離散数理工学 (5) 2015 年 11 月 17 日

演習問題 岡本 吉央

提出締切： 2015 年 11 月 24 日 講義終了時

復習問題 5.1 任意の正整数 $m \in \mathbb{Z}_+$ と整数 $a, b \in \mathbb{Z}$ に対して，

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

が成り立つことを証明せよ．

復習問題 5.2 次を満たす $x \in \mathbb{Z}_7$ は何か？ 定めよ．

$$(3-x) \bmod 7 = 6.$$

復習問題 5.3 次を満たす $x \in \mathbb{Z}_7$ は何か？ 定めよ．

$$3x \bmod 7 = 2.$$

復習問題 5.4 正整数 $a, b \in \mathbb{Z}_+$ が $\gcd(a, b) = 1$ を満たすとする．以下の問いに答えよ．

1. ある整数 $u, v \in \mathbb{Z}$ が存在して $ua + vb = 1$ と書けることを証明せよ．
2. 整数 $c \in \mathbb{Z}$ が $bc \bmod a = 0$ を満たすとき，$c \bmod a = 0$ が成り立つことを証明せよ．

復習問題 5.5 正整数 $m \in \mathbb{Z}_+$ と整数 $a \in \mathbb{Z}$ が $\gcd(m, a) = 1$ を満たすとする．以下の問いに答えよ．

1. 集合として

   $$\mathbb{Z}_m = \{ax \bmod m \mid x \in \mathbb{Z}_m\}$$

   が成り立つことを証明せよ．(ヒント：演習問題 5.4 を用いてもよい．)
2. 方程式

   $$ax \bmod m = b \bmod m$$

   は $\mathbb{Z}_m$ にただ 1 つだけ解を持つことを証明せよ．

復習問題 5.6 次を満たす $x \in \mathbb{Z}_{56}$ は何か？ 定めよ．

$$25x \bmod 56 = 1.$$

復習問題 5.7 $\mathbb{Z}_4$ は体ではない．なぜか？

補足問題 5.8 任意の正整数 $m \in \mathbb{Z}_+$ と整数 $a, b \in \mathbb{Z}$ に対して，

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

が成り立つことを証明せよ．

追加問題 5.9 正整数 $a, b, c \in \mathbb{Z}_+$ に対して，$\gcd(a, b) = 1$ かつ $\gcd(a, c) = 1$ が満たされるとき，$\gcd(a, bc) = 1$ が成り立つことを証明せよ．(ヒント：演習問題 5.4 を用いてもよい．)

追加問題 5.10 正整数 $m \in \mathbb{Z}_+$ と整数 $a, b \in \mathbb{Z}$ に対して，$a \bmod m = b \bmod m$ が満たされるとき，m の任意の正の約数 d に対して，$a \bmod d = b \bmod d$ が成り立つことを証明せよ．

追加問題 5.11

1. 素数 p と整数 r が $1 \leq r \leq p-1$ を満たすとき，二項係数 $\binom{p}{r}$ は p で割り切れることを証明せよ．
2. 素数 p と整数 x, y に対して，

   $$(x+y)^p \bmod p = (x^p + y^p) \bmod p$$

   が成り立つことを証明せよ．

復習問題 5.12 次を満たす $x \in \mathbb{Z}_{35}$ は何か？ 定めよ．

$$19x \bmod 35 = 27.$$

復習問題 5.13 次を満たす $x \in \mathbb{Z}_{111}$ は何か？ 定めよ．

$$47x \bmod 111 = 89.$$