分数で表現した中国の剰余定理

pulsar @物理のかぎプロジェクト

Date: tmp19441:5: (WARNING/2) Cannot extract empty bibliographic field “Date”.

整数論の分野では当然のことのように分数は使われていませんが，以外に分数による表現が分かりやすいことがあります．その例として，中国の剰余定理の内容と証明を分数を用いて説明します．また，同様の考え方で多項式の剰余の代わりに有理式を用いる説明を付記します．

中国の剰余定理とは

簡単のため 整数 a を正の整数 n で割った剰余 $a \bmod n$ を $|a|_n \quad (0 \leq |a|_n < n)$ で表わします．$|a|_3 = b,\ \ |a|_5 = c$ である $|a|_{15}$ は，中国の剰余定理により

$$|a|_{15} = |10b + 6c|_{15}$$

で求められます．この 10 と 6 を詳しく書くと，$10 = 5 \times |5|_3^{-1},\ 6 = 3 \times |3|_5^{-1}$ です．ここで $|5|_3^{-1}$ は $|5x|_3 = 1$ となる x （3 を法とする逆元）を意味します．また，$|a|_3 = b,\ |a|_5 = c,\ |a|_7 = d$ である $|a|_{105}$ （ $3 \times 5 \times 7 = 105$ ）は

$$|a|_{105} = |70b + 21c + 15d|_{105}$$

$$\begin{aligned} 70 &= 5 \times 7 \times |35|_3^{-1} \\ 21 &= 3 \times 7 \times |21|_5^{-1} \\ 15 &= 3 \times 5 \times |15|_7^{-1} \end{aligned}$$

です (ガウスの方法)．$m,\ n$ が互いに素であれば

$$mx + ny = 1$$

となる整数 $x,\ y$ が存在するという有名な性質を使って，上記の式を導いてみましょう．

分数による表現

以下では，有理数 r の整数部を Γr, 小数部 Δr ($0 \leq \Delta r < 1$) で表わします．例えば

$$\Gamma\left(-\frac{8}{3}\right) = -3, \quad \Delta\left(-\frac{8}{3}\right) = \frac{1}{3}$$

です．$5x+3y=1$ は

$$\frac{x}{3}+\frac{y}{5}=\frac{1}{15}$$

と書き換えることができるので，

$$\Delta\left(\frac{x'}{3}+\frac{y'}{5}\right)=\frac{1}{15},\quad \frac{x'}{3}=\Delta\frac{x}{3},\quad \frac{y'}{5}=\Delta\frac{y}{5}$$

$$\Delta\left(\frac{5x'}{3}+y'\right)=\Delta\frac{2x'}{3}=\frac{1}{3}$$

から，$x'=2$ であることが分かります．同様に $y'=2$ であることも分かり，任意の a に対して成立する

$$\Delta\left(\frac{2a}{3}+\frac{2a}{5}\right)=\Delta\left(\Delta\frac{2a}{3}+\Delta\frac{2a}{5}\right)=\Delta\frac{a}{15}$$

が得られます．

$$\Delta\frac{2a}{3}=\Delta\left(2\Gamma\frac{a}{3}+2\Delta\frac{a}{3}\right)=\Delta\left(2\Delta\frac{a}{3}\right)$$

ですから，上記の式を

$$\Delta\left(2\Delta\frac{a}{3}+2\Delta\frac{a}{5}\right)=\Delta\frac{a}{15}$$

と書き換えることができます．これが分数で表現した中国の剰余定理です．

先に示した $|a|_{15}=|10b+6c|_{15}$ に $b=3\Delta\frac{a}{3}$，$c=5\Delta\frac{a}{5}$ を代入すると

$$15\Delta\frac{a}{15}=15\Delta\frac{10\cdot 3\Delta\frac{a}{3}+6\cdot 5\Delta\frac{a}{5}}{15}=15\Delta\left(2\Delta\frac{a}{3}+2\Delta\frac{a}{5}\right)$$

となり，上式と等価であることを確認できます．$|a|_{105}=|70b+21c+15d|_{105}$ については

$$\frac{x}{3}+\frac{y}{5}=\frac{1}{15},\quad \frac{w}{15}+\frac{z}{7}=\frac{1}{105}$$

から

$$\Delta\left(\frac{x'}{3}+\frac{y'}{5}+\frac{z'}{7}\right)=\frac{1}{105}$$

$$\Delta\left(\frac{35x'}{3}+7y'+5z'\right)=\Delta\frac{2x'}{3}=\frac{1}{3}=\frac{35}{105},\ \cdots$$

となる x', y', z' を 2, 1, 1 として

$$\Delta\left(\frac{2}{3}+\frac{1}{5}+\frac{1}{7}\right)=\Delta\frac{106}{105}=\frac{1}{105}$$

$$\Delta\left(2\Delta\frac{a}{3}+\Delta\frac{a}{5}+\Delta\frac{a}{7}\right)=\Delta\frac{a}{105}$$

が得られます．実質的にはガウスの方法そのものですが，こちらの方が説明しやすいと思いませんか．

補遺

多項式 $P(x)$ を多項式 $G(x)$ で割ったときの商を $Q(x)$, 剰余を $R(x)$ として

$$\Gamma\frac{P(x)}{G(x)} = Q(x), \quad \Delta\frac{P(x)}{G(x)} = \frac{R(x)}{G(x)}$$

によって $\Gamma(P(x)/G(x))$, $\Delta(P(x)/G(x))$ の意味を定めると，整数のときと同様に剰余の代わりに有理式を用いて説明できます．例えば，ユークリッドの互除法を，整数の場合の

$$\Delta\frac{56}{21} = \frac{14}{21}, \quad \Delta\frac{21}{14} = \frac{7}{14}, \quad \Delta\frac{14}{7} = 0$$

と同様に,

$$\Delta\frac{x^2+2x+3}{x^2-1} = \frac{2x-4}{x^2-1}, \quad \Delta\frac{x^2-1}{x-2} = \frac{3}{x-2}, \quad \Delta\frac{x-2}{1} = 0$$

で計算過程を明示できます（この例では最後の分母が定数なので互いに素）．

あとがき

$a \bmod 3$ の代わりに $\Delta(a/3)$ を用いると，本文中の $\Delta(5x/3+y) = \Delta(2x/3)$ のような計算を分かり易く表現できます．分数を用いた表現の主役は作用素 Δ です．概して，複数の法に対する剰余を考えるときは分数による表現が有効であると思います．ただし，この表現は一般には通用しませんから，レポート等には使わないでください．