離散数理工学 (5) **2023 年 11 月 14 日**

演習問題 **岡本 吉央**

提出締切： 2023 年 11 月 21 日 午前 9:00

授業内問題 5.1 式 $(14 + x) \bmod 43 = 0$ を満たす $x \in \mathbb{Z}/43\mathbb{Z}$ をすべて答えよ．(注：43 は素数である．)

授業内問題 5.2 式 $5x \bmod 19 = 1$ を満たす $x \in \mathbb{Z}/19\mathbb{Z}$ をすべて答えよ．(注：19 は素数である．)

授業内問題 5.3 式 $90x \bmod 439 = 1$ を満たす $x \in \mathbb{Z}/439\mathbb{Z}$ をすべて答えよ．(注：439 は素数である．)

復習問題 5.4 任意の整数 a, b で，$b > 0$ となるものを考える．このとき，

$$a \bmod b = (a \bmod b) \bmod b$$

が成り立つことを証明せよ．

復習問題 5.5 任意の整数 a, a' と正整数 $n > 0$ を考える．このとき，$a \bmod n = a' \bmod n$ が成り立つための必要十分条件は，ある整数 q が存在して，$a - a' = nq$ となることである．これを証明せよ．

復習問題 5.6 任意の整数 a, a' と正整数 $n > 0$ を考える．このとき，

$$(a + a') \bmod n = ((a \bmod n) + (a' \bmod n)) \bmod n$$

が成り立つことを証明せよ．

復習問題 5.7 任意の正整数 $n \geq 2$ を固定する．任意の $x \in \mathbb{Z}/n\mathbb{Z}$ に対して，$x + y = 0$ を満たす $y \in \mathbb{Z}/n\mathbb{Z}$ が一意に存在することを証明せよ．

復習問題 5.8 任意の正整数 x, y で $x \geq y$ を満たすものを考える．このとき，$ax + by = \gcd(x, y)$ を満たす整数 a, b が存在することを証明せよ．ここで，$\gcd(x, y)$ は x と y の最大公約数を表す．(ヒント：ユークリッドのアルゴリズムの原理 (演習問題 2.8) を利用してみよ．)

復習問題 5.9 任意の素数 $p \geq 2$ と整数 a, b を考える．このとき，$ab \bmod p = 0$ ならば，$a \bmod p = 0$ または $b \bmod p = 0$ が成り立つことを証明せよ．

復習問題 5.10 任意の素数 $p \geq 2$ を固定する．任意の $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ に対して，$x \cdot y = 0$ を満たす $y \in \mathbb{Z}/p\mathbb{Z}$ が一意に存在することを証明せよ．(ヒント：演習問題 5.8 と 5.9 を用いてもよい．)

復習問題 5.11 $(32 + x) \bmod 89 = 0$ を満たす $x \in \mathbb{Z}/89\mathbb{Z}$ をすべて答えよ．(注：89 は素数である．)

復習問題 5.12 $32x \bmod 89 = 1$ を満たす $x \in \mathbb{Z}/89\mathbb{Z}$ をすべて答えよ．(注：89 は素数である．)

復習問題 5.13 $3x \bmod 61 = 1$ を満たす $x \in \mathbb{Z}/61\mathbb{Z}$ をすべて答えよ．(注：61 は素数である．)

補足問題 (発展) 5.14 任意の整数 a, b で，$b > 0$ となるものを考える．このとき，ある整数 q, r で

$$a = bq + r, \quad 0 \leq r < b$$

を満たすものが一意に存在することを次の流れに沿って証明せよ．(注：これは発展問題であるが，難しいわけではない．)

1. まず，存在性を証明する．a が 0 以上のときには，a に関する数学的帰納法で証明を進める．$a = 0$ のとき，そのような整数 q, r が存在することを証明せよ．
2. $a > 0$ のとき，a 未満の任意の非負整数 a' に対して，ある整数 q', r' が存在して，$a' = bq' + r'$ と $0 \leq r' < b$ を満たすことを仮定する．このとき，ある整数 q, r が存在して，$a = bq + r$ と $0 \leq r < b$ を満たすことを証明せよ．これで，a が 0 以上のときの存在性証明が終わった．
3. $a < 0$ のときに，存在性の証明を完了せよ．(ヒント：$-a$ を考えよ．)
4. 次に，一意性の証明を行う．整数 q, r, q', r' が存在して，$a = bq + r = bq' + r'$，$0 \leq r < b$，$0 \leq r' < b$ を満たすとする．このとき，$q = q'$ かつ $r = r'$ が成り立つことを証明せよ．

注：この問題の内容は剰余演算 mod の基盤となるものなので，この問題を解くために剰余演算を用いてはならない．

補足問題 5.15 任意の整数 a, a' と正整数 $n > 0$ を考える．このとき，

$$(a \cdot a') \bmod n = ((a \bmod n) \cdot (a' \bmod n)) \bmod n$$

が成り立つことを証明せよ．

追加問題 5.16 任意の整数 a, b と任意の素数 p に対して，

$$(a + b)^p \bmod p = (a^p + b^p) \bmod p$$

が成り立つことを証明せよ．(ヒント：二項定理．)

追加問題 5.17 素数ではない正の整数 $n \geq 4$ として任意のものを考える．このとき，「任意の整数 a, b に対して，$ab \bmod n = 0$ を満たすとき，$a \bmod n = 0$ または $b \bmod n = 0$ である」という性質は成り立たない．素数ではない任意の正の整数 $n \geq 4$ に対して，この性質が成り立たないことを示す反例を挙げよ．