

# PHƯƠNG TRÌNH ĐỒNG DƯ

Bài giảng điện tử

Ts. Lê Xuân Đại

Trường Đại học Bách Khoa TP HCM

Ngày 20 tháng 4 năm 2011

# Nội dung

## Đồng dư thức

Những khái niệm cơ bản

Tính chất của đồng dư thức

## Tập hợp các lớp thặng dư

Những khái niệm cơ bản

Tính chất

## Phương trình đồng dư

## Phương trình đồng dư bậc nhất một ẩn

## Hệ phương trình đồng dư bậc nhất một ẩn

## Bài tập

# Đồng dư thức

# Đồng dư thức

## Định nghĩa

*Cho  $m$  là số nguyên dương. Ta nói 2 số nguyên  $a, b$  đồng dư với nhau theo mô-đun  $m$  nếu trong phép chia  $a$  và  $b$  cho  $m$  ta được cùng một số dư. Kí hiệu  $a \equiv b \pmod{m}$*

# Đồng dư thức

## Định nghĩa

*Cho  $m$  là số nguyên dương. Ta nói 2 số nguyên  $a, b$  đồng dư với nhau theo mô-đun  $m$  nếu trong phép chia  $a$  và  $b$  cho  $m$  ta được cùng một số dư. Kí hiệu  $a \equiv b \pmod{m}$*

## Ví dụ

$$19 \equiv 3 \pmod{8}; \quad -25 \equiv 23 \pmod{8};$$

# Đồng dư thức

## Định nghĩa

*Cho  $m$  là số nguyên dương. Ta nói 2 số nguyên  $a, b$  đồng dư với nhau theo mô-đun  $m$  nếu trong phép chia  $a$  và  $b$  cho  $m$  ta được cùng một số dư. Kí hiệu  $a \equiv b \pmod{m}$*

## Ví dụ

$$19 \equiv 3 \pmod{8}; \quad -25 \equiv 23 \pmod{8};$$

## Định lý

*Các mệnh đề sau đây tương đương:*

1.  $a$  và  $b$  đồng dư với nhau theo mô-đun  $m$ ;

# Đồng dư thức

## Định nghĩa

Cho  $m$  là số nguyên dương. Ta nói 2 số nguyên  $a, b$  đồng dư với nhau theo mô-đun  $m$  nếu trong phép chia  $a$  và  $b$  cho  $m$  ta được cùng một số dư. Kí hiệu  $a \equiv b \pmod{m}$

## Ví dụ

$$19 \equiv 3 \pmod{8}; \quad -25 \equiv 23 \pmod{8};$$

## Định lý

Các mệnh đề sau đây tương đương:

1.  $a$  và  $b$  đồng dư với nhau theo mô-đun  $m$ ;
2.  $a - b$  chia hết cho  $m$ ;

# Đồng dư thức

## Định nghĩa

Cho  $m$  là số nguyên dương. Ta nói 2 số nguyên  $a, b$  đồng dư với nhau theo mô-đun  $m$  nếu trong phép chia  $a$  và  $b$  cho  $m$  ta được cùng một số dư. Kí hiệu  $a \equiv b \pmod{m}$

## Ví dụ

$$19 \equiv 3 \pmod{8}; \quad -25 \equiv 23 \pmod{8};$$

## Định lý

Các mệnh đề sau đây tương đương:

1.  $a$  và  $b$  đồng dư với nhau theo mô-đun  $m$ ;
2.  $a - b$  chia hết cho  $m$ ;
3. tồn tại số nguyên  $t$  sao cho  $a = b + mt$ .



# Đồng dư thức

## Định nghĩa

Cho  $m$  là số nguyên dương. Ta nói 2 số nguyên  $a, b$  đồng dư với nhau theo mô-đun  $m$  nếu trong phép chia  $a$  và  $b$  cho  $m$  ta được cùng một số dư. Kí hiệu  $a \equiv b \pmod{m}$

## Ví dụ

$$19 \equiv 3 \pmod{8}; \quad -25 \equiv 23 \pmod{8};$$

## Định lý

Các mệnh đề sau đây tương đương:

1.  $a$  và  $b$  đồng dư với nhau theo mô-đun  $m$ ;
2.  $a - b$  chia hết cho  $m$ ;
3. tồn tại số nguyên  $t$  sao cho  $a = b + mt$ .

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;
2.  $\forall a, b \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  suy ra  $b \equiv a \pmod{m}$

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;
2.  $\forall a, b \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  suy ra  $b \equiv a \pmod{m}$
3.  $\forall a, b, c \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  và  $b \equiv c \pmod{m}$  suy ra  $a \equiv c \pmod{m}$

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;
2.  $\forall a, b \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  suy ra  $b \equiv a \pmod{m}$
3.  $\forall a, b, c \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  và  $b \equiv c \pmod{m}$  suy ra  $a \equiv c \pmod{m}$

## Định lý

1. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ ;

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;
2.  $\forall a, b \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  suy ra  $b \equiv a \pmod{m}$
3.  $\forall a, b, c \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  và  $b \equiv c \pmod{m}$  suy ra  $a \equiv c \pmod{m}$

## Định lý

1. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ ;
2. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ ;

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;
2.  $\forall a, b \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  suy ra  $b \equiv a \pmod{m}$
3.  $\forall a, b, c \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  và  $b \equiv c \pmod{m}$  suy ra  $a \equiv c \pmod{m}$

## Định lý

1. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ ;
2. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ ;
3. Từ  $ac \equiv bc \pmod{m}$  và  $\text{ƯCLN}(c, m) = 1$  suy ra  $a \equiv b \pmod{m}$ ;



## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;
2.  $\forall a, b \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  suy ra  $b \equiv a \pmod{m}$
3.  $\forall a, b, c \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  và  $b \equiv c \pmod{m}$  suy ra  $a \equiv c \pmod{m}$

## Định lý

1. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ ;
2. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ ;
3. Từ  $ac \equiv bc \pmod{m}$  và  $\text{ƯCLN}(c, m) = 1$  suy ra  $a \equiv b \pmod{m}$ ;
4. Từ  $a \equiv b \pmod{m}$  suy ra  $ac \equiv bc \pmod{mc}$ ,  $\forall c \in \mathbb{Z}, c > 0$  và  $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ,  $0 < d \in \mathbb{Z}, d \mid \text{ƯCLN}(a, b, m)$ .

## Định lý

*Quan hệ đồng dư là một quan hệ tương đương trên tập số nguyên  $\mathbb{Z}$ , có nghĩa là*

1.  $\forall a \in \mathbb{Z}$  ta có  $a \equiv b \pmod{m}$ ;
2.  $\forall a, b \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  suy ra  $b \equiv a \pmod{m}$
3.  $\forall a, b, c \in \mathbb{Z}$  ta có từ  $a \equiv b \pmod{m}$  và  $b \equiv c \pmod{m}$  suy ra  $a \equiv c \pmod{m}$

## Định lý

1. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ ;
2. Từ  $a_1 \equiv b_1 \pmod{m}$  và  $a_2 \equiv b_2 \pmod{m}$  suy ra  $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ ;
3. Từ  $ac \equiv bc \pmod{m}$  và  $\text{ƯCLN}(c, m) = 1$  suy ra  $a \equiv b \pmod{m}$ ;
4. Từ  $a \equiv b \pmod{m}$  suy ra  $ac \equiv bc \pmod{mc}$ ,  $\forall c \in \mathbb{Z}, c > 0$  và  $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ,  $0 < d \in \mathbb{Z}, d \mid \text{ƯCLN}(a, b, m)$ .

# Tập hợp các lớp thặng dư

## Định nghĩa

*Khi chia một số nguyên bất kỳ cho  $m$  ta sẽ được số dư  $r$ . Tập hợp tất cả các số nguyên khi chia cho  $m$  có cùng số dư  $r$  tạo thành một lớp thặng dư  $\bar{r}$ . Tập hợp tất cả những lớp thặng dư đó được gọi là các lớp thặng dư mô-đun  $m$  và kí hiệu là  $\mathbb{Z}_m$ .*

# Tập hợp các lớp thặng dư

## Định nghĩa

*Khi chia một số nguyên bất kỳ cho  $m$  ta sẽ được số dư  $r$ . Tập hợp tất cả các số nguyên khi chia cho  $m$  có cùng số dư  $r$  tạo thành một lớp thặng dư  $\bar{r}$ . Tập hợp tất cả những lớp thặng dư đó được gọi là các lớp thặng dư mô-đun  $m$  và kí hiệu là  $\mathbb{Z}_m$ .*

## Ví dụ

*Trong  $\mathbb{Z}_8$ , lớp thặng dư  $\bar{3}(\text{mod } 8)$  là  $\bar{3} = \{x \in \mathbb{Z} \mid x \equiv 3(\text{mod } 8)\}$*

# Tính chất

## Định lý

# Tính chất

## Định lý

1. Tập hợp  $\mathbb{Z}_m$  có  $m$  lớp thặng dư.

# Tính chất

## Định lý

1. Tập hợp  $\mathbb{Z}_m$  có  $m$  lớp thặng dư.
2. Mỗi lớp thặng dư của  $\mathbb{Z}_m$  là hợp của  $k$  lớp thặng dư phân biệt của  $\mathbb{Z}_{km}$  ( $k > 1$ ).

## Định lý

(Định lý Euler.) Giả sử  $m$  là một số tự nhiên lớn hơn 1 và  $a$  là một số nguyên nguyên tố với  $m$ . Khi đó ta có  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

trong đó  $\varphi(m)$  được tính như sau:

# Tính chất

## Định lý

1. Tập hợp  $\mathbb{Z}_m$  có  $m$  lớp thặng dư.
2. Mỗi lớp thặng dư của  $\mathbb{Z}_m$  là hợp của  $k$  lớp thặng dư phân biệt của  $\mathbb{Z}_{km}$  ( $k > 1$ ).

## Định lý

(Định lý Euler.) Giả sử  $m$  là một số tự nhiên lớn hơn 1 và  $a$  là một số nguyên nguyên tố với  $m$ . Khi đó ta có  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

trong đó  $\varphi(m)$  được tính như sau:

$$\varphi(1) = 1.$$



# Tính chất

## Định lý

1. Tập hợp  $\mathbb{Z}_m$  có  $m$  lớp thặng dư.
2. Mỗi lớp thặng dư của  $\mathbb{Z}_m$  là hợp của  $k$  lớp thặng dư phân biệt của  $\mathbb{Z}_{km}$  ( $k > 1$ ).

## Định lý

(Định lý Euler.) Giả sử  $m$  là một số tự nhiên lớn hơn 1 và  $a$  là một số nguyên nguyên tố với  $m$ . Khi đó ta có  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

trong đó  $\varphi(m)$  được tính như sau:

$$\varphi(1) = 1.$$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$  với  $p$  là số nguyên tố,  $\alpha$  là một số tự nhiên khác 0.

# Tính chất

## Định lý

1. Tập hợp  $\mathbb{Z}_m$  có  $m$  lớp thặng dư.
2. Mỗi lớp thặng dư của  $\mathbb{Z}_m$  là hợp của  $k$  lớp thặng dư phân biệt của  $\mathbb{Z}_{km}$  ( $k > 1$ ).

## Định lý

(Định lý Euler.) Giả sử  $m$  là một số tự nhiên lớn hơn 1 và  $a$  là một số nguyên nguyên tố với  $m$ . Khi đó ta có  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

trong đó  $\varphi(m)$  được tính như sau:

$$\varphi(1) = 1.$$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$  với  $p$  là số nguyên tố,  $\alpha$  là một số tự nhiên khác 0.

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k}) \text{ với } n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

$p_1, p_2, \dots, p_k$  là những số nguyên tố.

# Phương trình đồng dư

## Định nghĩa

Cho  $f(x) \in \mathbb{Z}$ . Nếu với  $x = x_0$  ta có  $f(x_0) \equiv 0 \pmod{m}$  thì nói  $x_0$  là nghiệm đúng của phương trình  $f(x) \equiv 0 \pmod{m}$ .

# Phương trình đồng dư

## Định nghĩa

Cho  $f(x) \in \mathbb{Z}$ . Nếu với  $x = x_0$  ta có  $f(x_0) \equiv 0 \pmod{m}$  thì nói  $x_0$  là nghiệm đúng của phương trình  $f(x) \equiv 0 \pmod{m}$ .

## Định lý

Nếu  $x = \alpha$  là nghiệm đúng của phương trình  $f(x) \equiv 0 \pmod{m}$  thì mọi số nguyên thuộc lớp thặng dư  $\overline{\alpha} \pmod{m}$  đều là nghiệm đúng của phương trình  $f(x) \equiv 0 \pmod{m}$ .

# Phương trình đồng dư bậc nhất một ẩn

# Phương trình đồng dư bậc nhất một ẩn

## Định lý

*Phương trình  $ax \equiv b \pmod{m}$  trong đó  $a$  không chia hết cho  $m$ , có nghiệm khi và chỉ khi  $\text{ƯCLN}(a, m) = d$  là một ước của  $b$ . Khi phương trình này có nghiệm thì nó có  $d$  nghiệm.*

# Phương trình đồng dư bậc nhất một ẩn

## Định lý

*Phương trình  $ax \equiv b \pmod{m}$  trong đó  $a$  không chia hết cho  $m$ , có nghiệm khi và chỉ khi  $\text{ƯCLN}(a, m) = d$  là một ước của  $b$ . Khi phương trình này có nghiệm thì nó có  $d$  nghiệm.*

**Cách xác định nghiệm.**

# Phương trình đồng dư bậc nhất một ẩn

## Định lý

*Phương trình  $ax \equiv b \pmod{m}$  trong đó  $a$  không chia hết cho  $m$ , có nghiệm khi và chỉ khi  $\text{ƯCLN}(a, m) = d$  là một ước của  $b$ . Khi phương trình này có nghiệm thì nó có  $d$  nghiệm.*

## Cách xác định nghiệm.

Xét phương trình  $ax \equiv b \pmod{m}$  với điều kiện  $(a, m) = 1$  và  $1 < a < m$ .



# Phương trình đồng dư bậc nhất một ẩn

## Định lý

Phương trình  $ax \equiv b \pmod{m}$  trong đó  $a$  không chia hết cho  $m$ , có nghiệm khi và chỉ khi  $\text{ƯCLN}(a, m) = d$  là một ước của  $b$ . Khi phương trình này có nghiệm thì nó có  $d$  nghiệm.

## Cách xác định nghiệm.

Xét phương trình  $ax \equiv b \pmod{m}$  với điều kiện  $(a, m) = 1$  và  $1 < a < m$ .

Cách 1. Chia 2 vế cho  $a$

Nếu  $a$  là một ước của  $b$  thì ta được nghiệm  $x \equiv \frac{b}{a} \pmod{m}$ .

Nếu  $a$  không là ước của  $b$  thì do  $\text{ƯCLN}(a, m) = 1$  nên luôn có số nguyên  $k$  ( $1 \leq k \leq a - 1$ ) để  $b + km$  chia hết cho  $a$ . Khi đó phương trình đã cho tương đương với  $ax \equiv b + km \pmod{m}$  nên nó có nghiệm là  $x \equiv \frac{b + km}{a} \pmod{m}$ .

# Phương trình đồng dư bậc nhất một ẩn

## Định lý

Phương trình  $ax \equiv b \pmod{m}$  trong đó  $a$  không chia hết cho  $m$ , có nghiệm khi và chỉ khi  $\text{ƯCLN}(a, m) = d$  là một ước của  $b$ . Khi phương trình này có nghiệm thì nó có  $d$  nghiệm.

## Cách xác định nghiệm.

Xét phương trình  $ax \equiv b \pmod{m}$  với điều kiện  $(a, m) = 1$  và  $1 < a < m$ .

Cách 1. Chia 2 vế cho  $a$

Nếu  $a$  là một ước của  $b$  thì ta được nghiệm  $x \equiv \frac{b}{a} \pmod{m}$ .

Nếu  $a$  không là ước của  $b$  thì do  $\text{ƯCLN}(a, m) = 1$  nên luôn có số nguyên  $k$  ( $1 \leq k \leq a - 1$ ) để  $b + km$  chia hết cho  $a$ . Khi đó phương trình đã cho tương đương với  $ax \equiv b + km \pmod{m}$  nên nó có nghiệm là  $x \equiv \frac{b + km}{a} \pmod{m}$ .

Cách 2. Từ giả thiết  $(a, m) = 1$ , theo định lý Euler ta có  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . Nhân 2 vế cho  $b$  ta được và viết lại  $a(ba^{\varphi(m)-1}) \equiv b \pmod{m}$ . Ta sẽ được  $x \equiv ba^{\varphi(m)-1} \pmod{m}$

Ví dụ.

Ví dụ.

Giải phương trình

1.  $3x \equiv 5 \pmod{8}.$

Ví dụ.

Giải phương trình

1.  $3x \equiv 5 \pmod{8}.$

2.  $7x \equiv 3 \pmod{12}.$

# Hệ phương trình đồng dư bậc nhất một ẩn

# Hệ phương trình đồng dư bậc nhất một ẩn

Cho hệ phương trình đồng dư bậc nhất

$$\begin{cases} x \equiv b_1 (\text{mod } m_1) \\ x \equiv b_2 (\text{mod } m_2) \\ \dots\dots\dots \\ x \equiv b_k (\text{mod } m_k) \end{cases}$$

ở đây  $m_1, m_2, \dots, m_k$  là những số nguyên lớn hơn 1 và  $b_1, b_2, \dots, b_k$  là những số nguyên tùy ý.

# Hệ phương trình đồng dư bậc nhất một ẩn

Cho hệ phương trình đồng dư bậc nhất

$$\begin{cases} x \equiv b_1 (\text{mod } m_1) \\ x \equiv b_2 (\text{mod } m_2) \\ \dots\dots\dots \\ x \equiv b_k (\text{mod } m_k) \end{cases}$$

ở đây  $m_1, m_2, \dots, m_k$  là những số nguyên lớn hơn 1 và  $b_1, b_2, \dots, b_k$  là những số nguyên tùy ý.

## Định lý

*Nếu hệ phương trình đồng dư bậc nhất một ẩn có nghiệm thì nghiệm đó là duy nhất.*



# Hệ phương trình đồng dư bậc nhất một ẩn

Cho hệ phương trình đồng dư bậc nhất

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

ở đây  $m_1, m_2, \dots, m_k$  là những số nguyên lớn hơn 1 và  $b_1, b_2, \dots, b_k$  là những số nguyên tùy ý.

## Định lý

*Nếu hệ phương trình đồng dư bậc nhất một ẩn có nghiệm thì nghiệm đó là duy nhất.*

## Định lý

*(Định lý Trung Quốc.) Nếu các mô-đun  $m_1, m_2, \dots, m_k$  đôi một nguyên tố cùng nhau thì hệ phương trình đồng dư bậc nhất một ẩn có nghiệm.*



Cho hệ phương trình đồng dư bậc nhất

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

với điều kiện  $b_1 - b_2$  chia hết cho  $d = \text{ƯCLN}(m_1, m_2)$ . Lúc này  $x \equiv x_0 \pmod{m}$  trong đó  $x_0 = b_1 + m_1 t_0$ ,  $m = \text{BCNN}(m_1, m_2)$ . Trong đó  $t_0$  được tìm như sau:

Ta có  $x = b_1 + m_1 t \equiv b_2 \pmod{m_2}$ . Vì  $d = \text{ƯCLN}(m_1, m_2)$  là ước của  $b_1 - b_2$  nên phương trình  $b_1 + m_1 t \equiv b_2 \pmod{m_2}$  tương đương với phương trình  $\frac{m_1}{d} t \equiv \frac{b_2 - b_1}{d} \pmod{\frac{m_2}{d}}$ . Nhưng do  $\text{ƯCLN}(\frac{m_1}{d}, \frac{m_2}{d}) = 1$  nên nó có nghiệm  $t \equiv t_0 \pmod{\frac{m_2}{d}}$

Ví dụ.

## Ví dụ.

### 1. Giải hệ phương trình

$$\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 8 \pmod{15} \\ x \equiv -1 \pmod{12} \\ x \equiv 13 \pmod{35} \end{cases}$$

## Ví dụ.

### 1. Giải hệ phương trình

$$\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 8 \pmod{15} \\ x \equiv -1 \pmod{12} \\ x \equiv 13 \pmod{35} \end{cases}$$

### 2. Giải hệ phương trình

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

# Bài tập

## 1. Giải phương trình

1.  $3x \equiv 7 \pmod{8}$ .

2.  $5x \equiv 4 \pmod{11}$ .

3.  $7x \equiv 6 \pmod{13}$ .

4.  $13x \equiv 1 \pmod{27}$ .

## 2. Giải phương trình

1.  $6x \equiv 27 \pmod{33}$ .

2.  $10x \equiv 15 \pmod{65}$ .

3.  $18x \equiv 6 \pmod{42}$ .

4.  $15x \equiv 25 \pmod{70}$ .

## 1. Giải hệ phương trình

$$\begin{cases} x \equiv 4(mod\ 5) \\ x \equiv 2(mod\ 7) \\ x \equiv 3(mod\ 13) \end{cases}$$

## 2. Giải hệ phương trình

$$\begin{cases} 3x \equiv 5(mod\ 4) \\ 2x \equiv 3(mod\ 5) \\ 5x \equiv 1(mod\ 9) \end{cases}$$