アルゴリズム B 演習 第 13 回

2024 年 1 月 15 日

13　素数判定

問題

解答に際して，その問題より前にある問題の結果を用いてもよい．

13-1. $2^{132} \bmod 133$ を計算することで 133 が合成数であることを示せ．

13-2. 55 が擬素数となる底 b で $0 < b < 55$ を満たすものをすべて求めよ．

13-3. n を合成数とする．n のすべての素因数 p が $p^2 \nmid n$ かつ $(p-1) \mid (n-1)$ を満たすならば，n はカーマイケル数であることを示せ．

13-4. $561 = 3 \cdot 11 \cdot 17$ がカーマイケル数であることを示せ．

13-5. $n = 91$ として，$n - 1 = 2^s t$（t は奇数）と表す．$b = 3$ が条件

$$\begin{aligned} &b^t \equiv 1 \pmod{n} \quad \text{または} \\ &b^{2^r t} \equiv -1 \pmod{n} \text{ を満たす } r\ (0 \le r \le s-1) \text{ が存在する} \end{aligned} \tag{1}$$

を満たさないことを示し，n が合成数であることを示せ．

13-6. 55 が強擬素数となる底 b で $0 < b < 55$ を満たすものをすべて求めよ．

13-7. 非負整数 n に対して，$F_n = 2^{2^n} + 1$ をフェルマー数という．F_n が合成数ならば，F_n は 2 を底とする強擬素数であることを示せ．

13-8. n を 3 以上の奇数とする．ある整数 a に対して，

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$$

ならば，n は合成数である（オイラーの規準の対偶）．これを用いて，$n = 91$ が合成数であることを示せ．（この方法をソロヴェイ・シュトラッセンの素数判定法 (Solovay-Strassen primality test) という．）