アルゴリズム B 演習 第 11 回　　2023 年 12 月 18 日

11　二次合同式と平方剰余記号

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．$\varphi\colon \mathbb{N} \to \mathbb{N}$ をオイラーの φ 関数とする．

11-1. $\varphi(150)$ の値を求めよ．

11-2. $14^{2023} \bmod 33$ を計算せよ．

11-3. 任意の自然数 n に対して，

$$\sum_{d|n} \varphi(d) = n$$

が成り立つことを示せ．ただし，左辺は n のすべての正の約数 d に関する和を表す．

11-4. p を素数，a を p と互いに素な整数とする．a が p を法とする原始根であるための必要十分条件は，$p-1$ のすべての素因数 q に対して $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ が成り立つことであることを示せ．

11-5. 23 を法とする原始根を 1 つ求めよ．（すなわち，$(\mathbb{Z}/23\mathbb{Z})^\times$ の生成元を 1 つ求めよ．）

11-6. p が奇素数ならば，p^2 を法とする原始根が存在することを示せ．（すなわち，$(\mathbb{Z}/p^2\mathbb{Z})^\times$ が巡回群であることを示せ．）

11-7. 1 から 12 までの自然数のうち，法 13 に関する平方剰余であるものをすべて挙げよ．

11-8. p を奇素数とする．1 から $p-1$ までの自然数のうち，p を法とする平方剰余であるものは $\dfrac{p-1}{2}$ 個であることを示せ．