BÀI TẬP TUẦN 2

Bài 1. Giải các phương trình sau.
a) $6x \equiv 4 \pmod 8$
b) $5x \equiv 8 \pmod{10}$
c) $8x \equiv 5 \pmod{13}$
d) $6x \equiv 7 \pmod{23}$

a) $6x \equiv 4 \pmod 8$ (1)
$d = (6, 8) = 2$
Phương trình (1) $\Leftrightarrow 3x \equiv 2 \pmod 4$ (2)
có: $\phi(4) = 2 \Leftrightarrow 3^{\phi(4)} \equiv 1 \pmod 4$
$\Rightarrow$ Phương trình (2) $\Leftrightarrow 3.3^{2-1}.2 \equiv 2 \pmod 4$
$\Rightarrow x \equiv 6 \pmod 4 \Leftrightarrow x \equiv 2 \pmod 4$ là nghiệm của phương trình (2)
vậy nghiệm của phương trình (1) là:

$$\begin{cases} x \equiv 2 \pmod 8 \\ x \equiv 2 + \frac{8}{2} = 6 \pmod 8 \end{cases}$$

b) $5x \equiv 8 \pmod{10}$
$d = (5, 10) = 5$
mà $5 \nmid 8$ nên phương trình trên không có nghiệm

c) $8x \equiv 5 \pmod{13}$
$d = (8, 13) = 1$
có: $\phi(13) = 12 \Leftrightarrow 8^{\phi(13)} \equiv 1 \pmod{13}$
$\Leftrightarrow 8.8^{12-1}.5 \equiv 5 \pmod{13}$
vì $d = 1$ nên phương trình có nghiệm duy nhất là: $x \equiv 8^{11}.5 \pmod{13} \Leftrightarrow x \equiv 12 \pmod{13}$

d) $6x \equiv 7 \pmod{23}$
$d = (6, 23) = 1$
có: $\phi(23) = 22 \Leftrightarrow 6^{\phi(23)} \equiv 1 \pmod{13}$
$\Leftrightarrow 6.6^{22-1}.7 \equiv 7 \pmod{23}$
vì $d = 1$ nên phương trình có nghiệm duy nhất là: $x \equiv 6^{21}.7 \pmod{23} \Leftrightarrow x \equiv 5 \pmod{23}$

Bài 2. Áp dụng định lí thặng dư Trung Hoa giải các hệ phương trình đồng dư sau:
a) $\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$
b) $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$
c) $\begin{cases} x \equiv 3 \pmod{12} \\ x \equiv 4 \pmod{13} \\ x \equiv 5 \pmod{17} \end{cases}$

a) đặt $M = 11.17 = 187, n_1 = \frac{M}{11} = 17, n_2 = \frac{M}{17} = 11$
Áp dụng thuật toán Bezout ta có:
$n_1^{-1} = 17^{-1} = 2 \pmod{11}$
$n_2^{-1} = 11^{-1} = -3 \equiv 14 \pmod{17}$
Từ đó suy ra:

$$x \equiv 4.n_1.n_1^{-1} + 3.n_2.n_2^{-1} \pmod{187}$$
$$\Leftrightarrow x \equiv 4.17.2 + 3.11.14 \equiv 598 \equiv 37 \pmod{187}$$

b) đặt $M = 2.3.5 = 30, n_1 = \frac{M}{2} = 15, n_2 = \frac{M}{3} = 10, n_3 = \frac{M}{5} = 6$

Áp dụng thuật toán Bezout ta có:
$n_1^{-1} = 15^{-1} = -3 \equiv 1 \pmod{2}$
$n_2^{-1} = 10^{-1} = 1 \pmod{3}$
$n_2^{-1} = 6^{-1} = 1 \pmod{5}$
Từ đó suy ra:

$$x \equiv 1.n_1.n_1^{-1} + 2.n_2.n_2^{-1} + 3.n_3.n_3^{-1} \pmod{30}$$
$$\Leftrightarrow x \equiv 1.15.1 + 2.10.1 + 3.6.1 \equiv 53 \equiv 23 \pmod{30}$$

c) đặt $M = 12.13.17 = 2652, n_1 = \frac{M}{12} = 221, n_2 = \frac{M}{13} = 204, n_3 = \frac{M}{17} = 156$

Áp dụng thuật toán Bezout ta có:
$n_1^{-1} = 221^{-1} = 5 \pmod{12}$
$n_2^{-1} = 204^{-1} = 3 \pmod{13}$
$n_2^{-1} = 156^{-1} = 6 \pmod{17}$
Từ đó suy ra:

$$x \equiv 3.n_1.n_1^{-1} + 4.n_2.n_2^{-1} + 5.n_3.n_3^{-1} \pmod{2652}$$
$$\Leftrightarrow x \equiv 3.221.5 + 4.204.3 + 5.156.6 \equiv 10443 \equiv 2487 \pmod{2652}$$

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.
a) $a = 11$ và $p = 47$.
b) $a = 345$ và $p = 587$.
c) $a = 78467$ và $p = 104801$.

Cách 1: Dùng thuật toán Euclide mở rộng

a) $a = 11$ và $p = 47$.
có dạng:
$$11x + 47y = 1$$
theo thuật toán thì:
$$(x_0, y_0, d_0) = (1, 0, 11)$$
$$(x_1, y_1, d_1) = (0, 1, 47)$$
$$(x_2, y_2, d_2) = (1, -1, 11)$$
$$(x_3, y_3, d_3) = (-1, 4, 3)$$
$$(x_4, y_4, d_4) = (4, -17, 2)$$
$$(x_5, y_5, d_5) = (-17, 4, 1)$$
vậy ta có cặp $(x, y) = (-17, 4)$ hay $b \equiv -17 \pmod{47} \Leftrightarrow b \equiv 30 \pmod{47}$

b) $a = 345$ và $p = 587$.
có dạng:
$$345x + 587y = 1$$
theo thuật toán thì:
$$(x_0, y_0, d_0) = (1, 0, 345)$$
$$(x_1, y_1, d_1) = (0, 1, 587)$$

$$(x_2, y_2, d_2) = (1, -6, 345)$$
$$(x_3, y_3, d_3) = (-6, 7, 242)$$
$$(x_4, y_4, d_4) = (7, -20, 103)$$
$$(x_5, y_5, d_5) = (-20, 47, 36)$$
$$(x_6, y_6, d_6) = (47, -67, 31)$$
$$(x_7, y_7, d_7) = (-67, 114, 5)$$
$$(x_8, y_8, d_8) = (114, -67, 1)$$

vậy ta có cặp $(x, y) = (114, -67)$ hay $b \equiv 114 \pmod{587}$

c) $a = 78467$ và $p = 104801$.
có dạng:

$$78467x + 104801y = 1$$

theo thuật toán thì:

$$(x_0, y_0, d_0) = (1, 0, 78467)$$
$$(x_1, y_1, d_1) = (0, 1, 104801)$$
$$(x_2, y_2, d_2) = (1, -2, 78467)$$
$$(x_3, y_3, d_3) = (-2, 9, 26334)$$
$$(x_4, y_4, d_4) = (9, -434, 25799)$$
$$(x_5, y_5, d_5) = (-434, 443, 535)$$
$$(x_6, y_6, d_6) = (443, -1320, 119)$$
$$(x_7, y_7, d_7) = (-1320, 1763, 59)$$
$$(x_8, y_8, d_8) = (1763, -1320, 1)$$

vậy ta có cặp $(x, y) = (1763, -1320)$ hay $b \equiv 1763 \pmod{104801}$

Cách 2: Dùng định lý Fermat nhỏ

Phát biểu định lý Fermat như sau: Nếu một số nguyên a không chia hết cho số nguyên tố p, thì

$$a^{p-1} \equiv 1 \pmod{p}$$

hay

$$a^{p-2} \equiv a^{-1} \pmod{p}$$

a) $a = 11$ và $p = 47$.

$$b \equiv a^{-1} \equiv 11^{-1} \equiv 11^{47-2} \equiv 30 \pmod{47}$$

b) $a = 345$ và $p = 587$.

$$b \equiv a^{-1} \equiv 345^{-1} \equiv 345^{587-2} \equiv 114 \pmod{587}$$

c) $b = a = 78467$ và $p = 104801$.

$$a^{-1} \equiv 78467^{-1} \equiv 78467^{104801-2} \equiv 1763 \pmod{104801}$$