7 フェルマーの (小) 定理／mod p の原始根

p を素数とする. 前回の問題 6.2 を解くときに使ったと思うが, 任意の $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対し,

$$\bar{a} \cdot \bar{1}, \ldots, \bar{a} \cdot (\overline{p-1})$$

はどの二つも互いに異なる (ある $x, y \in \{1, \ldots, p-1\}$ について $\bar{a} \cdot \bar{x} = \bar{a} \cdot \bar{y}$ であったとすると, $\bar{a} \cdot (\overline{x-y}) = \bar{0}$ であるが, $\bar{a} \neq \bar{0}$ だから $\overline{x-y} = \bar{0}$, よって $\bar{x} = \bar{y}$). 従って上記の $p-1$ 個の元は $\bar{1}, \ldots, \overline{p-1}$ を並べ替えたものにすぎないので, すべてかけ合わせれば,

$$\bar{a}^{p-1} \cdot \bar{1} \cdots (\overline{p-1}) = \bar{1} \cdots (\overline{p-1}).$$

この両辺に $\bar{1} \cdots (\overline{p-1})$ の逆元をかければ, $\bar{a}^{p-1} = \bar{1}$ を得る. すなわち, 次の定理が得られた:

定理 7.1 p を素数とし, a を $a \not\equiv 0 \pmod{p}$ を満たす整数とすると,

$$a^{p-1} \equiv 1 \pmod{p}.$$

これは**フェルマーの (小) 定理**と呼ばれ, RSA 暗号などに応用されている重要な定理である. なお, これは後で学ぶラグランジュの定理の系としてもっと簡明に理解することもできるので覚えておこう.

さて, フェルマーの定理と問題 4.4 により, $(\mathbb{Z}/p\mathbb{Z})^\times$ の元の位数は $p-1$ の約数であることが分かる. さらに, 位数がちょうど $p-1$ の元が存在するなら, $(\mathbb{Z}/p\mathbb{Z})^\times$ はその元で生成される巡回群であるということになる.

定義 7.2 p を素数とする. 整数 a について, $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ の位数がちょうど $p-1$ のとき, a は mod p の**原始根**であるという. 言い換えれば, a が mod p の原始根であるとは $(\mathbb{Z}/p\mathbb{Z})^\times = \langle \bar{a} \rangle$ となることをいう.

以下, すべての素数について原始根が存在することを証明したい. まず, 次の補題を示す.

補題 7.3 p を素数, $f(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n$ $(c_0, \ldots, c_n \in \mathbb{Z})$ を整数係数の多項式とする. $n \geq 1$, $c_0 \not\equiv 0 \pmod{p}$ とするとき, $f(x) \equiv 0 \pmod{p}$ の解は $\{1, \ldots, p\}$ の中には高々 n 個しかない.

[1] ホームページ http://www.math.tsukuba.ac.jp/~amano/lec2012-2/e-algebra-ex/index.html

[証明] n に関する帰納法で証明する. まず $n=1$ のとき, $f(x)=c_0x+c_1$ だから,

$$f(x)\equiv 0 \pmod p \quad\Leftrightarrow\quad c_0x\equiv -c_1 \pmod p$$

となるが, $c_0 \not\equiv 0 \pmod p$ とこのプリントの最初に述べたことから, これの解は $\{1,\dots,p\}$ の中にはただ 1 つしか存在しない.

次に $n>1$ とし, $n-1$ 以下では成立と仮定する. $f(x)\equiv 0 \pmod p$ の解が $\{1,\dots,p\}$ の中に存在しないなら 0 個ということで OK. 解が存在する場合, $a\in\{1,\dots,p\}$ を一つの解とする. 多項式に関する剰余の定理により, $f(x)$ を $x-a$ で割った余りは $f(a)$ だから, ある $n-1$ 次の整数係数多項式 $f_1(x)$ が存在して

$$f(x)=(x-a)f_1(x)+f(a)$$

と書ける. $f(a)\equiv 0 \pmod p$ だから,

$$\begin{aligned} f(x)\equiv 0 \pmod p \quad&\Leftrightarrow\quad (x-a)f_1(x)\equiv 0 \pmod p \\ &\Leftrightarrow\quad x\equiv a \pmod p \ \text{ または } \ f_1(x)\equiv 0 \pmod p. \end{aligned}$$

ここで, $f_1(x)$ の最高次係数は c_0 だから, 帰納法の仮定により $f_1(x)\equiv 0 \pmod p$ の解は $\{1,\dots,p\}$ の中には高々 $n-1$ 個しかない. よって, $f(x)\equiv 0 \pmod p$ の解は $\{1,\dots,p\}$ の中に高々 n 個しか存在しない. □

定理 7.4 p を素数とするとき, $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である.

[証明] $(\mathbb{Z}/p\mathbb{Z})^\times$ の元のうち位数最大のものを a とおき, a の位数を n $(\le p-1)$ とする. ここでもし $n=p-1$ ならば $(\mathbb{Z}/p\mathbb{Z})^\times=\langle a\rangle$ となるから証明が終わる. そこで以下, $n<p-1$ として矛盾を導く. $A_n=\{x\in(\mathbb{Z}/p\mathbb{Z})^\times \mid x^n=\bar{1}\}$ とすると, 補題により A_n の元の個数は n を超えないので, ある $b\in(\mathbb{Z}/p\mathbb{Z})^\times\setminus A_n$ が存在する. b の位数を m とすると, m は n の約数ではない (もし m が n の約数だったとすると $b^n=\bar{1}$ となり, $b\notin A_n$ に反する). よって m と n の最小公倍数を l とすると, $n<l$. しかし $(\mathbb{Z}/p\mathbb{Z})^\times$ には位数 l の元が存在するはず (今回の演習問題とします) なので, これは a が位数最大の元であることと矛盾する. □

問題 7.5 G をアーベル群, $a,b\in G$ とする. a,b は位数有限とし, a の位数を n, b の位数を m とおく.

(1) n と m が互いに素なら ab の位数は nm となることを示せ.

(2) n と m の最小公倍数を l とすると, G には位数 l の元が存在することを示せ.

問題 7.6 次の (1)〜(5) で与えられる素数 p について, mod p の原始根を 1 つ以上求めよ.

(1) $p=7$ (2) $p=11$ (3) $p=23$ (4) $p=31$ (5) $p=41$

[コメント] 「1 つ以上」としていますが, 1 つでも見つければ $1,\dots,p-1$ の中から原始根となるものを全部見つけることは容易です.