

## 第10章 原始根

### 10.1 多項式に関する注意

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, 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(「因数定理」を忘れちゃった人は高校の教科書見てね). なお, 最高次係数が 1 の多項式をモニックな多項式とよぶことにする.

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  $g(x) \equiv 0 \pmod{p}$  の解である. 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「 $p$  が素数ならば,  $\mathbb{Z}/p\mathbb{Z}$  の元を係数とするモニックな  $n$  次方程式  $F(x) = \bar{0}$  の  $\mathbb{Z}/p\mathbb{Z}$  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,  $1, a, a^2, \dots, a^{s-1}$  はどの2つも  $m$  を法として合同ではない. なぜなら,  $a^i \equiv a^j \pmod{m}$  ( $0 \leq i < j \leq s-1$ ) 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  $s \leq j-i$  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  $\{\bar{1}, \bar{a}, \bar{a}^2, \dots, \bar{a}^{s-1}\}$  は,  $(\mathbb{Z}/m\mathbb{Z})^\times$  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  $\varphi(m)$  である整数  $g$  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  $\{1, 2, \dots, m-1\}$  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  $\bar{1}, \bar{g}, \bar{g}^2, \dots, \bar{g}^{\varphi(m)-1}$  は互いに相異なり, したがってこれらが  $(\mathbb{Z}/m\mathbb{Z})^\times$  のすべての元となる;

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{g}^j \mid 0 \leq j < \varphi(m)\} = \{\bar{g}^j \mid j \in \mathbb{Z}\}.$$

逆にこのような整数  $g$  は法  $m$  に関する原始根である. だって,  $g$  の法  $m$  に関する位数  $s$  が  $\varphi(m)$  より小さかったら, この節の初めに書いたように, 右辺は  $s$  個の元しか持たないから,  $(\mathbb{Z}/m\mathbb{Z})^\times$  になれないもん.

**補題 10.4** 自然数  $m, n > 1$  が整除関係  $n|m$  をみたすとき, 法  $m$  に関する原始根が存在するならば, 法  $n$  に関する原始根が存在する.

**証明** まず, 写像  $(\mathbb{Z}/m\mathbb{Z})^\times \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times, a + m\mathbb{Z} \mapsto a + n\mathbb{Z}$  が全射であることに注意する. このことは, 補題 8.7 の証明を少し改良すれば確かめられる(ちょいむず演習問題). いま,  $g \in \mathbb{Z}$  を法  $m$  に関する原始根とすれば,  $(\mathbb{Z}/m\mathbb{Z})^\times = \{g^j + m\mathbb{Z} \mid j \in \mathbb{Z}\}$  が成り立つから, 上の写像により, 法  $n$  についても  $(\mathbb{Z}/n\mathbb{Z})^\times = \{g^j + n\mathbb{Z} \mid j \in \mathbb{Z}\}$  であり, このことから  $g$  が法  $n$  に関する原始根であることが導かれる.

次の補題は, 前章の最後に扱った  $\lambda(m)$  の定義を見ればすぐに確認できる.

**補題 10.5**  $m$  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,  $\lambda(8) = 2 < 4 = \varphi(8)$  により, 法  $8$  に関する原始根は存在しない. また,  $p$  を奇素数とすると, 命題 9.6 (オイラーの定理の精密化) で扱った  $\psi$  を用いて,

$$\lambda(4p) \leq \psi(4p) = \text{lcm}(\varphi(4), \varphi(p)) = \text{lcm}(2, p-1) = p-1 < 2(p-1) = \varphi(4p)$$

だから, 法  $4p$  に関する原始根も存在しない. 同様にして, 相異なる奇素数  $p, q$  に対して, 法  $pq$  に関する原始根も存在しないことがわかる. これらの事実と, 補題 10.4 から次が得られる.

命題 10.6 法  $m$  に関する原始根が存在するならば,  $m = 2, 4, p^n$  または  $2p^n$  (ただし  $p$  は奇素数,  $n \geq 1$ ) である.

実は, この命題の逆も成り立つのだが, ここではまず次の定理の証明を与えよう.

定理 10.7 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  $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$  が  $x^{\lambda(p)} - \bar{1} = \bar{0}$  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,  $\lambda(p) | \varphi(p)$  であったから,  $\lambda(p) = \varphi(p)$  が導かれ, 補題 10.5 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 奇素数べきを法とする原始根

この節では, 奇素数(すなわち 2 でない素数)のべき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 10.8 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 10.9  $p$  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  $t \in \mathbb{Z}$  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  $t^2 \equiv t^3 \equiv \dots \equiv 0 \pmod{p^n}$  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  $l = mp$  ( $m \in \mathbb{N}$ ) 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 10.10  $p$  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,

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

いま,  $2(n-1) \geq n$  より,  ${}_p C_j (kp^{n-1})^j \equiv 0 \pmod{p^{n+1}}$  ( $2 \leq j \leq p-1$ ) 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(うっへえ, ギロン細かつ!). 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 10.8 の証明  $n=1$  の場合は定理 10.7 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 10.9 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 10.10 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 10.9 を用いて,  $g$  が法  $p^3$  に関する原始根であることがわかる. さらに補題 10.9 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.

さて, 奇素数のべき  $p^n$  について,  $(\mathbb{Z}/p^n\mathbb{Z})^\times$  と  $(\mathbb{Z}/2p^n\mathbb{Z})^\times$  の間に自然な全単射が存在することに注意すれば, 命題 10.6 および定理 10.8 から次の定理が得られる.

定理 10.11  $m$  を 2 以上の自然数とする. 法  $m$  に関する原始根が存在するためには,  $m=2, 4, p^n$  または  $2p^n$  (ただし  $p$  は奇素数,  $n \geq 1$ ) であることが必要十分である.