初等整数論 (8回目)

8. 原始根の応用

前回は原始根定理について解説した. 今回は原始根を応用して, 「ウィルソンの定理」や「第一補充法則」を証明する.

補題 8-1

奇素数 p と整数 a $(\gcd(a,p)=1)$ を考える.

(1) $a^2 \equiv 1 \pmod{p}$ のとき, $a \equiv \pm 1 \pmod{p}$.

(2) a が法 p の原始根のとき, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

(3) a が法 p の原始根のとき, $\{R_p(1),\ R_p(a^1),\ R_p(a^2), ...,\ R_p(a^{p-2})\} = \{1,\ 2,\ ..., p-1\}$ である. ただし, $R_p(n)$ は整数 n を p で割った余りを表す.

[証明]

(1) $(a-1)(a+1) \equiv 0 \pmod{p}$ より, $p \mid a-1$ または $p \mid a+1$. よって $a \equiv \pm 1 \pmod{p}$.

(2) フェルマーの小定理より

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \pmod{p}.$$

(1) から $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ となる. a は原始根であるから $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

(3) 次が成り立つことに注意する.

$$\{R_p(1),\ R_p(a^1),\ R_p(a^2), ...,\ R_p(a^{p-2})\} \subseteq \{1,\ 2,\ ..., p-1\}.$$

従って $R_p(1),\ R_p(a^1),\ R_p(a^2), ...,\ R_p(a^{p-2})$ が相異なることを示せばよい.

$R_p(a^j) = R_p(a^i)$ $(0 \leq i \leq j \leq p-2)$ とする. $a^j \equiv a^i \pmod{p}$ より $a^{j-i} \equiv 1 \pmod{p}$. a は原始根なので $p-1 \mid j-i$ である. $0 \leq j-i \leq p-2$ より $j = i$ が従う. 以上より $R_p(1),\ R_p(a^1),\ R_p(a^2), ...,\ R_p(a^{p-2})$ は相異なる.

□

定理 8-1 (ウィルソンの定理)

素数 p に対して

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

[**証明**]

$p=2$ のときは明らかなので, p が奇素数の場合を考える. 補題 8-1 (3) より

$$(p-1)! \equiv \prod_{i=0}^{p-2} R_p(a^i) \equiv \prod_{i=0}^{p-2} a^i \equiv \left(a^{\frac{p-1}{2}}\right)^{p-2} \pmod{p}.$$

補題 8-1 (2) より

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

であり, $p-2$ は奇数だから

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

□

問題 8-1　奇素数 p に対して

$$I = \left(\frac{p-1}{2}\right)!$$

と置く. このとき, I^2 を p で割った余りを求めよ.

問題 8-2　奇素数 p と自然数 n に対して

$$I = 1^n + 2^n + \cdots + (p-1)^n$$

と置く. このとき, I を p で割った余りを求めよ.

定理 8-2 (第一補充法則)

奇素数 p に対して,

$$x^2 \equiv -1 \pmod{p} \text{ が解を持つ} \iff p \equiv 1 \pmod{4}.$$

[**証明**]

$\Rightarrow$ について. $t^2 \equiv -1 \pmod{p}$ を満たす整数 t をとる. フェルマーの小定理より

$$(-1)^{\frac{p-1}{2}} \equiv t^{p-1} \equiv 1 \pmod{p}.$$

従って $\frac{p-1}{2}$ は偶数. よって $p \equiv 1 \pmod{4}$.

$\Leftarrow$ について. a を法 p の原始根とする. 補題 8-1(2) より

$$\left(a^{\frac{p-1}{4}}\right)^2 = a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

従って $x^2 \equiv -1 \pmod{p}$ が解を持つ.

□

定理 8-3

奇素数 p に対して次は同値である.

(1) $x^2 + y^2 = p$ を満たす整数 x, y が存在する.

(2) $p \equiv 1 \pmod 4$.

[証明]

(1) $\Rightarrow$ (2). p は奇数より, x, y のどちらかが奇数, もう一方は偶数である. よって

$$x = 2s, \ \ y = 2t + 1 \ \ (s, t \in \mathbb{Z})$$

としてよい. このとき,

$$p = x^2 + y^2 = 4(s^2 + t^2 + t) + 1 \equiv 1 \pmod 4.$$

(2) $\Rightarrow$ (1). 第一補充法則から $a^2 + 1 = pb$ を満たす自然数 a, b が取れる. 集合

$$S = \{(x, y) \in \mathbb{Z}^2 \ \mid \ 0 \leq x, y < [\sqrt{p}\,]\}$$

を考える. ここで, $[x]$ は x を超えない最大の整数を表す. このとき,

$$|S| = ([\sqrt{p}\,] + 1)^2 > p.$$

よって

$$x_1 - ay_1 \equiv x_2 - ay_2 \pmod p$$

を満たす相異なる元 (x_1, y_1), $(x_2, y_2) \in S$ が存在する. $x_3 = x_1 - x_2$, $y_3 = y_1 - y_2$ と置くと

$$0 < x_3^2 + y_3^2 < 2p. \qquad (\diamondsuit)$$

$x_3 \equiv ay_3 \pmod p$ より

$$x_3^2 + y_3^2 \equiv (a^2 + 1)y_3^2 \equiv 0 \pmod p. \qquad (\clubsuit)$$

式 $(\diamondsuit)$, $(\clubsuit)$ より $x_3^2 + y_3^2 = p$.

□

問題 8-3

(1) 次の等式を示せ.

$$(x^2 + y^2)(s^2 + t^2) = (xs - yt)^2 + (xt + ys)^2.$$

(2) $x^2 + y^2 = 65$ を満たす整数の組 (x, y) を一つ求めよ.

(3) $x^2 + y^2 = 110$ を満たす整数の組 (x, y) は存在しないことを示せ.