

応用数理情報概論 II 期末試験
2015 年 8 月 3 日

注意

- 答案用紙に 3 枚とも学修番号・氏名を書くこと.
- 答案用紙の裏面を用いてもよい.

問題

1. 次の整数 a, b, n に対して, 線形合同式 $ax \equiv b \pmod{n}$ を満たす整数 x で $0 \leq x < n$ の範囲にあるものをすべて求めよ.
(a) $a = 28, b = 11, n = 61$.
(b) $a = 105, b = 18, n = 171$.
2. 合同式 $x \equiv 6 \pmod{23}, x \equiv 25 \pmod{28}$ を満たす整数 x で $0 \leq x < 644$ の範囲にあるものをすべて求めよ.
3. 7^{1444} を 360 で割った剰余を求めよ.
4. $2465 = 5 \cdot 17 \cdot 29$ がカーマイケル数であることを示せ.
5. $\varphi(n)$ をオイラーの関数とする. $\varphi(n) = 3$ を満たす正の整数 n は存在しないことを示せ.
6. 公開鍵が $n = 91, e = 29$ である RSA 暗号によって平文 m が暗号文 71 に暗号化されたとする. このとき, 平文 m を求めよ.