多項式の合同式

整数のときと同様に多項式についても合同式を考えることができる。$f(x),\ g(x),\ m(x)$ を多項式とする。$f(x)-g(x)$ が $m(x)$ で割り切れるとき，$f(x)$ と $g(x)$ は $m(x)$ を法として合同であるといい $f(x)\equiv g(x)\pmod{m(x)}$ と書く。整数のときと同様に次の性質が成り立つ。

(1) $f(x)\equiv f(x)\pmod{m(x)}$

(2) $f(x)\equiv g(x)\pmod{m(x)} \Longrightarrow g(x)\equiv f(x)\pmod{m(x)}$

(3) $\begin{cases} f(x)\equiv g(x)\pmod{m(x)} \\ g(x)\equiv h(x)\pmod{m(x)} \end{cases} \Longrightarrow f(x)\equiv h(x)\pmod{m(x)}$

(4) $f(x)\equiv g(x)\pmod{m(x)} \Longrightarrow f(x)^n\equiv g(x)^n\pmod{m(x)}$ (n は自然数)

(5) $f(x)\equiv g(x)\pmod{m(x)} \Longrightarrow \begin{cases} h(x)f(x)\equiv h(x)g(x)\pmod{m(x)} \\ h(x)f(x)\equiv h(x)g(x)\pmod{h(x)m(x)} \end{cases}$

(6) $\begin{cases} f(x)\equiv g(x)\pmod{m(x)} \\ h(x)\equiv k(x)\pmod{m(x)} \end{cases} \Longrightarrow \begin{cases} f(x)+h(x)\equiv g(x)+k(x)\pmod{m(x)} \\ f(x)h(x)\equiv g(x)k(x)\pmod{m(x)} \end{cases}$

更に，$f(x)\equiv g(x)\pmod{m(x)}$ ということは $f(x)$ を $m(x)$ で割った余りと $g(x)$ を $m(x)$ で割った余りが等しいということを意味しているというのも整数の場合と同じである。従って $f(x)$ を $m(x)$ で割った余りを $r(x)$ とすると $f(x)\equiv r(x)\pmod{m(x)}$ となる。このことを利用して，標準的な方法で漸化式を満たす数列を作ることができる。

例　$m(x)=x^2-x-1$ とする。x^n を $m(x)$ で割った余りを p_nx+q_n とおくと，数列 $\{p_n\}$，$\{q_n\}$ は

漸化式：$x_{n+2}=x_{n+1}+x_n$ $\cdots$①

初期条件：$\begin{cases} p_0=0,\ p_1=1 \\ q_0=1,\ q_1=0 \end{cases}$ $\cdots$②

を満たす。

仮定より

$$x^{n+2} \equiv p_{n+2}x + q_{n+2} \pmod{m(x)}$$
$$x^{n+1} \equiv p_{n+1}x + q_{n+1} \pmod{m(x)}$$
$$x^{n} \equiv p_{n}x + q_{n} \pmod{m(x)}$$

である。よって

$$x^{n+2} - x^{n+1} - x^n \equiv (p_{n+2} - p_{n+1} - p_n)x + (q_{n+2} - q_{n+1} - q_n) \pmod{m(x)}$$

となる。ここで $x^{n+2} - x^{n+1} - x^n = x^n(x^2 - x - 1) = x^n m(x)$ であるから $x^{n+2} - x^{n+1} - x^n \equiv 0 \pmod{m(x)}$ となることに注意すると

$$(p_{n+2} - p_{n+1} - p_n)x + (q_{n+2} - q_{n+1} - q_n) \equiv 0 \pmod{m(x)}$$

である。これは $(p_{n+2} - p_{n+1} - p_n)x + (q_{n+2} - q_{n+1} - q_n)$ が $m(x)$ で割り切れるということを意味しているが，$(p_{n+2} - p_{n+1} - p_n)x + (q_{n+2} - q_{n+1} - q_n)$ は高々1 次式であり，一方 $m(x)$ は 2 次式であるから，$(p_{n+2} - p_{n+1} - p_n)x + (q_{n+2} - q_{n+1} - q_n)$ は恒等的に 0 でなければならない。よって

$$p_{n+2} - p_{n+1} - p_n = 0$$
$$q_{n+2} - q_{n+1} - q_n = 0$$

となる。従って確かに 数列 $\{p_n\}$，$\{q_n\}$ は 漸化式 ① を満たす。また，$n = 0$ のとき $x^n = 1$ であるから $m(x)$ で割った余りは $0 \cdot x + 1$ となり $p_0 = 0,\ q_0 = 1$ である。一方 $n = 1$ のとき $x^n = x$ であるから $m(x)$ で割った余りは $1 \cdot x + 0$ となり $p_1 = 1,\ q_1 = 0$ である。//

例 $x_{n+2} = x_{n+1} + x_n,\ x_0 = 0,\ x_1 = 1$ で定まる数列 $\{x_n\}$ の第 n 項を求めよ。

x^n を $x^2 - x - 1$ で割った余りを $p_n x + q_n$ とする。上の例より数列 $\{p_n\}$ は

漸化式：$p_{n+2} = p_{n+1} + p_n$

初期条件：$p_0 = 0,\ p_1 = 1$

を満たす。漸化式と初期条件が与えられれば数列はただひとつに決まるので，この $\{p_n\}$ が求めるべき数列である。

$$x^n = (x^2 - x - 1)g(x) + p_n x + q \quad \cdots ①$$

とする。$x^2-x-1=0$ の 2 解を $\alpha,\ \beta$ とし，① に代入すると

$$\alpha^n = p_n\alpha + q$$
$$\beta^n = p_n\beta + q$$

となる。よって $p_n = \dfrac{\alpha^n-\beta^n}{\alpha-\beta}$ となる。以上で答えは $x_n = \dfrac{\alpha^n-\beta^n}{\alpha-\beta}$ である。//

例
(1) x^n-nx-3 が $m(x)=x^2-x-1$ で割り切れるような n は 5 のみである。
(2) x^n-3x-n が $m(x)=x^2-x-1$ で割り切れるような n は存在しない。

x^n を $m(x)=x^2-x-1$ で割った余りを p_nx+q_n とする。

$$\begin{cases} p_{n+2}=p_{n+1}+p_n & \cdots ① \\ q_{n+2}=q_{n+1}+q_n & \cdots ② \end{cases}$$

$$\begin{cases} p_0=0,\ p_1=1 & \cdots ③ \\ q_0=1,\ q_1=0 & \cdots ④ \end{cases}$$

(1) $x^n \equiv p_nx+q_n \pmod{m(x)}$ であるから

$$x^n-nx-3 \equiv (p_n-n)x+(q_n-3) \pmod{m(x)}$$

である。よって x^n-nx-3 が $m(x)$ で割り切れるのは $(p_n-n)x+(q_n-3)\equiv 0 \pmod{m(x)}$ となるときである。ここで $(p_n-n)x+(q_n-3)$ は高々1 次式であり $m(x)$ は 2 次式であるから，恒等的に $(p_n-n)x+(q_n-3)=0$ でなければならない。よって

$$p_n = n \quad \cdots ⑤$$
$$q_n = 3 \quad \cdots ⑥$$

となるような n をすべて求めればよい。② と ④ より

n	0	1	2	3	4	5	6	$\cdots$
q_n	1	0	1	1	2	3	5	$\cdots$

である。$\{q_n\}$ は $n \geqq 3$ のとき単調増加であるから $n=5$ のときのみ $q_n=3$ となることがわかる。一方 ① と ③ より

n	0	1	2	3	4	5	6	$\cdots$
p_n	0	1	1	2	3	5	8	$\cdots$

となるので $n=5$ **のとき確かに** $p_n=n$ **も成り立つ。以上で** $n=5$ **である。**

(2) (1) **と同様に考えると**

$$p_n=3 \quad \cdots ⑤$$
$$q_n=n \quad \cdots ⑥$$

となるような n **をすべて求めればよいことがわかる。上の表より，** $p_n=3$ **となるのは** $n=4$ **のときであるが，** $q_4=2$ **であるから** $n=4$ **のとき** $q_n\neq n$ **である。よって 条件を満たす** n **は存在しない**//

［注］ $x^2-x-1=0$ **の** 2 **解を** $\alpha,\ \beta$ **とする。** $x^n-nx-3=(x^2-x-1)g(x)$ **へ，** $x=\alpha,\ \beta$ **を代入すると** $\alpha^n-n\alpha-3=0,\quad \beta^n-n\beta-3=0$ **である。つまり**

$$\alpha^n=n\alpha+3 \quad \cdots ①$$
$$\beta^n=n\beta+3 \quad \cdots ②$$

となる。①× ②**より** $\alpha^n\beta^n=(n\alpha+3)(n\beta+3)$ **つまり**

$$(\alpha\beta)^n=n^2\alpha\beta+3n(\alpha+\beta)+9$$

である。ここへ，解と係数の関係 $\alpha+\beta=1,\ \alpha\beta=-1$ **を代入して考えることで** n **を求めることもできる。**