「代 数 学 1」の text の略解等

練習 9.6. x, y, z は整数とする. $x^2+y^2=z^2$ ならば, $xyz \equiv 0 \bmod 60$ であることを示せ.

略解 $60=4\times3\times5$ で 4, 3, 5 はどの 2 つも互ひに素であるから

$$xyz \equiv 0 \bmod 4, \quad xyz \equiv 0 \bmod 3, \quad xyz \equiv 0 \bmod 5$$

を示せばよい. 最初の等式が最も厄介である. $\bmod 4$ で調べても埒があかないので, $\bmod 8$ で調べる. まづ, 8 を法とする剰余類環の完全代表系を $\{-3,-2,-1,0,1,2,3,4\}$ ととる. それぞれの平方は法 8 で 1, 4, 1, 0, 1, 4, 1, 0 になる. つまり 0, 1, 4 のいづれかになる. ここで x^2, y^2, z^2 がすべて 1 だと $x^2+y^2-z^2$ は $\equiv 0 \bmod 8$ にならない. 詳しく調べれば, 1 が入るのは $(x^2,y^2,z^2) \equiv (1,0,1)$ または $(1,0,1) \bmod 8$ の場合に限る. その他の場合も含めて, いづれにしても $4|xyz$ がいへる.
残りの 2 つの合同式は容易に示せる. □

練習 9.9. m, $n \in \mathbb{Z}$ とし, $d=\gcd(m,n)$ とせよ. x の連立合同式

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$$

が解を持つためには, $a \equiv b \bmod d$ であることが必要十分であることを示せ. また, m と n の最小公倍数を ℓ とすれば, 解を持つ場合, 解は $\bmod \ell$ でみれば唯 1 つである事を示せ.

証明 (必要性) 解 x があれば, $x \equiv a \bmod m$ より $x \equiv a \bmod d$ が得られ, $x \equiv b \bmod n$ より $x \equiv b \bmod n$ が得られるから $a \equiv b \bmod d$ である.
(十分性) $m=m'd$, $n=n'd$ とおく. $1=m's+n't$ なる s, $t \in \mathbb{Z}$ が存在する. これを使つて

$$x = an't + bm's$$

とおくと, これは 1 つの解である. 実際, $d|(b-a)$ だから

$$an't+bm's = a(1-m's)+bm's = a+(b-a)m's \equiv a \bmod m,$$
$$an't+bm's = an't+b(1-n't) = (a-b)n't+b \equiv b \bmod n.$$

また任意の 2 つの解を x_1, x_2 とすれば, $x_2-x_1 \equiv 0 \bmod m$, $x_2-x_1 \equiv 0 \bmod n$ である. これは $\operatorname{lcm}(m,n) \,\big|\, (x_2-x_1)$ を意味する[1)]. □

[1)] lcm =least common multiple, 最小公倍数.

練習 13.11. (Wilson の定理) p が素数のとき

$$(p-1)! \equiv -1 \bmod p$$

であることを証明せよ.

略解 【解 1】 多項式 $f(x) = x^{p-1} - 1$ を考へる. Fermat の小定理より $(\mathbb{Z}/p\mathbb{Z})^\times$ の元はすべて $f(x) = 0$ の解であるが, これは $p-1$ 次式なので, それらが丁度, 解の全体である. よつて

$$f(x) = (x - \overline{1})(x - \overline{2}) \cdots (x - \overline{p-1})$$

と因数分解される. 解と係数の関係より

$$-1 \equiv (-1)^{p-1}(p-1)! \bmod p.$$

$p-1$ は偶数なので,

$$-1 \equiv (p-1)! \bmod p.$$

【解 2】 法 p の原始根を g とせよ. $\overline{1}$, $\overline{2}$, $\cdots$, $\overline{p-1}$ は順序を度外視すれば, $\overline{1}$, g, $\cdots$, g^{p-1} であるから

$$(p-1)! \equiv g^{1+2+\cdots+(p-1)} \equiv g^{\frac{1}{2}(p-1)(p-2)} \equiv (-1)^{p-2} = -1.$$

ここで $p-2$ が奇数であることを使つた.

【解 3】 $(\mathbb{Z}/p\mathbb{Z})^\times$ の 1 と -1 以外は各元 a は a^{-1} と異る. これらの組を作つていくと, 排反な $\frac{1}{2}(p-3)$ 組ができる. よつて $(\mathbb{Z}/p\mathbb{Z})^\times$ のすべての元の積は $\bmod p$ で $1 \times (-1) \times 1^{\frac{1}{2}(p-1)} = -1$ になることがわかり, 所望の式を得る. □

練習 13.12. p は奇素数であつて, $a^{2^n} + 1$ の約数であるとせよ. このとき

$$p \equiv 1 \bmod 2^{n+1}$$

であることを示せ. (Hint : $(a \bmod p)$ の $(\mathbb{Z}/p\mathbb{Z})^\times$ における位数を求めよ.)

略解 仮定より

$$a^{2^n} \equiv -1 \bmod p.$$

このことから $\operatorname{ord} \overline{a} = 2^{n+1}$ であることがわかる. 実際, 上の式を平方すれば

$$a^{2^{n+1}} \equiv 1 \bmod p$$

であるから, $\operatorname{ord} \overline{a}$ は 2^{n+1} の約数であるが,

(一般に 群 G の元 a について $a^n = 1$ ならば $m = \operatorname{ord} a$ は n の約数である. なぜなら $n = mq + r$ $(0 \leqq r < m)$ とするとき $a^r = a^{n-mq} = a^n (a^m)^q = 1$ ゆゑ $r = 0$ でなくてはならない.)

2^{n+1} の真の約数 m について

$$a^{2^m} \equiv 1 \bmod p$$

であれば,

$$a^{2^{n+1}} \equiv 1 \bmod p$$

となり矛盾である. さて, 他方で Fermat の小定理から

$$a^{p-1} \equiv 1 \bmod p$$

であるので, $\operatorname{ord} \overline{a}$ は $p-1$ の約数である. つまり

$$p - 1 \equiv 0 \bmod 2^{n+1}.$$

よつて

$$p \equiv 1 \bmod 2^{n+1}$$

である.

□