Bài tập 2: Số học modun và hệ mã cổ điển

Số học modun

Bài 1

Hãy tính:

1. $15 \times 29 \mod 13$
2. $2 \cdot 29 \mod 13$
3. $2 \cdot 3 \mod 13$
4. $-11 \cdot 3 \mod 13$

Vành số nguyên $\mathbb{Z}_m$ bao gồm:

- Tập số nguyên $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$
- Hai phép toán "+" và "·" trên mọi $a, b \in \mathbb{Z}_m$ thoả mãn:

    1. $a + b = c \mod m$
    2. $a \cdot b = d \mod m.$

Nghịch đảo của $a \in \mathbb{Z}_m$, ký hiệu a^{-1} , định nghĩa bởi: $a \cdot a^{-1} = 1 \mod m.$

Bài 2

Nghịch đảo của 5 trong $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$, và $\mathbb{Z}_{13}$ là gì?

Bài 3

Hãy tính giá trị của $x \in \mathbb{Z}_1 3$ thoả mãn phương trình dưới đây mà không dùng máy tính:

- $x = 3^2 \mod 13$
- $x = 7^2 \mod 13$
- $x = 3^{10} \mod 13$
- $x = 7^{100} \mod 13$
- $x = \sqrt{3} \mod 13$

- $7^x = 11 \mod 13$

Câu hỏi

Khi nào thì phần tử $x \in \mathbb{Z}_m$ có nghịch đảo?

Hệ mã dịch

Bài tập 4

Hệ mã dịch có khoá $k \in \mathbb{Z}_{26}$ và hàm mã hoá

$$y = x + k \mod 26$$

Hàm giải mã là gì?

Hệ mã Affine

Bài 5

Hệ mã Affine có khoá $k = (a, b)$ với $a, b \in \mathbb{Z}_{26}$. Hàm mã hoá biến đổi thông điệp x thành bản mã y như sau:

$$y = a \cdot x + b \mod 26$$

Hàm giải mã là gì?

Bài 5

Hãy cài đặt hàm mã hoá và giải mã bằng C/C++ hoặc một ngôn ngữ lập trình khác.

Bài 6

Xét hệ mã affine với khoá $k = (a, b)$ với $a = 7, b = 22$.

1. Giải mã thông điệp dưới đây

   ```
   falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj
   ```

1. Ai viết dòng này?