アルゴリズム B 演習 第 15 回　　2024 年 1 月 29 日

15　離散対数問題

問題

15-1. 素朴な方法によって $3 \equiv 2^n \pmod{19}$ となる n を求めよ．

15-2. ρ 法によって $17 \equiv 2^n \pmod{59}$ となる n を求めよ．ただし，$S = \{1, 2, \ldots, 19\}$, $T = \{20, 21, \ldots, 38\}$, $U = \{39, 40, \ldots, 58\}$ として，初期値 $(1, 0, 0)$，写像

$$f(g, x, y) = \begin{cases} (17g, x+1, y) & (g \in S) \\ (g^2, 2x, 2y) & (g \in T) \\ (2g, x, y+1) & (g \in U) \end{cases}$$

を用いるものとする．

15-3. BSGS 法によって $31 \equiv 3^n \pmod{43}$ となる n を求めよ．

15-4. ポーリッヒ・ヘルマンのアルゴリズムによって $82 = 2^n \pmod{101}$ となる n を求めよ．