第10章　原始根

10.1　多項式に関する注意

多項式 $f(x)$ を一次式 $x-a$ で割ったときの余りは $f(a)$ であり，

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

をみたす $n-1$ 次多項式 $g(x)$ が存在する．とくに，$f(x)$ が $x-a$ で割り切れるための必要十分条件は $f(a)=0$ である．これらは，多項式に関する「剰余定理・因数定理」とよばれるものであるが，ここではさらに，$f(x)$ が整数係数で a が整数のとき，$g(x)$ として整数係数の多項式がとれることに注意する．

整数 m と整数係数の二つの多項式 $f_1(x), f_2(x)$ について，それぞれ同じ次数の係数が法 m に関して合同のとき，

$$f_1(x) \equiv f_2(x) \pmod{m}$$

と書くことにする．これは，$f_1(x) - f_2(x)$ を整理して得られる多項式の係数がすべて m の倍数であることを意味する．次の命題は，上記「剰余定理・因数定理」の合同式バージョンともいえるものであり，証明は簡単なので演習としておこう．なお，最高次係数が 1 の多項式を**モニック**な多項式よぶことにする．

命題 10.1 m を 2 以上の自然数，$f(x)$ をモニックな整数係数 n 次多項式，a を整数とする．もし，$f(a) \equiv 0 \pmod{m}$ が成り立つならば，

$$f(x) \equiv (x-a)g(x) \pmod{m}$$

をみたすモニックな整数係数 $n-1$ 次多項式 $g(x)$ が存在する．

とくに，素数を法とする場合にこの命題を適用することで，次の定理を得る．

定理 10.2 p を素数とする．モニックな整数係数 n 次多項式 $f(x)$ に対して，合同式

$$f(x) \equiv 0 \pmod{p}$$

の整数解は p を法として n 個以下である．

証明　もし整数解がひとつもなければ証明すべきことは何もないから，整数解があるとしてそれを a とする．以下，n に関する数学的帰納法を用いる．$n=1$ のときは，p を法として a のみが解であることはすぐにわかる．$n>1$ のときは，前命題より，モニックな整数係数 $n-1$ 次多項式 $g(x)$ がとれて

$$f(x) \equiv (x-a)g(x) \pmod{p}$$

と書ける．いま，整数 b も解だとすると

$$(b-a)g(b) \equiv f(b) \equiv 0 \pmod{p}$$

であるが，p は素数だから，$b \equiv a$ または $g(b) \equiv 0 \pmod{p}$．すなわち，p を法として a と合同でない整数解は $g(x) \equiv 0 \pmod{p}$ の解でなければならない．一方，この合同式は，帰納法の仮定より p を法として $n-1$ 個以下の整数解しか持たないから，n 次の場合に定理の主張が得られたことになる．□

定理は，「$\boldsymbol{Z}/p\boldsymbol{Z}$ の元を係数とするモニックな n 次方程式 $F(x)=\overline{0}$ の $\boldsymbol{Z}/p\boldsymbol{Z}$ における解の個数は n 以下である」と言い換えることができる．

10.2　原始根

整数 a の法 $m>1$ に関する位数が s ならば，$1,\ a,\ a^2,\ \cdots,\ a^{s-1}$ はどの 2 つも m を法として合同ではない．なぜなら，$a^i \equiv a^j \pmod{m}$ $(0 \le i < j \le s-1)$ と仮定すると，$a^{j-i} \equiv 1 \pmod{m}$ が得られ，位数 s の最小性より $s \le j-i$ となって矛盾するからである．したがってこれらの作る剰余類の集合 $\left\{\overline{1},\ \overline{a},\ \overline{a}^2,\ \cdots,\ \overline{a}^{s-1}\right\}$ は，$(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ において s 個の元からなる部分集合となる．

定義 10.3 自然数 $m>1$ に対して，法 m に関する位数が $\varphi(m)$ となる整数 g を法 m に関する**原始根**という．

位数は剰余類によって定まるから，必要ならば $\{1,2,\cdots,m-1\}$ から原始根を選ぶことができる．小さい m について調べてみると，法 $m=2,3,4,5$ に関してはそれぞれ $1,2,3,2$ が原始根としてとれ，とくに，法 $m=5$ に関しては，2 の他に 3 も原始根になっている．g が法 m に関する原始根ならば，上で述べたとおり，$\varphi(m)$ 個の剰余類 $\overline{1},\ \overline{g},\ \overline{g}^2,\ \cdots,\ \overline{g}^{\varphi(m)-1}$ は互いに相異なり，したがってこれらが $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ のすべての元となる;

$$(\boldsymbol{Z}/m\boldsymbol{Z})^\times = \left\{\, \overline{g}^j \,\middle|\, 0 \le j < \varphi(m) \,\right\} = \left\{\, \overline{g}^j \,\middle|\, j \in \boldsymbol{Z} \,\right\}.$$

逆にこのような整数 g は法 m に関する原始根である．次の補題は，前節最後に扱った $\lambda(m)$ の定義を見ればすぐに確認できる．

補題 10.4 m を 2 以上の自然数とするとき，法 m に関する原始根が存在するためには，$\lambda(m)=\varphi(m)$ が成り立つことが必要十分である．

たとえば，$\lambda(8) = 2 < 4 = \varphi(8)$ から，法 8 に関する原始根は存在しないことがわかる．このことも含め，原始根が存在しない法については次が成り立つ．

命題 10.5 $m = 2^n$ $(n \geq 3)$ または $m = kl$ (k, l は互いに素な 3 以上の奇数) のとき，法 m に関する原始根は存在しない．

証明は $\lambda(m) < \varphi(m)$ を確認すればよいが，詳細は（時間があれば）講義で述べることとし，ここでは次の定理の証明を与えよう．

定理 10.6 素数 p に対して，法 p に関する原始根が存在する．

証明 カーマイケルの定理（定理 9.11）より，すべての $\overline{a} \in (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ が $x^{\lambda(p)} - \overline{1} = \overline{0}$ の解となるから，前節の定理 10.2 より $\lambda(p) \geq \varphi(p)$ でなければならない．一方，$\lambda(p) \leq \varphi(p)$ であったから，$\lambda(p) = \varphi(p)$ が導かれ，補題 10.4 より原始根が存在する． □

小さな素数に対する最小自然数の原始根は次の表のようになる．

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
g	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2

表を眺めると，原始根に 2 が比較的多く現れることに気付く． そこで，「2 が原始根となる素数 p が無数に存在するのではないか」と期待される． これは**原始根に関するアルティン予想**とよばれる予想の一部であり，現在も完全には解決されていない． なお，原始根を求めるための簡単な方法は知られていないことを付け加えておく．

10.3 奇素数ベキを法とする原始根

この節では，奇素数（すなわち 2 でない素数）のベキを法とする場合を扱う． 目標となるのは次の定理である．

定理 10.7 任意の奇素数 p と自然数 n に対して，法 p^n に関する原始根が存在する．

定理の証明のために，補題を 2 つ用意する．

補題 10.8 p を素数，n を 2 以上の自然数，g を法 p^{n-1} に関する原始根とする． もし $g^{\varphi(p^{n-1})} \not\equiv 1 \pmod{p^n}$ ならば，g は法 p^n に関する原始根である．

証明 自然数 k が $g^k \equiv 1 \pmod{p^n}$ をみたすとして，$\varphi(p^n) | k$ を示せばよい． とくに，$g^k \equiv 1 \pmod{p^{n-1}}$ および，g が法 p^{n-1} に関する原始根であることより，ある自然数 l がとれて $k = l\varphi(p^{n-1})$ と書ける． 一方，$g^{\varphi(p^{n-1})} = 1 + t$ によって $t \in \boldsymbol{Z}$ を定めれば，仮定より $p^{n-1} | t$ かつ $p^n \nmid t$． とくに，$n \geq 2$ より $t^2 \equiv t^3 \equiv \cdots \equiv 0 \pmod{p^n}$ だから

$$g^k = (g^{\varphi(p^{n-1})})^l = (1+t)^l \equiv 1 + lt \pmod{p^n}.$$

一方，はじめに $g^k \equiv 1 \pmod{p^n}$ を仮定していたので，$p^n | lt$ であるが，$p^n \nmid t$ でもあったから $p|l$ が導かれる．そこで $l = mp$ $(m \in \boldsymbol{N})$ とおけば，

$$k = mp\varphi(p^{n-1}) = m\varphi(p^n),$$

よって k は $\varphi(p^n)$ の倍数である． □

補題 10.9 p を奇素数，g を法 p^2 に関する原始根とする．このとき，2 以上の任意の自然数 n に対して，$g^{\varphi(p^{n-1})} \not\equiv 1 \pmod{p^n}$ が成り立つ．

証明　n に関する数学的帰納法を用いる．まず，g が法 p^2 に関する原始根であることよりその位数が $\varphi(p^2)$ であり，$\varphi(p)$ がそれより小さいことから $g^{\varphi(p)} \not\equiv 1 \pmod{p^2}$，すなわち $n = 2$ のときは成り立つ．次に，$n \geq 2$ のとき正しいとすると，オイラーの定理を援用して

$$g^{\varphi(p^{n-1})} = 1 + kp^{n-1}, \quad k \not\equiv 0 \pmod{p}$$

と書けることがわかる．ここで $\varphi(p^n) = p\varphi(p^{n-1})$ だから，

$$g^{\varphi(p^n)} = (1 + kp^{n-1})^p = 1 + kp^n + \sum_{j=2}^{p-1} {}_pC_j (kp^{n-1})^j + (kp^{n-1})^p.$$

いま，$2(n-1) \geq n$ より，${}_pC_j (kp^{n-1})^j \equiv 0 \pmod{p^{n+1}}$ $(2 \leq j \leq p-1)$ であり，さらに，$p \geq 3$ より $p(n-1) \geq n+1$ がいえるから $(kp^{n-1})^p \equiv 0 \pmod{p^{n+1}}$ が成り立つ（うっへぇ，ギロン細かっ！）．これらの合同式に加えて，$p \nmid k$ に注意すれば

$$g^{\varphi(p^n)} \equiv 1 + kp^n \not\equiv 1 \pmod{p^{n+1}}$$

が得られ，$n+1$ のときも正しいことが導かれた． □

定理 10.7 の証明　$n = 1$ の場合は定理 10.6 で示されているので，法 p に関する原始根 g がとれる．もし $g^{\varphi(p)} = g^{p-1} \equiv 1 \pmod{p^2}$ ならば，

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \pmod{p^2}$$

であり，かつ $g+p$ も法 p に関する原始根なので，はじめから g は，$g^{\varphi(p)} \not\equiv 1 \pmod{p^2}$ をみたすものとしてよい．このとき，補題 10.8 によれば，g は法 p^2 に関する原始根でもある．そこで今度は補題 10.9 によって，任意の $n \geq 2$ に対して $g^{\varphi(p^{n-1})} \not\equiv 1 \pmod{p^n}$ が得られる．とくに $n = 3$ の場合を考えれば，再び補題 10.8 を用いて，g が法 p^3 に関しても原始根であることがわかる．さらに補題 10.8 を繰り返し適用すれば，定理の主張が示されることになる． □

上の証明をまとめると，奇素数 p について次のことがわかる．

- g が法 p に関する原始根ならば，g または $g+p$ は法 p^2 に関する原始根である．
- 法 p^2 に関する原始根は，任意の $n > 2$ について法 p^n に関する原始根でもある．