代数学序論, 第10回演習問題

2020/7/13 担当：那須

1 $\mathbb{Z}/n\mathbb{Z}$ の次の元 $a \pmod n$ に対し, a の n に関する位数 $\mathrm{ord}_n(a)$ を求めよ.

(1) $2 \pmod 7$
(2) $5 \pmod{11}$
(3) $4 \pmod{13}$
(4) $4 \pmod{17}$
(5) $7 \pmod{19}$
(6) $2 \pmod{23}$

2 $\mathbb{Z}/5\mathbb{Z}$ において 2 は原始根であり, 各元は 2 のべきとして次のように表される (べき表現):

元	1	2	3	4
べき表現	2^0	2^1	2^3	2^2

$\mathbb{Z}/7\mathbb{Z}$ の原始根 3 に関するべき表現を求めよ.

元	1	2	3	4	5	6
べき表現	3^0		3^1			

3 (1) $\mathbb{Z}/11\mathbb{Z}$ の原始根 2 に関するべき表現を求めよ.

元	1	2	3	4	5	6	7	8	9	10
べき表現	2^0	2^1								

(2) $\mathbb{Z}/11\mathbb{Z}$ の原始根をすべて求めよ.

(3) $\mathbb{Z}/11\mathbb{Z}$ の各元の位数を求めよ.

元	1	2	3	4	5	6	7	8	9	10
位数	1	10								

4 (原始根判定法を用いて) 次の整数が指定された法に関して原始根であることを示せ.

(1) $6 \pmod{13}$
(2) $3 \pmod{19}$
(3) $5 \pmod{37}$
(4) $2 \pmod{101}$

---

[1]解答 (ヒント)：

1 (1) 3 (2) 5 (3) 6 (4) 4 (5) 3 (6) 11

2 略 (7 を法として 3^i $(i = 0, 1, 2, 3, 4, 5)$ を計算すればよい.)

3 (1) 略 (11 を法として 2^i $(i = 0, 1, \ldots, 9)$ を計算すればよい.)

(2) $2, 6, 7, 8$

(3) 略 ($p = 11$, $\mathrm{ord}_p(a^t) = (p-1)/\gcd(p-1, t)$ を用いる.)

4 (1) $13 - 1 = 2^2 \cdot 3$ と素因数分解される. $6^{12/2} \equiv 12 \neq 1$ かつ $6^{12/3} \equiv 9 \neq 1$. 原始根判定法より 6 は原始根である.

(2) $19 - 1 = 2 \cdot 3^2$ と素因数分解される. $3^{18/2} \equiv 18 \neq 1$ かつ $3^{18/3} \equiv 7 \neq 1$. 原始根判定法より 3 は原始根である.

(3) $37 - 1 = 2^2 \cdot 3^2$ と素因数分解される. $5^{36/2} \equiv 36 \neq 1$ かつ $5^{36/3} \equiv 10 \neq 1$. 原始根判定法より 5 は原始根である.

(4) $101 - 1 = 2^2 \cdot 5^2$ と素因数分解される. $2^{100/2} \equiv 100 \neq 1$ かつ $2^{100/5} \equiv 95 \neq 1$. 原始根判定法より 2 は原始根である.

[1]※この講義に関する情報はホームページを参照. http://fuji.ss.u-tokai.ac.jp/nasu/2020/alg0.html