

アルゴリズム B 演習 レポート課題 No. 2

2016 年 1 月 8 日配布

提出日：2016 年 1 月 22 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. 数列 $\{F_n\}$ を

$$F_1 = F_2 = 1, \quad F_{n+2} = F_{n+1} + F_n \quad (n \geq 1)$$

で定義する. この漸化式によって F_n を計算するときのビット演算量は $O(n^2)$ であることを示せ. ただし, 四則演算のビット演算量として演習問題 No. 8 で与えたものを使うものとする.

2. 以下の問いに答えよ.

(a) 方程式 $446X + 187Y = 1$ を満たす整数 X, Y を一組求めよ.

(b) 合同式 $x \equiv 179 \pmod{446}$, $x \equiv 50 \pmod{187}$ を満たす整数 x で $0 \leq x < 446 \cdot 187$ の範囲にあるものを求めよ.

3. 以下の問いに答えよ. ただし, 6841 が素数であることは証明せずに用いてもよい.

(a) ルジャンドル記号 $\left(\frac{3757}{6841}\right)$ の値を求めよ.

(b) $3757^{3420} \pmod{6841}$ を求めよ.

4. 以下の問いに答えよ.

(a) $2^{1000} \pmod{1001}$ を計算することで 1001 が合成数であることを示せ.

(b) ミラー・ラビンの判定法を用いて 341 が合成数であることを示せ.