

応用数理情報概論 II レポート課題 No. 2

2015 年 7 月 13 日配布

提出日：2015 年 7 月 27 日

注意

- 1 枚目に学修番号・氏名を書くこと.
- レポートが複数枚にわたるときは, 左上をホッチキス等で綴じること.
- A4 レポート用紙を使用すること.

問題

1. 合同式 $x \equiv 2 \pmod{7}$, $x \equiv 15 \pmod{27}$ を満たす整数 x で $0 \leq x < 189$ の範囲にあるものを求めよ.
2. 以下の問いに答えよ.
 - (a) $7x \equiv 1 \pmod{13}$ を満たす整数 x で $0 \leq x < 13$ の範囲にあるものを求めよ.
 - (b) 7^{2015} を 13 で割った剰余を求めよ.
3. $91 = 7 \cdot 13$ は 3 を底とする擬素数であることを示せ.
4. $41041 = 7 \cdot 11 \cdot 13 \cdot 41$ がカーマイケル数であることを示せ.
5. n を非負整数とする. q がフェルマー数 $F(n) = 2^{2^n} + 1$ の素因数ならば, $q = 1 + 2^{n+1}r$ となる正の整数 r が存在することを示せ.
6. 公開鍵が $n = 55$, $e = 27$ である RSA 暗号によって平文 m が暗号文 19 に暗号化されたとする. このとき, 平文 m を求めよ.