解答例

STEP II 1997、第 4 問

純粋数学 • 剰余の定理

> **STEP II 1997、問 4**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/97-s2-q4

鍵となる考え方

次数 d の多項式で割ると、余りの次数は d 未満になる。しかも恒等式 被除数 $=$ 除数 $\times$ 商 $+$ 余り は**すべての** x について成り立つ。そこで、除数をゼロにするような x の値を代入する。すると商の項は消え、余りだけが残る。この問題で使うのはこのひとつの技法だけであり、それを三回使う。

解答

剰余の定理（remainder theorem）

$\mathrm{p}(x)$ を一次式 $x-a$ で割ると、商 $\mathrm{s}(x)$ と、次数が 1 未満の余り R が得られる。したがって R は定数であり、

$$\mathrm{p}(x) = (x-a)\,\mathrm{s}(x) + R \qquad \text{任意の} x.$$

これは x についての恒等式（identity）なので、$x = a$ を代入してよい。右辺の第一項は $0 \cdot \mathrm{s}(a) = 0$ となり、$\mathrm{p}(a) = R$ が残る。よって余りは $\mathrm{p}(a)$ であり、示すべきことが示された。

小問 (i)

剰余の定理により、与えられた余りの条件は

$$\mathrm{p}(1) = 3, \qquad \mathrm{p}(2) = 1, \qquad \mathrm{p}(3) = 5.$$

を意味する。$\mathrm{p}(x) = (x-1)(x-2)(x-3)\mathrm{q}(x) + \mathrm{r}(x)$ に $x = 1, 2, 3$ を代入すると、いずれの場合も第一項が消えるので、

$$\mathrm{r}(1) = 3, \qquad \mathrm{r}(2) = 1, \qquad \mathrm{r}(3) = 5.$$

考えてみよう $\mathrm{q}(x)$ については何もわかっていない。それは問題になるだろうか。

問題にはならない。$x = 1, 2, 3$ では因数 $(x-1)(x-2)(x-3)$ がゼロになるので、q が何であっても寄与しない。また、係数は高々三個しかないので、三つの値によって r は一意に定まる。

次数が高々二の多項式は、

$$\mathrm{r}(x) = A(x-1)(x-2) + B(x-1) + C,$$

と書いておくと便利である。こうすると、代入するたびに項がひとつずつ消えていくからである。

$$\begin{aligned} x = 1: &\quad C = 3, \\ x = 2: &\quad B + C = 1 \;\Rightarrow\; B = -2, \\ x = 3: &\quad 2A + 2B + C = 5 \;\Rightarrow\; 2A - 4 + 3 = 5 \;\Rightarrow\; A = 3. \end{aligned}$$

したがって

$$\mathrm{r}(x) = 3(x-1)(x-2) - 2(x-1) + 3 = 3x^2 - 11x + 11.$$

確かめると、$\mathrm{r}(1) = 3 - 11 + 11 = 3$、$\mathrm{r}(2) = 12 - 22 + 11 = 1$、$\mathrm{r}(3) = 27 - 33 + 11 = 5$ となる。

小問 (ii)

（問題文には一か所 $\mathrm{P}_n(x)$ と書かれているが、これは同じ多項式 $\mathrm{P}(x)$ を指している。）剰余の定理により、必要な条件は

$$\mathrm{P}(a) = a \qquad \text{ただし} a = 0, 1, \ldots, n.$$

である。多項式 x はすでにこの条件を満たしているが、次数が合わない。そこで代わりに $\mathrm{D}(x) = \mathrm{P}(x) - x$ を考える。必要なのは $a = 0, 1, \ldots, n$ に対して $\mathrm{D}(a) = 0$ となることである。したがって因数定理（factor theorem、余りが 0 の場合の剰余の定理）により、$x, x-1, \ldots, x-n$ のそれぞれが $\mathrm{D}(x)$ を割り切る。これら $n+1$ 個の一次因数は互いに異なるので、その積も $\mathrm{D}(x)$ を割り切り、その積の次数は $n+1$ である。

考えてみよう $\mathrm{P}(x)$ の次数をちょうど $n+1$ にするにはどうすればよいか。

$\mathrm{D}(x)$ をその積そのもの（望むならゼロでない定数倍）とすればよい。$n+1 \geq 2$ なので、x を加えてもその最高次の項 x^{n+1} が打ち消されることはない。よって

$$\mathrm{P}(x) = x + x(x-1)(x-2)\cdots(x-n)$$

は次数 $n+1$ をもち、$0 \leq a \leq n$ を満たす各整数 a に対して $\mathrm{P}(a) = a + 0 = a$ となる。これが求める種類の多項式である。

実は、この議論によってそのような多項式がすべて求まる。P が次数 $n+1$ をもち、与えられた余りの条件を満たすとすると、$\mathrm{D}(x) = \mathrm{P}(x) - x$ は次数が高々 $n+1$ で、次数 $n+1$ の積で割り切れる。したがってある定数 k を用いて $\mathrm{D}(x) = k\,x(x-1)\cdots(x-n)$ と書け、次数が $n+1$ となるためには $k \neq 0$ でなければならない。一般解は

$$\mathrm{P}(x) = x + k\,x(x-1)(x-2)\cdots(x-n), \qquad k \neq 0.$$

である。

検算

- $n = 1$ のとき $\mathrm{P}(x) = x + x(x-1) = x^2$ である。x で割った余りは 0、$x-1$ で割った余りは 1 であり、条件どおりである。
- (i) において、任意の q、たとえば $\mathrm{q}(x) = x$ をとって p をつくり、組立除法（synthetic division）で $x-1$、$x-2$、$x-3$ で割ると、余りは $3, 1, 5$ となる。
- コンピュータを用いて、剰余の定理を無作為に選んだ 1000 個の多項式で、小問 (i) を無作為に選んだ 100 通りの q で、小問 (ii) を $n = 1, \ldots, 11$ と $k = 1, -3, 7$ で確かめた。すべての余りが厳密に一致した。

よくある間違い

- 小問 (ii) で、多項式 $\mathrm{P}(x) = x$ そのものも条件を満たすが、次数が $n+1$ ではなく 1 であることを見落とす。次数を正しくするのは積の項である。
- $ax^2 + bx + c$ の係数についての三元連立方程式を解くのも誤りではないが、時間がかかる。入れ子の形 $A(x-1)(x-2) + B(x-1) + C$ を使えば消去の手間が省ける。

STEP のその先へ

小問 (i) は多項式補間（polynomial interpolation）の一例である。x の値が互いに異なる任意の m 個の点を通る、次数が m 未満の多項式はちょうどひとつ存在し、ここで用いた入れ子の形はそのニュートン（Newton）形式である。同じ推論を環（ring）の言葉で述べたものが、多項式に対する中国剰余定理（Chinese remainder theorem）である。すなわち、多項式を $x-1$、$x-2$、$x-3$ を法として知ることは、それらの積を法として知ることと同じである。Allenby の *Rings, Fields and Groups*（環・体・群）では、多項式環とこの定理が展開されている。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。