NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 1-4

2023 年 9 月 27 日

Assignment 1

Problem 1

设 a, b 是任意两个正整数, 则:

(1) a, b 的所有公倍数就是 $[a, b]$ 的所有倍数;

(2) $[a, b] = \frac{ab}{(a,b)}$.

解:

(1) 设正整数 $c = [a, b]$, 正整数 d 为 a, b 的任意公倍数, 即 $a \mid d, b \mid d$. 故对于两个正整数 c, d, 由定理 3(带余除法) 可知一定存在整数 q, r 使得 $d = qc + r$, 其中 $0 \leq r \leq c - 1$. 由于 $a \mid c$, $a \mid d$ 和 $r = d - qc$, 故有 $a \mid r$, 同理有 $b \mid r$, 故 r 是 a, b 的公倍数. 又因为 $r \leq c - 1$, 故 $r = 0$, 即 $d = qc$, 证毕.

(2) 设正整数 $d = \gcd(a, b)$ 和正整数 $l = [a, b]$. 由 $d \mid a$ 且 $d \mid b$ 可假设 $a = da_0, b = db_0$, 其中 a_0 和 b_0 互素, 故 $\frac{ab}{d} = a_0 b = b_0 a$ 是 a, b 的公倍数, 则由本题 (1) 结论可知 $l \mid \frac{ab}{d}$. 假设 m 是 a, b 的非零公倍数, 故有 $m = ka = ka_0 d$ 和 $b = b_0 d \mid m$, 因此有 $b_0 \mid ka_0$, 但 a_0 和 b_0 互素, 故有推论 11(2) 得到 $b_0 \mid k$, 因此有 $\frac{ab}{\gcd(a,b)} = a_0 b_0 d \mid m$. 因为 m 是 a, b 的公倍数而 l 是 a, b 的最小公倍数, 故 $\frac{ab}{\gcd(a,b)} = l = [a, b]$.

Problem 2

(1) 利用辗转相除法计算 13 和 31 的最大公因数;

(2) 设 a, b 是任意两个互素的正整数, 证明 $\gcd(a, a + b^2) = 1$ 且 $\gcd(ab, a^2 + b^2) = 1$.

解:

(1) 我们有

$$\begin{aligned} 31 &= 2 \times 31 && +5 \\ 13 &= 2 \times 5 && +3 \\ 5 &= 1 \times 3 && +2 \\ 3 &= 1 \times 2 && +1 \\ 2 &= 2 \times 1 \end{aligned}$$

因此 13 和 31 的最大公因数为 1.

(2) 由定理 10 可知, 根据 $\gcd(a,b) = 1$, 有 $\gcd(a,b^2) = 1$, 由定理 12 的注 12.1 可知, $\gcd(a, a+b^2) = \gcd(a,b^2) = 1$; 同样根据定理 12 的注 12.1 可知 $\gcd(a, a^2+b^2) = \gcd(a,b^2) = 1$, 同理 $\gcd(b, a^2+b^2) = 1$, 故由推论 11 的 (1) 得到结论 $\gcd(ab, a^2+b^2) = 1$.

Assignment 2

Problem 1

若 $a \equiv b \pmod{m_i}$, $i = 1, 2, \ldots, k$, 证明

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$

证明: 因为 $a \equiv b \pmod{m_i}$, 故 $m_i \mid a-b$, 其中 $i = 1, 2, \ldots, k$, 则 $a-b$ 是 $m_1, m_2, \ldots, m_k$ 的公倍数. 又因为 $[m_1, m_2, \ldots, m_k]$ 整除 $m_1, m_2, \ldots, m_k$ 的公倍数, 即 $[m_1, m_2, \ldots, m_k] \mid a-b$, 故 $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$.

Problem 2

设 m, n 是两个互素的正整数. $x_1, x_2, \ldots, x_{\phi(m)}$ 是模 m 的一个简化剩余系, $y_1, y_2, \ldots, y_{\phi(n)}$ 是模 n 的一个化剩余系, 证明 $my_1 + nx_1, my_1 + nx_2, \ldots, my_1 + nx_{\phi(m)}, \ldots, my_{\phi(n)} + nx_1, my_{\phi(n)} + nx_2, \ldots, my_{\phi(n)} + nx_{\phi(m)}$ 是模 mn 的一个简化剩余系.

证明: 首先证明这 $\varphi(m)\varphi(n)$ 个数都与 mn 互素. 只需证明对任意 $1 \le i \le \varphi(n), 1 \le j \le \varphi(m)$ 都有 $(my_i + nx_j, mn) = 1$ 即可. 利用反证法. 假设存在 $1 \le i' \le \varphi(n), 1 \le j' \le \varphi(m)$ 使得 $my_{i'} + nx_{j'}$ 与 mn 不互素, 则必定存在素数 p 使得 $p \mid my_{i'} + nx_{j'}$ 且 $p \mid mn$. 现证明 $p \mid mn$ 不成立, 从而可推出假设不成立. 若 $p \mid mn$ 成立, 则由推论 11 第 (3) 条知必有 $p \mid m$ 或 $p \mid n$.

情形 1. 若 $p \mid m$, 则 $p \mid nx_{j'}$. 因 $p \nmid x_{j'}$ (否则 p 为 $m, x_{j'}$ 的因子, 这与 $(m, x_{j'}) = 1$ 矛盾), 故 $p \mid n$, 这与 $(m,n) = 1$ 矛盾;

情形 2. 若 $p \mid n$, 则 $p \mid my_{i'}$. 因 $p \nmid y_{i'}$, 故 $p \mid m$, 这与 $(m,n)=1$ 矛盾.

因此, $p \nmid m$ 且 $p \nmid n$, 从而 $p \mid mn$ 不成立, 从而假设不成立. 于是, 对任意 $1 \le i \le \varphi(n), 1 \le j \le \varphi(m)$ 都有 $(my_i + nx_j, mn) = 1$.

其次证明对于模 mn 的一个简化剩余系, 其元素均有 $my_i + nx_j$ 的形式, 其中 $1 \le i \le \varphi(n), 1 \le j \le \varphi(m)$. 进一步, 由注 22.1 第 (1) 条 () 以及定理 28(这 $\varphi(mn)$ 个数对模 mn 两两不同余) 可知, 若能证明对任意 $x, y \in \mathbb{Z}$ 使得 $(my + nx, mn) = 1$ 时必有 $(x,m) = (y,n) = 1$ 则定理成立. 由 $(my + nx, mn) = 1$ 可得 $(my + nx, m) = (my + nx, n) = 1$ (否则若 $(my + nx, m) = d > 1$ 则显然 $(my + nx, mn) \ge d$). 于是由定理 3 或注 12.1 可得 $(nx, m) = (my, n) = 1$.

Assignment 3

RSA 和 Rabin 密码算法的结果分别参考课件 slice 的第 50 页和第 51 页.

引理 54

映射 $f : A \to B$ 是一一映射的充分必要条件是 f 是可逆映射.

证明:

必要性: 假设 f 是可逆映射, 则 f 存在逆映射 $f^{-1} : B \to A$. 对于 $\forall b \in B$, 我们都有 $f^{-1}(b) = a \in A$, 则 $f(a) = f(f^{-1}(b)) = b$, 因此 f 是满射; 假设 $a_1, a_2 \in A$ 且满足 $f(a_1) = f(a_2)$, 则有 $a_1 = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = a_2$, 故 f 是单射. 因此 f 是一一映射.

充分性: 若 f 是一一映射, 故根据 f 的满射性质有, 对于任意给定的 $b \in B$ 我们都能找到 $a \in A$ 使得 $f(a) = b$, 同时因为 f 是单射, 则 a 是唯一确定的; 因此定义映射 $g : B \to A$, 其中 $g(b) = a$, 则 $f(g(b)) = f(a) = b$ 和 $g(f(a)) = g(b) = a$, 因此 f 是可逆映射.

引理 55

设 $f : A \to B$ 和 $g : B \to C$ 都是一一映射, 则 $g \circ f : A \to C$ 也是一一映射, 并且 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

证明: 因为 f, g 都是一一映射, 根据引理 54 可知 f, g 都是可逆映射, 分别记为

f^{-1}, g^{-1}. 因此直接检验

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ f \circ f^{-1} \circ g^{-1} \\ &= g \circ (f \circ f^{-1}) \circ g^{-1} \\ &= g \circ \mathsf{id}_B \circ g^{-1} \\ &= g \circ g^{-1} \\ &= \mathsf{id}_C\end{aligned}$$

同理可以得到 $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathsf{id}_A$, 其中 $\mathsf{id}_A, \mathsf{id}_B$ 和 id_C 分别是集合 A, B 和 C 的恒等映射. 故 $g \circ f : A \to C$ 是可逆映射, 因此是一一映射.

Assignment 4

Problem

验证下列集合 G 与给定的运算能否构成群, 即判断是否满足群定义中的四个条件.

(1) $G = \mathbb{C}$ 为复数集, 运算为复数域上的乘法.

(2) $G = \mathbb{Z}$ 为整数集, 运算为整数上的减法.

(3) $G = \mathbb{R}$ 为实数集, 运算为 $\star$, 其定义如下:

$$a \star b = (a+1)(b+1) - 1, \forall a, b \in \mathbb{R}.$$

证明:

(1) 对于代数结构 $(\mathbb{C}, *)$, 我们有:

   (a) 由于复数乘复数的结果仍然是复数, 故代数结构满足封闭性.

   (b) 对于 $\forall a, b, c \in \mathbb{C}$, 都有 $a * (b * c) = (a * b) * c$, 故结合律成立.

   (c) 对于 $\forall a \in \mathbb{C}$, 我们有 $a * 1 = 1 * a = a$, 则 1 是单位元.

   (d) 但除了 0 以外的元素才有逆元: $a \in \mathbb{C} \setminus \{0\}$ 的逆元 $1/a$.

   因此该代数结构不构成群.

(2) 对于代数结构 $(\mathbb{Z}, -)$, 我们有:

   (a) 由于整数相减的结果仍然是整数, 故代数结构满足封闭性.

(b) 对于 $\forall a, b, c \in \mathbb{Z}$, 等式 $a-(b-c)=a-b+c=(a-b)-c$ 成立当且仅当 $c=0$, 故结合律不成立.

(c) 设 $\mathsf{id} \in \mathbb{Z}$ 为单位元, 对于 $\forall a \in \mathbb{Z}$, 我们有 $a-\mathsf{id}=\mathsf{id}-a=a$, 即 $\mathsf{id}=0$ 且 $\mathsf{id}=2a$, 故不存在单位元.

因此该代数结构不构成群.

(3) 对于代数结构 $(\mathbb{R}, \star)$, 我们有:

(a) 由于实数之间的加减乘的结果仍然是实数, 故代数结构满足封闭性.

(b) 对于 $\forall a, b, c \in \mathbb{R}$, 都有 $a \star (b \star c) = a \star ((b+1)(c+1)-1) = (a+1)\left((b+1)(c+1)-1+1\right)-1 = (a+1)(b+1)(c+1)-1$, 同时也有 $(a \star b) \star c = (a+1)(b+1)(c+1)-1$, 则 $a \star (b \star c) = (a \star b) \star c$, 故结合律成立.

(c) 假设 $\mathsf{id} \in \mathbb{R}$ 是单位元, 对于 $\forall a \in \mathbb{R}$, 我们有 $a \star \mathsf{id} = \mathsf{id} \star a = a$, 即 $(a+1)\mathsf{id} = 0$, 则 0 是单位元.

(d) $\forall a \in \mathbb{R}$, 其逆元为 a^{-1} 满足 $a \star a^{-1} = 0$, 即 $(a+1)(a^{-1}+1)-1=0 \Rightarrow (a+1)(a^{-1}+1)=1$, 但 $a=-1$ 时上式不成立, 故 -1 没有逆元.

因此该代数结构不构成群.