Logarit rời rạc

Toán Chuyên Đề

HUST

Ngày 30 tháng 11 năm 2017

Tài liệu tham khảo

- J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer-Verlag – Undergraduate Texts in Mathematics, 2nd Ed., 2014.
- T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein. *Introduction to Algorithms*, Third Edition (3rd ed.). The MIT Press. 2009.
- H. H. Khoái, P. H. Điển, *Số học thuật toán: cơ sở lý thuyết và tính toán thực hành*, NXB Đại học Quốc gia Hà Nội, 2003.

Nội dung

Nhắc lại

- Xét số nguyên tố (lớn) p và trường hữu hạn $\mathbb{F}_p$.
- Tồn tại căn nguyên thủy g, tức là mọi phần tử khác 0 của $\mathbb{F}_p$ đều là một lũy thức nào đó của g.
- Cụ thể

$$g^{p-1} = 1.$$

- Và

$$1,\ g,\ g^2,\ g^3,\ \cdots,\ g^{p-2} \in \mathbb{F}_p^*.$$

Định nghĩa

Xét g là một căn nguyên thủy của $\mathbb{F}_p$ và h là một phần tử khác 0 của $\mathbb{F}_p$. Bài toán Logarit rời rạc (DLP) là bài toán tìm một số mũ x thỏa mãn

$$g^x \equiv h \pmod{p}.$$

Số x được gọi là logarit rời rạc cơ sở g của h và ký hiệu $\log_g(h)$.

Bài tập

Hãy tính các logarit rời rạc sau.

1. $\log_2(13)$ cho số nguyên tố 23, cụ thể $p = 23, g = 2$ và bạn phải giải phương trình đồng dư $2^x \equiv 13 \pmod{23}$.
2. $\log_{10}(22)$ cho số nguyên tố $p = 47$.
3. $\log_{627}(608)$ cho số nguyên tố $p = 941$.

Ví dụ

- Xét số nguyên tố $p = 56509$, và ta có thể kiểm tra $g = 2$ là một căn nguyên thủy modun p.

Ví dụ

- Xét số nguyên tố $p = 56509$, và ta có thể kiểm tra $g = 2$ là một căn nguyên thủy modun p.
- Làm thế nào để tính $\log_2(38679)$?

Ví dụ

- Xét số nguyên tố $p = 56509$, và ta có thể kiểm tra $g = 2$ là một căn nguyên thủy modun p.
- Làm thế nào để tính $\log_2(38679)$?
- Một phương pháp là tính

$$2^0,\ 2^1,\ 2^2,\ 2^3,\ \cdots \pmod{56509}$$

cho đến khi được lũy thừa bằng 38679.

Ví dụ

- Xét số nguyên tố $p = 56509$, và ta có thể kiểm tra $g = 2$ là một căn nguyên thủy modun p.
- Làm thế nào để tính $\log_2(38679)$?
- Một phương pháp là tính

$$2^0,\ 2^1,\ 2^2,\ 2^3,\ \cdots \pmod{56509}$$

  cho đến khi được lũy thừa bằng 38679.
- Bạn có thể kiểm tra rằng

$$2^{11235} \equiv 38679 \pmod{56509}.$$

Nhận xét

Nếu bài toán Logarit rời rạc có nghiệm, vậy nó có vố số nghiệm vì

$$\begin{aligned} g^{x+k(p-1)} &= g^x \cdot g^{k(p-1)} \\ &= h \cdot 1^k && \text{(Định lý Fermat)} \\ &\equiv h \pmod{p}. \end{aligned}$$

Bài tập

Chứng minh rằng $\log_g$ là một hàm

$$\log_g : \mathbb{F}_p^* \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}.$$

Bài tập

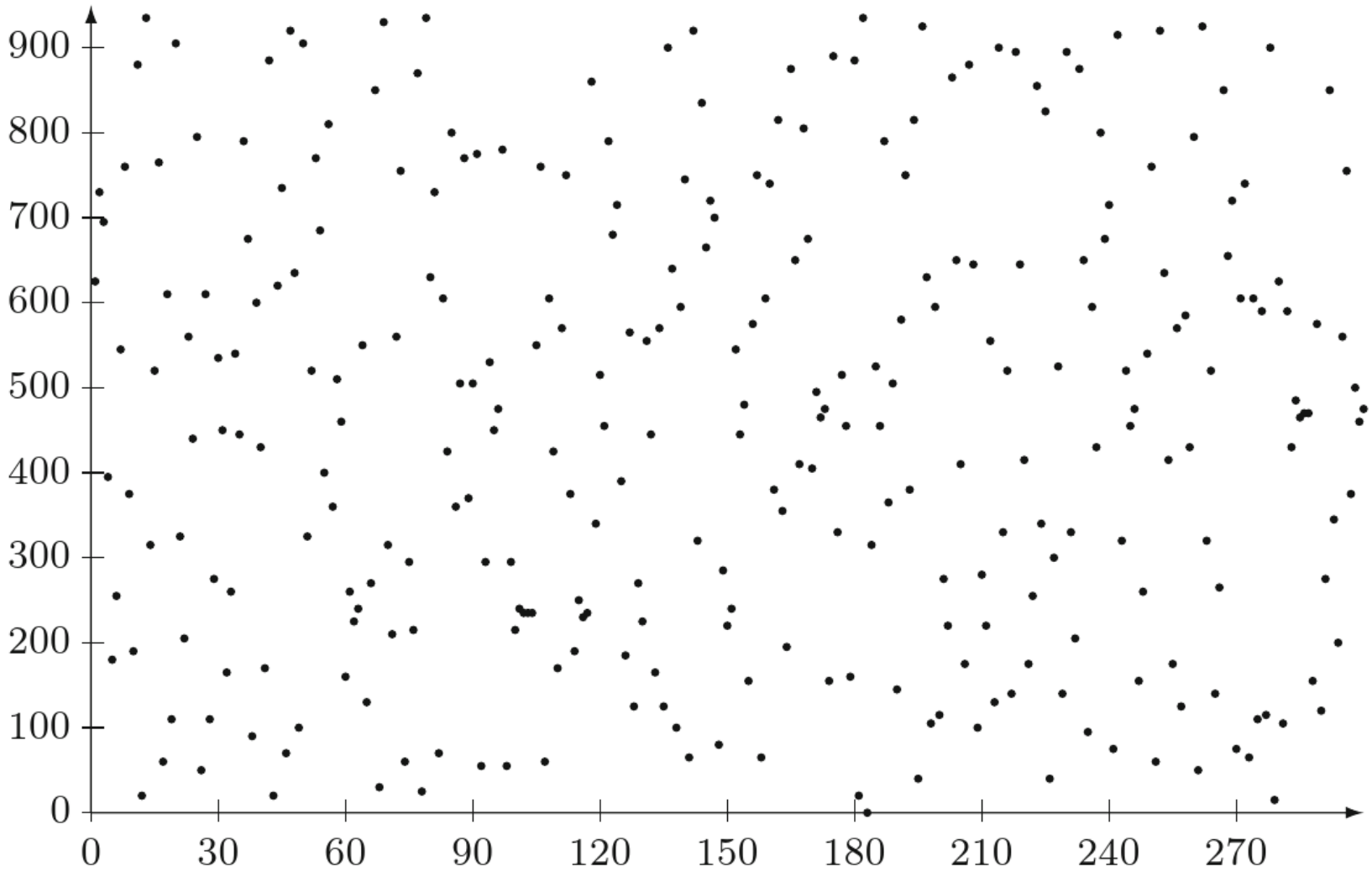
Chứng minh rằng

$$\log_g(ab) = \log_g(a) + \log_g(b).$$

Nhận xét

Bài toán logarit rời rạc không cần phải giả sử cơ sở g là một phần tử sinh của $\mathbb{F}_p$. Nói chung, xét $g \in \mathbb{F}_p^*$ và $h \in \mathbb{F}_p^*$, bài toán logarit rời rạc là xác định x sao cho $g^x \equiv h \pmod{p}$, giả sử rằng x tồn tại.

Tính ngẫu nhiên của lũy thừa $627^i \pmod{941}$



Bài toán logarit rời rạc trong nhóm

Định nghĩa

Xét nhóm G với phép toán $\star$. Bài toán Logarit rời rạc cho G là xác định số nguyên x thỏa mãn

$$\underbrace{g \star g \star \cdots \star g}_{x \text{ lần}} = h$$

với hai phần tử h và g trong G cho trước.

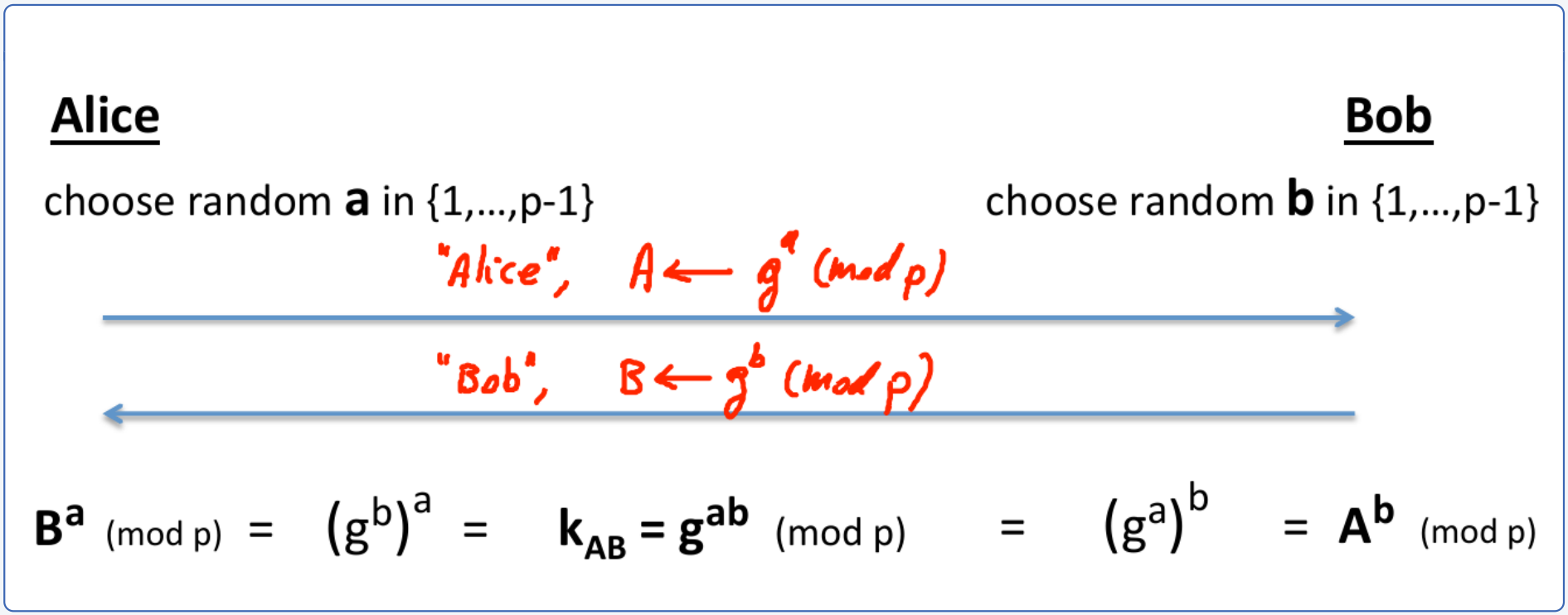
Nội dung

Bài toán

- Alice và Bob muốn trao đổi một khóa k chung dùng để mã hóa thông tin.
- Nhưng họ chỉ có một kênh trao đổi không an toàn: Thông tin truyền có thể bị nghe trộm.
- Liệu có cách để Alice và Bob trao đổi khóa mà dù bị Eve có nghe trộm?

Giao thức Diffie-Hellman

- Alice và Bob thống nhất một số nguyên tố (lớn) p và một số nguyên $g \pmod p$.
- Tốt nhất họ nên chọn g sao cho cấp của g trong $\mathbb{F}_p^*$ là một số nguyên tố lớn.
- Alice và Bob để hai giá trị p và g công khai (trên Website của của họ).



Ví dụ

- Alice và Bob thống nhất sử dụng số $p = 941$ và căn nguyên thủy $g = 627$.
- Alice chọn khóa bí mật $a = 347$.
- Bob chọn khóa bí mật $b = 781$.
- Hãy tính giá trị khóa chia sẻ của Alice và Bob.

Định nghĩa

Xét p là một số nguyên tố và g là một số nguyên. Bài toán Diffie-Hellman (DHP) là bài toán tính giá trị của

$$g^{ab} \pmod{p}$$

từ các giá trị $g^a \pmod{p}$ và $g^b \pmod{p}$.

DLP chọi DHP

Bài tập

Hãy chứng minh rằng DHP không khó hơn DLP. Có nghĩa rằng, nếu ta có thuật toán hiệu quả giải DLP, thì ta cũng có thuật toán hiệu quả giải DHP.

DLP chọi DHP

Bài tập

Hãy chứng minh rằng DHP không khó hơn DLP. Có nghĩa rằng, nếu ta có thuật toán hiệu quả giải DLP, thì ta cũng có thuật toán hiệu quả giải DHP.

Nhận xét

Ngược lại, giả sử rằng Eve có thuật toán hiệu quả giải DHP. Liệu cô ta có thể giải bài toán DLP? Đây vẫn là câu hỏi mở.

Bài tập

- Alice và Bob dùng số nguyên tố $p = 1373$ và cơ sở $g = 2$ để trao đổi khóa.

Bài tập

- Alice và Bob dùng số nguyên tố $p = 1373$ và cơ sở $g = 2$ để trao đổi khóa.
- Alice gửi Bob giá trị $A = 974$.

Bài tập

- Alice và Bob dùng số nguyên tố $p = 1373$ và cơ sở $g = 2$ để trao đổi khóa.
- Alice gửi Bob giá trị $A = 974$.
- Bob chọn số bí mật $b = 871$.

Bài tập

- Alice và Bob dùng số nguyên tố $p = 1373$ và cơ sở $g = 2$ để trao đổi khóa.
- Alice gửi Bob giá trị $A = 974$.
- Bob chọn số bí mật $b = 871$.
- Bob nên gửi cho Alice giá trị gì, và khóa bí mật họ chia sẻ là gì?

Bài tập

- Alice và Bob dùng số nguyên tố $p = 1373$ và cơ sở $g = 2$ để trao đổi khóa.
- Alice gửi Bob giá trị $A = 974$.
- Bob chọn số bí mật $b = 871$.
- Bob nên gửi cho Alice giá trị gì, và khóa bí mật họ chia sẻ là gì?
- Bạn có thể đoán được số bí mật a của Alice?

Nội dung

Một số tính chất của $\mathbb{F}_p^*$

- Có phần tử $1 \in \mathbb{F}_p^*$ thỏa mãn $1 \cdot a = a$.

Một số tính chất của $\mathbb{F}_p^*$

- Có phần tử $1 \in \mathbb{F}_p^*$ thỏa mãn $1 \cdot a = a$.
- Mọi phần tử $a \in \mathbb{F}_p^*$ đều có phần tử nghịch đảo a^{-1} thỏa mãn $a \cdot a^{-1} = 1$.

Một số tính chất của $\mathbb{F}_p^*$

- Có phần tử $1 \in \mathbb{F}_p^*$ thỏa mãn $1 \cdot a = a$.
- Mọi phần tử $a \in \mathbb{F}_p^*$ đều có phần tử nghịch đảo a^{-1} thỏa mãn $a \cdot a^{-1} = 1$.
- Phép nhân có tính chất kết hợp: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Một số tính chất của $\mathbb{F}_p^*$

- Có phần tử $1 \in \mathbb{F}_p^*$ thỏa mãn $1 \cdot a = a$.
- Mọi phần tử $a \in \mathbb{F}_p^*$ đều có phần tử nghịch đảo a^{-1} thỏa mãn $a \cdot a^{-1} = 1$.
- Phép nhân có tính chất kết hợp: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Phép nhân có tính chất giao hoán: $a \cdot b = b \cdot a$.

Tính chất của $\mathbb{F}_p^*$ liên quan đến phép cộng

- Có phần tử $0 \in \mathbb{F}_p^*$ thỏa mãn $0 + a = a$.

Tính chất của $\mathbb{F}_p^*$ liên quan đến phép cộng

- Có phần tử $0 \in \mathbb{F}_p^*$ thỏa mãn $0 + a = a$.
- Mọi phần tử $a \in \mathbb{F}_p^*$ đều có phần tử nghịch đảo $-a$ thỏa mãn $a + (-a) = 0$.

Tính chất của $\mathbb{F}_p^*$ liên quan đến phép cộng

- Có phần tử $0 \in \mathbb{F}_p^*$ thỏa mãn $0 + a = a$.
- Mọi phần tử $a \in \mathbb{F}_p^*$ đều có phần tử nghịch đảo $-a$ thỏa mãn $a + (-a) = 0$.
- Phép cộng có tính chất kết hợp: $a + (b + c) = (a + b) + c$.

Tính chất của $\mathbb{F}_p^*$ liên quan đến phép cộng

- Có phần tử $0 \in \mathbb{F}_p^*$ thỏa mãn $0 + a = a$.
- Mọi phần tử $a \in \mathbb{F}_p^*$ đều có phần tử nghịch đảo $-a$ thỏa mãn $a + (-a) = 0$.
- Phép cộng có tính chất kết hợp: $a + (b + c) = (a + b) + c$.
- Phép cộng có tính chất giao hoán: $a + b = b + a$.

Định nghĩa

Một nhóm bao gồm một tập G và một phép toán hai ngôi $\star$ trên G thỏa mãn ba tính chất:

Có đơn vị: Tồn tại một phần tử $e \in G$ sao cho

$$e \star a = a \star e = a \quad \text{với mọi } a \in G.$$

Định nghĩa

Một nhóm bao gồm một tập G và một phép toán hai ngôi $\star$ trên G thỏa mãn ba tính chất:

Có đơn vị: Tồn tại một phần tử $e \in G$ sao cho

$$e \star a = a \star e = a \quad \text{với mọi } a \in G.$$

Có nghịch đảo: Với mỗi phần tử $a \in G$ tồn tại $a^{-1} \in G$ sao cho

$$a \star a^{-1} = a^{-1} \star a = 1.$$

Định nghĩa

Một nhóm bao gồm một tập G và một phép toán hai ngôi $\star$ trên G thỏa mãn ba tính chất:

Có đơn vị: Tồn tại một phần tử $e \in G$ sao cho

$$e \star a = a \star e = a \quad \text{với mọi } a \in G.$$

Có nghịch đảo: Với mỗi phần tử $a \in G$ tồn tại $a^{-1} \in G$ sao cho

$$a \star a^{-1} = a^{-1} \star a = 1.$$

Kết hợp: $a \star (b \star c) = (a \star b) \star c$, với mọi $a, b, c \in G$.

Định nghĩa

Nhóm G với phép toán $\star$ có tính chất

Giao hoán: $a \star b = b \star a$ với mọi $a, b \in G$,

được gọi là nhóm giao hoán hoặc nhóm Abel.

Định nghĩa

- Nếu nhóm G có hữu hạn phần tử, ta gọi G là nhóm hữu hạn.

Định nghĩa

- Nếu nhóm G có hữu hạn phần tử, ta gọi G là nhóm hữu hạn.
- Cấp của nhóm G là số phần tử của G; nó thường được ký hiệu bởi $|G|$ hoặc $\#G$.

Ví dụ

- $G = F_p^*$ và $\star =$ phép nhân. Phần tử đơn vị là $e = 1$. Cấp của nhóm này là gì?

Ví dụ

- $G = F_p^*$ và $\star =$ phép nhân. Phần tử đơn vị là $e = 1$. Cấp của nhóm này là gì?
- $G = \mathbb{Z}/N\mathbb{Z}$ và $\star =$ phép cộng. Phần tử đơn vị là gì? Cấp của nhóm này là gì?

Ví dụ

- $G = F_p^*$ và $\star =$ phép nhân. Phần tử đơn vị là $e = 1$. Cấp của nhóm này là gì?
- $G = \mathbb{Z}/N\mathbb{Z}$ và $\star =$ phép cộng. Phần tử đơn vị là gì? Cấp của nhóm này là gì?
- $G = \mathbb{Z}$ và $\star =$ phép cộng. Phần tử đơn vị của nhóm này là gì? phần tử nghịch đảo của phần tử a là gì?

Ví dụ

- $G = F_p^*$ và $\star =$ phép nhân. Phần tử đơn vị là $e = 1$. Cấp của nhóm này là gì?
- $G = \mathbb{Z}/N\mathbb{Z}$ và $\star =$ phép cộng. Phần tử đơn vị là gì? Cấp của nhóm này là gì?
- $G = \mathbb{Z}$ và $\star =$ phép cộng. Phần tử đơn vị của nhóm này là gì? phần tử nghịch đảo của phần tử a là gì?
- $G = \mathbb{Z}$ và $\star =$ phép nhân có phải là nhóm không? Tại sao?

Ví dụ

- $G = F_p^*$ và $\star =$ phép nhân. Phần tử đơn vị là $e = 1$. Cấp của nhóm này là gì?
- $G = \mathbb{Z}/N\mathbb{Z}$ và $\star =$ phép cộng. Phần tử đơn vị là gì? Cấp của nhóm này là gì?
- $G = \mathbb{Z}$ và $\star =$ phép cộng. Phần tử đơn vị của nhóm này là gì? phần tử nghịch đảo của phần tử a là gì?
- $G = \mathbb{Z}$ và $\star =$ phép nhân có phải là nhóm không? Tại sao?
- $G = \mathbb{R}^*$ và $\star =$ phép nhân có phải là nhóm không? Tại sao?

Bài tập

- Một ví dụ của nhóm không giao hoán là

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a, b, c, d \in \mathbb{R} \text{ và } ad - bc \neq 0 \right\}$$

với $\star =$ phép nhân ma trận.

Bài tập

- Một ví dụ của nhóm không giao hoán là

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a, b, c, d \in \mathbb{R} \text{ và } ad - bc \neq 0 \right\}$$

  với $\star =$ phép nhân ma trận.
- Phần tử đơn vị của nhóm này là gì? Hãy tìm công thức tính phần tử nghịch đảo

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}.$$

Bài tập

- Một ví dụ của nhóm không giao hoán là

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a, b, c, d \in \mathbb{R} \text{ và } ad - bc \neq 0 \right\}$$

  với $\star =$ phép nhân ma trận.
- Phần tử đơn vị của nhóm này là gì? Hãy tìm công thức tính phần tử nghịch đảo

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}.$$

- Tại sao đây không phải là nhóm giao hoán?

Ví dụ

Nhóm tuyến tính tổng quát

$$GL_n(\mathbb{R}) = \{ \text{ ma trận thực } A \text{ kích thước } n \times n \text{ với } \det(A) \neq 0 \}$$

với $\star =$ phép nhân ma trận.

Thay $\mathbb{R}$ bởi trường hữu hạn $\mathbb{F}_p^*$, ta được nhóm $GL(\mathbb{F}_p^*)$.

Định nghĩa

Xét G là một nhóm và x là một số nguyên dương. Ta ký hiệu g^x là

$$g^x = \underbrace{g \star g \star \cdots \star g}_{x \text{ lần}}$$

Ví dụ

- g^x trong nhóm $\mathbb{F}_p^*$ theo nghĩa thông thường.

Ví dụ

- g^x trong nhóm $\mathbb{F}_p^*$ theo nghĩa thông thường.
- g^x trong nhóm $\mathbb{Z}/N\mathbb{Z}$ với phép cộng có nghĩa rằng

$$x \cdot g = g + g + \cdots + g$$

Định nghĩa

Xét nhóm G và một phần tử $a \in G$. Giả sử rằng có tồn tại số nguyên dương d sao cho $a^d = e$. Số nguyên nhỏ nhất d có tính chất này gọi là cấp của a. Nếu không tồn tại số nguyên như vậy thì a gọi là có cấp vô hạn.

Mệnh đề

- *Xét nhóm hữu hạn G. Vậy thì mọi phần tử của G có cấp hữu hạn.*

Bài tập: Hãy chứng minh mệnh đề trên.

Mệnh đề

- *Xét nhóm hữu hạn G. Vậy thì mọi phần tử của G có cấp hữu hạn.*
- *Hơn nữa, nếu $a \in G$ có cấp d và nếu $a^k = e$, vậy thì $d \mid k$.*

Bài tập: Hãy chứng minh mệnh đề trên.

Định lý (Lagrange)

- *Xét G là nhóm hữu hạn và xét $a \in G$. Vậy thì cấp của G chia hết cho cấp của a.*

Bài tập: Hãy chứng minh định lý trên.

Định lý (Lagrange)

- *Xét G là nhóm hữu hạn và xét $a \in G$. Vậy thì cấp của G chia hết cho cấp của a.*
- *Chính xác hơn, xét $n = \#G$ và d là cấp của a, tức a^d là lũy thừa nguyên dương nhỏ nhất bằng với e. Khi đó*

$$a^n = e \qquad \text{và} \qquad d \mid n.$$

Bài tập: Hãy chứng minh định lý trên.

Nội dung

Bài toán logarit rời rạc trong nhóm

Định nghĩa (Nhắc lại)

Xét nhóm G với phép toán $\star$. Bài toán Logarit rời rạc cho G là tìm số nguyên x thỏa mãn

$$g^x = h$$

với hai phần tử h và g trong G cho trước.

Mệnh đề (Chặn tầm thường cho DLP)

Xét nhóm G và $g \in G$ là một phần tử có cấp N. Vậy thì bài toán logarit rời rạc

$$g^x = h$$

có thể được giải trong thời gian $\mathcal{O}(N)$ bước, mỗi bước gồm phép nhân với g.

Mệnh đề (Thuật toán Babystep-Giantstep)

Xét nhóm G và $g \in G$ là một phần tử có cấp $N \geq 2$. Thuật toán sau đây giải bài toán logarit rời rạc $g^x = h$ trong $\mathcal{O}(\sqrt{N} \cdot \log N)$ bước.

1. *Đặt $n = 1 + \lfloor \sqrt{N} \rfloor$, cụ thể $n > \sqrt{N}$.*

Mệnh đề (Thuật toán Babystep-Giantstep)

Xét nhóm G và $g \in G$ là một phần tử có cấp $N \geq 2$. Thuật toán sau đây giải bài toán logarit rời rạc $g^x = h$ trong $\mathcal{O}(\sqrt{N} \cdot \log N)$ bước.

1. *Đặt $n = 1 + \lfloor \sqrt{N} \rfloor$, cụ thể $n > \sqrt{N}$.*
2. *Xây dựng hai danh sách:*

$$L_1: \quad e,\ g,\ g^2,\ g^3,\ \cdots,\ g^n,$$
$$L_2: \quad h,\ h \cdot g^{-n},\ h \cdot g^{-2n},\ h \cdot g^{-3n},\ \cdots,\ h \cdot g^{-n^2}.$$

Mệnh đề (Thuật toán Babystep-Giantstep)

Xét nhóm G và $g \in G$ là một phần tử có cấp $N \geq 2$. Thuật toán sau đây giải bài toán logarit rời rạc $g^x = h$ trong $\mathcal{O}(\sqrt{N} \cdot \log N)$ bước.

1. *Đặt $n = 1 + \lfloor \sqrt{N} \rfloor$, cụ thể $n > \sqrt{N}$.*
2. *Xây dựng hai danh sách:*
   L_1: $e,\ g,\ g^2,\ g^3,\ \cdots,\ g^n,$
   L_2: $h,\ h \cdot g^{-n},\ h \cdot g^{-2n},\ h \cdot g^{-3n},\ \cdots,\ h \cdot g^{-n^2}.$
3. *Tìm i, j thỏa mãn $g^i = h \cdot g^{-jn}$.*

Mệnh đề (Thuật toán Babystep-Giantstep)

Xét nhóm G và $g \in G$ là một phần tử có cấp $N \geq 2$. Thuật toán sau đây giải bài toán logarit rời rạc $g^x = h$ trong $\mathcal{O}(\sqrt{N} \cdot \log N)$ bước.

1. *Đặt $n = 1 + \lfloor \sqrt{N} \rfloor$, cụ thể $n > \sqrt{N}$.*
2. *Xây dựng hai danh sách:*
   L_1: $e,\ g,\ g^2,\ g^3,\ \cdots,\ g^n,$
   L_2: $h,\ h \cdot g^{-n},\ h \cdot g^{-2n},\ h \cdot g^{-3n},\ \cdots,\ h \cdot g^{-n^2}.$
3. *Tìm i, j thỏa mãn $g^i = h \cdot g^{-jn}$.*
4. *Vậy thì $x = i + jn$ là một nghiệm của $g^x = h$.*

Thuật toán Babystep-Giantstep (chi tiết)

- *Input:* Các phần tử $g, h \in G$; cấp N của g.
- *Output:* $x = \log_g(h)$.

$n = 1 + \lfloor \sqrt{N} \rfloor$
for $i = 0$ to n :
    Tính $g_i = g^i$
Sắp xếp các cặp (i, g_i) theo giá trị g_i
for $j = 0$ to n :
    Tính $h_j = h \cdot g^{-jn}$
    if $h_j == g_i$ với i nào đó : //Dùng tìm kiếm nhị phân
        return $x = i + jn$
return "không tồn tại x"

Bài tập

- Xét nhóm $\mathbb{F}_{29}^*$ có cấp $N = 29 - 1 = 28$.

Bài tập

- Xét nhóm $\mathbb{F}_{29}^*$ có cấp $N = 29 - 1 = 28$.
- Lấy $g = 2$ và $h = 17$.

Bài tập

- Xét nhóm $\mathbb{F}_{29}^*$ có cấp $N = 29 - 1 = 28$.
- Lấy $g = 2$ và $h = 17$.
- Ta có $n = 6$.

Bài tập

- Xét nhóm $\mathbb{F}_{29}^*$ có cấp $N = 29 - 1 = 28$.
- Lấy $g = 2$ và $h = 17$.
- Ta có $n = 6$.
- Ta đã tính các lũy thừa g^i như bảng dưới đây. Hãy hoàn thành nốt bảng và tìm $\log_2(17)$:

i	0	1	2	3	4	5	6
g^i	1	2	4	8	16	3	6
$h \cdot g^{-6i}$							

biết rằng $2^{-6} = 5$.

Nội dung

Bài toán

- Có một số vật ta chưa biết số lượng bao nhiêu.

Bài toán

- Có một số vật ta chưa biết số lượng bao nhiêu.
- Số này chia 3 dư 2.

Bài toán

- Có một số vật ta chưa biết số lượng bao nhiêu.
- Số này chia 3 dư 2.
- Số này chia 5 dư 3.

Bài toán

- Có một số vật ta chưa biết số lượng bao nhiêu.
- Số này chia 3 dư 2.
- Số này chia 5 dư 3.
- Số này chia 7 dư 2.

Bài toán

- Có một số vật ta chưa biết số lượng bao nhiêu.
- Số này chia 3 dư 2.
- Số này chia 5 dư 3.
- Số này chia 7 dư 2.
- Hỏi có bao nhiêu vật ?

Ví dụ

Tìm số nguyên x thỏa mãn đồng thời cả hai phương trình

$$x \equiv 1 \pmod 5 \qquad \text{và} \qquad x \equiv 9 \pmod{11}.$$

Nghiệm của phương trình thứ nhất là tập các số nguyên

$$x = 1 + 5y, \qquad y \in \mathbb{Z}.$$

Thế vào phương trình thứ hai, ta được

$$1 + 5y \equiv 9 \pmod{11} \qquad \Leftrightarrow \qquad 5y \equiv 8 \pmod{11}$$

Nhân cả hai vế với $5^{-1} \equiv 9 \pmod{11}$. Ta được

$$y \equiv 9 \cdot 8 \equiv 72 \equiv 6 \pmod{11}$$

Thay lại vào phương trình đầu ta được $x = 1 + 5 \cdot 6 = 31$.

Định lý (Định lý phần dư Trung Hoa)

Xét $m_1, m_2, \ldots, m_k$ là các số đôi một nguyên tố cùng nhau. Xét các số nguyên $a_1, a_2, \ldots, a_k$ bất kỳ. Khi đó hệ phương trình

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \cdots, \quad x \equiv a_k \pmod{m_k}$$

có một nghiệm $x = c$. Hơn nữa, nếu $x = c$ và $x = c'$ là hai nghiệm của hệ, vậy thì

$$c \equiv c' \pmod{m_1 m_2 \ldots m_k}.$$

Ví dụ

- Xét hệ ba phương trình sau đây

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 7, \qquad x \equiv 4 \pmod{16}.$$

Ví dụ

- Xét hệ ba phương trình sau đây

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 7, \qquad x \equiv 4 \pmod{16}.$$

- Dùng một nghiệm $x = 2$ của phương trình đầu để tìm nghiệm thỏa mãn cả hai phương trình đầu tiên. Ta được $x = 17$.

Ví dụ

- Xét hệ ba phương trình sau đây

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 7, \qquad x \equiv 4 \pmod{16}.$$

- Dùng một nghiệm $x = 2$ của phương trình đầu để tìm nghiệm thỏa mãn cả hai phương trình đầu tiên. Ta được $x = 17$.
- Dùng nghiệm này để tìm nghiệm thỏa mãn cả ba phương trình. Ta được $x = 164$.

Công thức nghiệm

- Xét $m_1, m_2, \ldots, m_k$ là các số đôi một nguyên tố cùng nhau. Xét các số nguyên $a_1, a_2, \ldots, a_k$ bất kỳ.
- Khi đó hệ phương trình

$$x \equiv a_1 \pmod{m_1}, \cdots, x \equiv a_k \pmod{m_k}$$

có nghiệm duy nhất

$$x = \sum_{i=1}^{k} a_i b_i M/m_i$$

trong đó: $M = m_1 \ldots m_k$ và $b_i = (M/m_i)^{-1} \pmod{m_i}$.

Đẳng cấu giữa $\mathbb{Z}_{pq}$ và $\mathbb{Z}_p \times \mathbb{Z}_q$

Ta có thể biểu diễn một phần tử của $\mathbb{Z}_{pq}$ bởi một phần tử của $\mathbb{Z}_p$ và một phần tử của $\mathbb{Z}_q$, và ngược lại.

Hơn nữa, nếu $x, y \in \mathbb{Z}_{pq}$ tương ứng với $(a, b), (c, d) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Khi đó

$$\begin{aligned} x + y &\rightarrow (a + c, b + d) \\ xy &\rightarrow (ac, bd) \end{aligned}$$

Ví dụ

Ta có thể viết:

$$\begin{aligned} 17 \in \mathbb{Z}_{35} &\longleftrightarrow (2, 3) \in \mathbb{Z}_5 \times \mathbb{Z}_7 \\ 2 \in \mathbb{Z}_{35} &\longleftrightarrow (2, 2) \in \mathbb{Z}_5 \times \mathbb{Z}_7 \\ 17 \times 2 \in \mathbb{Z}_{35} &\longleftrightarrow (4, 6) \in \mathbb{Z}_5 \times \mathbb{Z}_7 \end{aligned}$$

Câu hỏi

Bài tập

Cặp số $(3, 5) \in \mathbb{Z}_5 \times \mathbb{Z}_7$ tương ứng với số gì trong $\mathbb{Z}_{35}$?

Ứng dụng thực tế

Nếu ta cần thực hiện nhiều tính toán trên giá trị $x \in \mathbb{Z}_{pq}$ (ví dụ: ký hoặc giải mã RSA), thì ta có thể chuyển x về $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$ và thực hiện các tính toán trên (a, b).

Mệnh đề

Xét p là một số nguyên tố thỏa mãn $p \equiv 3 \pmod 4$. Xét a là số nguyên sao cho $x^2 \equiv a \pmod p$ có nghiệm, tức là a có căn bậc hai. Vậy thì

$$b \equiv a^{(p+1)/4} \pmod p$$

là một nghiệm; nó thỏa mãn $b^2 \equiv a \pmod p$.

Ví dụ

Một căn bậc hai của $a = 2201$ trong modun nguyên tố $p = 4127$ là

$$b \equiv a^{(p+1)/4} = 2201^{4128/4} = 2201^{1032} \equiv 3718 \pmod{4127}.$$

Ta có thể kiểm tra xem a có căn bậc hai không bằng cách bình phương b lên.

Tính căn trong modun m không nguyên tố

- Phân tích số m thành các thừa số nguyên tố,

Tính căn trong modun m không nguyên tố

- Phân tích số m thành các thừa số nguyên tố,
- tính căn trong modun thừa số nguyên tố này,

Tính căn trong modun m không nguyên tố

- Phân tích số m thành các thừa số nguyên tố,
- tính căn trong modun thừa số nguyên tố này,
- kết hợp lời giải dùng định lý phần dư Trung Hoa.

Ví dụ

- Để tìm nghiệm của phương trình

$$x^2 \equiv 197 \pmod{437}.$$

- Phân tích $437 = 19 \cdot 23$.
- Giải hai phương trình

$$y^2 \equiv 197 \equiv 7 \pmod{19} \qquad \text{và} \qquad z^2 \equiv 197 \equiv 13 \pmod{23}$$

Ví dụ

- Để tìm nghiệm của phương trình

$$x^2 \equiv 197 \pmod{437}.$$

- Phân tích $437 = 19 \cdot 23$.
- Giải hai phương trình

$$y^2 \equiv 197 \equiv 7 \pmod{19} \qquad \text{và} \qquad z^2 \equiv 197 \equiv 13 \pmod{23}$$

- Giải hai phương trình trên ta được $y \equiv \mp 8$ và $z \equiv \mp \pmod{23}$.

Ví dụ

- Để tìm nghiệm của phương trình

$$x^2 \equiv 197 \pmod{437}.$$

- Phân tích $437 = 19 \cdot 23$.
- Giải hai phương trình

$$y^2 \equiv 197 \equiv 7 \pmod{19} \qquad \text{và} \qquad z^2 \equiv 197 \equiv 13 \pmod{23}$$

- Giải hai phương trình trên ta được $y \equiv \mp 8$ và $z \equiv \mp \pmod{23}$.
- Chọn hai nghiệm nguyên dương ta được

$$x \equiv 8 \pmod{19} \qquad \text{và} \qquad x \equiv 6 \pmod{23}.$$

Ví dụ

- Để tìm nghiệm của phương trình

$$x^2 \equiv 197 \pmod{437}.$$

- Phân tích $437 = 19 \cdot 23$.
- Giải hai phương trình

$$y^2 \equiv 197 \equiv 7 \pmod{19} \qquad \text{và} \qquad z^2 \equiv 197 \equiv 13 \pmod{23}$$

- Giải hai phương trình trên ta được $y \equiv \mp 8$ và $z \equiv \mp \pmod{23}$.
- Chọn hai nghiệm nguyên dương ta được

$$x \equiv 8 \pmod{19} \qquad \text{và} \qquad x \equiv 6 \pmod{23}.$$

- Cuối cùng, ta được $x \equiv 236 \pmod{437}$.

Nội dung

Ý tưởng

- Từ phân tích thừa số nguyên tố của $m = m_1 \cdot m_2 \cdot m_3 \cdots m_t$, ta có thể dùng định lý phần dư Trung Hoa để giải phương trình theo modun m bằng cách giải các phương trình theo modun m_i.

Ý tưởng

- Từ phân tích thừa số nguyên tố của $m = m_1 \cdot m_2 \cdot m_3 \cdots m_t$, ta có thể dùng định lý phần dư Trung Hoa để giải phương trình theo modun m bằng cách giải các phương trình theo modun m_i.
- Trong bài toán logarit rời rạc ta cần giải

$$g^x \equiv h \pmod{p}$$

với $x \in \mathbb{Z}/(p-1)\mathbb{Z}$.

Ý tưởng

- Từ phân tích thừa số nguyên tố của $m = m_1 \cdot m_2 \cdot m_3 \cdots m_t$, ta có thể dùng định lý phần dư Trung Hoa để giải phương trình theo modun m bằng cách giải các phương trình theo modun m_i.
- Trong bài toán logarit rời rạc ta cần giải

$$g^x \equiv h \pmod{p}$$

  với $x \in \mathbb{Z}/(p-1)\mathbb{Z}$.
- Phân tích thừa số nguyên tố của $p-1$ có thể giúp tìm x nhanh hơn?

Định lý

Xét G là một nhóm và giả sử có thuật toán để giải bài toán logarit rời rạc cho mọi phần tử có cấp là lũy thừa của một số nguyên tố. Cụ thể, nếu g có cấp q^e và ta có thể giải $g^x = h$ trong $\mathcal{O}(S_{q^e})$ bước.

Bây giờ, xét $g \in G$ là một phần tử có cấp N, và giả sử N phân tích được thành tích các thừa số nguyên tố

$$N = q_1^{e_1} \cdot q_2^{e^2} \cdots q_t^{e_t}.$$

Khi đó, bài toán logarit rời rạc $g^x = h$ có thể giải trong

$$\mathcal{O}\left(\sum_{i=1}^{t} S_{q_i^{e_i}} + \log N\right).$$

dùng thuật toán Pohlig-Hellman.

Thuật toán Pohlig-Hellman

1. Với mỗi $1 \leq i \leq t$. Xét

$$g_i = g^{N/q_i^{e_i}} \qquad \text{và} \qquad h_i = h^{N/q_i^{e_i}}$$

Chú ý rằng g_i có cấp là lũy thừa của một số nguyên tố $q_i^{e_i}$, vậy thì ta dùng thuật toán đã biết để giải phương trình.

$$g_i^y = h_i.$$

Gọi $y = y_i$ là nghiệm.

2. Dùng định lý phần dư Trung Hoa để giải hệ phương trình

$$\begin{aligned} x &\equiv y_1 \pmod{q_1^{e_1}}, \\ x &\equiv y_2 \pmod{q_2^{e_2}}, \\ &\cdots \\ x &\equiv y_t \pmod{q_t^{e_t}}. \end{aligned}$$

Ví dụ

- Xét bài toán tính logarit rời rạc trong nhóm $\mathbb{F}_{31}^*$ có cấp

$$p - 1 = 30 = 5 \cdot 3 \cdot 2$$

Ví dụ

- Xét bài toán tính logarit rời rạc trong nhóm $\mathbb{F}_{31}^*$ có cấp

$$p - 1 = 30 = 5 \cdot 3 \cdot 2$$

- với $g = 3$ và $h = 26 = g^x$.

Ví dụ

- Xét bài toán tính logarit rời rạc trong nhóm $\mathbb{F}_{31}^*$ có cấp

$$p - 1 = 30 = 5 \cdot 3 \cdot 2$$

- với $g = 3$ và $h = 26 = g^x$.
- Ta có

$$\left(g^{30/5}\right)^x = h^{30/5} \quad \Rightarrow \quad (3^6)^x = 26^6 \quad \Rightarrow \quad 16^x = 1$$
$$\left(g^{30/3}\right)^x = h^{30/3} \quad \Rightarrow \quad (3^{10})^x = 26^{10} \quad \Rightarrow \quad 25^x = 5$$
$$\left(g^{30/2}\right)^x = h^{30/2} \quad \Rightarrow \quad (3^{15})^x = 26^{15} \quad \Rightarrow \quad 30^x = 30$$

Các phương trình trên đều theo modun 31.

Ví dụ (tiếp)

Giải mỗi phương trình ta được hệ

$$\begin{aligned} x &\equiv 0 \pmod 5 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 2 \end{aligned}$$

Giải hệ này ta được

$$x \equiv 5 \pmod{30}.$$

Đây chính là nghiệm của bài toán logarit. Thật vậy

$$3^5 \equiv 26 \pmod{31}.$$