数学アラカルト(問題)

第２回　公開鍵暗号の仕組み

問題 1. 次の式を満たす最小の正整数 x を求めよ.

(1) $5^{1001} \equiv x \pmod 3$

(2) $7^{122} \equiv x \pmod 5$

(3) $3^{2001} \equiv x \pmod 7$

(4) $7^{14} \times 8^{25} \equiv x \pmod 5$

問題 2. 次の分数のうち約分できない分数はいくつありますか. また, それらの和はいくつですか.

(1) $\frac{1}{14}+\frac{2}{14}+\cdots+\frac{14}{14}$

(2) $\frac{1}{24}+\frac{2}{24}+\cdots+\frac{24}{24}$

(3) $\frac{1}{22}+\frac{2}{22}+\cdots+\frac{22}{22}$

(4) $\frac{1}{28}+\frac{2}{28}+\cdots+\frac{28}{28}$

問題 3. 次の剰余類, 既約剰余類の演算の結果の表を求めよ.

(1) $\boldsymbol{Z}_5 = \{0, 1, 2, 3, 4\}$

(2) $\boldsymbol{Z}_5^* = \{1, 2, 3, 4\}$

(3) $\boldsymbol{Z}_8^* = \{1, 3, 5, 7\}$

(4) $\boldsymbol{Z}_{12}^* = \{1, 5, 7, 11\}$

問題 4. 素数 p, q および公開鍵 e が次の値のとき, 秘密鍵 d の値を求めよ.

(1) $p = 19$, $q = 23$, $e = 13$

(2) $p = 19$, $q = 23$, $e = 17$

(3) $p = 23$, $q = 29$, $e = 3$

(4) $p = 23$, $q = 29$, $e = 5$

問題 5. $N=187$($p=11$, $q=17$)のとき次の問に答えよ.

(1)公開鍵 $e=7$ のとき平文 $a=10$ を暗号化せよ.

(2)公開鍵 $e=9$ のとき平文 $a=10$ を暗号化せよ.

(3)公開鍵 $e=23$ のとき秘密鍵 d を求め, 暗号文 $b=20$ を複合化せよ.