

ベクトルの内積風 P の倍数判定法

～整数NをPで割った余りが内積計算で求められる～

平成20年2月2日(土) 第64回北数教数学教育実践研究会

北海道留萌高等学校 木村 尚士

例題1 次の整数を7で割った余り、13で割った余りはそれぞれいくらか求めよ。

(1) 2304165

(2) 74291865

〈解答例〉(1)を7で割った余りは、

$$\begin{array}{r} 2 \quad 3 \quad 0 \quad 4 \quad 1 \quad 6 \quad 5 \\ 1 \quad -2 \quad -3 \quad -1 \quad 2 \quad 3 \quad 1 \\ \hline 2 \quad -6 \quad 0 \quad -4 \quad 2 \quad 18 \quad 5 = 17 \quad \underline{3} \quad (\text{mod } 7) \end{array}$$

(1)を13で割った余りは、

$$\begin{array}{r} 2 \quad 3 \quad 0 \quad 4 \quad 1 \quad 6 \quad 5 \\ 1 \quad 4 \quad 3 \quad -1 \quad -4 \quad -3 \quad 1 \\ \hline 2 \quad 12 \quad 0 \quad -4 \quad -4 \quad -18 \quad 5 = -7 \equiv \underline{6} \quad (\text{mod } 13) \end{array}$$

〈解答例〉(2)を7で割った余りは、

$$\begin{array}{r} 0 \quad \quad \quad 2 \quad \quad \quad 1 \\ \times \quad 4 \quad 2 \quad 9 \quad 1 \quad 8 \quad 6 \quad 5 \\ 3 \quad 1 \quad -2 \quad -3 \quad -1 \quad 2 \quad 3 \quad 1 \\ \hline 0 \quad 4 \quad -4 \quad -6 \quad -1 \quad 2 \quad 18 \quad 5 = 18 \quad \underline{4} \quad (\text{mod } 7) \end{array}$$

(2)を13で割った余りは、

$$\begin{array}{r} 7 \quad 4 \quad 2 \quad 9 \quad 1 \quad 8 \quad 6 \quad 5 \\ -3 \quad 1 \quad 4 \quad 3 \quad -1 \quad -4 \quad -3 \quad 1 \\ \hline -21 \quad 4 \quad 8 \quad 27 \quad -1 \quad -32 \quad -18 \quad 5 = -28 \equiv -2 \\ \equiv \underline{11} \quad (\text{mod } 13) \end{array}$$

整数NをPで割った余りが内積計算で求められる

与えられた10進整数NをP (Pは自然数)で割った余りを求める方法について紹介する。次のように要素が整数のベクトルXとYを導入すると、求める余りは2つのベクトルの内積の値と合同になる。その計算は、実際に割り算を行うよりも計算量が少なく、与えられた整数NがPの倍数であるかどうか容易に判定することができる。

10進整数Nの下からn桁目の数を a_n ($n=1,2,3,\dots$)とおくと、各 a_1, \dots, a_n は0から9までのうちいずれかの整数値をとる。この a_n を成分とするベクトルXを次のように約束する。すなわち整数Nが、 $a_n \dots a_5 a_4 a_3 a_2 a_1$ のとき、

$$X = (a_1, a_2, a_3, a_4, a_5, \dots, a_n) \quad \text{と定める。}$$

次に、自然数Pに応じたベクトルYを以下のように生成する。

10進整数の下からn桁目の位である 10^{n-1} (ただし $n=1,2,3,\dots$)をPで割った余りを R_n とし、

$$Y = (R_1, R_2, R_3, R_4, \dots, R_n) \quad \text{と定める。}$$

XとYの内積を $X \cdot Y$ とするとき、次の合同式が成り立つ。

$$\text{Proposition 1) } \quad \text{与えられた10進整数 } N \equiv X \cdot Y \pmod{P}$$

$$\text{Proof) } \quad N = a_1 \times 10^0 + a_2 \times 10^1 + a_3 \times 10^2 + a_4 \times 10^3 + a_5 \times 10^4 + \dots + a_n \times 10^{n-1}$$

$$a_1 R_1 + a_2 R_2 + a_3 R_3 + a_4 R_4 + a_5 R_5 + \dots + a_n R_n \quad (\text{mod } P)$$

$$= X \cdot Y$$

Pに応じたベクトルYのうち、実際に活用できそうなものについて以下にまとめた。覚えて利用すれば、組立除法におけるかけ算と足し算程度の簡単な計算で、比較的大きな整数についても、Pで割った余りを容易に求めることができる。特に、素因数分解等の場面で実質活用できそうなものは で囲った。 〈続きは裏面へ〉

$P=2, 5, 10$ のとき、 $Y = (1, 0, 0, \dots, 0)$

$P=3, 9$ のとき、 $Y = (1, 1, 1, \dots, 1)$

$P=4$ のとき、 $Y = (1, 2, 0, 0, \dots, 0)$

$P=7$ のとき、 $Y = (1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, \dots)$

$P=8$ のとき、 $Y = (1, 2, 4, 0, \dots, 0)$

$P=11$ のとき、 $Y = (1, -1, 1, -1, \dots)$

$P=13$ のとき、 $Y = (1, -3, -4, -1, 3, 4, 1, -3, -4, -1, 3, 4, \dots)$

$P=17$ のとき、 $Y = (1, -7, -2, -3, 4, 6, -8, 5, -1, 7, 2, 3, -4, -6, 8, -5, \dots)$

$P=19$ のとき、 $Y = (1, -9, 5, -7, 6, 3, -8, -4, -2, -1, 9, -5, 7, -6, -3, 8, 4, 2, \dots)$

$P=37$ のとき、 $Y = (1, 10, -11, 1, 10, -11, \dots)$

$P=41$ のとき、 $Y = (1, 10, 18, 16, -4, 1, 10, 18, 16, -4, \dots)$

〈上記についての主な特徴等および補足説明〉

$P=7, 13$ のときの Y の成分の列は、 $R_{n+1} - R_n = R_{n+2}$ を満たしている。

■部分は、以下繰り返し現れる。

■部分は、以下その符号違いである ■部分と交互に繰り返し現れる。

問題 1 8 3 8 なる 5 けたの整数がある。この数が 4, 7, 9 および 11 で割り切れるとき、それぞれの□はいくらか。『モノグラフ シーズの「整数」(科学振興新社) 第 1 章 7. 倍数の判定法 問題 5 の 4 番』より)

～ この問題 1 について、本稿 “ベクトルの内積風 P の倍数判定法” を活用した解答例の紹介 ～

5 けたの整数を $8a3b8$ ($0 \leq a < 9, 0 \leq b < 9$) とおく、

11 で割り切れるための条件は、

$$-a - b + 19 \equiv 0 \pmod{11}$$

$$a + b \equiv 19 \pmod{11}$$

$$a + b \equiv 8 \pmod{11}$$

0 $a + b \equiv 18$ より、 $a + b = 8, 19, \dots$

9 で割り切れるための条件は、

$$a + b + 19 \equiv 0 \pmod{9}$$

$$a + b \equiv -19 \pmod{9}$$

$$a + b \equiv -1 \pmod{9}$$

0 $a + b \equiv 18$ より、 $a + b = 8, 17, \dots$

4 で割り切れるための条件は、

$$\begin{aligned} 2b + 8 &\equiv 0 \pmod{4} \\ b + 4 &\equiv 0 \pmod{2} \\ b &\equiv 0 \pmod{2} \end{aligned}$$

0 $b \equiv 0$ より、 $b = 0, 2, 4, 6, 8, \dots$

7 で割り切れるための条件は、

$$-a + 3b - 10 \equiv 0 \pmod{7}$$

$$-a + 3b \equiv 10 \pmod{7}$$

$$-a + 3b \equiv 3 \pmod{7}$$

$$-9 \leq -a \leq 0, 0 \leq 3b \leq 27 \text{ だから}$$

$$-9 \leq -a + 3b \leq 27 \text{ より、}$$

$$-a + 3b = -4, 3, 10, 17, 24, \dots$$

計算メモ

8 a 3 b 8 5 けたの整数

1 -1 1 -1 1 11 で割る

1 1 1 1 1 9 で割る

-3 -1 2 3 1 7 で割る

2 1 4 で割る

上記のいずれも、たてに掛けて足せば P で割った余りと合同な値が得られる。0 になれば P で割り切れる。

①かつ②より、 $a + b = 8$

③より、 $(a, b) = (0, 8), (2, 6), (4, 4), (6, 2), (8, 0)$

このうち④を満たすものは、 $(a, b) = (0, 8)$ のみである。

よって、千の位が 0 で、十の位が 8 である。