問題コーナー
第 2 回
西本 将樹

N
2006年 6月 1日出題
6月 22日締切
7月 7日解説

整数係数多項式 $Q(x)$ は，$\dfrac{Q(x)}{p}$ が整数係数多項式となるような素数 p が存在しないとき，原始多項式であるという（たとえば $2x^2+1$, $6x^3-2x^2+3x$ などは原始多項式であるが，$5x^3-5x$, 100 などは原始多項式ではない）.

原始多項式 $Q(x)$ に対して，次をみたすような整数 d の最大値を $d(Q)$ で表す：

- 条件：任意の整数 m に対して，d は $Q(m)$ を割り切る.

$Q(x)$ が n 次以下の原始多項式全体を動くとき，$d(Q)$ のとりうる値をすべて求めよ.

解説

本問の答えは「**$n!$ の（正の）約数すべて**」です（ただし，$n!$ は $1\times 2\times\cdots\times n$ を表すものとします）．このことを証明するには,

(1) n 次以下の原始多項式 $Q(x)$ に対し，$d(Q)$ は $n!$ の約数である.

(2) 任意の $n!$ の約数 l に対し，$d(Q)=l$ となるような n 次以下の原始多項式 $Q(x)$ が存在する.

の 2 つのことを証明する必要があります．今回の問題においては，上の (1) が証明できている人は (2) ができていなくても準正解としました.

いずれにおいても次の補題が重要な役割を果たします：

補題 1 連続する k 個の整数の積は $k!$ の倍数である.

証明 自然数 m に対し，$\dfrac{m(m+1)\cdots(m+k-1)}{k!}={}_m\mathrm{C}_k$ で，これは明らかに整数である．$m\leqq 0$ の場合も同様である．■

正解者のほとんどの人はこの性質を使っていました．では，(1) の証明から見ていきましょう.

◦○○ **解答例 1（kami 君の解答より）**

自然数 k に対し，$R_k(x)=(x-1)\cdots(x-k)$ とおく．$R_k(m)=0\,(1\geqq m\geqq k)$ であり，また補題 1 より，任意の自然数 m に対して $R_k(m)$ は $k!$ の倍数である．

$Q(x)$ を原始多項式とし，$d(Q)=l$ とする．n 次以下の整数係数多項式 $Q(x)$ はある整数 $a_0,a_1,\dots,a_n$ を用いて

$$Q(x)=a_nR_n(x)+a_{n-1}R_{n-1}(x)+\cdots+a_1R_1(x)+a_0$$

と書ける（具体的には, $Q(x)$ を $R_n(x)$ で割った商を a_n, $Q(x)-a_nR_n(x)$ を $R_{n-1}(x)$ で割った商を a_{n-1}，としていけばよい）．

任意の $j\,(0\leqq j\leqq n)$ に対し，$j!\,a_j$ は l の倍数であることを示す．$Q(1)=a_0$ より $j=0$ のときは成立．$0\leqq j\leqq k$ $(0\leqq k\leqq n-1)$ で成立すると仮定すると，

$$Q(k+2)=a_{k+1}R_{k+1}(k+2)+a_kR_k(k+2)+\cdots+a_1R_1(k+2)+a_0$$

であり，$a_jR_j(k+2)$ は補題 1 より $j!\,a_j$ の倍数，したがって l の倍数である．よって $a_{k+1}R_{k+1}(k+2)$ も l の倍数，つまり $(k+1)!\,a_{k+1}$ も l の倍数である．よって $j=k+1$ のときも成立するので，任意の j に対して $j!\,a_j$ は l の倍数である．

特に，任意の $j(0\leqq j\leqq n)$ に対し $n!\,a_j$ は l の倍数である．よって l と $n!$ の最大公約数を l' とすれば，$\dfrac{l}{l'}$ は $a_0,\dots,a_n$ すべてを同時に割り切るので，$Q(x)$ が原始多項式であるという仮定から $\dfrac{l}{l'}=1$．これより l が $n!$ の倍数であることが示された．

どのような値を取るかが分かりやすい多項式 $R_k(x)$ の和に分けて考えることにより，上手く証明できています．他にも，$Q(x)-Q(x+1)$ を考えることにより次数を下げていくものや，ある素数で割った余りのみに注目するものなどがありました．

$d(Q)$ が $n!$ の約数すべてをとりうることは容易に証明できます．

◦○○ **解答例 2（小池貴之君の解答より）**

l を $n!$ の約数として、

$$Q(x)=R_n(x)+l$$

とおくと，$Q(x)$ は最高次の係数が 1 なので明らかに原始多項式である．整数 m に対し $Q(m)=R_n(m)+l$ は l の倍数である．また，$Q(1)=l$ より，任意の整数 m に対して $Q(m)$ を割り切るような整数の最大値は l，つまり $d(Q)=l$．した

> がって任意の $n!$ の約数 l に対し，$d(Q)=l$ となるような n 次以下の原始多項式 $Q(x)$ が存在する．

他にも，$Q(x)=(x-a_1)\cdots(x-a_n)$ と 1 次式の積で書けるものの中から具体例を構成した人も居ましたが，結構複雑になります．実は筆者も最初解答例の構成法に気づかず，1 次式の積で作ったのですが，気がついてしまえばとても簡単でしたね．

感想欄より

> $n!$ 関連の「有名事実」だと思い込んでいたのですが，思い込みだったようです．

とても自然な問題なので，同じことを考えたことのある人は結構居ても不思議ではないですよね．$n!$ の約数になることは，昔僕も考えたことがあります．

> 難しかった．

難しいものほど，考えてできたときや，答えを見て納得したときの嬉しさは大きいですよね．

> 多少の論理の甘さや表記ミスは許してもらえると信じています。

証明の一部に誤りがある答案もいくつかありましたが，大筋が合っていて，多少の修正で正しくなるものについては正解としておきました．

> 訂正版です．

> 解答に欠陥があったのでまた修正します．

これでたぶん最後（にしたい）です.

お疲れさまでした（笑）.

夏季セミナー行きたいです.

少しでも良いセミナーになればという気持ちで準備させて頂いておりますので, 皆さん是非応募して下さいね.

(にしもと まさき
東京大学理科三類 2 年)