Tìm hiểu về mật mã đường cong Elliptic và ứng dụng

Nguyễn Đức Huy* Lê Thị Thùy Dung† Lưu Hiểu Huy‡

Mục lục

Tóm tắt nội dung

Mật mã đường cong Elliptic là phương pháp tiếp cận mã hóa khóa công khai dựa trên cấu trúc đại số của đường cong Elliptic trên các trường hữu hạn. Đường cong elliptic bao gồm các điểm thỏa mãn phương trình $Y^2 = X^3 + AX + B$ cùng với một điểm O ở vô cực. Chúng tôi sẽ giới thiệu và phân tích hệ mật mã dựa trên đường cong elliptic bao gồm các bài toán Logarit rời rạc, trao đổi khóa, mã hóa - giải mã, chữ kí số, ... và một số ứng dụng của nó trong mật mã như thuật toán phân tích thành nhân tử của đường cong elliptic Lenstra, thuật toán kiểm tra tính nguyên tố Pocklington-Lehmer.

1 Giới thiệu

2 Đường cong Elliptic

Một *đường cong Elliptic* là tập nghiệm của một phương trình có dạng

$$Y^2 = X^3 + AX + B$$

Các phương trình thuộc loại này được gọi là *phương trình Weierstrass* sau khi ông đã nghiên cứu chúng trong suốt thể kỉ XIX. Hai ví dụ cho đường cong elliptic:

$$E_1 : Y^2 = X^3 - 3X + 3$$

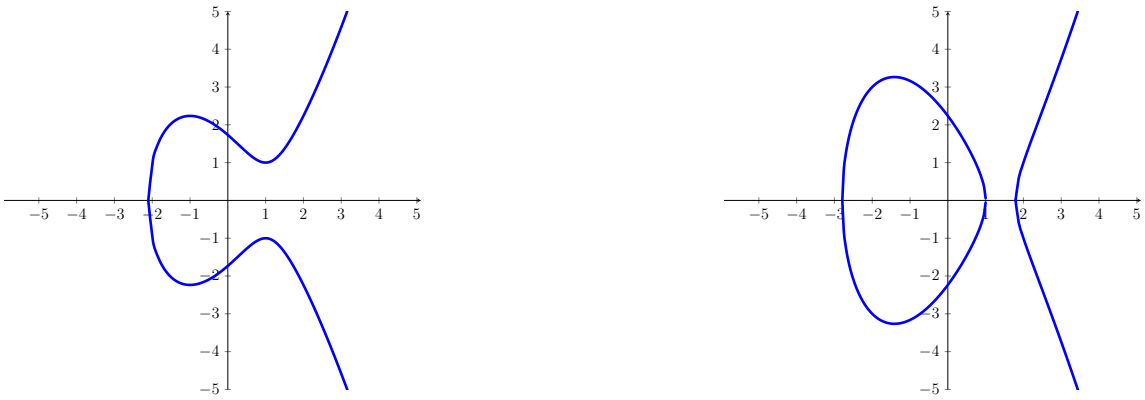
*Khoa Toán, Đại học Khoa học Tự Nhiên, mtait@math.ucsd.edu
†Khoa Toán, Đại học Khoa học Tự Nhiên, craig.timmons@csus.edu
‡Khoa Toán, Đại học Khoa học Tự Nhiên, craig.timmons@csus.edu

và

$$E_2 : Y^2 = X^3 - 5X + 5$$

được minh họa ở 1

Hình 1: Hình 1



Một điều tuyệt vời của đường cong elliptic là có một cách tự nhiên để chọn hai điểm trên đường cong và "cộng" chúng để tạo ra điểm thứ ba. Phép "cộng" được chúng tôi nhắc đến ở đây là một phép toán kết hợp hai điểm theo cách tương tự với phép cộng thông thường ở một vài khía cạnh (có tính chất giao hoán, kết hợp và có cách nhận dạng), nhưng rất khác ở những phần còn lại. Một trong những cách đơn giản để miêu tả "luật cộng"là sử dụng hình học.

Cho P và Q là hai điểm trên đường cong elliptic E, như minh họa ở Hình 2. Ta bắt đầu vẽ một đường thẳng L đi qua P và Q. Đường thẳng L sẽ cắt E tại ba điểm P, Q và một điểm R thứ ba. Ta lấy đối xứng điểm R qua trục Ox để được điểm R'. Điểm R' này gọi là *tổng của P và Q*, phép "cộng" này không giống phép cộng thông thường. Ta biểu thị phép "cộng" này bằng kí hiệu $\oplus$. Ta viết

$$P \oplus Q = R' \tag{1}$$

Example 1 *Cho đường cong elliptic E:*

$$Y^2 = X^3 - 15X + 18 \tag{2}$$

Điểm $P = (7, 16)$ và $Q = (1, 2)$ nằm trên E. Đường thẳng L nối P và Q có phương trình

$$L : Y = \frac{7}{3}X - \frac{1}{3} \tag{3}$$

Để tìm giao điểm của E và L, ta thay Y ở phương trình (3) vào phương trình (2) để tìm X. Ta có

$$\begin{aligned} (\tfrac{7}{3}X - \tfrac{1}{3})^2 &= X^3 - 15X + 18 \\ \tfrac{49}{9}X^2 - \tfrac{14}{9}X + \tfrac{1}{9} &= X^3 - 15X + 18 \\ 0 &= X^3 - \tfrac{49}{9}X^2 - \tfrac{121}{9}X + \tfrac{161}{9} \end{aligned}$$

Thông thường, việc tìm nghiệm của phương trình bậc ba không đơn giản, nhưng ta đã biết trước 2 giao điểm của L và E là P và Q, nên rõ ràng phương trình trên có 2 nghiệm $X = 1$ và $X = 7$. Từ đó, ta dễ dàng tìm được nghiệm còn lại

$$X^3 - \frac{49}{9}X^2 - \frac{121}{9}X + \frac{161}{9} = (X-7)\,.\,(X-1)\,.\,(X+\frac{23}{9})$$

Thay $X = -\frac{23}{9}$ vào phương trình (3) ta được điểm $R = (-\frac{23}{9}, -\frac{170}{27})$. Cuối cùng, lấy đối xứng qua trục Ox ta được

$$P \oplus Q = (-\frac{23}{9}, \frac{170}{27})$$

Điều gì xảy ra khi ta cộng điểm P với chính nó? Khi điểm Q tiến dần đến P, đường thẳng L sẽ trở thành tiếp tuyến của E tại P. Vậy, để cộng điểm P với chính nó, ta đơn giản chỉ cần lấy L là tiếp tuyến của E tại P, minh họa ở hình 3. Khi đó L giao E tại P và một điểm R khác, điểm P được tính 2 lần.

Example 2 *Tiếp tục với đường cong E và điểm P*
Để sau viết tiếp

Vấn đề thứ hai là khi ta cố gắng cộng điểm $P = (a, b)$ với điểm đối xứng của nó qua trục Ox $P' = (a, -b)$. Đường thẳng L đi qua P và P' có phương trình $x = a$, chỉ cắt E tại 2 điểm P và P'. (Hình 4) Vậy nên không có giao điểm thứ ba. Giải pháp là tạo thêm một điểm $\mathcal{O}$ ở "vô cực". Chính xác hơn, điểm $\mathcal{O}$ không tồn tại trên mặt phẳng Oxy, nhưng ta giả định nó nằm trên mọi đường thẳng đứng. Ta có:

$$P \oplus P' = \mathcal{O}$$

Tiếp theo, ta cần tìm cách cộng điểm $\mathcal{O}$ với điểm $P = (a, b)$ thuộc E. Đường thẳng L nối P với $\mathcal{O}$ là đường thẳng đứng đi qua P và cắt E tại $P' = (a, -b)$. Để cộng P với $\mathcal{O}$, ta lấy điểm đối xứng với P' qua trục Ox, ta được điểm P. Nói cách khác $P \oplus \mathcal{O} = P$, vậy điểm $\mathcal{O}$ có vai trò như số 0 trong phép cộng elliptic.

Example 3

Definition 1 *Một đường cong elliptic E là tập nghiệm của một phương trình Weierstrass:*

$$E : Y^2 = X^3 + AX + B$$

cùng với một điểm $\mathcal{O}$ ở vô cùng, trong đó hẳng số A và B thỏa mãn

$$4A^3 + 27B^2 \neq 0$$

Phép cộng trên E được định nghĩa như sau. Cho 2 điểm P và Q là 2 điểm thuộc E. L là đường thẳng nối P và Q, hoặc là đường tiếp tuyến của E tại P nếu $P = Q$. Khi đó, giao điểm của E và L là ba điểm P, Q và R, với $\mathcal{O}$ là một điểm ở vô cực, năm trên mọi đường thẳng đứng. $R = (a, b)$, tổng của P và Q là điểm $R' = (a, -b)$. Tổng này được ký hiệu là $P \oplus Q$, cơ thể viết đơn giản $P + Q$.

Remark 1 *Tại sao cần thỏa mãn điều kiện $4A^3 + 27B^2 \neq 0$?*

Đại lượng $\Delta_E = 4A^3 + 27B^2$ được gọi là *phân thức của E*. $\Delta_E \neq 0$ là điều kiện để đa thức $X^3 + AX + B$ có 3 nghiệm phân biệt, khi phân tích thành nhân tử $X^3 + AX + B$ ta được:

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3)$$

Ta biểu diễn điểm đối xứng của P bởi $\ominus P = (a, -b)$, hoặc đơn giản hơn là $-P$; ta định nghĩa $P \ominus P$ (hay $P - Q$) là $P \oplus (\ominus Q)$. Tương tự, lặp lại phép cộng nhiều lần là biểu diễn của phép nhân một điểm với một số nguyên,

$$nP = \underbrace{P + P + P + \ldots + P}_{\text{n số hạng}}$$

Theorem 2.1 *Cho đường cong elliptic E. Luật cộng trên E thỏa mãn các tính chất sau:*

(a)	$P + \mathcal{O}$	$=$	$\mathcal{O} + P = P$	$\forall P \in E$	*[Cộng với điểm $\mathcal{O}$]*
(b)	$P + (-P)$	$=$	$\mathcal{O}$	$\forall P \in E$	*[Nghịch đảo]*
(c)	$(P + Q) + R$	$=$	$P + (Q + R)$	$\forall P, Q, R \in E$	*[Kết hợp]*
(d)	$P + Q$	$=$	$Q + P$	$\forall P, Q \in E$	*[Giao hoán]*

Theorem 2.2 *Phải implement*

3 Đường cong elliptic trên trường hữu hạn

Các ứng dụng về mật mã của đường cong Elliptic đa số chỉ sử dụng các đường cong trên trường hữu hạn.

3.1 Sơ bộ

Definition 2 *Trường là một tập hợp K có nhiều hơn một phần tử, được định nghĩa hai phép toán cộng và nhân, ký hiệu bởi dấu (+) và dấu (.). Trường thỏa mãn các tính chất của số học.*

Các tính chất số học: TODO:

1. Tính kết hợp
2. Tính giao hoán
3. Đơn vị cộng và đơn vị nhân
4. Nghịch đảo phép cộng
5. Nghịch đảo phép nhân
6. Tính phân phối

Definition 3 *Trường hữu hạn (còn gọi là trường Galois) là những trường có hữu hạn số phần tử. Bậc của một trường hữu hạn là số phần tử của nó, là số nguyên tố hoặc lũy thừa nguyên tố.*

Trường hữu hạn là cơ bản trong một số lĩnh vực toán học và khoa học máy tính, bao gồm lý thuyết số, hình học đại số, lý thuyết Galois, hình học hữu hạn, mật mã và lý thuyết mã hóa.

Xét F_p là một trường hữu hạn (hữu hạn số phần tử nguyên dương):

$$F_p = \{0, 1, 2, \dots p-1\}$$

Với p là một số nguyên tố. F_p giống như cách viết Z/mZ là vành các số nguyên modulo m.

3.2 Đường cong elliptic trên trường hữu hạn

Để áp dụng hệ quả của đường cong Elliptic vào mật mã, ta xét các đường cong mà các điểm của nó có toạ độ xác định trong F_p

Ta định nghĩa một đường cong elliptic E trên trường hữu hạn F_q là một phương trình có dạng:

$$E : Y^2 = X^3 + AX + B \text{ với các hằng số } A, B \in F_p \text{ thỏa mãn } 4A^3 + 27B^2 \neq 0$$

Tập hợp các điểm trên E có toạ độ thuộc F_p được kí hiệu bởi

$$E(F_p) = \{(x, y) : x, y \in F_p \text{ thỏa mãn } y^2 = x^3 + Ax + B\} \cup \mathcal{O}$$