13 合同式・中国剰余定理・フェルマーの小定理

整数 a, b に対し, a, b の最大公約数を $\mathrm{GCD}(a, b)$ と書くことにする.

問題 13.1 a, b, m, n を整数, $m, n > 1$ とする.

(1) $a \equiv b \pmod{mn}$ ならば $a \equiv b \pmod{m}$ かつ $a \equiv b \pmod{n}$ であることを示せ.

(2) もし $\mathrm{GCD}(m, n) = 1$ ならば上記の逆も成立することを示せ.

(3) $\mathrm{GCD}(m, n) = 1$ でないときは (1) の逆は一般に成立しない. $a \equiv b \pmod{m}$ かつ $a \equiv b \pmod{n}$ であっても $a \equiv b \pmod{mn}$ ではないような例を挙げよ.

問題 13.2 b, c, m を整数, $m > 1$ とする. 合同式 $cx \equiv b \pmod{m}$ を満たすような $x \in \mathbb{Z}$ が存在するための必要十分条件は $\mathrm{GCD}(c, m) \mid b$ であることを示せ.

問題 13.3 次を満たす整数 x をひとつ求めよ.

(1) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{7} \end{cases}$

(2) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{11} \end{cases}$

問題 13.4 次を求めよ.

(1) 100^{30} を 7 で割った余り.

(2) $1^{30} + 2^{30} + 3^{30} + \cdots + 10^{30}$ を 31 で割った余り.

[1] ホームページ http://www.math.tsukuba.ac.jp/~amano/lec2012-2/e-algebra-ex/index.html