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、

2	3	0	4	1	6	5	
1	−2	−3	−1	2	3	1	
2	−6	0	−4	2	18	5	＝17≡$\underline{3}$　(mod7)

(1)を 13 で割った余りは、

2	3	0	4	1	6	5	
1	4	3	−1	−4	−3	1	
2	12	0	−4	−4	−18	5	＝−7≡$\underline{6}$　(mod13)

〈解答例〉(2)を 7 で割った余りは、

0			2		1			
$\cancel{7}$	4	2	$\cancel{9}$	1	$\cancel{8}$	6	5	
3	1	−2	−3	−1	2	3	1	
0	4	−4	−6	−1	2	18	5	＝18≡$\underline{4}$　(mod7)

(2)を 13 で割った余りは、

7	4	2	9	1	8	6	5	
−3	1	4	3	−1	−4	−3	1	
−21	4	8	27	−1	−32	−18	5	＝−28≡−2

≡$\underline{11}$　(mod13)

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$\mathbb{X}$と$\mathbb{Y}$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も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（$n=1,2,3,\cdots$）とおくと、各 $a_1,\cdots,a_n$ 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$\mathbb{X}$を次のように約束する。すなわち整数Ｎが、 $a_n\cdots a_5\,a_4\,a_3\,a_2\,a_1$　のとき、

$\mathbb{X}$ ＝（$a_1, a_2, a_3, a_4, a_5,\cdots, a_n$）　　と定める。

次に、自然数 P に応じたベクトル$\mathbb{Y}$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 $n=1,2,3\cdots$ ）をＰで割った余りを R_n とし、

$\mathbb{Y}$ ＝（$R_1, R_2, R_3, R_4,\cdots, R_n$）　　と定める。

$\mathbb{X}$と$\mathbb{Y}$の内積を$\mathbb{X}\cdot\mathbb{Y}$とするとき、次の合同式が成り立つ。

Proposition１）　与えられた１０進整数Ｎ≡$\mathbb{X}\cdot\mathbb{Y}$　(mod P)

Proof ）

$$
\begin{aligned}
N &= a_1\times10^0+a_2\times10^1+a_3\times10^2+a_4\times10^3+a_5\times10^4+\cdots+a_n\times10^{n-1}\\
&\equiv a_1R_1+a_2R_2+a_3R_3+a_4R_4+a_5R_5+\cdots+a_nR_n \quad (\mathrm{mod}\ P)\\
&= \mathbb{X}\cdot\mathbb{Y} \qquad \blacksquare
\end{aligned}
$$

Ｐに応じたベクトル$\mathbb{Y}$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$\boxed{}$で囲った。

〈続きは裏面へ…〉

Ｐ＝2 , 5 , 10 のとき、$\mathbb{Y}$ ＝（ 1 , 0 , 0 ,…, 0 ）

Ｐ＝3 , 9 のとき、　$\mathbb{Y}$ ＝（ 1 , 1 , 1 ,…, 1 ）

Ｐ＝4 のとき、　$\mathbb{Y}$ ＝（ 1 , 2 , 0 , 0 ,…, 0 ）

Ｐ＝７のとき、　$\mathbb{Y}$ ＝（ 1 , 3 , 2 ,－1 ,－3 ,－2 , 1 , 3 , 2 ,－1 ,－3 ,－2 ,… ）

Ｐ＝８のとき、　$\mathbb{Y}$ ＝（ 1 , 2 , 4 , 0 ,…, 0 ）

Ｐ＝１１のとき、　$\mathbb{Y}$ ＝（ 1 ,－1 , 1 ,－1 ,… ）

Ｐ＝１３のとき、　$\mathbb{Y}$ ＝（ 1 ,－3 ,－4 ,－1 , 3 , 4 , 1 ,－3 ,－4 ,－1 , 3 , 4 ,… ）

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

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

Ｐ＝３７のとき、　$\mathbb{Y}$ ＝（ 1 , 10 ,－11 , 1 , 10 ,－11 ,… ）

Ｐ＝４１のとき、　$\mathbb{Y}$ ＝（ 1 , 10 , 18 , 16 , －4 , 1 , 10 , 18 , 16 , －4 ,… ）

〈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$\mathbb{Y}$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 シリーズ 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 8 a 3 b 8 (0≦a≦9 , 0≦b≦9) とおく、

11 で割り切れるための条件は、

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

$a+b\equiv 19$

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

0≦a＋b≦18 より、a＋b＝8 ……①

9 で割り切れるための条件は、

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

$a+b\equiv -19$

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

0≦a＋b≦18 より、a＋b＝8 , 17 ……②

4 で割り切れるための条件は、

$2b+8\equiv 0 \pmod 4$

$b+4\equiv 0 \pmod 2$

$b\equiv 0 \pmod 2$

0≦b≦9 より、b＝0 , 2, 4 , 6 , 8 ……③

7 で割り切れるための条件は、

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

$-a+3b\equiv 10$

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

－9≦－a ≦0 , 0≦3b≦27 だから

－9≦－a＋3b ≦27 より、

－a＋3b＝－4 , 3 , 10, 17, 24 ……④

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、<u>千の位が 0 で、十の位が 8 である</u>。

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。