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

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

*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

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:

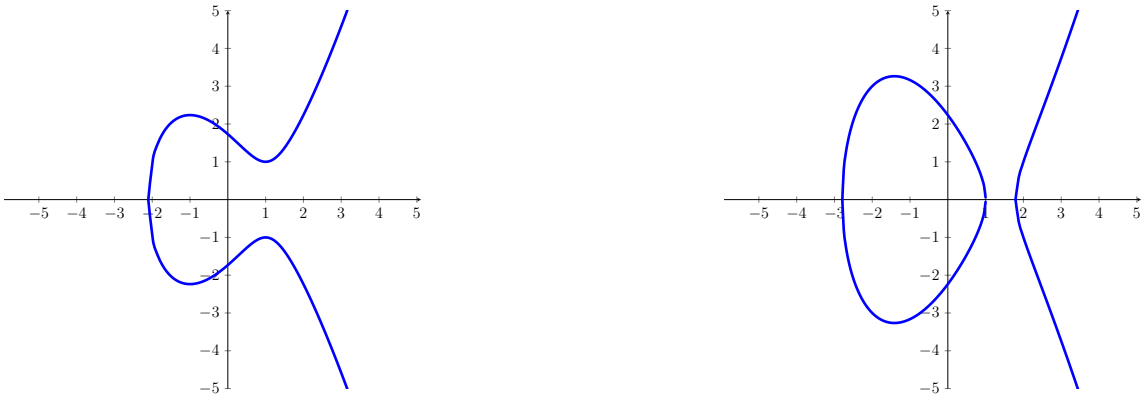
$$E_1 : Y^2 = X^3 - 3X + 3$$

và

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

được minh họa ở Hình 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:*

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

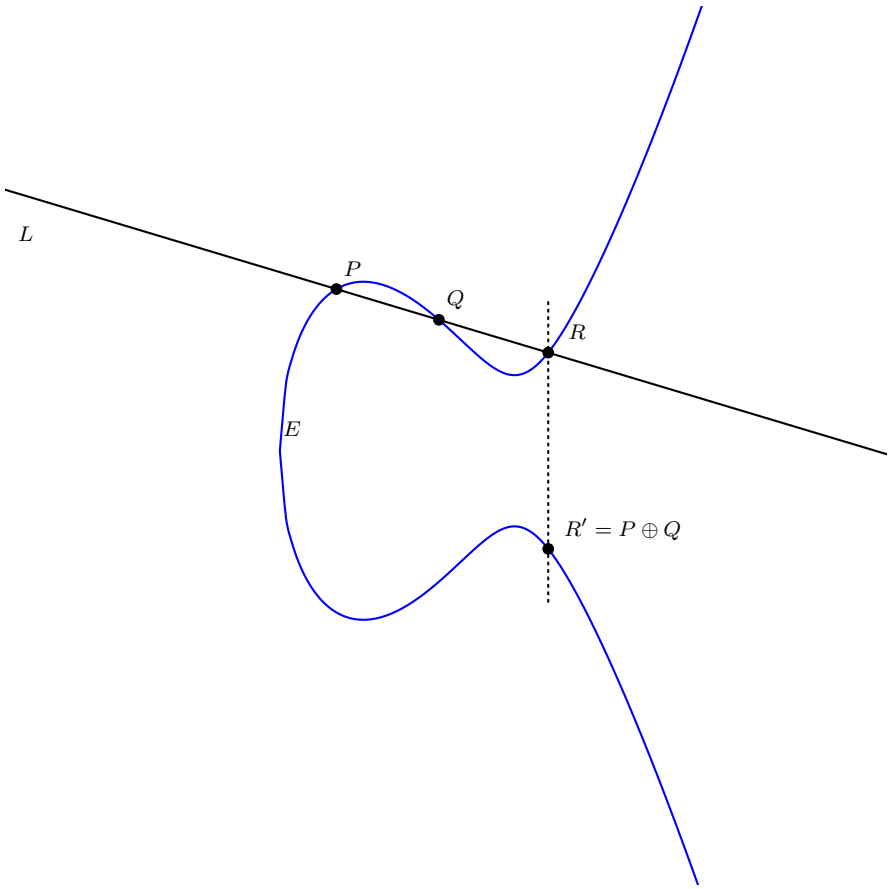
Điểm $P = (7, 16)$ và $Q = (1, 2)$ nằm trên E. Đường thẳng L nối P và Q có phương trình

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

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

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

Hình 2: Hình 2



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

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

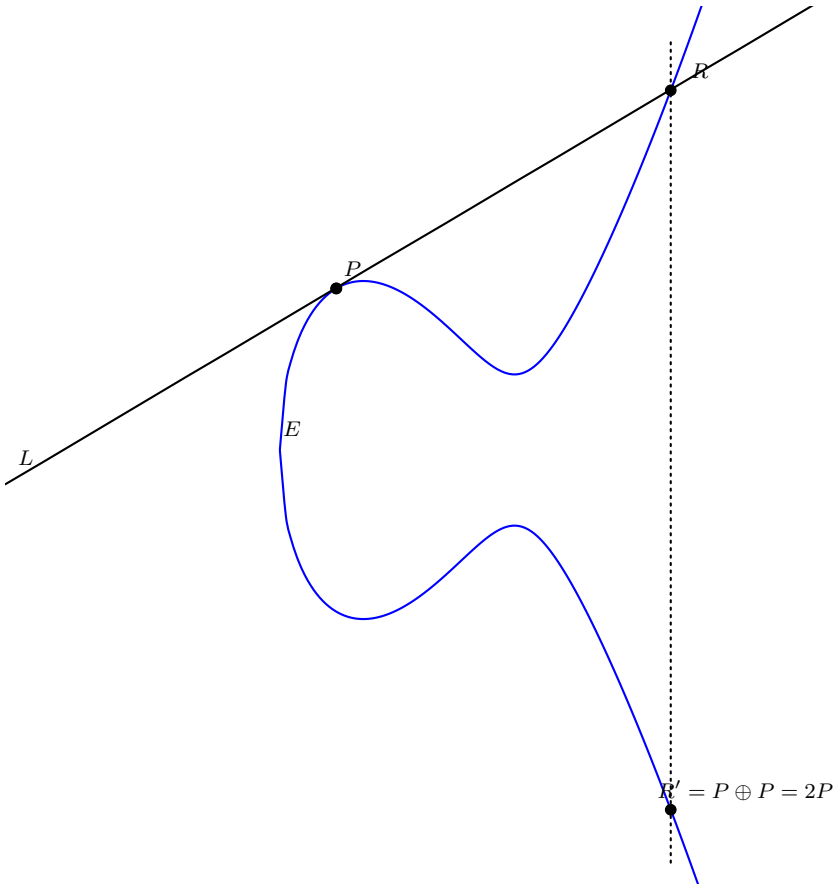
Thay $X = -\frac{23}{9}$ vào phương trình (3) ta được điểm $R = (-\frac{23}{9}, -\frac{170}{27})$. Cuối cùng, lấy đối xứng qua trục Ox ta được

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

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.

Hình 3: Hình 3



Example 2 *Tiếp tục với đường cong E và điểm P ở ví dụ 1, ta tính $P \oplus P$.*

Ta tìm độ dốc tại P của E bằng cách đạo hàm 2 vế phương trình (2). Ta được

$$2\frac{dY}{dX} = 3X^2 - 15, \text{ suy ra } \frac{dY}{dX} = \frac{3X^2 - 15}{2Y}$$

Thay tọa độ điểm $P = (7, 16)$ ta được độ dốc $\lambda = \frac{33}{8}$, nên đường tiếp tuyến của E tại P có phương trình

$$L : Y = \frac{33}{8}X - \frac{103}{8} \tag{4}$$

Tiếp theo, thay Y ở phương trình (4) vào phương trình (2):

$$\begin{aligned} (\frac{33}{8}X - \frac{103}{8})^2 &= X^3 - 15X + 18 \\ X^3 - \frac{1089}{64}X^2 + \frac{2919}{32}X - \frac{9457}{64} &= 0 \\ (X-7)^2 \cdot (X - \frac{193}{64}) &= 0 \end{aligned}$$

Ta đã biết trước $X = 7$ là nghiệm bội 2 của phương trình bậc 3 nên dễ dàng phân tích thành nhân tử và tìm được nghiệm còn lại. Cuối cùng, thay $X = \frac{193}{64}$ vào phương trình (4) ta được $Y = -\frac{233}{512}$. Đổi dấu Y ta được

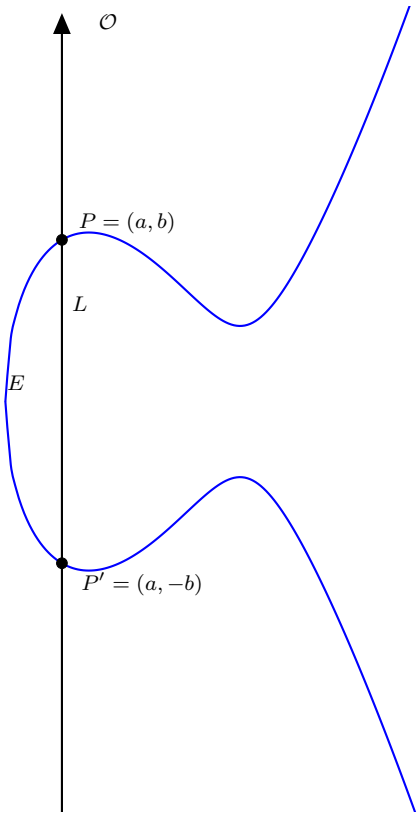
$$P \oplus P = (\frac{193}{64}, \frac{233}{512})$$

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.

Hình 4: Hình 4



Example 3 *Tiếp tục với đường cong E ở ví dụ 1 và điểm $T = (3, 0)$.*

Chú ý điểm T nằm trên E và tiếp tuyến tại T là đường thẳng đứng $X = 3$. Vậy nếu cộng điểm T với chính nó, ta được $T \oplus T = \mathcal{O}$.

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 hằng số A và B thỏa mãn

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

Luật 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 $\mathcal{O}$ được hiểu là điểm nằm trên mọi đường thẳng đứng. $R = (a, b)$, tổng của P và Q là điểm $R' = (a, -b)$. Tổng này được ký hiệu là $P \oplus Q$, có thể viết đơn giản $P + Q$.

Ta biểu diễn điểm đối xứng của P bởi $\ominus P = (a, -b)$, hoặc $-P$; 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,

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

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, nếu phân tích thành nhân tử $X^3 + AX + B$ ta được:

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

trong đó e_1, e_2, e_3 là các số phức, thì

$$4A^3 + 27B^2 \neq 0 \qquad \text{khi và chỉ khi} \qquad e_1, e_2, e_3 \text{ phân biệt}$$

Phép cộng không hoàn toàn đúng đối với đường cong có $\Delta_E = 0$ nên chúng tôi thêm điều kiện $\Delta_E \neq 0$ khi nêu khái niệm đường cong elliptic.

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]

Proof. Như đã giải thích trước đó, dễ thấy tính cộng với điểm $\mathcal{O}$ và tính nghịch đảo là đúng vì $\mathcal{O}$ nằm trên mọi đường thẳng đứng. Tính giao hoán dễ dàng chứng minh vì đường thẳng qua P và Q cũng là đường thẳng qua Q và P.

Phần còn lại cần chứng minh của định lý 2.1 là tính kết hợp. Có nhiều cách để chứng minh tính kết hợp, nhưng không cách nào trong số chúng đơn giản. Sau khi có đủ các

kiến thức cần thiết về luật cộng trên E (2.2), bạn đọc có thể sử dụng để tự chứng minh. Có thể tìm thấy những chứng minh rõ ràng hơn ở [1], [4] hoặc [5] và một vài quyển sách khác về đường cong elliptic. ■

Tiếp theo, chúng ta sẽ chứng minh một vài công thức để dễ dàng cộng và trừ các điểm trên một đường cong elliptic. Những công thức này sử dụng hình học giải tích, tính toán vi phân và một vài thao tác đại số cơ bản. Chúng tôi đưa kết quả dưới dạng một định lý và đưa ra chứng minh sau đó.

Theorem 2.2 (Thuật toán cộng đường cong Elliptic) *Cho*

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

là một đường cong elliptic và P_1 và P_2 là hai điểm trên E.

1. *Nếu $P_1 = \mathcal{O}$ thì $P_1 + P_2 = P_2$.*
2. *Ngược lại, nếu $P_2 = \mathcal{O}$ thì $P_1 + P_2 = P_1$.*
3. *Ngược lại, viết $P_1 = (x_1, y_2)$ và $P_2 = (x_2, y_2)$.*
4. *Nếu $x_1 = x_2$ và $y_1 = -y_2$ thì $P_1 + P_2 = \mathcal{O}$.*
5. *Nếu không, định nghĩa λ bởi*

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{nếu } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{nếu } P_1 = P_2. \end{cases}$$

Và ta có $P_1 + P_2 = (x_3, y_3)$, trong đó:

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{và} \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

Proof. Phần (1) và (2) của định lý 2.2 là đúng, và (4) là trường hợp đường thẳng qua P_1 và P_2 là đường thẳng đứng, nên $P_1 + P_2 = \mathcal{O}$. (lưu ý, vẫn đúng với trường hợp $y_1 = y_2 = 0$.) Còn phần (5), ta để ý rằng λ là hệ số góc của đường thẳng đi qua P_1 và P_2, và cũng là hệ số góc của tiếp tuyến tại P_1 nếu $P_1 = P_2$. Trong cả 2 trường hợp, đường thẳng L đều có phương trình $Y = \lambda X + \nu$ với $\nu = y_1 - \lambda x_1$. Thế Y vào phường trình đường cong E ta được:

$$(\lambda X + \nu)^2 = X^3 + AX + B$$

nên

$$X^3 - \lambda^2 X^2 + (A - 2\lambda\nu)X + (B - \nu^2) = 0$$

Phương trình trên có 2 nghiệm đã biết trước là x_1 và x_2. Ta gọi nghiệm còn lại là x_3, phân tích thành nhân tử ta được

$$X^3 - \lambda^2 X^2 + (A - 2\lambda\nu)X + (B - \nu^2) = (X - x_1)(X - x_2)(X - x_3)$$

Đồng nhất hệ số 2 vế, ta được $x_3 = \lambda^2 - x_1 - x_2$. Cuối cùng, để tìm được $P_1 + P_2$, ta thay x_3 vào phương trình L để tìm giao điểm còn lại của L và E rồi lấy đối xứng qua Ox. ■

3 Đường cong elliptic trên trường hữu hạn

Trong phần trước, chúng ta đã phát triển lý thuyết về đường cong elip về mặt hình học. Tuy nhiên, để áp dụng lý thuyết về đường cong elliptic vào mật mã, chúng ta cần xem xét các đường cong elliptic mà các điểm của nó có tọa độ trong một trường hữu hạn F_p. 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.

Definition 4 (Bình phương modulo) *Cho số nguyên dương* $m \geq 2$*. Số nguyên a được gọi là bình phương modulo m nếu* $\gcd(a, m) = 1$ *và phương trình*

$$x^2 \equiv a(\mod m)$$

có nghiệm

Definition 5 (Nghịch đảo modulo) *Với một số nguyên a, ta gọi nghịch đảo modulo m của a là* a^{-1} *là số nguyên thỏa mãn:*

$$a * a^{-1} \equiv 1(\mod m)$$

Chú ý rằng không phải lúc nào a^{-1} *cũng tồn tại. Ví dụ với* $m = 4, a = 2$*, ta không thể tìm được* a^{-1} *thỏa mãn đẳng thức trên.*

Definition 6 (Thặng dư bình phương) *Một số nguyên q gọi là thặng dư bình phương theo modulo m nếu nó đồng dư với một số chính phương theo modulo m. Nói cách khác, tồn tại số nguyên x thỏa mãn:*

$$x^2 \equiv q(\mod m)$$

Ngược lại, q được gọi là phi thặng dư bình phương

Definition 7 (Modular square root) *Một Modular square root r của số nguyên a theo modulo m là một số nguyên thỏa mãn:*

$$r^2 \equiv a(\mod m)$$

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

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

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

Ta định nghĩa một đường cong elliptic E trên trường hữu hạn $\mathbb{F}_q$ 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 $\mathbb{F}_p$ được kí hiệu bởi

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

Remark 2 *Vì một vài lí do mà chúng tôi sẽ giải thích ở phần sau, ở đây, chúng tôi thêm điều kiện $p \geq 3$. Những đường cong Elliptic trên trường $\mathbb{F}_2$ có vai trò quan trọng trong mật mã, nhưng chúng rất phức tạp, nên chúng ta sẽ thảo luận về chúng ở phần 7.*

Example 4 *Xem xét đường cong elliptic*

$$E : Y^2 = X^3 + 3X + 8 \quad \textit{trên trường } F_{13}$$

Ta tìm các điểm thuộc $E(\mathbb{F}_{13})$ bằng cách thay tất cả giá trị của $X = 0, 1, 2, \ldots, 12$ và kiểm tra với mỗi giá trị của X, $X^3 + 3X + 8$ có là bình phương modulo của 13 hay không. Ví dụ, thay $X = 0$, ta có $X^3 + 3X + 8 = 8$ và 8 không phải bình phương modulo của 13. Tiếp theo, thay $X = 1$, ta được $X^3 + 3X + 8 = 12$ và 12 là bình phương modulo của 13. Nó có 2 nghiệm

$$5^2 \equiv 12(\mod 13) \quad \text{và} \quad 8^2 \equiv 12(\mod 13)$$

.

Ta tìm được 2 điểm $(1,5)$ và $(1,8)$ thuộc $E(\mathbb{F}_{13})$. Tiếp tục theo cách này, ta kết thúc với tập hoàn chỉnh gồm 9 điểm:

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}.$$

Cho $P_1 = (x_1, y_1)$ và $P_2 = (x_2, y_2)$ thuộc $E(\mathbb{F}_p)$. Ta định nghĩa tổng $P_1 + P_2$ có tọa độ (x_3, y_3) thu được bằng cách áp dụng thuật toán cộng (2.2). Vì tọa độ các độ các điểm đó nằm trong trường $\mathbb{F}_p$, ta thu được (x_3, y_3) có tọa độ trong trường $\mathbb{F}_p$. Nhưng điều này vẫn chưa đủ chỉ ra (x_3, y_3) có thể thuộc $E(\mathbb{F}_p)$ hay không.

Theorem 3.1 *Cho E là đường cong elliptic trên $\mathbb{F}_p$ và P và Q là 2 điểm thuộc $E(\mathbb{F}_p)$.*

- *Thuật toán cộng đường cong elliptic áp dụng cho P và Q (2.2) đưa ra một điểm trong $E(\mathbb{F}_p)$. Điểm này được kí hiệu bởi $P + Q$.*
- *Luật cộng trên $E(\mathbb{F}_p)$ thỏa mãn tất cả các tính chất được liệt kê ở định lý 2.1. Nói cách khác, luật cộng này làm cho $E(\mathbb{F}_p)$ thành nhóm hữu hạn.*

Proof.

■

Example 5 *Tiếp tục với đường cong E từ ví dụ 4*

$$E : Y^2 = X^3 + 3X + 8 \quad \text{trên trường } \mathbb{F}_{13}$$

Áp dụng thuật toán cộng (2.2) để cộng $P(9,7)$ và $Q(1,8)$, trước hết, ta tính hệ số góc của L:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-7}{1-9} = \frac{1}{-8} = \frac{1}{5} = 8$$

vì các tính toán [1] đang được thực hiện trên trường $\mathbb{F}_{13}$ nên $-8 = 5$ và $\frac{1}{5} = 5^{-1} = 8$. Tiếp tục, ta tính

$$\nu = y_1 - \lambda x_1 = 7 - 8 \cdot 9 = -65 = 0.$$

Cuối cùng:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 = 64 - 9 - 1 = 54 = 2, \\ y_3 &= -(\lambda x_3 + \nu) = -8 \cdot 2 = -16 = 10. \end{aligned}$$

Và ta hoàn thành việc tính toán

$$P + Q = (1,8) + (9,7) = (2,10) \in E(\mathbb{F}_{13})$$

Tương tự, ta dùng thuật toán cộng để cộng điểm $P = (9,7)$ với chính nó. Lưu ý ta vẫn đang thực hiện tính toán trên trường $\mathbb{F}_{13}$, ta có:

[1] Đây là lúc thích hợp để hiểu rằng, $\frac{1}{5}$ chỉ là *kí hiệu* cho một nghiệm của phương trình $5x = 1$. Để gán một giá trị cho $\frac{1}{5}$, bạn phải biết giá trị đang ở trường nào. Trong trường $\mathbb{Q}$, giá trị của $\frac{1}{5}$ là một số bình thường, nhưng ở trường $\mathbb{F}_{13}$ giá trị của $\frac{1}{5}$ là 8 ($\frac{1}{5} = 5^{-1}$ và nghịch đảo modulo 13 của 5 là 8).

$$\begin{aligned}\lambda &= \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 9^2 + 3}{2 \cdot 7} = \frac{246}{14} = 1\\ \nu &= y_1 - \lambda x_1 = 7 - 1 \cdot 9 = 11.\end{aligned}$$

sau đó

$$\begin{aligned}x_3 &= \lambda^2 - x_1 - x_2 = 1 - 9 - 9 = 9\\ y_3 &= -(\lambda x_3 + \nu) = -1 \cdot 9 - 11 = 6.\end{aligned}$$

nên $P + P = (9, 7) + (9, 7) = (9, 6) \in E(\mathbb{F}_{13})$. Theo cách đó, ta có thể cộng mọi cặp điểm trong $E(\mathbb{F}_{13})$, kết quả được thể hiện ở Bảng 1

Hình 5: Phép cộng $E : Y^2 = X^3 + 3X + *$ trên trường $\mathbb{F}_{13}$

	$\mathcal{O}$	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
$\mathcal{O}$	$\mathcal{O}$	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
$(1,5)$	$(1,5)$	$(2,10)$	$\mathcal{O}$	$(1,8)$	$(9,7)$	$(2,3)$	$(12,2)$	$(12,11)$	$(9,6)$
$(1,8)$	$(1,8)$	$\mathcal{O}$	$(2,3)$	$(9,6)$	$(1,5)$	$(12,11)$	$(2,10)$	$(9,7)$	$(12,2)$
$(2,3)$	$(2,3)$	$(1,8)$	$(9,6)$	$(12,11)$	$\mathcal{O}$	$(12,2)$	$(1,5)$	$(2,10)$	$(9,7)$
$(9,6)$	$(9,6)$	$(2,3)$	$(12,11)$	$(12,2)$	$(1,8)$	$(9,7)$	$\mathcal{O}$	$(1,5)$	$(2,10)$
$(9,7)$	$(9,7)$	$(12,2)$	$(2,10)$	$(1,5)$	$(12,11)$	$\mathcal{O}$	$(9,6)$	$(2,3)$	$(1,8)$
$(12,2)$	$(12,2)$	$(12,11)$	$(9,7)$	$(2,10)$	$(9,6)$	$(1,5)$	$(2,3)$	$(1,8)$	$\mathcal{O}$
$(12,11)$	$(12,11)$	$(9,6)$	$(12,2)$	$(9,7)$	$(2,3)$	$(2,10)$	$(1,8)$	$\mathcal{O}$	$(1,5)$

Tập điểm trong $E(\mathbb{F}_p)$ là tập hữu hạn. Chính xác hơn, có p cách chọn X và mỗi cách chọn X, phương trình

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

cho nhiều nhất 2 nghiệm Y. Thêm điểm $\mathcal{O}$, $\#E(\mathbb{F}_p)$ có tối đa $2p + 1$ điểm.

Khi gán giá trị cho X, có ba trường hợp xảy ra với đại lượng

$$X^3 + AX + B$$

Thứ nhất, nó là thặng dư bình phương và có hai Modular square root, ta được hai điểm thuộc $E(\mathbb{F}_p)$, trường hợp này xảy ra khoảng 50%. Thứ hai, nó không là thặng dư bình phương, ta bỏ qua X, trường hợp này cũng chiếm khoảng 50%. Thứ ba, $X^3+AX+B = 0$, ta được một điểm thuộc $E(\mathbb{F}_p)$, trường hợp này rất hiếm xảy ra [2]. Theo đó, số phần tử của $E(\mathbb{F}_p)$ xấp xỉ

$$\#E(\mathbb{F}_p) \approx 50\% \cdot (2p + 1) = p + 1.$$

Một định lý nổi tiếng của Hasse, sau này được Weil và Deligne tổng quát hóa rộng rãi, nói rằng điều này đúng với các dao động ngẫu nhiên

Theorem 3.2 (Hasse) *Cho E là đường cong elliptic trên trường F_p. Thì*

$$\#E(\mathbb{F}_p) = p + 1 - t_p \text{ với } t_p \text{ thỏa mãn } |t_p| \leq 2\sqrt{p}.$$

[2] Phép đồng dư $X^3 + AX + B \equiv 0 (\mod p)$ có nhiều nhất ba nghiệm, và nếu p lớn, tỉ lệ chọn ngẫu nhiên một trong số chúng là rất nhỏ.

Definition 8 *Đại lượng $t_p = p + 1 - \#E(\mathbb{F}_p)$ ở định lý 3.2 được gọi là dấu vết của Frobenius trên $E/\mathbb{F}_p$.*

t_p xuất hiện dưới dạng dấu vết của một ma trận 2x2 có vai trò như phép biến đổi tuyến tính trên một không gian vector 2 chiều liên kết với $E/\mathbb{F}_p$.

Example 6 *Cho phương trình E:*

$$E : Y^2 = X^3 + 4X + 6$$

Chúng ta có thể coi E là đường cong elliptic trên trường F_p cho các trường hữu hạn $\mathbb{F}_p$ khác nhau và đếm số điểm thuộc $E(\mathbb{F}_p)$. Bảng 2 liệt kê các kết quả với những số nguyên tố đầu tiên, cùng giá trị của t_p để so sánh với giá trị của $2\sqrt{p}$.

Hình 6: Số điểm và dấu vết Frobenius của $E : Y^2 = X^3 + 4X + 6$

p	$\#E(\mathbb{F}_p)$	t_p	$2\sqrt{p}$
3	4	0	3.46
5	8	-2	4.47
7	11	-3	5.29
11	16	-4	6.63
13	14	0	7.21
17	15	3	8.25

Remark 3 *Định lý Hasse cho ta một giới hạn của $\#E(\mathbb{F}_p)$, nhưng không cung cấp một phương pháp để tính giá trị này. Về nguyên tắc, để tìm $\#E(\mathbb{F}_p)$, ta có thể thay từng giá trị của X rồi kiểm tra giá trị của $X^3 + AX + B$ dựa vào bảng thặng dư bình phương p, nhưng độ phức tạp thời gian là $O(p)$, rất kém hiệu quả. Schoof [2] đã tìm ra một phương pháp tốt hơn để tính $\#E(\mathbb{F}_p)$ trong thời gian $O(\log^6(p))$. Nghĩa là ông ấy tìm được một thuật toán có thời gian đa thức. Thuật toán của Schoof được cải thiện bởi Elkies và Atkin, với tên gọi là thuật toán SEA [3].*

4 Bài toán Logarit rời rạc

Cho số nguyên tố p và a, b là các số nguyên không chia hết cho p. Giả sử ta biết tồn tại một số nguyên k thỏa mãn

$$a^k \equiv b \pmod{p}$$

Bài toán Logarit rời rạc cổ điển là tìm ra k. Vì $k + (p - 1)$ cũng là nghiệm, nên k .....

Tài liệu

[1] Halmos, F. G. P. Graduate texts in mathematics 84.

[2] Schoof, R. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation 44*, 170 (1985), 483–494.

[3] Schoof, R. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux 7*, 1 (1995), 219–254.

[4] Silverman, J. H. *The arithmetic of elliptic curves*, vol. 106. Springer, 2009.

[5] Silverman, J. H., and Tate, J. T. *Rational points on elliptic curves*, vol. 9. Springer, 1992.