Đường cong Elliptic
(trước và sau quantum)

Main Author , 2nd Author, 3rd Author

School of Computer Science
University of Windsor

Ngày 16 tháng 4 năm 2022

Table of Contents

Introduction

Definition

Ta định nghĩa bài toán logarit rời rạc trên một nhóm với phép nhân các số nguyên theo modulo p, $\mathbb{Z}_{/\mathbb{Z}_p}$, như sau:
Cho $g, a \in \mathbb{Z}_{/\mathbb{Z}_p}$, với a là phần tử của nhóm cyclic có phần tử sinh g, tìm số nguyên k thỏa mãn:

$$g^k \equiv a \pmod{p} \tag{1}$$

Definition

Ta định nghĩa bài toán phân tích rời rạc như sau: Cho một số nguyên N, có ước là hai số nguyên tố lớn p và q. Tìm p và q.

Preliminaries

[Vishwanath and Nagappan, 2010]

Definition

Một *nhóm* là một cấu trúc đại số bao gồm:

- Một tập phần tử G
- Một toán tử đóng $(\cdot)$ trên tập G thỏa mãn tính chất kết hợp. Nghĩa là $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, với mọi $a, b, c \in G$.
- Một phần tử đơn vị 1, để $a \cdot 1 = a$ với mọi $a \in G$.
- Tồn tại phần tử nghịch đảo $a^{-1} \in G$ nếu $a \in G$ để $a^{-1} \cdot a = 1$.

Một *nhóm* thỏa mãn thêm điều kiện toán tử hai ngôi có thêm tính giao hoán (hay $a \cdot b = b \cdot a$) là nhóm giao hoán hoặc *nhóm Abel*

Example

Với tập số nguyên $\mathbb{Z}$ được trang bị toán tử $+$ và xem số 0 như phần tử đơn vị, xem các cặp số nguyên có dấu ngược nhau là các cặp nghịch đảo, ta có một *nhóm*.
Ngược lại, tập số tự nhiên $\mathbb{N}$ không phải một nhóm vì không định nghĩa được phần tử nghịch đảo.

Definition

Cho nhóm G được trang bị toán tử $(\cdot)$ với phần tử đơn vị 1. Với mỗi $a \in G$, *bậc* của a, là số nguyên n nhỏ nhất thỏa mãn:

$$\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n} = 1 \quad (2)$$

Tập $\{a, a^2, a^3, a^4, \ldots, a^n\}$ là nhóm cyclic con của G có bậc n, a được gọi là *phần tử sinh* của nhóm đó.

Preliminaries

Definition

Một *trường* là một cấu trúc đại số bao gồm:

- Tập G là tập đóng dưới phép cộng và phép nhân.
- Phép cộng và phép nhân phải có tính kết hợp trên tập G.
- Phép cộng và phép nhân phải có tính giao hoán trên tập G.
- Tồn tại phần tử nghịch đảo cho cả phép cộng và phép nhân.
- Phép nhân có tính chất phân phối đối với phép cộng: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- Phần tử đơn vị của phép cộng và phép nhân phải khác nhau.

Definition

Tính đặc trưng của trường F là số n nhỏ nhất thỏa mãn tổng của n phần tử 1 bằng 0. Kí hiệu $char(F) = n$.

Example

Nếu tính đặc trưng của F, $char(F)$, là 2 và phần tử đơn vị là 1, thì $1 + 1 = 0$.
Nếu $char(F) = 3$ thì $1 + 1 + 1 = 0$.

Definition

Trường Galois là trường bao gồm một tập hữu hạn phần tử.

Example

Tập số nguyên theo modulo số nguyên tố p, $\mathbb{Z}_{/\mathbb{Z}}$ là một trường Galois.
Với p phần tử, 0 đến $p-1$, kí hiệu $GF(p)$.

Phần còn lại, ta sẽ đề cập nhiều hơn đến trường của số nguyên tố $GF(p)$, tổng quát hơn là $GF(p^n)$.

Basic

Definition

Một đường cong elliptic $E(F)$ là một tập điểm trên trường F, thỏa mãn phương trình có dạng:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5 \tag{3}$$

Trong đó $a_1, a_2, a_3, a_4, a_5 \in F$.

Nếu ta giả sử tính đặc trưng của F khác 2, hay $1 + 1 = 2 \neq 0$, phương trình có thể viết lại dưới dạng:

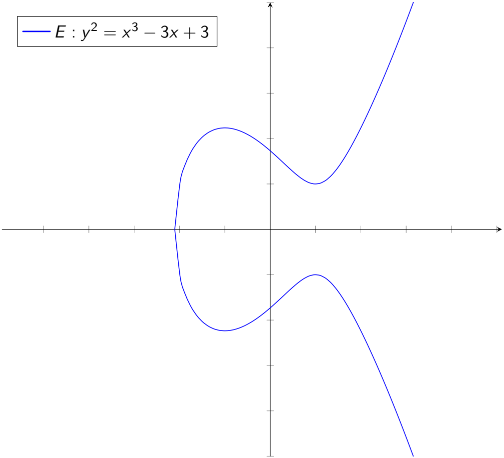
$$y^2 = x^3 + a_3x^2 + a_4x + a_5 \tag{4}$$

Phương trình có thể rút gọn hơn nữa nếu tính đặc trưng của trường khác 3, ta được phương trình đơn giản hơn, được gọi là phương trình Weierstrass.

$$y^2 = x^3 + ax + b \,|_{a=a_4, b=a_5} \tag{5}$$

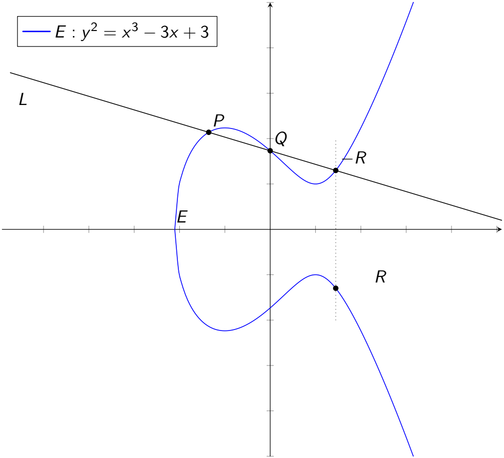
Đồ thị

Hình: Đường cong Elliptic E trên $\mathbb{R}^2$



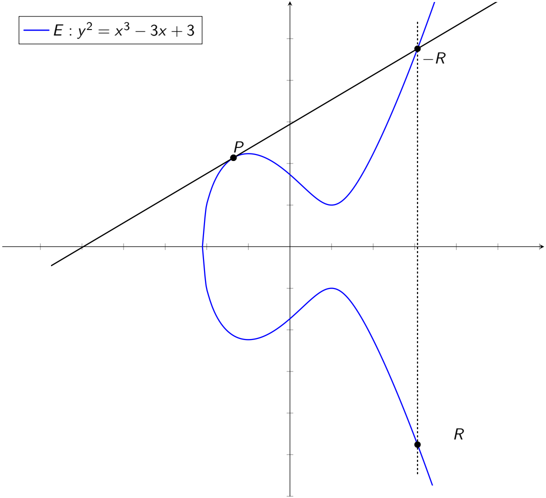
Đồ thị

Hình: Cộng hai điểm P và Q trên E



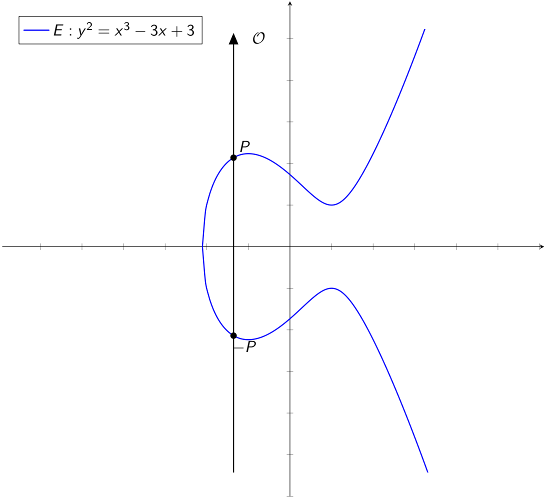
Đồ thị

Hình: Cộng hai điểm P và P trên E



Đồ thị

Hình: Cộng hai điểm P và $-P$ trên E



Tính $P + Q$ nếu $P(x_1, y_1)$ và $Q(x_2, y_2)$ phân biệt

Để sau

Tính $P + Q$ nếu $P(x_1, y_1)$ và $Q(x_2, y_2)$ phân biệt

Sử dụng phép cộng này, ta định nghĩa phép *nhân vô hướng* trên nhóm G

Definition

Phép *nhân vô hướng* trên nhóm G là phép cộng một điểm nhiều lần.

$$nP = \underbrace{P + P + \ldots + P}_{n} \tag{6}$$

Thuật toán nhân đôi và cộng

Algorithm 1: Nhân đôi và cộng

```
input  : n, P
output: R = nP
begin
    Q ← P
    E ← O
    while n > 0 do
        if n ≡ 1 (mod 2) then
            R ← R + Q
        else
            R ← R + Q
            Q ← 2 · Q
            n ← ⌊n/2⌋
        end
    end
    return R
end
```

References I

Vishwanath, K. V. and Nagappan, N. (2010).
Characterizing cloud computing hardware reliability.
SoCC '10, pages 193–204, New York, NY, USA. Association for Computing Machinery.