 - \frac{x_1}{z_1} - \frac{x_2}{z_2} = \frac{u^2z_1z_2 - v^2\left(x_1z_2 - x_2z_1\right)}{v^2z_1z_2}$

- Ta viết : $x_3 = k\left(u^2z_1z_2 - v^2\left(x_1z_2 - x_2z_1\right)\right)$

$$z_3 = kv^2z_1z_2$$

- Ta thu được $\frac{y_3}{z_3}$ tổng của những điểm (nhưng không là điểm thứ ba trên đường thẳng .

$$-\frac{y_3}{z_3} = \frac{y_1}{z_1} + m\left(\frac{x_3}{z_3} - \frac{x_1}{z_1}\right)$$

$$-y_3 = y_1kv^2z_2 + m\left(x_3 - x_1kv^2z_2\right)$$

$$-y_3 = kv^2y_1z_2 + \frac{ux_3}{v} - kuvx_1z_2$$

$$y_3 = -kv^2y_1z_2 - \frac{ux_3}{v} + kuvx_1z_2$$

$$y_3 = -kv^2y_1z_2 - \frac{u\left(k\left(u^2z_1z_2 - v^2\left(x_1z_2 + x_2z_1\right)\right)\right)}{v} + kuvx_1z_2$$

$$y_3 = -kv^2y_1z_2 - \frac{ku^3z_1z_2}{v} + kuv\left(x_1z_2 + x_2z_1\right) + kuvx_1z_2$$

Từ đó ta kết luận rằng $k = v\kappa$ nếu không thì chúng ta phải loại ra những phần dư trong mẫu thức . Do đó

$$y_3 = -kv^3 y_1 z_2 - ku^3 z_1 z_2 + kuv^2 x_1 z_2 + kuv^2 x_2 z_1$$
$$= -ku^3 z_1 z_2 + 2kuv^2 x_1 z_2 + kuv^2 x_2 z_1 - kv^3 y_1 z_2$$

- Ta chú ý rằng : $\frac{y_2}{z_2} - \frac{y_1}{z_1} = \frac{u}{v}\left(\frac{x_2}{z_2} - \frac{x_1}{z_1}\right)$

Ta quy đồng thì thu được : $uv^2\left(x_1 z_2 - x_2 z_1\right) + v^3\left(y_2 z_1 - y_1 z_2\right) = 0$

- Nếu ta cho $k = 2$ và thêm giá trị zerô thì ta thu được :

$$y_3 = u\left(3v^2\left(x_1 z_2 + x_2 z_1\right) - 2u^2 z_1 z_2\right) - v^3\left(y_1 z_2 + y_2 z_1\right)$$

- Biểu thức dùng để cộng 2 điểm phân biệt có thể được trình bày như sau :

$$x_3 = 2u^2 v z_1 z_2 - 2v^3\left(x_1 z_2 - x_2 z_1\right)$$
$$y_3 = u\left(3v^2\left(x_1 z_2 + x_2 z_1\right) - 2u^2 z_1 z_2\right) - v^3\left(y_1 z_2 + y_2 z_1\right)$$
$$z_3 = 2v^3 z_1 z_2$$

- Một cách tương tự , ta có công thức cộng một điểm với chính nó như sau :

$$m = 3x_1^2 + Az_1^2$$
$$x_3 = 2y_1 z_1\left(m^2 - 8x_1 y_1^2 z_1\right)$$
$$y_3 = -m^3 + 12mx_1 y_1^2 z_1 - 8y_1^4 z_1^2$$
$$z_3 = 8y_1^3 z_1^3$$

2.2 ĐIỂM XOẮN CỦA ĐƯỜNG CONG ELLIPTIC TRÊN TRƯỜNG SỐ

2.2.1 Tổng quan

- Chủ đề về điểm hữu tỷ trên đường cong elliptic có thể được xem như là một thành phần của lý thuyết về phương trình Diophantine. Việc nghiên cứu về những đường cong elliptic càng trở nên thiết thực khi bắt đầu với những đường cong elliptic được dùng trong lĩnh vực mật mã. Những nghiên cứu sau không tập trung vào những đường cong elliptic trong lĩnh vực mật mã , thay vào đó, sẽ tập trung tìm hiểu về công cụ cơ bản để hiểu về những điểm hữu tỷ trên một đường cong elliptic mà nghiệm mà thành phần tọa độ của chúng có thể được biểu diễn thành các phân số.

- Với mỗi phép toán 2 ngôi $\oplus$, ta có thể biến tập hợp những điểm hữu tỷ ký

hiệu $C(\mathbb{Q})$ thành một nhóm giao hoán. Hơn nửa, ta có thể phân biệt các thành phần thành những điểm xoắn và những điểm không xoắn mà bậc hữu hạn hay bậc vô hạn tương ứng . Khi xem xét tập hợp những điểm xoắn , ký hiệu $C(\mathbb{Q})_{tors}$, ta nhận thấy rằng tập hợp này lập thành một nhóm con . Điều đó được biết đến đối với một đường cong elliptic C trên $\mathbb{Q}$, chứa một điểm có bậc hữu hạn m với $1 \le m \le 10$ hay m = 12 . Chính xác hơn , tập hợp những điểm có bậc hữu hạn trên $C(\mathbb{Q})$ lập thành một nhóm con có một trong 2 dạng sau :

(i) Một nhóm cyclic có bậc N với $1 \le N \le 10$ hay N = 12

(ii) Tích của một nhóm cyclic cấp 2 và một nhóm cyclic có cấp 2N với $1 \le N \le 4$.

- Đặc trưng đã nêu của $C(\mathbb{Q})_{tors}$ được biết đến từ định lý Mazur

Định lý 64 (định lý Nagell- Lutz) : Cho $y^2 = f(x) = x^3 + ax^2 + bx + c$ là một đường cong bậc ba không suy biến với các hệ số nguyên a , b, c và D là biệt thức của f(x) với $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Giả sử P(x, y) là một điểm hữu tỷ có cấp hữu hạn , thì x và y là các số nguyên . Nếu y = 0 thì P có cấp bằng hai , trái lại thì y là ước số của D

- Khi đường cong bâc ba ở dạng chuẩn thì định lý Nagell –Lutz cho ta một phương pháp để tìm ra những điểm có cấp hữu han trên đường cong elliptic . Phương pháp đó đơn giản : tính D và tìm hết tất cả các số nguyên là ước số của D . Những số đó đều là giá trị có thể của y . Từ đó , ta thế giá trị y vào đường cong và hệ số của đuòng bậc ba , thì ta thu được giá trị nguyên x . Mặt khác , có một kết quả mạnh hơn của Nagell- Lutz chỉ ra rằng y^2 cũng là ước số của D chứ không chỉ là y . Điều đó có nghĩa là ta chỉ cần tìm trên những bình phương là ước số của D thay vì trên từng số nguyên . Sau khi có tất cả các (x , y) thỏa định lý , ta chỉ cần kiểm tra xem đâu là điểm xoắn .

- Nhằm có được một phương pháp để tìm những điểm hữu tỷ xoắn trên một đường cong cho trước , có một cách được dùng là tìm những điểm xoắn có cấp xác định trên đường cong . Với mỗi số nguyên n , tồn tại môt đa thức với các hệ số hữu tỷ , gọi là $\psi_n(x)$ mà những nghiệm của đa thức này là những giá trị x của những điểm xoắn có cấp n . Với những điểm xoắn hữu tỷ cấp n , ta tập trung xem xét những nghiệm hữu tỷ của $\psi_n(x)$.

Ví dụ 37: Để tìm tất cả những điểm xoắn cấp ba của đường cong

$y^2 = x^3 + bx + c$, ta sử dụng $\psi_3(x) = 3x^4 + 6bx^2 + 12cx - b^2$. Tìm nghiệm của $\psi_3(x)$, ta sẽ có thành phần x của những điểm xoắn . Để tìm giá trị y , ta thay các giá trị x vào đường cong elliptic và giải chúng tìm ra y . Lưu ý rằng , bởi đường cong của chúng ta có y^2 , ta sẽ thu được hai giá trị y cho mỗi giá trị x . Với mỗi giá trị x sẽ có hai điểm xoắn .

- Lưu ý rằng $\psi_n(x)$ sẽ cho tất cả các điểm xoắn có thể tìm đươc có cấp n , kể cả hữu tỷ và không hữu tỷ . Nếu $\psi_n(x)$ không có nghiệm hữu tỷ thì không có điểm xoắn hữu tỷ có cấp n

- Mặc dù những kiến thức về đường cong elliptic trên $\mathbb{Q}$ là rất nhiều , ở đây muốn mở rộng hơn nữa khi xem xét các đường cong elliptic trên các trường số đại số . Một trường số đại số là một mở rộng của trường hữu hạn số hữu tỷ . Điều đó có nghĩa là , đây là một trường chứa $\mathbb{Q}$, hữu hạn chiều , nếu được xét như là một không gian vectơ trên $\mathbb{Q}$. Hay nói cách khác là : cho $\mathbb{Q}$ và bổ sung thêm vào nó một nghiệm số của đa thức mà nghiệm đó không xác định trên $\mathbb{Q}$. Điều đó cho ta một trường chứa $\mathbb{Q}$ và tất cả các tổ hợp tuyến tính của lũy thừa của nghiệm bổ sung

- Ta chú ý đến đường cong $X_0(11) : y^2 = x^3 - 4x^2 - 160x - 1264$ trên trường số đại số $\mathbb{Q}(\varsigma_{11})$ với ς_{11} là một nghiệm không hữu tỷ của $x^{11} - 1 = 0$ tức là một nghiệm của $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$

- Khi xem xét kích cỡ của nhóm con xoắn của $X_0(11)$ trên $\mathbb{Q}(\varsigma_{11})$, ta nhận thấy nhóm con này có lực lượng là 5 cùng lực lượng với nhóm con xoắn trên $\mathbb{Q}$. Thực sự , 5 điểm giống nhau hình thành 2 nhóm con xoắn . Do đó đối với $X_0(11)$, việc xác định nhóm con xoắn không hiệu quả bởi việc tìm những điểm trên $\mathbb{Q}(\varsigma_{11})$ thay vì trên $\mathbb{Q}$

2.2.2 Nội dung

2.2.2.1 Các đường cong – Một cách nhìn khác

- Trước khi tìm hiểu về những đường cong elliptic , ta nhắc lại vài định nghĩa cơ bản , bắt đầu bằng việc định nghĩa lại về một đường cong . Một đường cong C là một biểu thức f(x,y) = 0 với f là một đa thức $f \in \mathbb{Z}[x, y]$. Ta luôn giả sử rằng các đường cong ta xét

không thể rút gọn được (nghĩa là f là một đa thức bất khả quy và trơn nghĩa là hệ phương trình $\begin{cases} f(x,y)=0 \\ \partial_x f=0 \\ \partial_y f=0 \end{cases}$ vô nghiệm

- Một nghiệm hữu tỷ của đường cong là một cặp (x , y) với $x,y\in\mathbb{Q}$ và f(x, y) = 0 . Nghiệm nguyên của đường cong là cặp (x , y) với $x,y\in\mathbb{Z}$ và f(x ,y) = 0 . Những định nghĩa nghiệm hữu tỷ và nghiệm nguyên cho ta hai tập con tự nhiên của đường cong được ký hiệu là $C(\mathbb{Q})$ và $C(\mathbb{Z})$

- Khó khăn khi tìm $C(\mathbb{Q})$ phụ thụôc vào bậc cuả đường cong .Kiến thức về những đường cong tuyến tính không phải là quá phức tạp . Do đó thay vì chú y đến những đừong cong bâc hai , ta hãy xem nó như là những conic

2.2.2.2 Điểm hữu tỷ trên conic

- Dạng tổng quát của một đường cong bậc hai hay một conic là :

$$f(x,y)=ax^2+bxy+cy^2+dx+ey+f=0$$

Với $a,b,c,d,e,f\in\mathbb{Z}$. Để tìm hiểu làm thế nào tìm $C(\mathbb{Q})$ cho một đường bậc hai , ta hãy xem ví dụ cơ bản trong viêc tìm $C(\mathbb{Q})$ của đường tròn đơn vị :

$$(C): x^2+y^2=1 .$$

- Khi ta vẽ một đường tròn đơn vị , có 4 điểm hữu tỷ (là các điểm nguyên) trên đường tròn là (1,0) ; (0,1) ; (-1,0) ; (0,-1) . Một vài điểm hữu tỷ khác dễ dàng nhận ra như $\left(\frac{3}{5},\frac{4}{5}\right);\left(\frac{5}{13},\frac{12}{13}\right)$. Lưu ý rằng , tối thiểu có 2 điểm có dạng $x=\frac{m}{n};y=\frac{l}{n}$ mà ước chung lớn nhất cuả m và n là 1 ; l và n là 1 . Khi ta thay giá trị x , y vào C , ta có $\left(\frac{m}{n}\right)^2+\left(\frac{l}{n}\right)^2=1\Rightarrow m^2+l^2=n^2$. Do đó (m , l , n) là một bộ ba Pitagore nguyên thủy . Quá trình đó cũng có chiều ngược lại và tạo nên quan hệ 1 – 1 giữa bộ ba P nguyên thủy và những điểm hữu tỷ trên đường tròn đơn vị . Do đó ta dễ dàng nhận thấy những ví dụ về điểm hữu tỷ trên đường tròn đơn vị có quan hệ với những

bộ ba Pitagore nguyên thủy. Một câu hỏi được đặt ra là làm thế nào để tìm tất cả những điểm hữu tỷ trên đường tròn đơn vị

2.2.2.3 Phương pháp tìm nghiệm hữu tỷ đối với đường bậc hai

- Bước đầu tiên trong việc giải quyết vấn đề trên là chọn một điểm hữu tỷ trên đường cong . Ta có thể chọn bất kỳ điểm nào , ví dụ chọn $P_0 = (-1,0)$ nhằm dễ dàng cho việc tính toán các bước kế tiếp .

- Giả sử ta viết được phương trình đường thẳng qua P_0 có hệ số góc t là

$y = t(x + 1)$ (1)

- Nếu $P \in C(\mathbb{Q})$ khác P_0 , thì đường thẳng nối P và P_0 có hệ số góc hữu tỷ Điều ngược lại ở đây là : Liệu có đường thẳng có hệ số góc hữu tỷ đi qua P_0 cắt đường tròn đơn vị tại một điểm $P \in C(\mathbb{Q})$ khác P_0 ? Câu trả lời là : Có . Do đó ta có thể nhận thấy một phương pháp để tham số hóa tất cả những điểm hữu tỷ dựa trên P_0 với tham số hữu tỷ t .

- Ta chứng minh điều ngược lại bằng cách cho $y = t(x + 1)$ cắt $x^2 + y^2 = 1$ .Thay $y = t(x + 1)$ ta có : $(1+t^2)x^2 + 2t^2x + t^2 - 1 = 0$ (2)

- Do x = -1 là một nghiệm , và do cách chọn P_0 , phân tích (2) ta có :

$$x^2 + t^2(x+1)^2 - 1 = 0 \Leftrightarrow (x+1)\left[x(t^2+1) + t^2 - 1\right] = 0 \Leftrightarrow x = -1 \vee x = \frac{1-t^2}{t^2+1} \quad (3)$$

- Ta biết rằng hệ số góc t được cho là một số hữu tỷ . Do đó (3) là một số hữu tỷ nghĩa là x là hữu tỷ . Thay (3) vào (1) , ta thu được :

$$y = t\left(\frac{1-t^2}{t^2+1} + 1\right) = \frac{2t}{1+t^2}$$

- Do đó, ta nhận thấy rằng điều ngược lại là đúng. Ta có thể tham số hóa $C(\mathbb{Q})$ như sau : $C(\mathbb{Q}) = \left\{\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \middle| t \in \mathbb{Q}\right\}$

- Phương pháp tìm điểm hữu tỷ trên có thể dùng cho bất kỳ biểu thức bậc hai với giả sử rằng ta đã có một điểm hữu tỷ. $C(\mathbb{Q})$ có thể là tập rỗng hay tập có kích cỡ vô hạn và trong trường hợp này được tham số hóa bởi một tham số hữu tỷ.

2.2.2.4 Không gian xạ ảnh.

Định nghĩa 65 : Một đường cong xạ ảnh là tập hợp các không điểm của một đa thức thuần nhất ba biến số F(x,y,z) = 0 với giả thiết rằng F có các hệ số nguyên. Lưu ý rằng F(x,y,z) là thuần nhất có bậc d nếu $F(kx,ky,kz) = k^d F(x,y,z)$ với mọi hằng số k.

- Những đường cong chúng ta đang xem xét có hai biến số và không bị giới hạn bởi sự thuần nhất. Bất kỳ một đường cong hai ẩn có thể trở nên thuần nhất ba ẩn . Xét f là một đường cong hai ẩn và thay $x = \frac{X}{Z}$ và $y = \frac{Y}{Z}$, thì f(x,y) = 0 trở thành $f\left(\frac{X}{Z},\frac{Y}{Z}\right) = 0$; để cho dễ viết , ta ký hiệu là F(X, Y, Z) = 0.

- Đặc biệt hơn, nếu ta nhân vào hai vế của $f\left(\frac{X}{Z},\frac{Y}{Z}\right) = 0$ bởi Z^d với d là bậc lớn nhất của các hạng tử riêng của f, ta có biểu thức thuần nhất F(X, Y, Z) = 0. Việc thay thế và nhân thêm vào này có thể được thực hiện bởi việc bổ sung vào mỗi đơn thức có tổng bậc là d với d xác định như trên. Ví dụ, cho đường cong $y^2 = x^3 + x^2 + 17$ có thể trở thành $Y^2Z = X^3 + X^2Z + 17Z^3$.

- Việc giới thiệu biến phụ nhằm biến đường cong phẳng f(x,y) = 0 vào trong mặt phẳng xạ ảnh $\mathbb{P}^2$. Xét tập hợp các bộ ba $(X,Y,Z) \in \mathbb{C}^3$ trừ (0,0,0). Trên tập hợp này, ta giới thiệu một quan hệ tương đương :

$$(X,Y,Z) \sim (\lambda X, \lambda Y, \lambda Z) \text{ với } \lambda \in \mathbb{C}^X \quad .$$

- Mặt phẳng xạ ảnh phức $\mathbb{P}^2$ là tập hợp các lớp tương đương của quan hệ tương đương trên. Dựa trên định nghĩa, hai điểm là tương đương nếu chúng có tọa độ tỷ lệ . Ta viết không gian xạ ảnh là:

$$\mathbb{P}^2 = \{(X,Y,Z) \mid X,Y,Z \in \mathbb{C}\} / \sim = \{[X:Y:Z]\}$$

- Điều đó có nghĩa là $[x:y:z] = [\lambda x:\lambda y:\lambda z]$ với $\lambda \neq 0$. Ví dụ như $[1:0,5:1,5]$ cùng là một điểm trong không gian xạ ảnh như $[2:1:3]$

- Vậy những điểm xạ ảnh này có liên quan gì đến quá trình thuần nhất ta mô tả ở trên. Cho [X:Y:Z] trong $\mathbb{P}^2$ với $Z \neq 0$, ta luôn có thể viết

$[X:Y:Z]=\left[\frac{X}{Z}:\frac{Y}{Z}:1\right]$ .Nếu F(X,Y,Z) = 0 và $Z\neq 0$ thì $(x,y)=\left(\frac{X}{Z},\frac{Y}{Z}\right)$ trên đường cong ban đầu f(x,y) = 0, ngược lại cho điểm (x,y) trên f(x,y) = 0, ta có 1 điểm xạ ảnh [x:y:1] trên F(X,Y,Z) = 0. Lưu ý rằng đường cong xạ ảnh F(X,Y,Z) = 0 chứa tất cả những điểm trên f(x,y) = 0 khi $Z\neq 0$ nhưng thêm vào những điểm tại vô cực khi Z = 0. Những điểm thêm vào nhằm hoàn chỉnh đường cong để đạt được những kết quả khác .

2.2.3 Đường cong elliptic

2.2.3.1 Định nghĩa

Định nghĩa 66: Một đường cong elliptic trên $\mathbb{Q}$ là một đường cong xạ ảnh (không suy biến) trơn bậc ba, trang bị trên đó điểm hữu tỷ cơ bản 0.(F có hệ số hữu tỷ)

- Một dạng cơ bản của đường cong elliptic là:

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

- Đây là dạng mà Pari dùng để giới thiệu về một đường cong elliptic mới. Pari là một chương trình toán học hữu ích khi làm việc với những đường cong elliptíc cũng như là với những ngành khác của toán học.

2.2.3.2 Dạng Weierstrass

- Ta luôn dùng những đường cong ở dạng chuẩn đươc gọi là dạng Weierstrass. Tổng thể là bất kỳ biểu thức bậc ba nào cũng có thể viết dưới dạng này. Dạng Weierstrass cổ điển là $y^2 = 4x^3 - g_2x - g_3$

- Một dạng khác của dạng Weierstrass mà ngày nay dùng nhiều hơn dạng đề cập đến ở trên là: $y^2 = x^3 + ax^2 + bx + c$.

- Do đó từ bây giờ, tất cả những đường cong ta xét đều ở dạng Weierstrass.

2.2.3.3 Nhắc lại định nghĩa

- Dựa trên định nghĩa trên, có ba điều kiện mà ta gặp khi xét một đường cong bất kỳ có là đường cong elliptic.

* Thứ nhất: Đường cong phải là xạ ảnh.

* Thứ hai: Đường cong phải trơn nghĩa là gradien của F

$\left\langle \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z} \right\rangle$ không đồng thời triệt tiêu (ba thành phần của vectơ trên không đồng thời

bằng 0) trên đường cong. Điều đó cho ta thấy sẽ không có giao điểm tự cắt hay nút thắt trên đồ thị của những đường cong và phần đồ thị bậc ba sẽ có ba nghiệm khác biệt. Ta có thể thấy rằng : $y^2 = x^3 + ax^2 + bx + c$ là trơn khi và chỉ khi đa thức bậc ba theo x không có nghiệm trùng nhau.

2.2.3.4 Nhắc lại về không gian xạ ảnh

- Điều kiện thứ ba trên đường cong phải liên kết điểm hữu tỷ cơ bản 0. Điều đó có nghĩa là $C(\mathbb{Q})$ của đường cong elliptic C không bao giờ rỗng, C luôn có ít nhất một điểm hữu tỷ. Thực sự, C bị hạn chế là một đường cong xạ ảnh, ta luôn có một cách viết hợp lý về điểm cơ bản hữu tỷ.

- Trong không gian xạ ảnh, f(x,y) = 0 trở thành F(X,Y,Z) = 0 và do đó, ta hạn chế f trở thành một đường cong elliptic. Điều đó có nghĩa là khi f trở nên thuần nhất, tất cả các hạng tử của hai vế của biểu thức sẽ có tối thiểu một lũy thừa của Z, ngoại trừ hệ số X^3. Do đó, tất cả những đường cong ta xét có dạng:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

- Nếu Z = 0 thì tất cả các hệ số trở nên 0 trừ X^3 và ta thu được $X^3 = 0 \Leftrightarrow X = 0$. Ta thu được một điểm xạ ảnh đơn $[0:Y:0] = [0:1:0]$ tại chỗ giao nhau của đường cong và đường thẳng tại vô cực Z = 0. Ta gọi điểm này tại vô cực $[0:1:0]$.

- Thực sự rằng những đường cong elliptic do định nghĩa là những đường cong xạ ảnh; đường cong elliptic C chứa điểm tại vô cực. Điều đó có ý nghĩa rằng điểm hữu tỷ cơ bản được đề cập trong định nghĩa của những đường cong elliptic thì tương đương với điểm tại vô cực. Do qui ước, bất cứ khi nào đường cong của chúng ta là Weierstrass thì điểm 0 sẽ được xem là điểm gốc của đường cong.

2.2.4 Luật nhóm

2.2.4.1 Định nghĩa $\oplus$

- Xét đường cong elliptic $y^2 = x^3 + ax^2 + bx + c$ ta sẽ định nghĩa một phép toán hai ngôi, kí hiệu $\oplus$ trên $C(\mathbb{Q})$. Cho P và Q thuộc $C(\mathbb{Q})$ với $P = (x_1, y_1); Q = (x_2, y_2)$. Giả sử rằng ta có thể vẽ một đường thẳng nối P và Q. Dễ dàng nhận ra rằng tồn tại một điểm mà đường thẳng cắt đường cong elliptic. Ta cố gắng tìm ra tọa độ giao điểm này.

- Dùng hệ số góc của đường thẳng, ta có $\overrightarrow{PQ} := y - y_1 = \lambda(x - x_1)$ với $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, ta có $y = y_1 + \lambda(x - x_1)$, thay y vào đường cong elliptic, ta thu được: $y^2 = \lambda^2(x - x_1)^2 + 2\lambda(x - x_1)y_1 + y_1^2 = x^3 + ax^2 + bx + c$

Chuyển tất cả qua vế phải ta thu được :

$$0 = x^3 + x^2(a - \lambda^2) + x(b + 2x_1\lambda^2 - 2\lambda y_1) + c - \lambda^2 x_1{}^2 + 2\lambda x_1 y_1 - y_1^3$$

- Do đây là một đa thức bậc ba theo x nên có 3 nghiệm. Ta có

$$x^3 + x^2(a - \lambda^2) + x(b + 2x_1\lambda^2 - 2\lambda y_1) + c - \lambda^2 x_1{}^2 + 2\lambda x_1 y_1 - y_1^3$$
$$= (x - x_1)(x - x_2)(x - x_3)$$

Dùng hệ thức Viette, cho phép ta tìm được các hệ số của x dưới dạng những nghiệm của đa thức, ta có $-(x_1 + x_2 + x_3)$ là hệ số của x^2 mà x_1 và x_2 từ P và Q, do đó ta có: $x_3 = \lambda^2 - a - x_1 - x_2$ với x_3 là hữu tỷ. Giá trị x_3 này là giá trị x của giao điểm. Từ đây, thay x_3 vào đường thẳng, ta thu được y_3 cũng là hữu tỷ. Giao điểm của đường thẳng PQ và đường cong elliptic có tọa độ hữu tỷ $(x_3; y_3)$.

- Vì đường thẳng nối hai điểm nên $C(\mathbb{Q})$ cắt đường cong tại điểm khác trên $C(\mathbb{Q})$, điều đó tương tự với điều chúng ta nhận thấy với conic . Thực tế với những đuờng cong bậc ba có y^2, nên luôn tìm được điểm thứ tư trên $C(\mathbb{Q})$ gọi tên là $P * Q$ có tọa độ $(x_3; -y_3)$. Chúng ta định nghĩa điểm thứ tư này là $P \oplus Q$

2.2.4.2 $(P * Q) \oplus (P \oplus Q)$

- Từ định nghĩa của $\oplus$, ta có vài chú ý. Trước tiên, điều gì sẽ xảy ra nếu ta thực hiện $(P * Q) \oplus (P \oplus Q)$. Ta không thể dùng các phương pháp thông thường vì λ không tồn tại. Giải pháp là đặt $(P * Q) \oplus (P \oplus Q)$ bằng điểm tại vô cực, kí hiệu là O. Chú ý rằng ta đang làm việc với những đường cong xạ ảnh. Bởi vì ta làm việc trên đường cong elliptic, ta chú ý rằng: - O = O . Ngoài ra, đường thẳng nối $P * Q$ và $P \oplus Q$ cắt đường cong tại một điểm thứ ba.

- Dễ dàng nhận ra rằng P + O = P và ta thu được:

i) $P \oplus O = P$

ii) $P * Q \oplus P \oplus Q = O$

2.2.4.3 $P \oplus P$

- Mặc dù ta đã định nghĩa $\oplus$ giữa hai điểm phân biệt, $P \oplus O$ khả nghịch $\oplus$, bây giờ ta định nghĩa phép $\oplus$ giữa một điểm và chính nó. Ta không thể dùng phương pháp thông dụng bởi vì λ không tồn tại. Câu hỏi về định nghĩa $P \oplus P$ phụ thuộc vào câu trả lời ta chọn hệ số góc như thế nào?

- Cách tốt nhất để xác định λ là lấy đạo hàm đường cong tại P và sử dụng giá trị này làm hệ số góc. Cách dễ nhất để tìm λ là dùng phép lấy đạo hàm ẩn. Ví dụ, cho đường cong $y^2 = x^3 + 17$. Lấy đạo hàm ẩn trên đường cong, ta có: $2yy' = 3x^2 \Rightarrow \lambda = y' = \frac{3x^2}{2y}$

.

- Tổng quát, ta có: $\lambda = y' = \frac{3x^2 + 2ax + b}{2y} = \frac{f'(x)}{2y}$

- Để có được hệ số góc tại điểm P, ta sẽ thêm vào hệ số a, b, c và tọa độ của điểm P. Do đó, λ được xác định.

- Điều đó dẫn đến sự thuận lợi nhằm có được một biểu thức hoàn hảo cho 2P thay vì cho tọa độ của chính P. Nếu ta thay $\lambda = \frac{f'(x)}{2y}$ vào biểu thức $y^2 = (\lambda x + x_1)^2$ quy đồng mẫu số chung, thay y^2 bởi f(x) ta có được:

Tọa độ x trong 2(x,y) là $\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$

- Điều đó dẫn đến rằng việc cộng một điểm vào chính nó một lần, hai lần, ba lần, n lần là một điều thú vị khi tìm hiểu về những đường cong elliptic. Bởi vì, với một số điểm $P \in C(\mathbb{Q})$, luôn tồn tại một số nguyên n nhỏ nhất sao cho nP = O với $nP = \underbrace{P \oplus P \oplus P \oplus \ldots\ldots\ldots \oplus P}_{n \text{ lần}}$. Bất kỳ điểm nào thỏa thuộc tính trên với n tồn tại thì được gọi là điểm xoắn cấp hữu hạn n. Bất kỳ điểm nào mà không tồn tại n thì được gọi là điểm xoắn cấp vô hạn.

2.2.4.4 Đường cong elliptic và $\oplus$

- Ta nhận thấy rằng, tập hợp những điểm hữu tỷ trên một đường cong elliptic với quan hệ $\oplus$ sẽ ứng với một đơn vị O duy nhất và làm cho mọi điểm có nghịch đảo. Kết hợp những điều đó thì tập hợp những điểm hữu tỷ trên đường cong elliptic là một nhóm. Vậy $C(\mathbb{Q})$ là một nhóm với $\oplus$.

- Thật ra, $C(\mathbb{Q})$ là một nhóm cho phép ta khảo sát như là sự tồn tại cấu trúc của nhóm. Sự phân loại cấu trúc của nhóm hữu tỷ được đề cập bởi định lý Mordell – Weil.

Định lý 67: Cho C là một đường cong bậc ba không suy biến, thì $C(\mathbb{Q})$ là một nhóm abel hữu hạn sinh đẳng cấu với $\mathbb{Z}^r \oplus F$

với $\mathbb{Z}^r = \underbrace{Z \times Z \times Z \times .... \times Z}_{\text{r lan}}$;

F= $\{ P \in C(\mathbb{Q}) |$ P có cấp hữu hạn $\}$

r = rank : là số lượng phần tử sinh tối thiểu.

- Định lý trên chỉ ra rằng nếu C là đường cong bậc ba không kỳ dị thì $C(\mathbb{Q})$ là hữu hạn sinh. Điều đó có nghĩa là: tồn tại hữu hạn những điểm trên $C(\mathbb{Q})$ mà ta có thể lấy tất cả các tổ hợp tuyến tính giữa những điểm đó. Chúng sinh ra $C(\mathbb{Q})$

2.2.5 Điểm xoắn

2.2.5.1 Định nghĩa điểm xoắn

- Mỗi điểm trên một đường cong elliptic thuộc một trong hai dạng: một điểm với cấp hữu hạn hay cấp vô hạn. P là một điểm có cấp hữu hạn nghĩa là tồn tại một số nguyên nhỏ nhất n sao cho nP = 0. Nếu n không tồn tại thì P là điểm có cấp vô hạn. Một cách khác, P là một điểm có cấp vô hạn nghĩa là ta không thể tìm được một điểm tại vô cực bằng cách cộng P vào chính nó một số lần . Sự khác biệt giữa những điểm hữu hạn và vô hạn dẫn đến định nghĩa sau:

Định nghĩa 68: Một điểm $P \in C(\mathbb{Q})$ được gọi là điểm xoắn có cấp n nếu P có cấp n. Tập hợp tất cả những điểm xoắn của một đường cong elliptic C sẽ tạo thành một nhóm con hữu hạn của C(Q), gọi là $C(\mathbb{Q})_{tor}$. Vậy

$C(\mathbb{Q})_{tor}$ = $\{ P \in C(\mathbb{Q}) |$ P có cấp hữu hạn $\} \subseteq C(\mathbb{Q})$

2.2.5.2 Điểm có cấp 2

- Ta thực sự muốn biết điều gì về những điểm có cấp hữu hạn. Bắt đầu với cấp 2. ta cần 2P = 0 với $P \neq 0$.

- Đặt P = (x,y) thì –P = (x,-y) .

Do đó 2P = 0 ⇔ P = -P ⇔ (x,y) = (x,-y) ⇔ y = 0

- Do đó, tất cả những điểm cấp 2 phải có y = 0. Lấy $x \in C$, ta có thể tìm được bốn điểm cấp 2 là: $S = \{0;(\alpha_1,0);(\alpha_2,0);(\alpha_3,0)\}$ trong đó $\alpha_1,\alpha_2,\alpha_3$ là những nghiệm của $x^3 + ax^2 + bx + c$. Ta có S là một nhóm cấp Bốn, là tích trực tiếp của hai nhóm cấp 2.

- Nếu ta giới hạn x là số thực, ta có hai khả năng: hoặc cả ba nghiệm là số thực, trong trường hợp này ta có nhóm Bốn; hay chỉ có một nghiệm là số thực thì ta có một nhóm cyclic cấp 2.

- Tương tự, nếu ta giới hạn x trên Q, thì ta có hai khả năng, cộng với khả năng S = $\{0\}$, không có nghiệm hữu tỷ.

2.2.5.3 Điểm cấp 3

- Điểm xoắn có cấp 3 là những điểm thỏa mãn 3P = 0 ⇔ 2P = -P sử dụng công thức nhân đôi cho ta thấy giá trị x của 2P dựa trên giá trị x của
P = (x,y). Ta cần 2P = -P = (-x,y) nghĩa là giá trị x của 2P phải bằng với giá trị x của (-P). Vậy ta có biểu thức: $x = \dfrac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$

- Bằng cách nhân chéo và chuyển vế các số hạng, ta thu được một biểu thức đơn giản của x. Ta gọi biểu thức đó là ψ_3 . Vậy: $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + \left(4ac - b^2\right)$

- Những nghiệm của đa thức là giá trị x của điểm có cấp 3.

- Nếu $x \in \mathbb{C}$, ta sẽ có bốn nghiệm phân biệt. Ta biết những nghiệm này phân biệt vì ta có thể dễ dàng nhận thấy rằng $\psi_3(x)$và $\psi_3'(x)$ không có những nghiệm chung . Trong trường hợp chúng có một nghiệm chung thì f(x) và f'(x)có một nghiệm chung , điều này mâu thuẫn với f(x) là không suy biến. Thay bốn nghiệm của $\psi_3(x)$vào đường cong elliptic sẽ cho ta tất cả 8 điểm phân biệt . Với những điểm đó, ta sẽ có 9 điểm cấp 3 gồm 8

điểm đề cập ở trên và điểm tại vô cực O. Khi đó, sẽ có một nhóm giao hoán có cấp 9 với mỗi thành phần có cấp 3, và đó là tích của hai nhóm cyclic có cấp 3.

- Nếu ta hạn chế x trên R, ta sẽ luôn thu được một nhóm cyclic có cấp 3. Nếu $x \in \mathbb{Q}$, ta sẽ chỉ có nhóm cyclic cấp 3 hay nhóm tầm thường $\{0\}$.

- Không quá khó để nhận ra rằng ta có thể sử dụng cách trên khi tìm những điểm xoắn có cấp 3 để tìm những điểm xoắn có cấp cao hơn ba.

2.2.5.4 Định lý Nagell – Lutz

- Số lượng những điểm có cấp vô hạn nhiều hơn điểm có cấp hữu hạn. Điều đó là hiển nhiên khi ta cố gắng tìm hiểu những phần tử trên $C(\mathbb{Q})_{tor}$ bởi các tính toán. Thực tế, đó là điều không tưởng khi tìm kiếm những điểm xoắn của một đường cong bằng phương pháp phỏng đoán và kiểm tra. Định lý sau được đưa ra bởi hai nhà toán học Trygue Nagell (1895-1988) công bố 1935 và Elisabeth Lutz (1937) sẽ giúp cho việc tìm $C(\mathbb{Q})_{tor}$ dễ dàng hơn

Định lý 69 : Cho đường cong $y^2 = f(x) = x^3 + ax^2 + bx + c$. Nếu P = (x,y) là một điểm hữu tỷ có bậc hữu hạn thì khi đó x và y là những số nguyên, và ta có y = 0 (điểm có cấp 2) hay y là ước số của D với D là biệt thức $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$

- Sử dụng định lý này cho ta một cách để tìm tất cả những điểm hữu tỷ có cấp hữu hạn. Một điểm hữu tỷ trên một đường cong elliptic có thể có các hệ số nguyên với y là ước của D và không là điểm hữu tỷ xoắn.

- Có một dạng mạnh hơn của định lý Nagell- Lutz như sau

Định lý 70 : Cho $y^2 = f(x) = x^3 + ax^2 + bx + c$ là một đường cong bậc ba không suy biến với các hệ số nguyên a, b, c và D là biệt thức của đa thức bậc ba f(x), $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Nếu P(x , y) là điểm hữu tỷ có cấp hữu hạn thì x và y là những số nguyên và khi y = 0 thì P có cấp 2 hay y^2 là ước số của D.

- Định lý Nagell – Lutz cho ta một phương pháp để tìm kiếm những điểm hữu tỷ có cấp hữu hạn trên một đường cong elliptic. Quá trình khá đơn giản: tính D và tìm các số nguyên là ước số của D . Đó là tất cả các giá trị có thể của y. Từ đó, ta thay đổi mỗi giá trị

y vào đường cong và tìm được số nguyên x. D càng lớn thì quá trình càng dài. Tuy nhiên , theo định lý Nagell – Lutz vì y^2 là ước số của D , ta chỉ cần chú ý đến những số chính phương là ước số của D thay vì từng số nguyên. Điều đó sẽ loại bớt các giá trị y khi ta thực hiện. Sau khi có được tất cả (x,y) thỏa mãn giả thiết định lý, ta chỉ cần kiểm tra từng cặp số nào thực sự là điểm xoắn.

- Lưu ý rằng định lý Nagell – Lutz không thể dùng để chứng minh một điểm hữu tỷ có cấp hữu hạn, nhưng nó có thể được dùng để chứng minh một điểm hữu tỷ có cấp không hữu hạn.

2.2.5.5 Định lý Mazur

- Định lý Mazur sau đây cho một mô tả cấu trúc của nhóm $C(\mathbb{Q})_{tor}$

Định lý 71: Cho C là một đường cong bậc ba hữu tỷ, không suy biến và giả sử rằng $C(\mathbb{Q})$ chứa một điểm có cấp hữu hạn m thì $1 \leq m \leq 10$ hay m = 12 . Hơn nữa, tập hợp các điểm có cấp hữu hạn trên $C(\mathbb{Q})$ là một nhóm con của $C(\mathbb{Q})$ có dạng sau:

i) Một nhóm cyclic có cấp N với $1 \leq N \leq 12$ hay N = 12

ii) Tích của một nhóm cyclic có cấp 2 và một nhóm cyclic có cấp 2N với $1 \leq N \leq 4$

- Định lý trên chỉ ra rằng sẽ không có điểm hữu tỷ xoắn có cấp lớn hơn 12, không có điểm hữu tỷ xoắn có cấp 11.

2.2.5.6 $\psi_n(x)$

- Giả sử rằng ta đã tìm được tất cả những điểm hữu tỷ xoắn của một cấp nào đó thay vì tìm kiếm tất cả những điểm hữu tỷ xoắn. Mục 2.2.5.2 và 2.2.5.3 đã chỉ ra những điểm xoắn có cấp 2 và 3.

* Với cấp 3 ta dùng

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$$

* Với cấp 2 ta dùng $\psi_2(x) = x^3 + ax^2 + bx + c$ mà những nghiệm tương ứng với những giá trị của đường cong elliptic khi y = 0.

* Từ 4P = 0 => 2P = -2P cho ta

$$\psi_4(x) = 4y\left(x^6 + 5bx^4 + 20cx^3 - 5b^2x^2 - 4bcx - 8c^2 - b^3\right)$$

- Những nghiệm của phương trình $\psi_4(x)=0$ có thể được dùng để tìm những điểm xoắn có cấp 4.

- Khi $\psi_4(x)=0$ cho ta điểm cấp 2 (ứng với y = 0) hay

$x^6+5bx^4+20cx^3-5b^2x^2-4bcx-8c^2-b^3=0$ cho ta điểm có cấp 4.

- Từ đó, ta có thể tìm ra biểu thức $\psi_n(x)$ với mỗi số nguyên n mà nghiệm của $\psi_n(x)$ là những giá trị x của mỗi điểm có bậc n. Nếu n >4, tập hợp các biểu thức đệ quy tiếp tục cho phép ta một cách thức dễ dàng để tính $\psi_n(x)$.

Dùng $\psi_2(x)=2y$ và $\psi_3(x)=3x^4+4ax^3+6bx^2+12cx+(4ac-b^2)$ Ta có :

Định nghĩa 72 :

$$\psi_{2n+1}(x)=\psi_{n+2}(x)\psi_n(x)^3-\psi_{n-1}(x)\psi_{n+1}(x)^3 \text{ với } n\geq 2$$

$$\psi_{2n}(x)=\frac{\psi_n(x)\left[\psi_{n+2}(x)\psi_{n-1}(x)^2-\psi_{n-2}(x)\psi_{n+1}(x)^2\right]}{2y} \text{ với } n\geq 3$$

- Lưu ý ngắn về $\psi_n(x)$: những nghiệm của những đa thức này là những điểm xoắn có cấp n. Những đa thức này chứa cả những điểm hữu tỷ xoắn và không hữu tỷ xoắn của một đường cong được cho. Khi phân tích những đa thức này thành thừa số, ta thấy rằng không có giá trị x nguyên, hay không có nghiệm nguyên dẫn đến giá trị y nguyên. Khi đó sẽ không có điểm hữu tỷ xoắn của cấp đó. Hơn nữa, $\psi_{13}(x)$ sẽ có ít nhất một nghiệm thực, tuy nhiên sẽ không bao giờ có nghiệm nguyên. Đó là kết luận trực tiếp từ định lý Mazur.

2.3 MỘT SỐ THUẬT TOÁN XÁC ĐỊNH ĐIỂM XOẮN HỮU TỶ TRÊN ĐƯỜNG CONG ELLIPTIC

2.3.1 Giới thiệu

- Cho K là một trường số và E là một đường cong elliptic trên K . Theo định lý Mordell- Weil [Sil 86] thì ta có $E(K)$ (nhóm các điểm hữu tỷ trên K) là một nhóm hữu hạn sinh . Điều đó có nghĩa là $E(K)_{tors}$ nhóm các điểm hữu tỷ xóăn trên K là hữu hạn . Bây giờ ta sẽ tập trung vào trường hợp K = $\mathbb{Q}$.Định lý Mazur [Sil 86] giới thiệu cho ta về nhóm $E(K)_{tors}$

- Một phương pháp dùng để tính toán những điểm hữu tỷ xoắn trên đường cong elliptic là dùng định lý Nagell – Lutz [Sil 86] . Điều cốt lõi của phương pháp này là sự phân tích thành thừa số biệt thức của đường cong elliptic và biệt thức này có thể có những ước số chính phương , dẫn đến việc tối ưu tính toán . Phương pháp này không còn phù hợp cho đến khi Doud [Dou 98] phát hiện ra thuật toán thời gian đa thức sử dụng nhiều kỹ thuật giải tích phức tạp và thực hiện theo thời gian bậc ba mà kích cỡ nguồn vào là kích cỡ của hệ số của đường cong elliptic

- Thuật toán " Thời gian bậc hai mềm " (" Mềm " là nơi mà sự phân tích logarith không tồn tại) được phát triển bởi Garcia –Selfa dựa trên việc tính toán trên dạng " Tate " cơ bản của đường cong elliptic .Quá trình đó dùng thuật toán
" Tìm căn bậc hai Loos " và không sử dụng đến bất kỳ điều gì về sự liên quan giữa biệt thức của F_m và biệt thức của đường cong elliptic . Do đó một số nguyên tố khác được dùng để tính những nghiệm của F_m với mỗi m

- Chúng ta cũng chú ý đến mối quan hệ giữa $\Delta(f_m)$ biệt thức của f_m của m - đa thức chia và Δ biệt thức của đường cong elliptic . Với việc sử dụng
Magma và Pari –GP , ta có thể tính toán biệt thức của những đa thức với giá trị m đủ nhỏ mà cho ta sự ước đóan sau :

$$\Delta(f_m)=\begin{cases}(-1)^{\frac{m-1}{2}}\, m^{d-1}\Delta^{\frac{d(d-1)}{6}} & m=2k+1\ ,\ k\in\mathbb{Z}\\ 2^4\, m^{d-4}\Delta^{\frac{d(d-1)}{6}} & m=2k\ ,\ k\in\mathbb{Z}\end{cases}$$

Với d= deg(f_m)

2.3.2 Các đa thức chia

- Cho K là một trường số và $\overline{K}$ là bao đóng đại số của K . Cho E là một đường cong elliptic trên K cho bởi dạng Weierstrass : $y^2=x^3+ax+b$ với $a,b\in\mathbb{R}$ và $\mathbb{R}$ là vành các số nguyên của K

Định lý 73: $E(\overline{K})[m]=(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$ [Sil 86]

- Định nghĩa ψ_m như sau :

$$\psi_1 = 1 \ ; \psi_2 = 2y \ \ ; \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$\psi_4 = \left(2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8abx - 2a^3 - 16b^2\right)\psi_2$$

$$\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3 \qquad k \geq 2$$

$$\psi_{2k} = \frac{\left(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2\right)\psi_k}{\psi_2} \quad k \geq 2$$

- Định nghĩa với $m > 2$: $f_m = \begin{cases} \psi_m & \text{khi } m = 2k+1 \text{ , } k \in \mathbb{Z} \\ \dfrac{\psi_m}{\psi_2} & \text{khi } m = 2k \text{ ,} k \in \mathbb{Z} \end{cases}$

- Tọa độ x của những điểm m –xoắn của E tương ứng với những nghiệm của f_m[BSS 99] . Cho $P \in E\left(\overline{K}\right)$ sao cho P không là điểm xoắn cấp hai . Do đó $P \in E[m] \Leftrightarrow f_m\left(x(P)\right) = 0$

- Giả sử d là bậc của f_m với $d = \dfrac{m^2-1}{2}$ nếu m lẻ và $d = \dfrac{m^2-4}{2}$ nếu m chẵn và hệ số cao nhất của f_m là m nếu m lẻ và $\dfrac{m}{2}$ nếu m chẵn trong đó $m > 2$.

- Giả sử S là miền nguyên với trường thương L và bao đóng đại số $\overline{L}$. Lấy $g \in S[X]$ với n là bậc của g và $lc(g)$ là hệ số cao nhất . Giả sử α_i là những nghiệm của g trong $\overline{L}$ .Ta định nghĩa biệt thức của g là : $\Delta(g) = \dfrac{(-1)^{\frac{n(n-1)}{2}}.R(g,g')}{l(g)}$ Với R(g , g') là tích chập của g và g' .

Ta có : $\Delta(g) = lc(g)^{n-1+\deg(g')}.\prod_{1 \leq i < j \leq n}\left(\alpha_i - \alpha_j\right)^2$

- Cho $f = x^3 + ax + b$ và $\Delta(f) = -\left(4a^3 + 27b^2\right)$, thì biệt thức của đường cong elliptic được xác định là : $\Delta(E) = -16\left(4a^3 + 27b^2\right)$. Từ đây , ta sẽ luôn giả thiết rằng E là một đường cong elliptic trên $\mathbb{Q}$ được cho bởi $y^2 = x^3 + ax + b$ với $a, b \in \mathbb{Z}$. Điều đó dẫn đến

các đa thức chia có hệ số nguyên và biệt thức $\Delta(f_m) \in \mathbb{Z}$, điều này là rõ ràng do định định nghĩa các biệt thức dưới dạng ma trận Sylvester [Coh 00]

Bổ đề 74 : Cho m = 2k + 1 > 1 là số nguyên , ta có

1. $f \mid f'_m$
2. $2^2 \mid f'_m$
3. $m \mid \psi'_m$
4. $m^{d-1} \mid \Delta(f_m)$

Chứng minh :

1) Ta có $f'_3 = 12f$: bổ đề đúng . Ta chứng minh cho trường hợp các chỉ số lẻ (trường hợp chỉ số chẵn tương tự)

- Giả sử $f \mid f'_i$ với mọi i lẻ và i < m . Cho k là một số lẻ , ta có

$\psi_{2k+1} = f_{2k+1} = f_{k+2}f_k^3 - (f_{k-1}\psi_2)(f_{k+1}\psi_2)^3 = f_{k+2}f_k^3 - f_{k-1}f_{k+1}^3\psi_2^4 = f_{k+2}f_k^3 - 2^4 f_{k-1}f_{k+1}^3 f^2$ Mặt khác $f'_{2k+1} = f'_{k+2}f_k^3 + 3f_{k+2}f_k^2f'_k - 2^4\left(f_{k-1}f_{k+1}^3\right)' f^2 - 2^5 f_{k-1}f_{k+1}^3 ff'$

f chia hết f'_{k+2} và f'_k do giả thiết quy nạp , do đó f chia hết mỗi hệ số trong f'_{2k+1} . Đặc biệt f chia hết f'_{2k+1} , trái lại f_{2k+1} sẽ có các nghiệm lặp

2) Chứng minh tương tự 1

3) Cho mỗi giá trị m , thì $m \mid \left(\psi_m^2\right)'$ và $p \not\mid \psi_m^2$ với p là số nguyên tố lẻ

[Cas 49]. Giả sử $m = \prod_i p_i$ với p_i là số nguyên tố lẻ . Do ở phần trên $m \mid \psi_m\psi'_m$ nên $p_i \mid \psi_m\psi'_m$ và do đó cũng có $p_i \not\mid \psi_m$. Do đó $p_i \mid \psi'_m$ và $m \mid \psi'_m$

4) Từ phần 3 , ta có $lc(f_m) = m$ và định nghĩa của các biệt thức , các hệ số f'_m được lặp lại trong $\frac{m^2-1}{2}$ dòng

Bổ đề 75 : Cho m = 2k > 2 là số nguyên thì :

1. $k \mid \Delta(f_m)$
2. $2^2 \mid f'_m$
3. $m \mid \Delta(f_m)$

Chứng minh :

1) Ta có : $lc(f_m) = k$ và hệ số của x^{d-1} của f_m là 0 .Xét ma trận kết hợp $R(f_m, f'_m)$. Cột đầu tiên của ma trận có giá trị là k tại vị trí (1;1) và $k\frac{m^2-4}{2}$ tại $\left(\frac{m^2-4}{2}, 1\right)$ và 0 tại các vị trí còn lại . Cột thứ 2 có giá trị là k tại vị trí (2,2) và $k\frac{m^2-4}{2}$ tại vị trí $\left(\frac{m^2-4}{2}+1, 2\right)$ và 0 tại các vị trí khác . Do đó $k^2 \mid R(f_m, f'_m)$ và $k \mid \Delta(f_m)$ do định nghĩa biệt thức .

2)

- Ta có $2^2 \mid f'_4$: bổ đề đúng với trường hợp cơ bản

- Giả sử $2^2 \mid f'_i$ với i chẵn , i < m . Bây giờ

$$f'_{2k} = \left(f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2\right)f'_k + \left(f'_{k+2}f_{k-1}^2 + f_{k+2}.2.f_{k-1}f'_{k-1} - f'_{k-2}f_{k+1}^2 - f_{k-2}.2.f_{k+1}f'_{k+1}\right)f_k$$

Giả sử rằng k lẻ (tương tự cho trường hợp k chẵn) , từ bổ đề trên ta biết 2^2 chia hết $f'_k; f'_{k+2}; f'_{k-2}$. Do giả thiết quy nạp , 2^2 cũng chia hết f'_{k-1}, f'_{k+1} .

Do đó $2^2 \mid f'_m$

Bổ đề 76 : Giá nguyên tố của $\Delta(f_m)$ = giá nguyên tố của m $\cup$ giá nguyên tố của Δ , với m > 2 là số nguyên

Chứng minh : Ta có 2 và m chia hết $\Delta(f_m)$. Do đó ta chỉ cần chứng minh rằng khi (m ; p) = 1 thì giá nguyên tố của $\Delta(f_m)$ bằng với tập hợp những số nguyên tố mà E có sự rút gọn xấu trên $\mathbb{Q}$

- Cho E là 1 đường cong elliptic trên $\mathbb{Q}_p$. Cho L là sự mở rộng hữu hạn của $\mathbb{Q}_p$. Cho $\rho = (\pi)$ là số nguyên tố trong p vành các số nguyên của L , F_ρ là trường phần dư và e là

chỉ số rẽ nhánh

- Giả sử $x = u^2 x' + r\ ;\ y = u^3 y' + su^2 x' + t$ là phép đổi tọa độ được cho bởi dạng Weierstrass thu gọn đối với E/L xác định bởi E' .Biệt thức Δ' của E' thỏa mãn $v_\rho(\Delta') = v_\rho\left(u^{-12}\Delta\right)$

- Giả sử x_i và x_i' , $1 \le i \le d$ là những nghiệm của đa thức m - chia kết hợp với E và E' tương ứng . Với $i \ne j$, ta có

$$v_\rho\left(x_i' - x_j'\right) = v_\rho\left(\frac{x_i - r}{u^2} - \frac{x_j - r}{u^2}\right) = v_\rho\left(\frac{x_i - x_j}{u^2}\right)$$

Do đó $v_\rho\left(x_i - x_j\right) = 2v_\rho(u) + v_\rho\left(x_i' - x_j'\right)$

- Kế tiếp , ta xét giá trị của biệt thức của đa thức m- chia bậc m liên kết của E trên $\mathbb{Q}_p$

$$v_\rho\left(\Delta(f_m)\right) = (2d-2)\,v_\rho\left(lc(f_m)\right) + 2\sum_{1\le i<j\le d}\left(2v_\rho(u) + v_\rho\left(x_i' - x_j'\right)\right)$$

- Vậy , ta có thể giả sử rằng (m , p) = 1 , chú ý rằng $v_\rho(.) = ev_\rho(.)$. Vì $v_\rho(m) = 0$, ta có $v_\rho\left(lc(f_m)\right) = v_\rho(m) = 0$ khi m lẻ và $v_\rho\left(lc(f_m)\right) = v_\rho\left(\frac{m}{2}\right) = 0$ khi m chẵn

Trường hợp 1 : Cho E là một đường cong elliptic mà có sự rút gọn tốt trên $\mathbb{Q}_p$. Đặt $L = \mathbb{Q}_p\left(E\left(\overline{\mathbb{Q}_p}\right)[m]\right)$ là một mở rộng hữu hạn của $\mathbb{Q}_p$ sao cho trên đó E có sự rút gọn tốt [Sil 94] nghĩa là $v_\rho(\Delta') = 0$ và $v_\rho(u) = \frac{v_\rho(\Delta)}{12}$

Hơn nữa , ánh xạ thu gọn đồng dư $\rho : E(L)[m] \to \overline{E}\left(F_\rho\right)[m]$ là phép nhúng [Sil 86] (mệnh đề VII.3.1) và do đó $v_\rho\left(x_i' - x_j'\right) = 0$ với $i \ne j$ và ta có $v_\rho\left(\Delta(f_m)\right) = \frac{d(d-1)}{6}v_\rho(\Delta)$

Do đó , nếu p là số nguyên tố cho sự thu gọn tốt trên $E/\mathbb{Q}$ thì $p \not| \Delta(f_m)$ và nếu p là số nguyên tố của sự thu gọn không tốt thì $p | \Delta(f_m)$

Trường hợp 2 : Cho E là một đường cong elliptic với sự thu gọn tích trên $\mathbb{Q}_p$. Cho $L \supset \mathbb{Q}_p\left(E\left(\overline{\mathbb{Q}_p}\right)[m]\right)$ là một mở rộng hữu hạn của $\mathbb{Q}_p$ sao cho E có sự thu gọn tích nghĩa là $v_\rho(\Delta') > 0$ và $v_\rho\left(c_4'\right) = 0$. Ta biết rằng $v_\rho\left(c_4'\right) = v_\rho\left(u^{-4}c_4\right)$ nên $v_\rho(u) = \frac{v_\rho(c_4)}{4}$. Do đó $j = \frac{c_4^3}{\Delta}$ và

$$v_\rho(c_4) = \frac{1}{3}\left(v_\rho(\Delta) + v_\rho(j)\right)$$

$$v_\rho\left(\Delta(f_m)\right) = \frac{d(d-1)}{6}\left(v_\rho(\Delta) + v_\rho(j)\right) + \sum_{1\le i<j\le d} 2v_\rho\left(x_i^{\cdot} - x_j^{\cdot}\right) \ge 0$$

Bây giờ , $v_\rho(\Delta) + v_\rho(j)$ phụ thuộc vào E có sự thu gọn tích hay tổng trên $\mathbb{Q}_p$. Trong mỗi trường hợp thì luôn tồn tại i và j sao cho $v_\rho\left(x_i^{\cdot} - x_j^{\cdot}\right) > 0$. Do đó $v_\rho\left(\Delta(f_m)\right) > 0$. Do đó nếu p là số nguyên tố của sự rút gọn không tốt (tích hay tổng) của E trên $\mathbb{Q}$ thì $p \mid \Delta(f_m)$

2.3.3 Thuật toán

Định lý 77 : [Sil 86] (Nagell- Lutz) Cho E là một đường cong elliptic trên $\mathbb{Q}$với dạng Weierstrass $y^2 = x^3 + ax + b$ với $a; b \in \mathbb{Z}$. Giả sử rằng $O \ne P \in E(\mathbb{Q})_{tors}$ thì x(P) , y(P) $\in \mathbb{Z}$ và y(P) = 0 hay $y(P)^2 \mid \left(4a^3 + 27b^2\right)$

Định lý 78 : [Sil 86] (Mazur)

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \le n \le 10 \text{ ; } n = 12 \quad \text{(i)} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \le n \le 4 \quad \text{(ii)} \end{cases}$$

- Giả sử $P \in E(\mathbb{Q})_{tors}$ thi x(P) là nghiệm của $x^3 + ax + b - y(P)^2$ và do Nagell – Lutz ta có $y(P)^2 \mid \left(4a^3 + 27b^2\right)$ dẫn đến $x(P) \mid \left(b - \frac{4a^3 + 27b^2}{k}\right)$ với

$k \in \mathbb{Z}$. Do đó , tọa độ của những điểm xoắn là O(C) với C= $\max\left(\left|a^3\right|, \left|b^2\right|\right)$

- Sau đây là bổ đề Hensel :

Bổ đề 79 : Cho $u \in \mathbb{Z}_p$ và $h \in \mathbb{Z}_p[x]$, lấy k thỏa $p^k \mid h'(u)$ và giả sử rằng $p^{n+k} \mid h(u)$ với n > k Đặt $\delta = \dfrac{p^{-k}h(u)}{p^{-k}h'(u)}$ và $v = u - \delta$ thì

$$v \equiv u \bmod p^n \ ; \ p^{2n} \mid h(v) \ ; \ p^k \mid h'(v)$$

Bổ đề trên đã dẫn đến một phương pháp hiệu quả để tìm ra những điểm được tạo từ những nghiệm của đa thức mà đảm bảo rằng quá trình sẽ không tốn quá nhiều thời gian (softly – linear time)

- Như đã trình bày ở phần giới thiệu , thuật tóan được thực hiên như sau : Cho một đường cong elliptic E trên $\mathbb{Q}$, ta xem nó như là một đường cong trên $\mathbb{Q}_l$ và tìm những điểm m – xoắn $\mathbb{Q}_l$ - hữu tỷ và sau đó ta kiểm tra xem chúng có thuộc $E(\mathbb{Q})$. Số nguyên tố l được chọn sao cho sự thu gọn E trên $\mathbb{Q}_l$ là tốt . Những số nguyên m được chọn dựa trên định lý Mazur là : 2 ,3 , 4, 5 ,7 , 8, 9

Giả sử rằng ta muốn tính nghiệm của các đa thức m - chia . Nếu l > 2 là một số nguyên tố và l m thì bổ đề trên cho ta những nghiệm của f_m là phân biệt đồng dư l .Với bổ đề Hensel , ta có thể lấy ra một nghiệm F_l của f_m trên $\mathbb{Q}_l$ với k = 0 .Trong trường hợp nếu p là số nguyên tố tốt cho sự thu gọn và $p^i \mid m$ thì ta có thể lấy một nghiệm F_p của f_{p^i} và dùng bổ đề Hensel với k = i [Sat 00]

Bổ đề 80: Cho E là một đường cong ordinary trên $\mathbb{Q}_p$ cho bởi dạng Weierstrass $y^2 = x^3 + ax + b$ có sự thu gọn tốt tại p với p > 2 và $ab \neq 0$. Giả sử $E\left(\mathbb{Q}_p^{ur}\right)\left[p^i\right] \neq O$. Nếu $P \in E\left(\mathbb{Q}_p^{ur}\right)\left[p^i\right]$ là một điểm không tầm thường thì $v_p\left(\partial\psi_{p^i}\left(x(P)\right)\right) = i$.

- Bổ đề trên đóng vai trò quan trọng trong thuật tóan . Nếu số nguyên tố được chọn là 3 , 5, 7 thì ta tính được điểm 3 ,9 ,5, 7 – xoắn .

- Bổ đề được dùng cho những đường cong elliptic ordinary do đó trước khi áp dụng bổ đề , ta phải loại bỏ những trường hợp supersingular . Quá trình dưới đây là cách để kiểm tra tính supersingular [BSS 99]: Cho E là một đường cong elliptic trên $\mathbb{Q}_p$ mà có sự thu gọn tốt tại p . E supersingular nếu

* $p \geq 5$ và $\#\overline{E}(F_p) = p + 1$

* p =2, 3 và $\#\overline{E}(F_p) = 1, p + 1, 2p + 1$

Thuật tóan :

Đầu vào : Cho một đường cong elliptic E có dạng $y^2 = x^3 + ax + b$ với $a; b \in \mathbb{Z}$

Đầu ra : $\langle T; t \rangle_i$ với $T \in E(\mathbb{Q})[t]$ và i = 1 ;2 và những điểm sinh của $E(\mathbb{Q})_{tors}$

1. Chọn một số nguyên tố $l > 2$ và $l \quad \Delta$

2. Dùng f tính $E(\mathbb{Q}_l)[2]$ ✗

3. $r \leftarrow \#E(\mathbb{Q})[2] - 1$. Lấy R_1 ….R_r là tọa độ x của những điểm không tầm thường

4. Nếu r = 0 thì

(a) Cho p = 3 , 5 , 7 và thực hiện như sau :

(i) Nếu p ✗ $\#\overline{E}(F_l)$ thì quay trở lại bắt đầu của quá trình lặp và thực hiện lại với số nguyên tố kế tiếp

(ii) Dùng f_p tính $Q \in E(\mathbb{Q}_l)[p] \setminus \{O\}$

(iii) Nếu $Q \notin E(\mathbb{Q})$ thì quay trở lại bắt đầu của quá trình lặp và thực hiện lại với số nguyên tố kế tiếp

(iv) Nếu p = 5 , 7 trở lại $\langle Q, p \rangle$

(v) Nếu $3^2 \mid \#\overline{E}(F_l)$ thì

+ Dùng f_9 tính $S \in E(\mathbb{Q}_l)[9] \setminus E(\mathbb{Q}_l)[3]$. Nếu $S \notin E(\mathbb{Q})$ thì trở lại $\langle Q; 3 \rangle$ và trái lại thì quay về $\langle S; 9 \rangle$

+ Trường hợp khác trở lại $\langle Q; 3 \rangle$

(b) Trở lại $\langle O; 1 \rangle$

5. Nếu r = 1 thì

(a) Với p = 3 , 5 thực hiện như sau :

(i) Nếu p ✗ $\#\overline{E}(F_l)[p]$ thì quay trở lại điểm bắt đầu của quá trình lặp và thực hiện lại với số nguyên tố kế tiếp

(ii) Dùng f_p tính $Q \in E(\mathbb{Q}_l)[p] \setminus \{0\}$

(iii) Nếu $Q \notin E(\mathbb{Q})$ thì quay trở lại điểm bắt đầu của quá trình lặp và thực hiện lại với số nguyên tố kế tiếp

(iv) $U \leftarrow R_1 + Q$

(v) Nếu p = 5 ,7 trở lại $\langle U, 10 \rangle$

(vi) Nếu $4 \nmid \#\overline{E}(F_l)$ thì trở lại $\langle U, 6 \rangle$

(vii) Dùng f_4 tính $V \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$

(viii) Nếu $V \in E(\mathbb{Q})$ thì

+ Trở lại $\langle V + Q, 12 \rangle$

+ Hoặc trở lại $\langle U, 6 \rangle$

(b) Nếu $4 \nmid \#\overline{E}(F_l)$ thì trở lại $\langle R_1, 2 \rangle$

(c) Dùng f_4 tính $W \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$

(d) Nếu $W \in E(\mathbb{Q})$ thì

+ Nếu $8 \nmid \#\overline{E}(F_l)$ thì trở lại $\langle W, 4 \rangle$

+ Dùng f_8 tính $Z \in E(\mathbb{Q}_l)[8] \setminus E(\mathbb{Q}_l)[4]$

+ Nếu $Z \in E(\mathbb{Q})$ thì

* Trở lại $\langle Z, 8 \rangle$

* Hoặc trở lại $\langle W, 4 \rangle$

(e) Trở lại $\langle R_1, 2 \rangle$

6. Nếu r = 3 thì

(a) Thực hiện như sau :

(i) Nếu $3 \nmid \#\overline{E}(F_l)$ thì thoát vòng lặp

(ii) Dùng f_3 tính $Q \in E(\mathbb{Q}_l)[3] \setminus \{0\}$

(iii) Nếu $Q \in E(\mathbb{Q})$ thì

A . $U \leftarrow R_1 + Q$

B. Trở lại $\langle U,6\rangle$ và $\langle R_2,2\rangle$

(b) Thực hiện như sau :

(i) Nếu $8 \not| \#\overline{E}(F_l)$ thì trở lại $\langle R_1,2\rangle$ và $\langle R_2,2\rangle$

(ii) Dùng f_4 tính $W \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$

(iii) Nếu $W \in E(\mathbb{Q})$ thì

* Nếu $16 \not| \#\overline{E}(F_l)$ thì trở lại $\langle W,4\rangle$ và $\langle R_2,2\rangle$

* Dùng f_8 tính $Z \in E(\mathbb{Q}_l)[8] \setminus E(\mathbb{Q}_l)[4]$

* Nếu $Z \in E(\mathbb{Q})$ thì

- Trở lại $\langle Z,8\rangle$ và $\langle R_2,2\rangle$

- hay trở lại $\langle W;4\rangle$ và $\langle R_2;2\rangle$

(c) Trở lại $\langle R_1,2\rangle$ và $\langle R_2,2\rangle$

Bổ đề 81 : Thuật tóan là thỏa yêu cầu

Chứng minh : Nếu $\#E(\mathbb{Q})[2] = 4$ thì do định lý 78 , chúng là trường hợp (ii) của Mazur .Ngược lai nếu trường hợp (ii) xảy ra thì do giả thiết $\#E(\mathbb{Q})[2] = 1,2$ dẫn đến mâu thuẫn

- Chọn số nguyên tố l > 2 sao cho E có sự thu gọn tốt tại l và do đó ánh xạ thu gọn $E(\mathbb{Q}_l)[m] \to \overline{E}(F_l)[m]$ là phép nhúng với tất cả m thỏa

(m ,l) = 1 [Sil 86] . Hơn nữa ánh xạ $E(\mathbb{Q})[p] \to E(\mathbb{Q}_l)[p]$ là phép nhúng

- Do đó trước tiên chúng ta tính những điểm trên $E(\mathbb{Q}_l)[2]$ và kiểm tra xem nếu chúng ta có 1, 2, 4 điểm trên $E(\mathbb{Q})[2]$.

2.3.4 Sự phân tích thời gian hoàn thành :

- Cho M(N) là các toán tử bít cần thiết để thực hiện phép nhân hai số có kích cỡ N . Chúng ta giả sử rằng thuật tóan nhân số nguyên nhanh nhất giống như Schonhage – Strassen [GG 99] được dùng trong trường hợp M(N) = O(NlogNloglogN) = O(N)

- Một số nguyên có kích cỡ N có thể được biểu diễn p –adically bằng cách dùng đệ quy để tìm ra sự chuyển đổi cơ số [GG 99] trên thời gian $0\left(M\left(N\log p\right)\log N\right)$

- Để tìm ra số nguyên tố l , ta tính f và những đa thức m- chia với m = 3, 4, 5, 7, 8, 9 và kích cỡ của các hệ số của những đa thức bị giới hạn bởi $O\left(\log C\right) = O\left(\log \Delta\right)$

- Trong trường hợp độ lớn của số nguyên tố này là $O\left(\log \Delta\right)$ thì thời gian để tính $\#\overline{E}(F_l)$ là không đáng kể và nghiệm F_l – hữu tỷ của các đa thức chia là $O\left(\log \Delta\right)$

- Khi ta tìm được một nghiệm gần đúng ta dùng phép nâng Hensel để tính chính xác $\mathbb{Q}_l$ - hữu tỷ .

2.3.5 Biệt thức của các đa thức DIV :

- Khi tính toán biệt thức của các đa thức m - chia , ta tìm được một công thức được biểu thị qua $\Delta\left(f_m\right)$, hệ số m ,và biệt thức của đường cong elliptic E

- Dùng Magma chạy trên PentiumIV 1.80Ghz ; 128MB Ram ; Windows XP , ta tính được biệt thức theo bảng sau :

m	d	$\Delta\left(f_m\right)$	Thời gian
3	4	$-3^3\Delta^2$	0
4	6	$2^4.4^2\Delta^5$	0
5	12	$5^{11}\Delta^{22}$	0.047s
6	16	$2^4 6^{12}\Delta^{40}$	0.234s
7	24	$-7^{23}\Delta^{92}$	7.407s
8	30	$2^4 8^{26}\Delta^{145}$	1ph 0.437s
9	40	$9^{39}\Delta^{260}$	15ph 56.953s
10	48	$2^4 10^{44}\Delta^{376}$	1h 34ph 37.984s

11	60	$-11^{59}\Delta^{590}$	13h 15ph 27.812s
12	70	$2^4 12^{66}\Delta^{805}$	50h 36ph 25.907s

- Dựa vào trên , ta có giả thuyết sau :

$$\Delta(f_m)=\begin{cases}(-1)^{\frac{m-1}{2}}\, m^{d-1}\Delta^{\frac{d(d-1)}{6}} & \text{khi } m = 2k+1 \text{ , } k \in \mathbb{Z} \\ 2^4 m^{d-4}\Delta^{\frac{d(d-1)}{6}} & \text{khi } m = 2k \text{ , } k \in \mathbb{Z}\end{cases}$$

Dựa trên bổ đề 76 , ta thấy rằng , giả thuyết trên xảy ra khi (m , p) = 1 và E là đường cong elliptic có sự thu gọn tốt trên $\mathbb{Q}_p$ .Dưa trên đó , ta thu được vài kết quả như trên [BH 05]

Bổ đề 82 : Giả thuyết trên đúng khi m = p là số nguyên tố lẻ và E là một đường cong elliptic thu gọn tốt trên $\mathbb{Q}_p$

Chứng minh: Cho $L=\mathbb{Q}_p\left(E\left(\overline{\mathbb{Q}_p}\right)[m]\right)$ là sự mở rộng hữu hạn của $\mathbb{Q}_p$ sao cho trên đó E có sự thu gọn tốt nghĩa là $v_p(\Delta')=0$ và $v_p(u)=v_p(\Delta)/12$ và $lc\left(f_p\right)=p$

Trường hợp 1 : Gỉa sử $\overline{E}$ trên F_p là một đường cong elliptic siêu kỳ dị . Khi đó $\overline{E}\left(F_p\right)=0$ và $E_1(L)[p]\cong E(L)[p]$

- Cho t_i là những tọa độ địa phương của những điểm mà tọa độ x là x_i' và tọa độ y là dương . Xét các hệ số t_i ta biết rằng $x_i'=t_i^{-2}-a't_i^2+0\left(t_i^3\right)$ và $y_i'=-t_i^{-3}+a't_i+0\left(t_i^2\right)$. Do đó

$$v_p\left(x_i'-x_j'\right)=v_p\left(t_i^{-2}-t_j^{-2}\right)=v_p\left(t_i-t_j\right)+v_p\left(t_i+t_j\right)-2v_p\left(t_i\right)-2v_p\left(t_j\right)$$

- Với mỗi i , ta có $v_p(t_i) > 0$ vì những tham số địa phương là những phần tử của một nhóm đường cong elliptic tức là phần tử của ideal tối đại của vành các số nguyên của L . Ta biết $t_i \neq \pm t_j; 1\le i<j\le\frac{m^2-1}{2}$ và

$v_p(t_i) = \frac{e}{p^2-1} = \frac{e}{2d}$ với mọi i [BG 03] , và ta có $t_i \oplus t_j = t_i + t_j$ + hệ số của bậc cao hơn của những hạng tử này . Do đó $v_p(t_i \oplus t_j) = v_p(t_i + t_j)$ vì gía trị của các hệ số bậc cao hơn thực sự tất cả những giá trị còn lại . Tương tự như thế $v_p(t_i \ominus t_j) = v_p(t_i - t_j)$.

Do đó $v_p(x_i' - x_j') = \frac{(-2)e}{2d} = -\frac{e}{d}$

- Ta có

$$v_p(\Delta(f_p)) = (2d-2)v_p(p) + \frac{d(d-1)}{6}v_p(\Delta) + 2\sum_{1\le i<j\le d} v_p(x_i' - x_j')$$

$$= (2d-2)e + \frac{d(d-1)}{6}v_p(\Delta) + 2d(d-1)\frac{-e}{2d} = (d-1)e + \frac{d(d-1)}{6}v_p(\Delta)$$

- Do đó $v_p(\Delta(f_p)) = d-1+\frac{d(d-1)}{6}v_p(\Delta)$

Trường hợp 2 : Cho $\overline{E}$ trên F_p là một đường cong elliptic ordinary . Do đó $\overline{E}(F_p)[p] = \mathbb{Z}/p\mathbb{Z}$ và dãy khớp ngắn $0 \to E_1(L)[p] \to E(L)[p] \to \overline{E}(F_p)[p] \to 0$ là đẳng cấu với dãy ngắn $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$

- Đặt $\langle Q \rangle = E_1(L)[p]$ và $P \in E(L)[p] \setminus E_1(L)[p]$ thì

$$\psi_p(X) = \prod_{1\le i\le \frac{p-1}{2}} (X - x(iQ)) \prod_{1\le i\le \frac{p-1}{2}; 0\le j\le p-1} (X - x(iP + jQ))$$

- Cho t_i là tham số địa phương của điểm iQ , ta có $v_p(t_i) = \frac{e}{p-1}$ [BG 03] . Do đó :

$$x(iP+jQ)=\left(\frac{(y(jQ)-y(iP))}{(x(jQ)-x(iP))}\right)^2-x(iP)-x(jQ)$$

$$=\left(\frac{-t_j^{-3}+a't_j+0(t_j^2)-y(iP)}{t_j^{-2}-a't_j^2+0(t_j^3)-x(iP)}\right)^2-x(iP)-t_j^{-2}+a't_j^2+0(t_j^3)$$

$$=t_j^{-2}\left(\frac{-1-y(iP)t_j^3+a't_j^4+0(t_j^5)}{1-x(iP)t_j^2-a't_j^4+0(t_j^5)}\right)^2-x(iP)-t_j^{-2}+a't_j^2+0(t_j^3)$$

$$=t_j^{-2}+2x(iP)+2y(iP)t_j+3x(iP)^2t_j^2+4x(iP)y(iP)t_j^3+....-x(iP)-t_j^{-2}+a't_j^2+0(t_j^3)$$

$$=x(iP)+2y(iP)t_j+3x(iP)^2t_j^2+a't_j^2+0(t_j^3)$$

- Ta xét : $\sum_{1\le i<j\le d}2v_p(x_i'-x_j')$

1) $\sum_{1\le i<j\le\frac{p-1}{2}}2v_p(x(iQ)-x(jQ))=2(-2)\frac{e}{p-1}\frac{(p-1)(p-3)}{2^3}$

2) $\sum_{1\le i;j\le\frac{p-1}{2};0\le k\le p-1}2v_p(x(iQ)-x(jP+kQ))=2(-2)\frac{e}{p-1}.\frac{(p-1)^2p}{2^2}$

3) $\sum_{1\le i\le\frac{p-1}{2};0\le j_1<j_2\le p-1}2v_p(x(iP+j_1Q)-x(iP+j_2Q))=2.\frac{e}{p-1}.\frac{p(p-1)^2}{2^2}$

4) $\sum_{1\le i_1<i_2\le\frac{p-1}{2};0\le j_1<j_2\le p-1}2v_p(x(i_1P+jQ)-x(i_2P+jQ))=0$

5) $\sum_{1\le i_1<i_2\le\frac{p-1}{2};0\le j_1<j_2\le p-1}2v_p(x(i_1P+j_1Q)-x(i_2P+j_2Q))=0$

6) $\sum_{1\le i_1<i_2\le\frac{p-1}{2};0\le j_2<j_1\le p-1}2v_p(x(i_1P+j_1Q)-x(i_2P+j_2Q))=0$

Ta có :

$$* \quad \sum_{1\le i<j\le d} 2v_p\left(x_i^{'} - x_j^{'}\right)$$

$$= 2(-2)\frac{e}{p-1}.\frac{(p-1)(p-3)}{2^3} + 2(-2)\frac{e}{p-1}.\frac{(p-1)^2 p}{2^2} + 2\frac{e}{p-1}.\frac{(p-1)^2 p}{2^2}$$

$$= -(d-1)e$$

$$* \quad v_p\left(\Delta\left(f_p\right)\right) = (2d-2)v_p(p) + \frac{d(d-1)}{6}v_p(\Delta) + 2\sum_{1\le i<j\le d} v_p\left(x_i^{'} - x_j^{'}\right)$$

$$= (2d-2)e + \frac{d(d-1)}{6}v_p(\Delta) - (d-1)e = (d-1)e + \frac{d(d-1)}{6}v_p(\Delta)$$

Do đó $v_p\left(\Delta\left(f_m\right)\right) = d - 1 + \frac{d(d-1)}{6}v_p(\Delta)$

Bổ đề được chứng minh

2.4 MỘT SỐ CÁC KẾT QUẢ TRÊN CÁC ĐƯỜNG CONG ĐẶC BIỆT

Thí dụ 38 :

- Cho đường cong $y^2 + y = x^3 - x^2 - 10x - 20$. Ta sẽ biến đổi lại

$$y^2 + y = \left(y + \frac{1}{2}\right)^2 - \frac{1}{4} = x^3 - x^2 - 10x - 20$$

- Cộng $\frac{1}{4}$ vào các vế và thay $Y = y + \frac{1}{2}$, ta thu được

$$Y^2 = x^3 - x^2 - 10x - 20 + \frac{1}{4}$$

- Viêc đổi biến này dẫn đến việc thay đổi hệ trục mà hệ trục mới Y bằng trục cũ cộng thêm $\frac{1}{2}$. Thực hiện sự thay đổi $\bar{y} = d^3 Y$ và $\bar{x} = d^2 x$. Thay $Y = d^{-3}\bar{y}$ và $x = d^{-2}\bar{x}$, ta có

$$d^{-6}\bar{y}^2 = d^{-6}\bar{x}^3 - d^{-4}\bar{x}^2 - 10d^{-2}\bar{x} - 20 + \frac{1}{4}$$

Từ đây , nhân thêm d^6 vào toàn bộ biểu thức , ta thu được :

$$\bar{y}^2 = \bar{x}^3 - d^2\bar{x}^2 - 10d^4\bar{x} - 20d^6 + \frac{d^6}{4}$$

Cho d = 2 , ta thu được : $\bar{y}^2 = \bar{x}^3 - 4\bar{x}^2 - 160\bar{x} - 1264$

Thí dụ 39 :

- Tìm $C(\mathbb{Q})_{tor}$ đối với đường cong $y^2 = x^3 + 4$ (a = 0,b= 0,c =4, D= 432)

- Những giá trị có thể của y là $\{0,1,-1,2,-2,3,-3,4,-4,6,-6,12,-12\}$

$0 \Rightarrow 0 = x^3 + 4 \Rightarrow x^3 = -4 \Rightarrow x \notin \mathbb{Z} \Rightarrow$ không có điểm ứng với y = 0

$\pm 1 \Rightarrow 1 = x^3 + 4 \Rightarrow -3 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow$ không có điểm ứng với y = ± 1

$\pm 2 \Rightarrow 4 = x^3 + 4 \Rightarrow x^3 = 0 \Rightarrow x = 0 \Rightarrow$ (0 ;2) và (0 ; -2)

$\pm 3 \Rightarrow 9 = x^3 + 4 \Rightarrow 5 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow$ không có điểm ứng với y = ± 3

$\pm 4 \Rightarrow 16 = x^3 + 4 \Rightarrow 12 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow$ không có điểm ứng với y = ± 4

$\pm 6 \Rightarrow 36 = x^3 + 4 \Rightarrow 32 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow$ không có điểm ứng với y = ± 6

$\pm 12 \Rightarrow 144 = x^3 + 4 \Rightarrow 140 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow$ không có điểm ứng với y = ± 12

Tất cả những điểm có thể là : $(0,2) \to 2(0,2) = (0,-2) \Rightarrow 2P = -P \Rightarrow$ cấp 3

$(0,-2) \to 2(0,-2) = (0,2) \Rightarrow 2P = -P \Rightarrow$ cấp 3.

O $\to$ cấp 1.

Do đó $C(\mathbb{Q})_{tor} = \{O ; (0 ,2);(2,-2)\}$.

Cấu trúc của $C(\mathbb{Q})_{tor}$ là một nhóm cyclic cấp 3.

KẾT LUẬN

Ngoài phần kiến thức chuẩn bị và một số nội dung trình bày các phương pháp mô tả đường cong Elliptic theo các quan điểm khác nhau , trong Luận văn đã tiếp cận một số ý tưởng khai thác các đặc trưng định tính của đường cong Elliptic được mô tả qua các định lý Nagell – Lutz , Mordell – Weil và Mazur để tìm hiểu phương pháp xây dựng thuật toán xác định các điểm hữu tỷ xoắn trên đường cong Elliptic

TÀI LIỆU THAM KHẢO

[Ber] D. J. Bernstein, *Detecting perfect powers in essentially linear time*. Math. Comp. 67 (1998), no. 223, 1253-1283.

[BG 03] J. Boxall and D. Grant . Singular torsion point. *Mathematical Research Letters* , 10, 2003

[BH 05] I.A. Burhanuddin and M-D Huang . *Discriminant of the vision polynomial of an elliptic curve* . Preprint , 2005

[Bo] E. Bombieri, *The Mordell conjecture revisited*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 17 (1990), no. 4, 615-640. Errata-corrige: "*The Mordell conjecture revisited*". Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 18 (1991), no. 3, 473

[BSS 99] I.Blake , G. Seroussi and N . Smart *Elliptic Curves in Cryptography* , Cambride University Press , Cambride , 1999

[Cas 49] J.W .S Cassels . *A note on the division values of p(u)* , Proc of Cambride Philos , Soc 45: 167 – 172 , 1949

[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.

[Coh 00] Cohen . *A Course in Computational Algebraic Number Theory* , Springer – Verlag , Berlin , 2000

[Cr] J. E. Cremona, *Algorithms for modular elliptic curves. Second edition*. Cambridge University Press, Campridge, 1997.

[Dou 98] D.Doud . *A procedure to calculate torsion of elliptic curves over* $\mathbb{Q}$, Manuscripta Mathematica , 96 : 463 – 469 . 1998

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

[Fa] G.Flatings, *Endlichkeitssatze fur abelsche Varietaten uber*

Zahlkorpern.(German)Invent. Math. 73 (1983), no. 3, 349-366. English translation: pp. 9-27 in Arithmetic geometry, eds. G. C ornell and J. Silverman, Springer-Verlag, New York-Berlin, 1986

[Fri 01] 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).

[Ful 74] Fulton W. *Algebraic Curves., An Introduction to Algebraic Geometry*. Mathematic Lecture Notes Series. (1974).

[Full] 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.

[GG 99] J . von zur Gathen and J. Gerhard . Modern Computer Algebra . Cambridge , Cambridge , 1999

[GOT 02] I .Garcia , M. A. Olallah , and J.M. Tornero . *Computing the rational torsion of an elliptic curve using the tate normal form* J. Number Theory 96: 76 – 88 , 2002

[Ha] R. Hartshorne, *Algebraic geometry. Graduate Texes in Mathematics* 52, Springer-Verlag, New york-heidelberg, 1977.

[Har 77] Hartshorne. R. *Algebraic Geometry*. Springer GTM 52. (1977)

[Har95] 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

[HS] M.Hinry and Silverman, *Diophantine geometry. An introduction*. Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2000.

[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

[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

[Kun85] Ernst kunz. *Introduction to commutative algebra and algebraic geometry*. Birkhauser Boston Inc., Boston, MA, 1985. Tranleted from the German by Michael Ackerman, With a preface by David Mumford

[La] S. Lang, *Number Theory. III. Diophantine geometry*. Encyclopaedia of Mathematical Sciences 60, Springer-Verlag, Berlin, 1991

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

[Maz] B. Mazur, *Arithmetic on curves*. Bull. Amer. Math. Soc. (N.S) 14 (1986), no. 2, 207-259

[Mil 06] Milne J. S. *Elliptic Curves*. BookSurge Publishers (2006).

[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),

[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.

[Mol] 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

[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 nlosbare diophantische Gleichungen, J. Reine Angew. Math. 184 (1942),12-18

[Sat 00] T.Satoh . *The canonical lift of an ordinary elliptic curve over a finite field and its point counting* . J . Ramanujan Math . Soc 15(4): 247 – 270 , 2000

[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

[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, Ẹ. Vieweg & Sohn, Braunschweig, 1989

[Sha1] I. R. Shafarevich, *Basic algebraic geome try. 1. Varieties in rojectivespace. Second edition*. Translated from the 1988 Russian edition and with notes by Miles Reid. Springer-Verlag, Berlin 1994.

[Sha2] 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.

[Sha94] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer-verlag, Berlin, second edition, 1994. Vari-eties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.Robert J. Walker. *Algebraic curves.* Springer-Verlag, New York, 1978. Reprint of the 1950 edition.

[Sil 86] Silverman J. H. *The Arithmetic of Elliptic Curves*. Springer (**1986**).

[Sil 92] Silverman J. H. and Tate J. *Rational Points on Elliptic urves.*Springer (1992).

[Sil 94] J.H . Silverman . *Advanced Topics in the Arithmetic of Elliptic Curves* ,Springer – Verlag , New York , 1994

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

[Vo] P. Vojta, *Siegel's theorem in the compact case.* Ann. of Math. (2) 133 (1991), no. 3, 509-548.

[Was 03] Washington L. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC: New York. 2003