12. 整数の問題 (追加)

p が素数のとき $(\mathbb{Z}/p\mathbb{Z})^\times$ が巡回群になることの証明と, その応用に関する問題を少し追加します.

問題 12.1. $f(X), g(X)$ を整数係数の多項式とする ($f(X), g(X) \in \mathbb{Z}[X]$). 整数 n (> 1) について, $f(X) - g(X)$ の係数がすべて n で割り切れるとき, $f(X) \equiv g(X) \pmod{n}$ と書く.

(1) $f(X) \in \mathbb{Z}[X]$, $a \in \mathbb{Z}$ とする. もし $f(a) \equiv 0 \pmod{n}$ ならば, ある $g(X) \in \mathbb{Z}[X]$ が存在して $f(X) \equiv (X - a)g(X) \pmod{n}$ となることを示せ.

(2) p を素数, $f(X) \in \mathbb{Z}[X]$, f の次数を k とする. $k \geq 1$ のとき, $f(a) \equiv 0 \pmod{p}$ を満たす整数 a は 0 から $p - 1$ までの間に高々 k 個しかないことを示せ.

問題 12.2. n を 2 以上の整数とするとき, $1, \ldots, n - 1$ のうち n と互いに素な数の個数を $\varphi(n)$ と表し, これをオイラー関数という. また, $n = 1$ のときは $\varphi(1) = 1$ とする.

(1) $\mathrm{GCD}(m, n) = 1$ のとき, $\varphi(mn) = \varphi(m)\varphi(n)$ となることを示せ.

(2) p を素数, k を正整数とするとき, $\varphi(p^k) = p^{k-1}(p - 1)$ となることを示せ.

(3) d を n の (正の) 約数とするとき, $1, \ldots, n - 1$ のうち n との最大公約数が d となる数の個数は $\varphi(n/d)$ 個であることを示せ.

(4) n の (正の) 約数をすべて重複なく列挙して $d_1, \ldots, d_m$ と書くとき $\varphi(d_1) + \cdots + \varphi(d_m) = n$ となることを示せ.

(5) G を位数 n の巡回群とするとき, G の元のうち位数が n のものの個数は全部で $\varphi(n)$ 個であることを示せ.

問題 12.3. p を素数とする. $p - 1$ の (正の) 約数 d に対し, $(\mathbb{Z}/p\mathbb{Z})^\times$ の元のうち位数が d となるものの個数を $\psi(d)$ と書く.

(1) $p - 1$ の (正の) 約数を重複なく列挙して $d_1, \ldots, d_n$ と書くとき, $\psi(d_1) + \cdots + \psi(d_n) = p - 1$ となることを示せ. (ヒント: ラグランジュの定理.)

(2) $\psi(d) > 0$ となる d をとる. 定義より $(\mathbb{Z}/p\mathbb{Z})^\times$ の元のうち位数が d となるものが存在するのでそれを x とする. このとき $(\mathbb{Z}/p\mathbb{Z})^\times$ の位数 d の元はすべて x で生成される巡回群 $\langle x \rangle$ に含まれていることを示せ. (問題 12.1 (2) を使う.)

(3) 上記の (1)(2) と問題 12.2 (4)(5) を用いて, $p - 1$ のすべての (正の) 約数 d について $\psi(d) = \varphi(d)$ となることを示せ.

[注意] この問題を (3) までやると, とくに $\psi(p - 1) > 0$ となることがいえるので, $(\mathbb{Z}/p\mathbb{Z})^\times$ が巡回群であることが証明できたことになる.

問題 12.4. p を素数とする. 次を示せ.

(1) 任意の $a \in \mathbb{Z}$ に対し, もし $\mathrm{GCD}(a,p)=1$ なら $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

(2) $(p-1)! \equiv -1 \pmod{p}$.

(3) $p>3$ ならば $\quad 1^2+2^2+\cdots+(p-1)^2 \equiv 0 \pmod{p}$.

問題 12.5. (1) $x^{10} \equiv 10 \pmod{1998}$ となる正整数 x のうち最小のものを求めよ.

(2) $x^{2009} \equiv 2010 \pmod{21}$ となる正整数 x のうち最小のものを求めよ.

(3) $x^{2009} \equiv 2010 \pmod{22}$ となる正整数 x のうち最小のものを求めよ.

(1) は 1998 年 (平成 10 年) に雑誌「数学セミナー」に載っていた問題です. その今年度版を作ってみましたが, (1) ほど面白くはありません.