mod$p$ での多項式

整数係数の多項式 $f(x)$ を mod$p$ で考えることにする。以下では p は素数とする。整数係数の多項式

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$
$$g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n$$

に対して，

$$a_0 \equiv b_0,\ a_1 \equiv b_1,\ \cdots,\ a_n \equiv b_n \pmod{p}$$

となるとき，$f(x)$ と $g(x)$ は mod$p$ で合同であるといい，$f(x) \equiv g(x) \pmod{p}$ と書く。とくに，$f(x) \equiv 0 \pmod{p}$ とは，$f(x)$ の係数がすべて p で割り切れることを意味する。そうすると，

$f_1(x) \equiv f_2(x),\ g_1(x) \equiv g_2(x) \pmod{p}$ のとき
$f_1(x) \pm g_1(x) \equiv f_2(x) \pm g_2(x),\ f_1(x)g_1(x) \equiv f_2(x)g_2(x) \pmod{p}$ である。

$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ において，$a_0 \not\equiv 0 \pmod{p}$ のとき，$f(x)$ の mod$p$ に関する次数は n であるという。

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$
$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m$$

をそれぞれ n 次，m 次とすると，

$$f(x)g(x) = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + \cdots + a_nb_m$$

であるが，p が素数なので $a_0 \not\equiv 0,\ b_0 \not\equiv 0 \pmod{p}$ より $a_0b_0 \not\equiv 0 \pmod{p}$ となり $f(x)g(x)$ の mod$p$ に関する次数は $n+m$ となる。これより次が示される。

［命題 1］

$f(x)g(x) \equiv 0 \pmod{p}$ ならば $f(x) \equiv 0 \pmod{p}$ または $g(x) \equiv 0 \pmod{p}$ である。

［証明］ $f(x) \not\equiv 0 \pmod{p}$ かつ $g(x) \not\equiv 0 \pmod{p}$ とすると，$f(x),\ g(x)$ の最高次の係数は mod$p$ で 0 でないから，$f(x)g(x)$ の最高次の係数も mod$p$ で 0 でない。これは $f(x)g(x) \equiv 0 \pmod{p}$ に反する。■

［注］上の命題より，$f(x)g(x) \equiv f(x)h(x) \pmod{p}$ かつ $f(x) \not\equiv 0 \pmod{p}$ のとき，$g(x) \equiv h(x) \pmod{p}$ となることが分かる。

［定理（mod$p$ での割り算の基本定理）］

$f(x),\ g(x)$ は整数係数多項式で，$g(x)$ の mod$p$ に関する次数を n とすると

$$f(x) \equiv g(x)h(x) + r(x) \pmod{p}$$

で，$r(x)$ の mod$p$ に関する次数が $n-1$ 以下であるような整数係数多項式 $h(x),\ r(x)$ の組が mod$p$ でただひと組存在する。

［証明］$g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,\ \ a_0 \not\equiv 0$ とする。p は素数で a_0 と p は互いに素であるから，$a_0b \equiv 1 \pmod{p}$ となる b が存在する。そこで

$$g_1(x) = x^n + ba_1x^{n-1} + \cdots + ba_{n-1}x + ba_n$$

とおくと，$g_1(x)$ は最高次の係数が 1 の整数係数多項式で，

$$\begin{aligned} bg(x) &= ba_0x^n + ba_1x^{n-1} + \cdots + ba_{n-1}x + ba_n \\ &\equiv x^n + ba_1x^{n-1} + \cdots + ba_{n-1}x + ba_n \\ &= g_1(x) \end{aligned}$$

となるから

$$g(x) \equiv g_1(x) \pmod{p}$$

である。さて，$g_1(x)$ の最高次の係数は 1 であるから，$f(x)$ を $g(x)$ で割ると，商も余りもまた整数係数となる。商を $h(x)$，余りを $r(x)$ とおくと,$r(x)$ の次数は $n-1$ 以下であるから，mod$p$ に関する $r(x)$ の次数も $n-1$ 以下となる。

$$f(x) = g_1(x)h(x) + r(x)$$

を mod$p$ で考えると，$g(x) \equiv g_1(x) \pmod{p}$ より

$$f(x) \equiv g(x)h(x) + r(x) \pmod{p}$$

となる。ここで，また

$$\begin{aligned} f(x) &\equiv g(x)h_1(x) + r_1(x) \pmod{p} \\ f(x) &\equiv g(x)h_2(x) + r_2(x) \pmod{p} \end{aligned}$$

とすると

$$g(x)\,(h_1(x)-h_2(x)) \equiv r_2(x)-r_1(x)$$

である。ここでもし $h_1(x)-h_2(x) \not\equiv 0$ とすると，左辺の mod$p$ に関する次数は n 以上となる。しかし 右辺の mod$p$ に関する次数は $n-1$ 以下であるから，これは矛盾である。よって，$h_1(x) \equiv h_2(x) \pmod p$ であり，従ってまた $r_1(x) \equiv r_2(x) \pmod p$ でもある。これで一意性も示された。■

さて，割り算の基本定理が成り立つので mod$p$ での多項式は，mod$p$ での既約多項式に因数分解できる。

［例］

(1) $x^2+1 \equiv (x-2)(x+2) \pmod 5$ である。
(2) $x^2+1 \equiv (x-5)(x+5) \pmod{13}$ である。
(3) mod7 に関しては x^2+1 は既約である。

［注］すべての整数 x に対して $f(x) \equiv 0 \pmod p$ であっても，mod$p$ の多項式として $f(x) \equiv 0 \pmod p$ とは限らない。例えば $f(x)=x^p-x$ とおくと，

(1) $x \equiv 0 \pmod p$ のときは明らかに $f(x) \equiv 0 \pmod p$
(2) $x \not\equiv 0 \pmod p$ のときは，Fermat の定理から $x^{p-1} \equiv 1 \pmod p$ であるから $f(x)=x\left(x^{p-1}-1\right) \equiv 0 \pmod p$

となるので，すべての整数 x に対して $f(x) \equiv 0 \pmod p$ であるが，多項式としては $f(x) \not\equiv 0 \pmod p$ である。

逆に，多項式として $f(x) \equiv 0 \pmod p$ のときは，すべての整数 x に対して $f(x) \equiv 0 \pmod p$ である。

［例（剰余定理・因数定理）］ $f(x)$ を整数係数多項式とし a を整数とする。そうすると基本定理より

$$f(x) \equiv (x-a)h(x)+r \pmod p$$

なる整数 r がある（いま $x-a$ の mod$p$ に関する次数は１である）。ここで $x=a$ とすると $r \equiv f(a) \pmod p$ となる（剰余定理）。従って，mod$p$ で考えるとき，$f(x)$ が $x-a$ で割り切れるための必要十分条件は $f(a) \equiv 0 \pmod p$ となることである。

［例（Wilson の定理）］ $f(x) = x^{p-1} - 1$ とおく。$x = 1, 2, \cdots, p-1$ のとき Fermat の定理によって $x^{p-1} \equiv 1 \pmod{p}$ である。従って

$$f(1) \equiv f(2) \equiv \cdots \equiv f(p-1) \equiv 0 \pmod{p}$$

となる。よって，因数定理を繰り返し用いると，mod p で考えるとき $x^{p-1} - 1$ は $(x-1)(x-2)\cdots(x-(p-1))$ で割り切れることになる。そして，この両者の次数と最高次の係数を考えると

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}$$

とわかる。そこで $x = 0$ とすると

$$-1 \equiv (-1)(-2)\cdots(-(p-1)) \pmod{p}$$

となる。つまり

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

である。ここで p が奇素数なら $(-1)^{p-1} = 1$ であるから，$(p-1)! \equiv -1 \pmod{p}$ となる。また $p = 2$ のときは $-1 \equiv 1 \pmod{2}$ であるから，いずれにしても

p が素数のとき $(p-1)! \equiv -1 \pmod{p}$

となる。これを Wilson の定理という。

［注］ m が２つ以上の素数の積（同じ素数でもよい）であるときは，

$$(m-1)! \not\equiv -1 \pmod{m}$$

であることが次のようにして分かる。
p を m を割り切る素数とし $m = pq$ とおく。そして

$$(m-1)! \equiv -1 \pmod{m}$$

と仮定する。そうすると $(m-1)! = -1 + mt = -1 + pqt$ と書ける。ここで $p < m - 1$ であるから $(m-1)!$ は p で割り切れる。よって

$$0 \equiv (m-1)! \equiv -1 + pqt \equiv -1 \pmod{p}$$

となり $0 \equiv -1 \pmod{p}$ となるが，これは矛盾である。