

情報基礎数学 I テスト問題

2010.07.26. 実施 (吉原)

(注) 答えだけでなく、ポイントとなる途中経過も書くこと。

1 一次不定方程式 $119x + 105y = 28$ について：

- (1) 一組の特殊解をユークリッドの互除法を用いて求めよ。
- (2) 次に一般解も求めよ。

2 オイラー関数 $\varphi(n)$ について以下の問いに答えよ。

- (1) $\varphi(n) = 4$ の解を求めよ。
- (2) p を素数とすると $\varphi(n) = p$ に解があればすべて求めよ。

3 次の連立一次合同式を解け。

$$\begin{cases} x \equiv 4 \pmod{9} \\ x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{11} \end{cases}$$

4 暗号化鍵 $(n, e) = (91, 5)$ をもつ暗号文 $y = 9$ を解読せよ。すなわち、暗号化鍵 $(91, 5)$ から復号化鍵 d を求め、暗号文 y を復号化し、もとの文 x を求めよ。