

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

Bài tập tuần 2

Đồng dư và một số tính chất

Môn học: Nhập môn mã hóa mật mã

CSC15005_22MMT

Sinh viên:

Nguyễn Hồ Đăng Duy

22127085

22MMT

Giảng viên hướng dẫn:

Nguyễn Đình Thúc

Trần Hà Sơn

Nguyễn Văn Quang Huy

Ngày 15 tháng 10 năm 2024



Mục lục

1	Bài 1	2
2	Bài 2	3
3	Bài 3	5
4	Bài 4	8

1 Bài 1

Giải các phương trình sau

a) $6x \equiv 4 \pmod{8}$

Phương trình có nghiệm vì $(6, 8) = 2$ và $2 \mid 4$.

Vì $x_0 = 2$ thỏa phương trình nên phương trình sẽ có nghiệm:

$$x = 2 + \frac{8}{2}k = 2 + 4k \text{ với } k \in \{0; 1\}.$$

- $k = 0 \rightarrow x = 2$

- $k = 1 \rightarrow x = 6$

Vậy phương trình có các nghiệm $x = 2$ và $x = 6$

b) $5x \equiv 8 \pmod{10}$

Phương trình không có nghiệm vì $(5, 10) = 5$ và $5 \nmid 8$.

c) $8x \equiv 5 \pmod{13}$

Phương trình có nghiệm duy nhất vì $(8, 13) = 1$

Ta có:

$$5.8x \equiv 5.5 \pmod{13}$$

$$\Leftrightarrow x \equiv 12 \pmod{13}$$

Vậy phương trình có nghiệm duy nhất $x \equiv 12 \pmod{13}$

d) $6x \equiv 7 \pmod{23}$

Phương trình có nghiệm duy nhất vì $(6, 23) = 1$

Ta có:

$$4.6x \equiv 4.7 \pmod{23}$$

$$\Leftrightarrow x \equiv 5 \pmod{23}$$

Vậy phương trình có nghiệm duy nhất $x \equiv 5 \pmod{23}$

2 Bài 2

Áp dụng định lí thặng dư Trung Hoa giải các hệ phương trình đồng dư sau

$$\text{a) } \begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$$

Ta có $M = 11 \cdot 17 = 187$

1) $M_1 = 187/11 = 17$. Giải phương trình $17y \equiv 1 \pmod{11}$

Ta có:

$$\begin{aligned} 17y &\equiv 1 \pmod{11} \\ \Leftrightarrow 6y &\equiv 1 \pmod{11} \\ \Leftrightarrow y &\equiv 2 \pmod{11} \end{aligned}$$

2) $M_1 = 187/17 = 11$. Giải phương trình $11y \equiv 1 \pmod{17}$

Ta có:

$$\begin{aligned} 11y &\equiv 1 \pmod{17} \\ \Leftrightarrow y &\equiv 14 \pmod{17} \end{aligned}$$

Vậy hệ có nghiệm $x_0 = 4 \cdot 17 \cdot 2 + 3 \cdot 11 \cdot 14 = 598 \pmod{360}$

$$\text{b) } \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

Ta có $M = 2 \cdot 3 \cdot 5 = 30$

1) $M_1 = 30/2 = 15$. Giải phương trình $15y \equiv 1 \pmod{2}$

Ta có:

$$\begin{aligned} 15y &\equiv 1 \pmod{2} \\ \Leftrightarrow y &\equiv 1 \pmod{2} \end{aligned}$$

2) $M_2 = 30/3 = 10$. Giải phương trình $10y \equiv 1 \pmod{3}$

Ta có:

$$\begin{aligned} 10y &\equiv 1 \pmod{3} \\ \Leftrightarrow y &\equiv 1 \pmod{3} \end{aligned}$$

3) $M_3 = 30/5 = 6$. Giải phương trình $6y \equiv 1 \pmod{5}$

Ta có:

$$\begin{aligned} 6y &\equiv 1 \pmod{5} \\ \Leftrightarrow y &\equiv 1 \pmod{5} \end{aligned}$$

Vậy hệ có nghiệm $x_0 = 1 \cdot 15 \cdot 1 + 2 \cdot 1 \cdot 10 + 3 \cdot 1 \cdot 6 = 53 \pmod{30}$

$$\text{c) } \begin{cases} x \equiv 3 \pmod{12} \\ x \equiv 4 \pmod{13} \\ x \equiv 5 \pmod{17} \end{cases}$$

Ta có $M = 12.13.17 = 2652$

1) $M_1 = 2652/12 = 221$. Giải phương trình $221y \equiv 1 \pmod{12}$

Ta có:

$$221y \equiv 1 \pmod{12}$$

$$\Leftrightarrow 5y \equiv 1 \pmod{12}$$

$$\Leftrightarrow y \equiv 5 \pmod{12}$$

2) $M_2 = 2652/13 = 204$. Giải phương trình $204y \equiv 1 \pmod{13}$

Ta có:

$$204y \equiv 1 \pmod{13}$$

$$\Leftrightarrow 9y \equiv 1 \pmod{13}$$

$$\Leftrightarrow y \equiv 3 \pmod{13}$$

3) $M_3 = 2652/17 = 156$. Giải phương trình $156y \equiv 1 \pmod{17}$

Ta có:

$$256y \equiv 1 \pmod{17}$$

$$\Leftrightarrow 3y \equiv 1 \pmod{17}$$

$$\Leftrightarrow y \equiv 6 \pmod{17}$$

Vậy hệ có nghiệm $x_0 = 3.221.5 + 4.204.3 + 5.156.6 = 10443 \pmod{2652}$

3 Bài 3

Cho số nguyên tố p , số nguyên b được gọi là nghịch đảo của a modulo p nếu thỏa mãn $ab \equiv 1 \pmod{p}$. Hãy tìm nghịch đảo của a (modulo p) trong các trường hợp sau bằng hai cách: Cách thứ nhất dùng thuật toán Euclide mở rộng, cách thứ hai sử dụng định lý Fermat nhỏ.

Thuật toán Euclide mở rộng

Vì $ab \equiv 1 \pmod{p}$ nên ta có $ab + px = 1$ với x nguyên.

a) $a = 11$ và $p = 47$

Gán $(x_0, y_0, r_0) = (1, 0, 47)$ và $(x_1, y_1, r_1) = (0, 1, 11)$

Ta có:

$$\begin{aligned}(1, 0, 47) - 4 \cdot (0, 1, 11) &= (1, -4, 3) \\ (0, 1, 11) - 3 \cdot (1, -4, 3) &= (-3, 13, 2) \\ (1, -4, 3) - 1 \cdot (-3, 13, 2) &= (4, -17, 1) \\ (-3, 13, 2) - 2 \cdot (4, -17, 1) &= (-11, 47, 0)\end{aligned}$$

Suy ra: $11 \cdot (-17) + 47 \cdot 4 = 1$.

Vậy $b \equiv -17 \pmod{47}$ hay $b \equiv 30 \pmod{47}$

b) $a = 345$ và $p = 587$

Gán $(x_0, y_0, r_0) = (1, 0, 587)$ và $(x_1, y_1, r_1) = (0, 1, 345)$

Ta có:

$$\begin{aligned}(1, 0, 587) - 1 \cdot (0, 1, 345) &= (1, -1, 242) \\ (0, 1, 345) - 1 \cdot (1, -1, 242) &= (-1, 2, 103) \\ (1, -1, 242) - 2 \cdot (-1, 2, 103) &= (3, -5, 36) \\ (-1, 2, 103) - 2 \cdot (3, -5, 36) &= (-7, 12, 31) \\ (3, -5, 36) - 1 \cdot (-7, 12, 31) &= (10, -17, 5) \\ (-7, 12, 31) - 6 \cdot (10, -17, 5) &= (-67, 114, 1) \\ (10, -17, 5) - 5 \cdot (-67, 114, 1) &= (345, -587, 0)\end{aligned}$$

Suy ra: $345 \cdot 114 + 587 \cdot (-67) = 1$.

Vậy $b \equiv 114 \pmod{587}$

c) a = 78467 và p = 104801

Gán $(x_0, y_0, r_0) = (1, 0, 104801)$ và $(x_1, y_1, r_1) = (0, 1, 78467)$

Ta có:

$$\begin{aligned} (1, 0, 104801) - 1.(0, 1, 78467) &= (1, -1, 26334) \\ (0, 1, 78467) - 2.(1, -1, 26334) &= (-2, 3, 25799) \\ (1, -1, 26334) - 1.(-2, 3, 25799) &= (3, -4, 535) \\ (-2, 3, 25799) - 48.(3, -4, 535) &= (-146, 195, 119) \\ (3, -4, 535) - 4.(-146, 195, 119) &= (587, -784, 59) \\ (-146, 195, 119) - 2.(587, -784, 59) &= (-1320, 1763, 1) \\ (587, -784, 59) - 59.(-1320, 1763, 1) &= (78467, -104801, 0) \end{aligned}$$

Suy ra: $78467.1763 + 104801.(-1320) = 1$.

Vậy $b \equiv 1763 \pmod{104801}$

Định lý Fermat nhỏ

Từ yêu cầu đề bài ta có $ab \equiv 1 \pmod{p}$ Theo định lý Fermat nhỏ, ta có $a^{p-1} \equiv 1 \pmod{p}$ nếu a và p nguyên tố cùng nhau. Từ đó ta có:

$$a^{p-1} = a.a^{p-2} \equiv 1 \pmod{p} \Rightarrow b \equiv a^{p-2} \pmod{p}$$

a) a = 11 và p = 47

Vì $(11, 47) = 1$ nên ta có thể áp dụng định lý Fermat nhỏ $\Rightarrow b \equiv 11^{45} \pmod{47}$ Ta có:

- $11^5 \equiv 29 \pmod{47}$
- $11^{15} = (11^5)^3 \equiv 29^3 \pmod{47} \Leftrightarrow 11^{15} \equiv 43 \pmod{47}$
- $11^{45} = (11^{15})^3 \equiv 43^3 \pmod{47} \Leftrightarrow 11^{45} \equiv 30 \pmod{47}$

Vậy $b \equiv 30 \pmod{47}$

b) a = 345 và p = 587

Vì $(345, 587) = 1$ nên ta có thể áp dụng định lý Fermat nhỏ $\Rightarrow b \equiv 345^{585} \pmod{587}$ Ta có:

- $345^3 \equiv 40 \pmod{587}$
- $345^9 = (345^3)^3 \equiv 40^3 \pmod{587} \Leftrightarrow 345^9 \equiv 17 \pmod{587}$
- $345^{45} = (345^9)^5 \equiv 17^5 \pmod{587} \Leftrightarrow 345^{45} \equiv 491 \pmod{587}$
- $345^{585} = (345^{45})^{13} \equiv 491^{13} \pmod{587}$

Tương tự:

- $491^2 = 241081 \equiv 411 \pmod{587}$
- $491^4 = (491^2)^2 \equiv 411^2 \pmod{587} \Leftrightarrow 491^4 \equiv 452 \pmod{587}$

- $491^8 = (491^4)^2 \equiv 452^2 \pmod{587} \Leftrightarrow 491^8 \equiv 28 \pmod{587}$
- $491^{13} = 491^8 \cdot 491^4 \cdot 491 \equiv 28 \cdot 452 \cdot 491 \pmod{587}$ hay $491^{13} \equiv 114 \pmod{587}$

Vậy $b \equiv 345^{585} \pmod{587}$ suy ra $b \equiv 114 \pmod{587}$

c) a = 78467 và p = 104801

Vì $(78467, 104801) = 1$ nên ta có thể áp dụng định lý Fermat nhỏ $\Rightarrow b \equiv 78467^{104799} \pmod{104801}$
Ta có:

- $78467^2 = 6157070089 \equiv 11339 \pmod{104801}$
- $78467^4 = (78467^2)^2 \equiv 11339^2 \pmod{104801} \Leftrightarrow 78467^4 \equiv 86895 \pmod{104801}$
- $78467^8 = (78467^4)^2 \equiv 86895^2 \pmod{104801} \Leftrightarrow 78467^8 \equiv 38577 \pmod{104801}$
- $78467^{16} = (78467^8)^2 \equiv 38577^2 \pmod{104801} \Leftrightarrow 78467^{16} \equiv 10729 \pmod{104801}$
- $78467^{32} = (78467^{16})^2 \equiv 10729^2 \pmod{104801} \Leftrightarrow 78467^{32} \equiv 39943 \pmod{104801}$
- $78467^{64} = (78467^{32})^2 \equiv 39943^2 \pmod{104801} \Leftrightarrow 78467^{64} \equiv 57626 \pmod{104801}$
- $78467^{128} = (78467^{64})^2 \equiv 57626^2 \pmod{104801} \Leftrightarrow 78467^{128} \equiv 31390 \pmod{104801}$
- $78467^{256} = (78467^{128})^2 \equiv 31390^2 \pmod{104801} \Leftrightarrow 78467^{256} \equiv 97899 \pmod{104801}$
- $78467^{512} = (78467^{256})^2 \equiv 97899^2 \pmod{104801} \Leftrightarrow 78467^{512} \equiv 57950 \pmod{104801}$
- $78467^{1024} = (78467^{512})^2 \equiv 57950^2 \pmod{104801} \Leftrightarrow 78467^{1024} \equiv 64057 \pmod{104801}$
- $78467^{2048} = (78467^{1024})^2 \equiv 64057^2 \pmod{104801} \Leftrightarrow 78467^{2048} \equiv 25696 \pmod{104801}$
- $78467^{4096} = (78467^{2048})^2 \equiv 25696^2 \pmod{104801} \Leftrightarrow 78467^{4096} \equiv 38116 \pmod{104801}$
- $78467^{8192} = (78467^{4096})^2 \equiv 38116^2 \pmod{104801} \Leftrightarrow 78467^{8192} \equiv 77994 \pmod{104801}$
- $78467^{16384} = (78467^{8192})^2 \equiv 77994^2 \pmod{104801} \Leftrightarrow 78467^{16384} \equiv 99593 \pmod{104801}$
- $78467^{32768} = (78467^{16384})^2 \equiv 99593^2 \pmod{104801} \Leftrightarrow 78467^{32768} \equiv 84606 \pmod{104801}$
- $78467^{65536} = (78467^{32768})^2 \equiv 84606^2 \pmod{104801} \Leftrightarrow 78467^{65536} \equiv 57334 \pmod{104801}$

Vì $104799 = 65536 + 32768 + 4096 + 2048 + 256 + 64 + 16 + 8 + 4 + 2 + 1$

Suy ra $78467^{104799} \equiv 57334 \cdot 84606 \cdot 38116 \cdot 25696 \cdot 97899 \cdot 57626 \cdot 10729 \cdot 38577 \cdot 86895 \cdot 11339 \cdot 78467 \pmod{104801}$

Hay $78467^{104799} \equiv 1763 \pmod{104801}$

Vậy $b \equiv 1763 \pmod{104801}$

4 Bài 4

Bob và Alice sử dụng một hệ thống mật mã trong đó khóa riêng của họ là một số nguyên tố (lớn) k , bản rõ (plaintexts) và bản mã (ciphertexts) là các số nguyên. Bob mã hóa thông điệp m bằng cách tính tích $c = km$. Eve chặn được hai bản mã sau:

$$c_1 = 12849217045006222 \text{ và } c_2 = 6485880443666222$$

Hãy sử dụng giải thuật tìm ước chung lớn nhất để tìm khóa (private key) của Alice và Bob.

Ta có mối quan hệ giữa c_1, c_2 và khóa private key k như sau:

$$c_1 = k.m_1 \text{ và } c_2 = k.m_2$$

Với m_1, m_2 là thông điệp ban đầu. Suy ra k là ước chung của cả c_1 và c_2 .

Theo đề bài thì $k = \gcd(c_1, c_2)$. Áp dụng thuật toán Euclide, ta có:

$$\begin{aligned} 12849217045006222 &= 6485880443666222 * 1 + 6363336601340000 \\ 6485880443666222 &= 6363336601340000 * 1 + 122543842326222 \\ 6363336601340000 &= 122543842326222 * 51 + 113600642702678 \\ 122543842326222 &= 113600642702678 * 1 + 8943199623544 \\ 113600642702678 &= 8943199623544 * 12 + 6282247220150 \\ 8943199623544 &= 6282247220150 * 1 + 2660952403394 \\ 6282247220150 &= 2660952403394 * 2 + 960342413362 \\ 2660952403394 &= 960342413362 * 2 + 740267576670 \\ 960342413362 &= 740267576670 * 1 + 220074836692 \\ 740267576670 &= 220074836692 * 3 + 80043066594 \\ 220074836692 &= 80043066594 * 2 + 59988703504 \\ 80043066594 &= 59988703504 * 1 + 20054363090 \\ 59988703504 &= 20054363090 * 2 + 19879977324 \\ 20054363090 &= 19879977324 * 1 + 174385766 \\ 19879977324 &= 174385766 * 114 + 0 \end{aligned}$$

Vậy private key $k = 174385766$