CAO HỌC KHTN – KHOA HỌC MÁY TÍNH 2021

Ôn thi giữa kỳ, cuối kỳ môn: Phương pháp Toán cho Tin học

Chú ý các dạng Toán.

- Tính số phần tử của $U(\mathbb{Z}_n)$ theo công thức phi.

- Mã hóa RSA trên các trường:

  + Số nguyên.

  + Đa thức.

  + Ma trận vuông cấp hai.

Bài 1.

a) Tập hợp U($\mathbb{Z}_{135}$) có bao nhiêu phần tử? Hãy liệt kê 5 phần tử lớn hơn 10 của tập này.

b) Những cặp số nguyên dương (***E***, ***D***) thỏa mãn $(\mathbf{a}^{E})^{D} = \mathbf{a}$ với mọi **a** ∈ U($\mathbb{Z}_{135}$) phải thỏa mãn điều kiện gì?

c) Hãy chỉ ra 3 cặp số nguyên dương (***E***, ***D***) với ***E*** < ***D*** mà ta có thể mã hóa các phần tử của U($\mathbb{Z}_{135}$) bằng ***E*** để có các bản mã và giải mã các bản mã bằng ***D*** để có các bản rõ.

Z[n]: là tập hợp các số {0,1,2,…,n-1} → hiểu là số dư khi chia một số nguyên bất kỳ cho n.

U(Z[n]): là các phần tử khả nghịch, tức là sẽ có nghịch đảo trong Z[n].

VD. n=8 → số 3 thuộc U(Z[8]) vì 3.3=1 trong Z[8], còn số 4 không phải.

-3 = 5 trong Z[8], 100 = 4 trong Z[8].

Tổng quát: $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ thì $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$.

Bài 1. a) Ta có: 135 = 3.3.3.5 = 3^3.5.

Số phần tử của U(Z[135]) = phi(135) = 135.(1-1/3)(1-1/5) = 135.2/3.4/5= 72.

Liệt kê các phần tử: 11, 13, 14, 16, 17, … lấy các số không chia hết cho 3 và 5.

b) Mã hóa RSA: a → a^E (mã hóa) → (a^E)^D = a^(ED) = a (giải mã).

<u>Định lý Euler</u>: a^phi(n) = 1 trong Z[n] với mọi a khả nghịch (tức là thuộc U(Z[n]).

Đặc biệt: a^72 = 1 trong Z[135].

ED = 72+1=73 → a^73 = a^72.a = 1.a=a trong Z[135].

ED = 2.72+1=145 → a^145 = (a^144).a = (a^72)^2.a = 1^2.a = a trong Z[135].

ED = 3.72+1=217

Điều kiện: ED chia 72 dư 1 → dùng được.

1 < E < D< 72 và $ED = \bar{1}$ trong Z[phi(135)]=Z[72].

c) Ta chọn các cặp số từ điều kiện trên.

145 → (E,D)=(5,29); 217 → (E,D)=(7,31);

Cần liệt kê tất cả: E, D khả nghịch trong Z[72].

72=2^3.3^2

(5,7,11,13,17,...) → phi(72) số như vậy: 72*(1-1/2)(1-1/3)=72.1/2.2/3=24.

5*29 chia 72 dư 1.

7*31 chia 72 dư 1.

11*59 chia 72 dư 1.

1	5	7	11								29	31											
1	29	31	59								5	7											

Cách tìm số 59: Lại áp dụng định lý Euler: 11^phi(72)=11^24 = 1 trong Z[72].

→ Số nghịch đảo của 11 chính là 11^23 → tìm số dư khi chia cho 72.

Từ đó tìm được 11*59.

Bài 2

Đặt $\boldsymbol{n}$=231. Xét vành $\mathbb{Z}_n$ với phép cộng và nhân modulo. Gọi U($\mathbb{Z}_n$) là tập các phần tử đơn vị (phần tử khả nghịch với phép nhân) của $\mathbb{Z}_n$.

a) Điều kiện cần và đủ mà a phải thỏa mãn để $\bar{a} \in U(\mathbb{Z}_n)$?

b) U($\mathbb{Z}_n$) có bao nhiêu phần tử?

c) Tìm điều kiện cho hai số nguyên dương *K1, K2, 1<K1<K2<**n*** để ta có $(x^{K1})^{K2} = x$ với mọi $x \in U(\mathbb{Z}_n)$.

d) Với *K1, K2* như thế nào thì $(x^{K1})^{K2} = x$ với mọi $x \in \mathbb{Z}_n$?

(Đề giữa kỳ 2011)

a) Điều kiện cần & đủ: số a phải nguyên tố cùng nhau với n → gcd(a,n)=1.

231 = 11.21=3.7.11.

phi(231)=231.(1-1/3).(1-1/7).(1-1/11)=120.

→ có 120 số U(Z[231]) và 231-120 số thuộc phần còn lại; nghĩa là nó sẽ có ước chung nào đó với 231, tức là nó sẽ chia hết 3 hoặc 7 hoặc 11.

d) Điều kiện vẫn như cũ: K1.K2 = 1+k.phi(n) với k là số nguyên: định lý Euler.

x^(K1.K2) = x^(1+k.phi(n))=x.x^k(phi(n))=x đúng với mọi x thuộc Z[n], không nhất thuộc phải thuộc U(Z[n]).

Bài 3

Gọi U($\mathbb{Z}_{35}$) là tập các phần tử khả nghịch với phép nhân của $\mathbb{Z}_{35}$.

a) U($\mathbb{Z}_{35}$) có bao nhiêu phần tử?

b) Tập U($\mathbb{Z}_{35}$) có tạo thành nhóm đối với phép nhân hay không?

c) Tìm cấp của mỗi tử trong U($\mathbb{Z}_{35}$) theo phép toán nhân.

(Giữa kỳ 2012)

b) Tạo thành nhóm với phép nhân?

Nhóm: tập hợp các số trên đó có chọn ra một phép toán (cộng, nhân, ...) thỏa mãn:

- Phần tử đơn vị: 1.

- Phần tử nghịch đảo: có, mỗi số trong U(Z[35]) đều có nghịch đảo.

- Đóng với phép toán đó: tích của số trong U(Z[35]) → cũng thuộc U(Z[35).

- Tính kết hợp: (a.b).c) = a.(b.c)

Tổng quát: ký hiệu phép toán *, phần tử đơn vị là e: với mọi a thì a*e = e*a = a.

VD. tập hợp số nguyên và phép cộng → phần tử đơn vị: 0.

tập hợp số nguyên và phép nhân → phần tử đơn vị: 1.

gcd(a,35)=gcd(b,35)=1 → gcd(ab,35)=1.

VD: tập hợp các số lẻ → không đóng với phép cộng nhưng đóng với phép nhân.

c) Cấp là số nguyên dương k nhỏ nhất để a^k = phần tử đơn vị trong nhóm đó.

Phi(35)=35.4/5.6/7=24.

U(Z[35])={1,2,3,4,6,....} có phần tử đơn vị là 1.

1^1=1 trong Z[35] → cấp = 1.

2^24 = 1 trong Z[35], thử các ước của 24 → có số 12: 2^12=1 (thử 2^8, 2^6 không được) → cấp = 12.

3^24 = 1 trong Z[35], ...

Chú ý: muốn tìm cấp của số a trong U(Z[n]) → dựa theo phi(n) → xét thêm một số ước lớn của phi(n) để tìm xem có ước k nào mà: a^k = 1 trong Z[n].

Bài 2

Gọi U($\mathbb{Z}_{70}$) là tập các phần tử khả nghịch với phép nhân của $\mathbb{Z}_{70}$.

a) U($\mathbb{Z}_{70}$) có bao nhiêu phần tử?

b) Tập U($\mathbb{Z}_{70}$) có tạo thành nhóm đối với phép nhân hay không?

c) Tìm cấp của mỗi tử trong U($\mathbb{Z}_{70}$) theo phép toán nhân.

d) Tập U($\mathbb{Z}_{70}$) có thể mã hóa bởi ánh xạ $f(x)= x^D$ và giải mã bởi ánh xạ ngược $g(y) = y^E$ với D và E là hai số nguyên khác nhau hay không?

e) Có thể mở rộng câu d) nói trên trong đó ta thay tập U($\mathbb{Z}_{70}$) bởi toàn bộ tập $\mathbb{Z}_{70}$ hay không?

(giữa kỳ 2018)

Đề thi giữa kỳ

PHƯƠNG PHÁP TOÁN

(90 phút – được phép dùng tài liệu)

Bài 1.

Tập $D\left[\sqrt{5}\right]=\left\{x+y\sqrt{5}/x,y\in \mathbf{Z}; x^2-5y^2=1\right\}$ với phép nhân có tạo thành nhóm hay không? Hãy chứng minh hay cho phản ví dụ.

Bài 2.

Tập hợp $\mathbb{Z}_{1024} \setminus \{\ \overline{0}\ \}$ có tạo thành nhóm với phép nhân hay không? Hãy chứng minh hay cho phản ví dụ.

Bài 3.

Đặt n = 231 và xét $\mathbb{Z}_n$ với phép cộng. Gọi U($\mathbb{Z}_n$) là tập các phần tử khả nghịch nhân của tập $\mathbb{Z}_n$.

a) Cho một ví dụ $\overline{a} \in U(\mathbb{Z}_n)$ và cho biết nghịch đảo nhân của $\overline{a}$.

b) U($\mathbb{Z}_n$) có bao nhiêu phần tử?

c) Tìm điều kiện cho hai số nguyên dương D, E để ta có $(x^E)^D = x$ với mọi $x \in \mathbb{Z}_n$. Nhờ đó ta có thể mã hóa các phần tử trong $\mathbb{Z}_n$ bằng E và giải mã bằng D.

d) Liệt kê ba cặp khóa (E, D) tiêu biểu (nếu có, nếu không thì giải thích) nhằm để mã hóa và giải mã các phần tử của $\mathbb{Z}_n$.

1 < E < D < phi(n) và ED = 1+k.phi(n).

Câu 2. Z[1024]\{0} → 1023 số: {1,2,...,1023} có tạo thành nhóm với phép nhân không?

- Đơn vị: 1.

- Kết hợp: có.

- Đóng với phép nhân: a,b thuộc tập đó thì a*b cũng thuộc tập đó?

→ 32*64 chia hết cho 1024 nên 32 * 64 = 0 trong Z[1024].

- Khả nghịch: 2 không nguyên tố cùng nhau với 1024 → không có nghịch đảo.

Bài 1

Xét tập hợp $\mathbb{M} = \left\{ \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} / x, y, z \in \mathbb{Z}_{39};\ (xz)^2 = \bar{1} \right\}$ với phép nhân ma trận.

a) Phép nhân ma trận có là phép toán trên tập $\mathbb{M}$ hay không?

b) Tập $\mathbb{M}$ với phép nhân ma trận có tạo thành nhóm hay không?

c) Tập $\mathbb{M}$ có bao nhiêu phần tử?

d) Tập $\mathbb{M}$ có thể mã hóa bởi ánh xạ $f(x) = x^D$ và giải mã bởi ánh xạ $g(y) = y^E$ với D và E là hai số nguyên khác nhau hay không? Nếu có thể, hãy liệt kê hay mô tả tập hợp gồm tất cả các cặp (D, E) như vậy.

(Đề giữa kỳ K28)

Ma trận: m x n: m dòng và n cột

Phép cộng 2 ma trận → cùng kích thước → cộng theo vị trí tương ứng.

Phép nhân 2 ma trận: (m x n) nhân (n x k) = ma trận (m x k).

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} -1 & 3 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} (a) & (c) \\ (b) & (d) \end{bmatrix}.$$

(a) = hàng 1, cột 1: 1*(-1)+2*0= -1.
(b) = hàng 2, cột 1: 3(-1)+4.0=-3.
(c) = hàng 1, cột 2: 1.3+2.3=9
(d) = hàng 2, cột 2: 3.3+4.3=21.

Ma trận đơn vị: E = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ → mọi ma trận cùng kích thước: E*A=A.

a) Hỏi phép nhân ma trận có đóng trên **M** không?

$$\begin{bmatrix} x & 0 \\ y & z \end{bmatrix} \times \begin{bmatrix} x' & 0 \\ y' & z' \end{bmatrix} = \begin{bmatrix} xx' & 0 \\ yx'+zy' & zz' \end{bmatrix}.$$

Kiểm tra:

- Góc trên bên phải vẫn là 0.

- Các số xx’,yx’+zy’,zz’ vẫn thuộc Z[39].

- Kiểm tra: (xx’)^2.(zz’)^2 = x^2.(x’)^2.z^2.(z’)^2=(xz)^2.(x’z’)^2=1.1=1.

→ thỏa → câu trả lời là có.

b) Kiểm tra yếu tố nhóm.

- <u>Đơn vị</u>: E=$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$;

- <u>Đóng</u>;

- <u>Kết hợp</u>: đúng theo tính chất phép nhân ma trận.

- <u>Khả nghịch</u> (?): với một ma trận A bất kỳ trong M, phải có A’ để A.A’ = E.

$$\begin{bmatrix} x & 0 \\ y & z \end{bmatrix} \times \begin{bmatrix} x' & 0 \\ y' & z' \end{bmatrix} = \begin{bmatrix} xx' & 0 \\ yx'+zy' & zz' \end{bmatrix}.$$

Muốn tích ở vế phải là E → cần chọn (x’,y’,z’) để sao cho : xx’=zz’=1 và yx’+zy’=0.

- Với xx’=1 vì đề (x.z)^2=1 trong Z[39] nên x thuộc U(Z[39]) → tồn tại x’.

- Tương tự với z, cũng có z’ để zz’=1. <u>Chọn được x’ và z’ rồi.</u>

- Xét yx’+zy’=0: nhân 2 vế cho z’ → z’(yx’+zy’)=z’.0 = 0 hay

z’.y.x’ + (zz’).y’=0 hay z’.y.x’ + y’ = 0 → y’ = - z’.y.x’.

c) Tập hợp M có mấy phần tử? $\begin{bmatrix} x & 0 \\ y & z \end{bmatrix}$

x,y,z tùy ý trong Z[39] → x,y,z có 39 khả năng → 39^3.

Còn có thêm ràng buộc (xz)^2 = 1.

(xz)^2 chia 39 dư 1 → (xz)^2 = 39k+1 → (xz)^2 nguyên tố cùng nhau với 39 → x và z cũng phải nguyên tố cùng nhau.

A.B.C = 1 trong Z[39] → Cả A lẫn B lẫn C đều nguyên tố cùng nhau với 39 → thuộc U(Z[39]).

Ta có 39=3.13.

Chọn x → x thuộc U(Z[39]): phi(39)=39.(1-1/3).(1-1/13)=24 nên x có 24 khả năng.

Chọn z phải chọn theo x để sao cho (xz)^2 = 1.

Xét điều kiện: a^2=1 trong Z[39] → a^2-1 chia hết cho 39.

(a-1)(a+1) chia hết cho 39=3.13.

- Nếu a-1 chia hết 39 → a=1 trong Z[39].
- Nếu a+1 chia hết cho 39 → a=-1 trong Z[39].
- Nếu a-1 chia hết cho 3, a+1 chia hết cho 13 → a=25 trong Z[39].
- Nếu a-1 chia hết cho 13, a+1 chia hết cho 3 → a=14 trong Z[39].

Trở lại bài toán: xz = 1,-1,14,25 → với mỗi x trong U(Z[39]) sẽ 4 cách chọn z.

Vậy số ma trận trong M sẽ là: 39.24.4 = 3744.

Trong trường hợp tổng quát: a^2-1 trong Z[pq] với p,q nguyên tố.

(a-1)(a+1) chia hết cho p.q.

- Nếu a-1 chia hết cho p, q → a-1 chia hết cho pq → a=1 trong Z[pq]
- Nếu a+1 chia hết cho p, q → a+1 chia hết cho pq → a=-1 trong Z[pq]
- Nếu a-1 chia hết cho p, a+1 chia hết cho q → luôn tồn tại duy nhất số a trong Z[pq] thỏa mãn điều này, đúng theo định lý số dư Trung Hoa.
- Nếu a+1 chia hết cho p, a-1 chia hết cho q → tương tự.
- ⇨ Tổng quát Z[pq], luôn có 4 số.

VD: số a chia 5 dư 1 và chia 3 dư 2 → từ 1,2,...,15 chắc chắn có duy nhất 1 số a như thế.

d) RSA cho phiên bản ma trận.

Với ma trận x thuộc M → x^(ED) = x.

Cần có công thức tổng quát để tìm lũy thừa của ma trận.

Bằng quy nạp, ta sẽ chứng minh công thức $\boxed{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m = \begin{pmatrix} a^m & 0 \\ b\cdot\dfrac{a^m-c^m}{a-c} & c^m \end{pmatrix}}$ với mọi $m = 1,2,3,\ldots$

Ghi chú. Công thức này dự đoán được nhờ tính thử vài giá trị m nhỏ.

Thật vậy, với $m=1$ thì đẳng thức trên đúng.

Giả sử ta đã có kết quả trên với m, xét lũy thừa $m+1$ thì theo công thức nhân ma trận:

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^{m+1} = \begin{pmatrix} a^m & 0 \\ b\cdot\dfrac{a^m-c^m}{a-c} & c^m \end{pmatrix}\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} a^{m+1} & 0 \\ b\cdot\dfrac{a(a^m-c^m)}{a-c}+b\cdot c^m & c^{m+1} \end{pmatrix}.$$

Chú ý rằng $b\cdot\dfrac{a(a^m-c^m)}{a-c}+b\cdot c^m = \dfrac{b}{a-c}\left(a(a^m-c^m)+(a-c)c^m\right) = b\cdot\dfrac{a^{m+1}-c^{m+1}}{a-c}$. Do đó, khẳng định cũng đúng với $m+1$ và theo quy nạp thì nó đúng với mọi m.

Nếu a=c, ta có $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} = \begin{pmatrix} a^2 & 0 \\ 2ab & a^2 \end{pmatrix}$; $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}^3 = \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}\begin{pmatrix} a^2 & 0 \\ 2ab & a^2 \end{pmatrix} = \begin{pmatrix} a^3 & 0 \\ 3a^2b & a^3 \end{pmatrix}$

Tổng quát: $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}^m = \begin{pmatrix} a^m & 0 \\ ma^{m-1}b & a^m \end{pmatrix}$. Khi đó, xét với m = 33. Phi(33)^2 → m = 0 trong Z[33]. Từ công thức trên, chúng ta cần chọn ED = m để sao cho ma trận lũy thừa x^m quay trở về x ban đầu, tức là cần có: a^m = a, c^m = c và $b \cdot \frac{a^m - c^m}{a - c} = b$.

Đối với 2 điều kiện đầu: dùng điều kiện RSA với số nguyên trong Z[39]: m = 1 trong Z[phi(39)]=Z[24] → **ED = 1 trong Z[24].**

Ta có: $b \cdot \frac{a^m - c^m}{a - c} = b \Leftrightarrow b\left(\frac{(a^m - a) - (c^m - c)}{a - c}\right) = 0$ đúng vì đã có a^m=a, c^m=c.

Bài 3

Xét tập hợp *M* gồm các ma trận vuông 2x2 có dạng $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ với a, b, c ∈ $\mathbb{Z}_{33}$. Tập *M* là một vành với phép cộng và nhân ma trận, phần tử 0 là $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ và phần tử 1 là $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Gọi U(*M*) là tập các ma trận của *M* khả nghịch với phép nhân ma trận.

a) Tính φ(33).

b) Tìm điều kiện cần và đủ mà *a*, *b*, *c* phải thỏa mãn để $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in$ U(*M*).

c) Đếm số lượng các phần tử của U(*M*).

d) Chứng minh $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ với mọi ma trận $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in$ U(*M*) ~ $m = 33\,(\varphi(33))^2$.

e) Đề xuất một sơ đồ mã hóa công khai các phần tử của U(*M*). Cho ví dụ về một cặp khóa (*E*, *D*).

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}?$$

a) phi(33)=33.2/3.10/11=20.

b) Z[33].

Cần chọn a',b',c' để có: aa'=1, cc'=1, a'b+b'c=0 → phải có a,c thuộc U(Z[33]).

a'b+b'c=0 ⇔ c'(a'b+b'c)=0 ⇔ b' = -c'.a'.b nên nếu có c',a' rồi thì luôn chọn được b'.

Vậy điều kiện cần và đủ: a,c thuộc U(Z[33]).

<u>Cách khác</u>: điều kiện khả nghịch ⇔ định thức: ac – b.0 = ac thuộc U(Z[33]).

c) Đếm số phần tử: b có 33 cách chọn còn a, c mỗi số 20 cách → 33.20^2 ma trận.

d) Cmr với m = 33.20^2 thì luôn có $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}^m = \begin{pmatrix} a^m & 0 \\ b\cdot\dfrac{a^m - c^m}{a-c} & c^m \end{pmatrix} \text{ với a khác c.}$$

Theo định lý Euler: a^phi(33)=1 với mọi a thuộc U(Z[33]) → a^20 = 1.

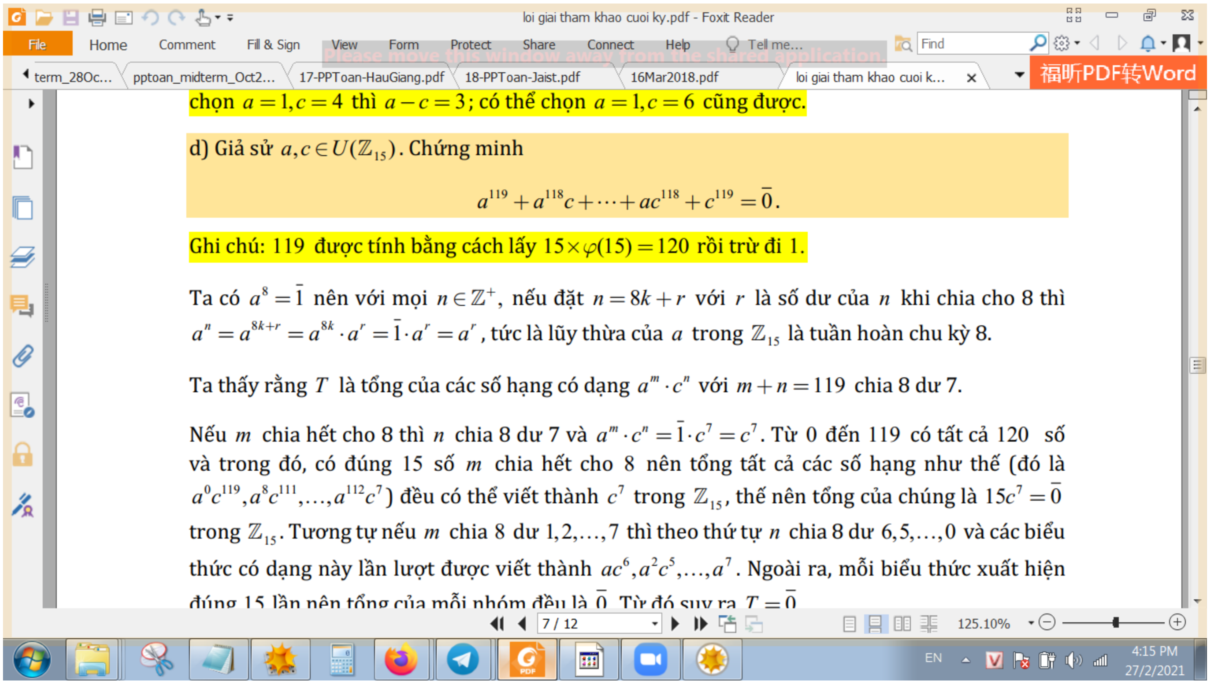
nên a^m=a^(33.20^2) = (a^20)^(33.20)=1^(33.20)=1.

Tương tự cũng có c^m=1.

Cần c/m: $b\cdot\dfrac{a^m-c^m}{a-c}=0$ trong Z[33]. Ta có đẳng thức

$$a^m - c^m = (a-c)(a^{m-1} + a^{m-2}c + a^{m-3}c^2 + \cdots + ac^{m-2} + c^{m-1}).$$

Đang có a^m-c^m=1-1=0 → tích (a-c)(...)=0 trong Z[33].



chọn $a=1, c=4$ thì $a-c=3$; có thể chọn $a=1, c=6$ cũng được.

d) Giả sử $a, c \in U(\mathbb{Z}_{15})$. Chứng minh

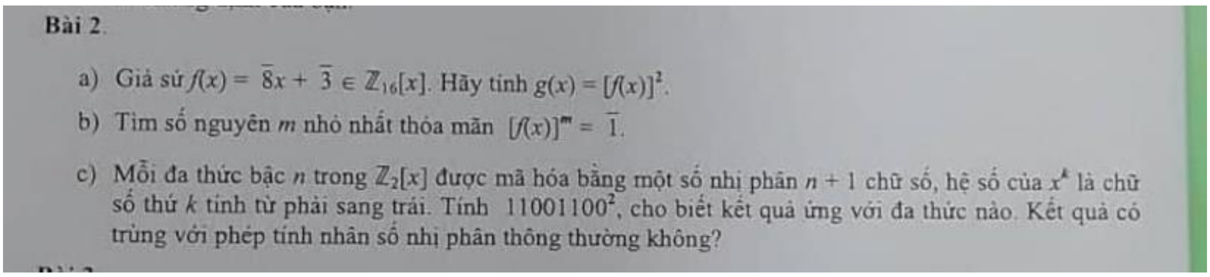
$$a^{119} + a^{118}c + \cdots + ac^{118} + c^{119} = \bar{0}.$$

Ghi chú: 119 được tính bằng cách lấy $15\times\varphi(15)=120$ rồi trừ đi 1.

Ta có $a^8=\bar{1}$ nên với mọi $n\in\mathbb{Z}^+$, nếu đặt $n=8k+r$ với r là số dư của n khi chia cho 8 thì $a^n = a^{8k+r} = a^{8k}\cdot a^r = \bar{1}\cdot a^r = a^r$, tức là lũy thừa của a trong $\mathbb{Z}_{15}$ là tuần hoàn chu kỳ 8.

Ta thấy rằng T là tổng của các số hạng có dạng $a^m\cdot c^n$ với $m+n=119$ chia 8 dư 7.

Nếu m chia hết cho 8 thì n chia 8 dư 7 và $a^m\cdot c^n = \bar{1}\cdot c^7 = c^7$. Từ 0 đến 119 có tất cả 120 số và trong đó, có đúng 15 số m chia hết cho 8 nên tổng tất cả các số hạng như thế (đó là $a^0c^{119}, a^8c^{111}, \ldots, a^{112}c^7$) đều có thể viết thành c^7 trong $\mathbb{Z}_{15}$, thế nên tổng của chúng là $15c^7=\bar{0}$ trong $\mathbb{Z}_{15}$. Tương tự nếu m chia 8 dư $1, 2, \ldots, 7$ thì theo thứ tự n chia 8 dư $6, 5, \ldots, 0$ và các biểu thức có dạng này lần lượt được viết thành $ac^6, a^2c^5, \ldots, a^7$. Ngoài ra, mỗi biểu thức xuất hiện đúng 15 lần nên tổng của mỗi nhóm đều là $\bar{0}$. Từ đó suy ra $T=\bar{0}$



Bài 2.

a) Giả sử $f(x) = \bar{8}x + \bar{3} \in \mathbb{Z}_{16}[x]$. Hãy tính $g(x) = [f(x)]^2$.

b) Tìm số nguyên m nhỏ nhất thỏa mãn $[f(x)]^m = \bar{1}$.

c) Mỗi đa thức bậc n trong $\mathbb{Z}_2[x]$ được mã hóa bằng một số nhị phân $n+1$ chữ số, hệ số của x^k là chữ số thứ k tính từ phải sang trái. Tính 11001100^2, cho biết kết quả ứng với đa thức nào. Kết quả có trùng với phép tính nhân số nhị phân thông thường không?

(8x+3)^2 = 64x^2+2.8x.3+9 = 0.x^2+0.x+9 → (8x+3)^2 = 9 trong Z16[x].

(8x+3)^2 = 9 -> (8x+3)^4 = 9^2 = 81 = 1 trong Z16[x].

11001100 → X^7+X^6+X^3+x^2 = x^6(x+1)+x^2(x+1)=(x+1)(x^6+x^2)=x^2(x^4+1)(x+1).

Bình phương:

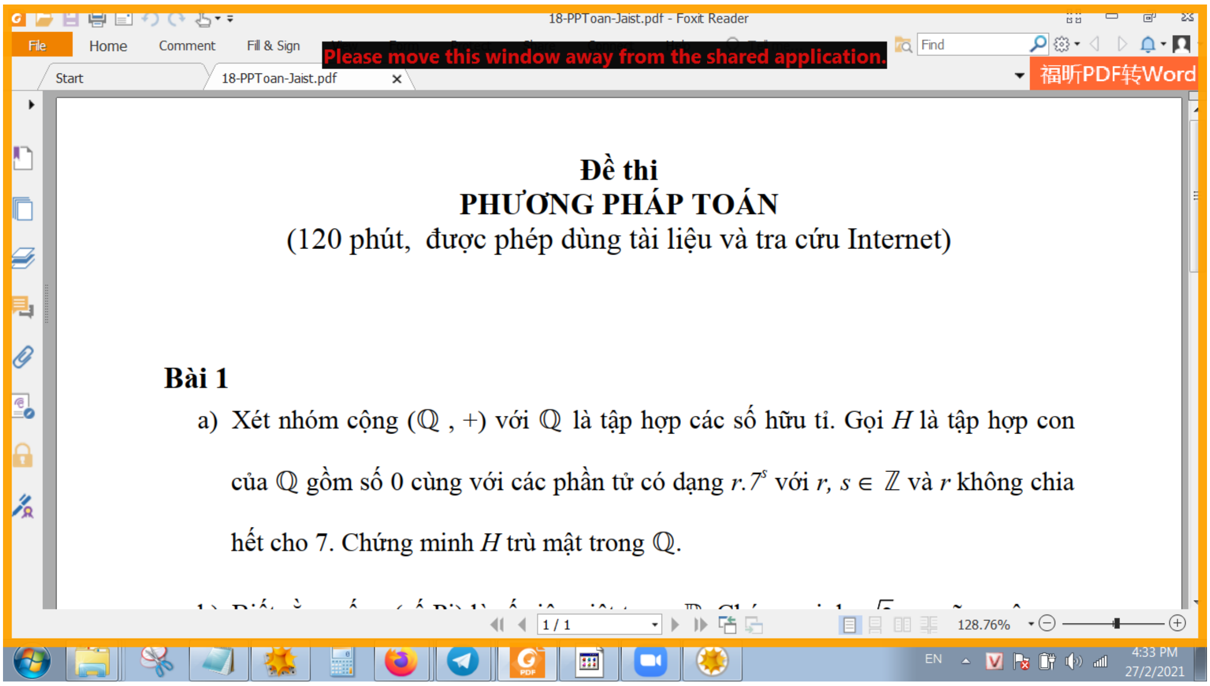
X^4(x^4+1)^2.(x+1)^2

=x^4(x^8+2x^4+1)(x^2+2x+1)=x^4(x^8+1)(x^2+1)

=(x^12+x^4)(x^2+1)

=x^14+x^12+x^6+x^4=101000001010000

So sánh với việc bình phương thông thường → nói chung là không trùng khớp



Đề thi
PHƯƠNG PHÁP TOÁN
(120 phút, được phép dùng tài liệu và tra cứu Internet)

Bài 1

a) Xét nhóm cộng $(\mathbb{Q}, +)$ với $\mathbb{Q}$ là tập hợp các số hữu tỉ. Gọi H là tập hợp con của $\mathbb{Q}$ gồm số 0 cùng với các phần tử có dạng $r.7^s$ với $r, s \in \mathbb{Z}$ và r không chia hết cho 7. Chứng minh H trù mật trong $\mathbb{Q}$.

Trù mật (dense): tập X mà trù mật trong tập Y → nếu giữa 2 phần tử của Y thì luôn tìm được phần tử của X.

VD: tập số hữu tỷ thì trù mật trong tập số thực, vì giữa 2 số thực bất kỳ, luôn có số hữu tỷ.

Cần c/m H trù mật trong Q.

Chọn tùy ý hai số hữu tỷ: a và b với a<b. Cần chỉ ra cách chọn r, s nguyên để sao

a < r.7^s < b.

- Chọn s là số nguyên âm, đặt s = -x với x nguyên dương là số sẽ chọn sau.

7^s = 7^(-x) = 1/7^x, viết lại:

a < r / 7^x < b hay a.7^x < r < b.7^x.

Ta thấy khoảng cách giữa 2 số đầu & cuối: b.7^x – a.7^x = 7^x.(b-a). Chọn x đủ lớn để sao cho 7^x.(b-a) > 1 → giữa nó sẽ có nguyên, chọn r là số nguyên đó → xong!

Bên dưới là đề cuối kỳ năm trước.

ĐỀ THI PHƯƠNG PHÁP TOÁN

(120 phút – được phép dùng tài liệu)

Bài 1.

a) Tập hợp $U(\mathbb{Z}_{35})$ có bao nhiêu phần tử? Hãy liệt kê các phần tử $\overline{a}$ của tập này mà $a > 5$.

b) Những cặp số nguyên dương (E, D) thỏa mãn $(a^E)^D = a$ với mọi $a \in \mathbb{Z}_{35}$ phải thỏa mãn điều kiện gì?

c) Nếu có, hãy chỉ ra 1 cặp số nguyên dương (E, D) với $E < D$ mà ta có thể mã hóa các phần tử của $\mathbb{Z}_{35}$ bằng E để có các bản mã và giải mã các bản mã bằng D để có các bản rõ; nếu không hãy giải thích tại sao.

Bài 2.

a) Trong vành đa thức $\mathbb{Z}_{18}[x]$, hãy chia đa thức $f(x) = \overline{8}\,x^5 + \overline{3}\,x^3 + \overline{4}\,x + \overline{9}$ cho đa thức $g(x) = \overline{5}\,x^3 + \overline{3}\,x + \overline{6}$ theo thuật chia *Euclid*. Giải thích rõ tại sao có thể chia được cho $g(x)$ mặc dù $g(x)$ không đơn khởi.

b) Tìm tất cả các đa thức bậc nhất trong $\mathbb{Z}_6[x]$ mà có 2 nghiệm là $\overline{2}$ và $\overline{5}$.

c) Trong vành đa thức $\mathbb{Z}_9[x]$, hãy đơn giản đa thức

$$h(x) = \left(\overline{3}x + \overline{1}\right)^3.$$

d) Đa thức $t(x) = \overline{3}x + \overline{1}$ có khả nghịch nhân trong $\mathbb{Z}_9[x]$ hay không? Nếu có, cho biết đa thức nghịch đảo của nó.

e) *Có tổng cộng bao nhiêu đa thức bậc 2 trong $\mathbb{Z}_{20}[x]$?*

Bài 3. Xét trường $\mathbb{F} = \mathbf{GF}(5^3)$ có 125 phần tử.

Trường $\mathbb{F}$ này có thể sinh ra bởi một đa thức bất khả quy (BKQ) bậc mấy trong $\mathbb{Z}_5[x]$?

Cho ví dụ về 1 đa thức BKQ như trong *Câu a*, có chứng minh tính BKQ.

Mỗi phần tử trong $\mathbb{F}$ có thể viết như số trong hệ cơ số nào, với mấy chữ số ?

Những cặp số nguyên dương (E, D) thỏa mãn mô hình mã hóa/giải mã $(a^E)^D = a$ với mọi $a \in \mathbb{F}$ phải thỏa mãn điều kiện gì? Cho ví dụ một cặp số như vậy, minh họa.

HẾT