# 図で解く中国式剰余定理

次のような問題を考えよう．

**問題.** 5 で割ると 3 余り，3 で割ると 1 余る数を 15 で割ったときの余りを求めよ．

この問題は，連立合同式や，一次不定方程式の整数解の問題として，次のように解かれるのが一般的である：

求める余りを $n$ とおくと，$0 \leq n < 15$ であり，条件から，

$$\begin{cases} n \equiv 3 \mod 5 \\ n \equiv 1 \mod 3 \end{cases} \iff \begin{cases} n = 5x + 3 \ (x \text{ は整数}) \\ n = 3y + 1 \ (y \text{ は整数}) \end{cases}$$

が成り立つ．等式 $5x + 3 = 3y + 1$ は，3 を法として，$x \equiv 2 \mod 3$ と解けるので，$k$ を整数として，$x = 3k + 2$ とかける．よって，

$$n = 5(3k + 2) + 3 = 15k + 13 \equiv 13 \mod 15$$

と計算でき，求める余りは，13 である．

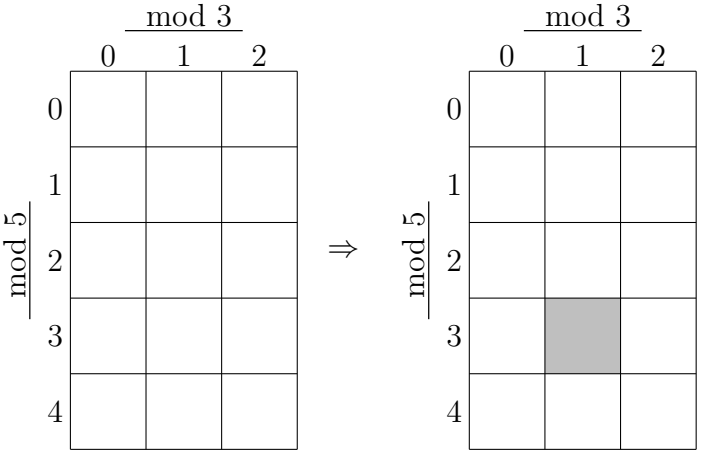
この解法で問題ないのだが，理解を深めるために，次のような表を使った解法を紹介する．まず，右のような表を作り，

$$\begin{cases} 5 \text{ で割ると } 3 \text{ 余る} \\ 3 \text{ で割ると } 1 \text{ 余る} \end{cases}$$

という条件に対応して，

$$\begin{cases} \mod 5 \text{ の } 3 \text{ 行と} \\ \mod 3 \text{ の } 1 \text{ 列の} \end{cases}$$

重なるところに印をつける．
（行と列の番号は 0 から始まっていることに注意する）

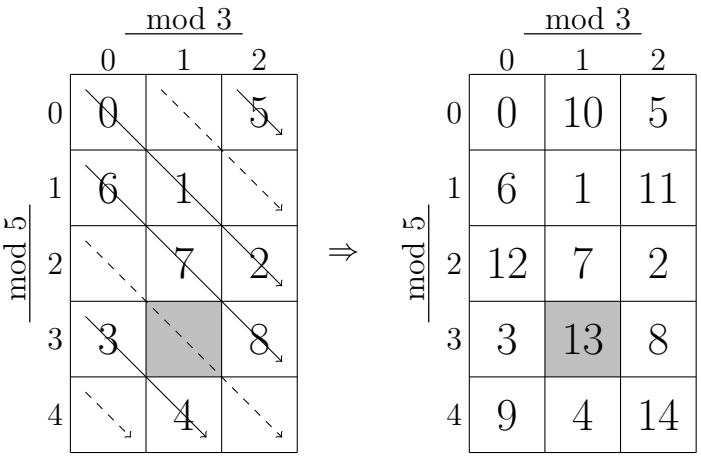



次に，左上のマスから，斜め右下方向に，$0, 1, 2, \cdots$ と順に数字を入れる．その際，

- 右端に着くと次の行の左端
- 下端に着くと次の列の上端

という順に数字を入れる．

最終的に，はじめに印をつけた部分にある数字が答えである．よって，求める余りは，13 である．




---

**補足.** 表の作り方から，上の問題において，横の行には $\mod 5$ で合同な数たちが，縦の列には $\mod 3$ で合同な数たちがそれぞれ並んでいることがわかる．よって例えば，5 で割って 3 余り，3 で割って 1 余る数は，表の 3 行 1 列（番号に注意！！）のマスに位置していることがわかる．

上の問題の解が存在して，それが一意的であるということを保証する中国式剰余定理と呼ばれる定理がある．

**定理** (中国式剰余定理). $m_1,\ m_2$ を互いに素な自然数とし，$m = m_1 m_2$ とする．このとき，

$$\begin{cases} n \equiv a_1 \mod m_1 \\ n \equiv a_2 \mod m_2 \end{cases}$$

を満たす $n\ (0 \leq n < m)$ が一意的に存在する．

中国式剰余定理を集合の言葉で言い換えるために，いくつか記号を定義する．自然数 $m$ に対して，集合 $R_m$ を

$$R_m := \{0, 1, 2, \cdots, m-1\}$$

と定義し，$m$ を法とする余りの集合（mod $m$ の集合）と呼ぶことにする[1]．また，2 つの集合 $A,\ B$ に対して，$A$ と $B$ の要素の組を要素に持つ集合 $A \times B$ を

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

と定義し，$A$ と $B$ の直積集合という．

**例.**
- 5 を法とする余りの集合は，$R_5 = \{0, 1, 2, 3, 4\}$ である．
- mod 3 の集合と，mod 5 の集合の直積集合は，$R_3 \times R_5 = \{(a, b) \mid a \in R_3,\ b \in R_5\}$ であり，$(1, 3) \in R_3 \times R_5$ などがその要素である．また要素の個数は，$3 \times 5 = 15$ である．

これらの記号を用いて，中国式剰余定理の主張は次のように言い換えることができる．

**定理** (中国式剰余定理). $m_1,\ m_2$ を互いに素な自然数とし，$m = m_1 m_2$ とする．このとき，集合 $R_{m_1} \times R_{m_2}$ の各要素と，集合 $R_m$ の各要素が，一対一に対応する：

$$R_3 \times R_5 \ni (a, b) \longleftrightarrow c \in R_{15}$$

上の問題を例として，各要素の具体的な対応を考える．集合 $R_{15}$ の要素から，集合 $R_3 \times R_5$ の要素への対応は簡単である：

$$R_{15} \ni 13 \longrightarrow (13 \bmod 3,\ 13 \bmod 5) \equiv (1, 3) \in R_3 \times R_5$$

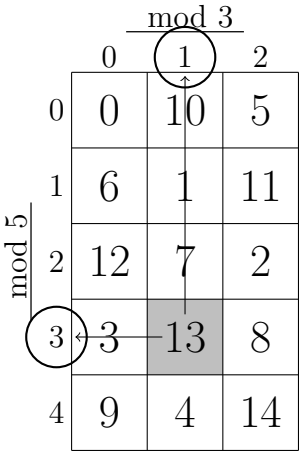
のように，$13 \in R_{15}$ に対して，$R_3$ の要素には，13 を 3 で割った余り 1 を対応させ，$R_5$ の要素には，13 を 5 で割った余り 3 を対応させれば良いのである．

難しいのは逆の対応，すなわち，集合 $R_3 \times R_5$ の要素に集合 $R_{15}$ の要素を対応させることである．この難しい側の対応を与えるということが，上の（連立合同式の）問題を解くということなのであるが，この一対一対応をまとめたものが，上で紹介した，15 マスの表なのである．

マス内の数字 $0, 1, 2, \cdots, 14$ が，集合 $R_{15}$ の要素であり，列番号 $0, 1, 2$ が $R_3$ の要素，行番号 $0, 1, \cdots, 4$ が $R_5$ の要素である．これから，中国式剰余定理の一対一対応は，この表の

$$R_{15} \ni \text{マス内の番号} \longleftrightarrow (\text{列番号，行番号}) \in R_3 \times R_5$$

という対応によって，完全に決定されることがわかる．




[1] この記号と名称は一般的ではない．