NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Assignment 20

2023 年 12 月 22 日

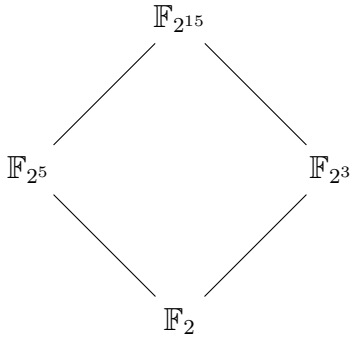
Problem 1

在有限域 $\mathbb{F}_p$ 中, p 是素数. 证明: 对任意 $a, b \in \mathbb{F}_p$ 有 $(a+b)^p = a^p + b^p$.

Problem 2

给出 $\mathbb{F}_{2^{12}}$ 的所有子域以及子域的子域.

示例: $\mathbb{F}_{2^{15}}$ 的结果是为



Problem 3

证明: 有限域 $\mathbb{F}_{2^n}$ 的任意元素是某个元素的平方, 即 $\mathbb{F}_{2^n} = \{x^2 : x \in \mathbb{F}_{2^n}\}$.

Answer 20

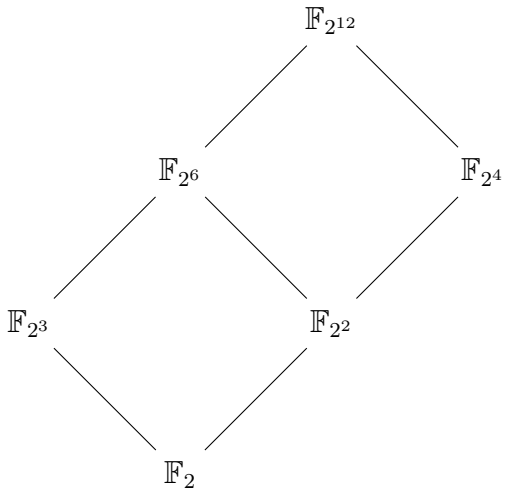
Problem 1

在有限域 $\mathbb{F}_p$ 中, p 是素数. 证明: 对任意 $a, b \in \mathbb{F}_p$ 有 $(a+b)^p = a^p + b^p$.

解: 因为 $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$. 故仅需证明对任意 $1 \le k \le p-1$, p 整除 $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ 即可. 注意到 $\binom{p}{k}$ 是整数, 即, 从 $\frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!}$ 中可得到 $k!(p-k)! \mid p \cdot (p-1)!$, 又因为 p 是素数, 故 $k!(p-k)! \nmid p$, 故有 $k!(p-k)! \mid (p-1)!$, 因此 $p \mid \binom{p}{k}$. 所以对任意 $a, b \in \mathbb{F}_p$ 有 $(a+b)^p = a^p + b^p$.

Problem 2

给出 $\mathbb{F}_{2^{12}}$ 的所有子域以及子域的子域.



Problem 3

证明: 有限域 $\mathbb{F}_{2^n}$ 的任意元素是某个元素的平方, 即 $\mathbb{F}_{2^n} = \{x^2 : x \in \mathbb{F}_{2^n}\}$.

解: 考虑映射 $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, 函数映射关系为 $\phi(x) = x^2$, 其中 $x \in \mathbb{F}_{2^n}$. 这是一个一一映射: 假设有 $\phi(x) = \phi(y)$, 则 $x^2 = y^2$, 即 $x^2 + y^2 = (x + y)^2 = 0$, 但有限域中无零因子, 故 $x = y$, 即映射为单射; 此外 $\mathbb{F}_{2^n}$ 是有限的, 所以是满射. 因此为一一映射, 所以有 $\mathbb{F}_{2^n} = \{x^2 : x \in \mathbb{F}_{2^n}\}$.