

# 自然数 $a$ の $n$ 乗の研究

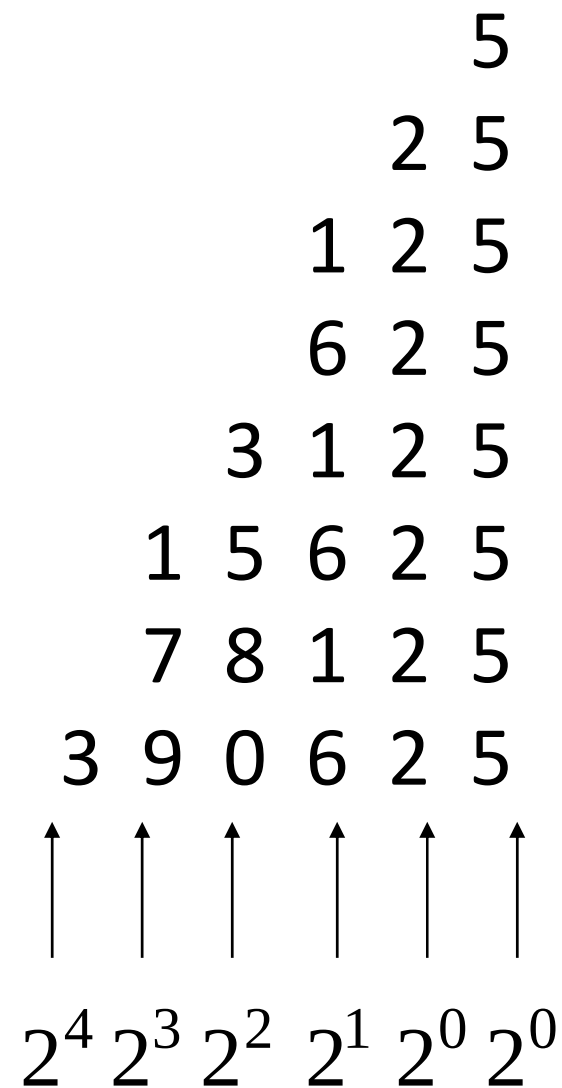
津山高専電気電子工学科 3年

小津野 将, 新免 泰陽

# $5^n$ の研究

m桁の周期の長さ:

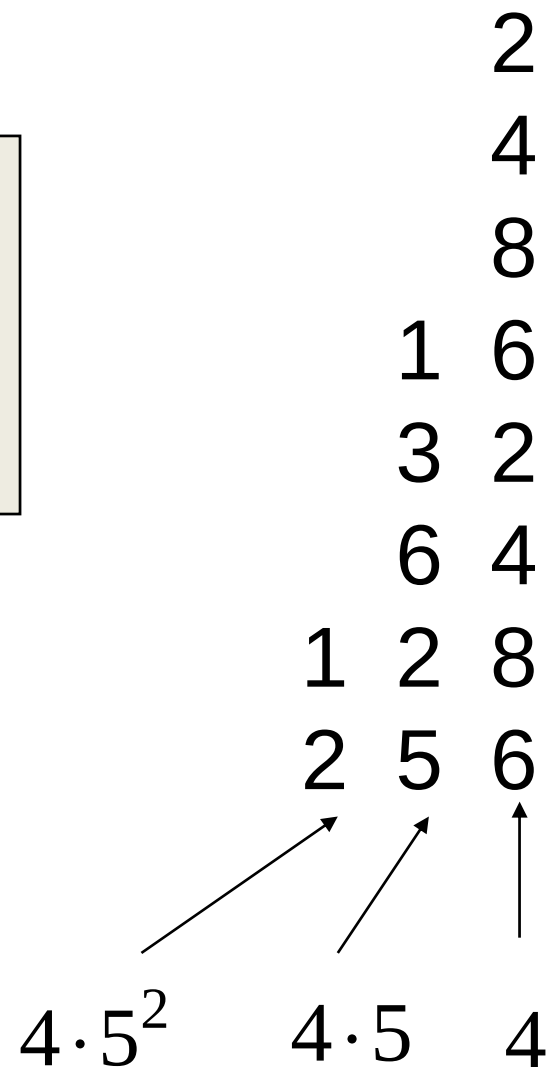
$$2^{m-2} \quad (m \geq 2)$$



# $2^n$ の研究

m桁の周期の長さ:

$$4 \cdot 5^{m-1}$$



# $2^n \sim 9^n$ の $m$ 桁の周期の長さ

$$2^n$$

$$4 \times 5^{m-1}$$

$$3^n$$

$$4 \times 10^{m-2}$$

$$4^n$$

$$2 \times 5^{m-1}$$

$$5^n$$

$$2^{m-2}$$

$$6^n$$

$$5^{m-1}$$

$$7^n$$

$$4 \times 10^{m-1}$$

$$8^n$$

$$4 \times 5^{m-1}$$

$$9^n$$

$$2 \times 10^{m-2}$$

# $5^n$ に関する定理

$$\text{【定理1】} \quad 5^{2^m} \equiv 1 \pmod{2^{m+2}}$$

$$\begin{aligned} \text{【系1】} \quad 5^{n+j2^m} &\equiv 5^n \pmod{10^{m+2}} \\ n &\geq m+2 \end{aligned}$$

# 定理1の証明

$$5 = 4 + 1$$

$$5^2 = 4^2 + {}_2C_1 \times 4 \times 1 + 1^2 = 4^2 + 2^3 + 1$$

$$(5^2)^2 = 4^4 + \cdots + {}_2C_1 \times 2^3 + 1 = 4^4 + \cdots + 2^4 + 1$$

$$((5^2)^2)^2 = 4^8 + \cdots + {}_2C_1 \times 2^4 + 1 = 4^8 + \cdots + 2^5 + 1$$

⋮

$$5^{2^{m-2}} = 4^{2^{m-2}} + \cdots + {}_2C_1 \times 2^{m-1} + 1 = 4^{2^{m-2}} + \cdots + 2^m + 1$$

$$5^{2^m} = 4^{2^m} + \cdots + {}_2C_1 \times 2^{m+1} + 1 = 4^{2^m} + \cdots + 2^{m+2} + 1$$

$$\therefore 5^{2^m} \equiv 1 \pmod{2^{m+2}}$$

# 系1の証明

定理1より、

$$5^{2^m} = 4^{2^m} + \cdots + 2^{m+2} + 1$$

両辺に

$5^n$  ( $n > m + 2$ ) を掛ける。

$$5^{n+2^m} = 5^n \times 4^{2^m} + \cdots + 5^n \times 2^{m+2} + 5^n$$

ここで  $n > m + 2$  より、 $5^n = 5^{n'} \times 5^{m+2}$  と書ける。

$$5^{n+2^m} = 5^{n'} \times 10^{m+2} \times 4^{m'} + \cdots + 5^{n'} \times 10^{m+2} + 5^n$$

$$\therefore 5^{n+2^m} \equiv 5^n \pmod{10^{m+2}}$$

(  $j = 1$  の時の証明は終了。 )

## ( $j \geq 2$ の時の証明)

$5^{n+2^m} \equiv 5^n \pmod{10^{m+2}}$  の両辺に  $5^{2^m}$  を掛ける。

$$5^{2^m} \times 5^{n+2^m} = 5^{2^m} \times 4^{2^m} + \cdots + 5^{2^m} \times 2^{m+2} + 5^{2^m} \times 5^n$$

$$5^{n+2 \times 2^m} = 5^{n'} \times 10^{m+2} \times 4^{m'} + \cdots + 5^{n'} \times 10^{m+2} + 5^{n+2^m}$$

$$\therefore 5^{n+2 \times 2^m} \equiv 5^{n+2^m} \pmod{10^{m+2}}$$

$j = 2$  の場合は、 $j = 1$  の場合を使うと、

$$5^{n+2 \times 2^m} \equiv 5^{n+2^m} \equiv 5^n \pmod{10^{m+2}}$$

この議論を繰り返して、

$$5^{n+j2^m} \equiv 5^n \pmod{10^{m+2}} //$$

# 周期性との関連

以下の式は  $5^n$  の周期性を表している。

$$5^{n+j2^m} \equiv 5^n \pmod{10^{m+2}} // \\ (j = 1, 2, 3, \dots)$$

この周期性は、次の図のような意味を持つ。

|   |   |   | $m = 2$<br>(4飛び) | $m = 1$<br>(2飛び) | 5 |
|---|---|---|------------------|------------------|---|
|   |   |   |                  | 2                | 5 |
|   |   |   |                  | 1                | 2 |
|   |   |   |                  | 6                | 2 |
|   |   |   | 3                | 1                | 2 |
|   |   |   | 1                | 5                | 6 |
|   |   |   | 7                | 8                | 1 |
|   |   |   | 3                | 0                | 6 |
| 1 | 9 | 5 | 3                | 1                | 2 |
| 9 | 7 | 6 | 5                | 6                | 2 |

# 定理1の一般化 ( $2p$ 進数での周期性)

【定理2】  $p$  を素数とする。

$$p^{2^m} \equiv 1 \pmod{2^{m+t}}$$

ただし,  $t$  は  $p = 2^t + 1$  をみたす数。

【系2】  $p^{n+j2^m} \equiv p^n \pmod{(2p)^{m+t}}$

\* 系2の意味は,  $2p$  進数で  $p^n$  を表したときの周期が  $2^m$  であることを表している。

## さらに一般化 ( $ap$ 進数での周期性 )

$\gcd(a, p) = 1$  のとき, フェルマーの小定理より,  
 $a^d \equiv 1 \pmod{p}$  となる最小の  $d$  が存在する。

【定理3】  $a^{dp^m} \equiv 1 \pmod{p^{m+t}}$

ただし,  $t$  は  $a^d = p^t L + 1$  をみたす数。

【系3】  $a^{n+jp^m} \equiv a^n \pmod{(ap)^{m+t}}$

\* 系3の意味は,  $ap$  進数で  $a^n$  を表したときの  
周期が  $p^m$  であることを表している。

# 周期性に関連した定理

1 7 6 9 9 7 6 7 2 4 4 4 7 4 8 0 2 7 7 2 6 1 8 9 7  
3 9 8 1 1 9 8 9 4 6 6 6 9 6 0 2 4 9 9 4 8 3 0 1 9  
5 1 0 3 3 1 0 1 6 8 8 8 1 8 2 4 6 1 1 6 0 5 2 3 1  
7 3 2 5 5 3 2 3 8 0 0 0 3 0 4 6 8 3 3 8 2 7 4 5 3  
9 5 4 7 7 5 4 5 0 2 2 2 5 2 6 8 0 5 5 0 4 9 6 7 5

上の図は  $6^n$  の4桁目を5分割してそれぞれ順番に並べたもの。

$a^n (a \neq 5)$  の  $m$  桁目の1周期分の数を  
5分割してそれぞれ順番に並べると、その各桁に現れ  
る数は1～9までの偶数または奇数が1つずつしか現  
れない。

# 群 $\mathbb{Z}/10\mathbb{Z}$ の部分群との比較

群  $\mathbb{Z}/10\mathbb{Z}$  を考え, その部分群を  $\langle a \rangle$  とする。  $\# \langle a \rangle$  と  $a^n$  の縦周期の長さを比較する。

(例)

( $m$  は桁とする。)

|          | $\# \langle a \rangle$ | $a^n$ の縦周期の長さ       |
|----------|------------------------|---------------------|
| $a = 5$  | 2                      | $2^{m-2}$           |
| $a = 2$  | 5                      | $4 \times 5^{m-1}$  |
| $a = 3$  | 10                     | $4 \times 10^{m-1}$ |
| $a = 36$ | 5                      | $5^{m-1}$           |

# 予想

$a^n$  を縦に並べて,  $m$ 桁目の数列  $\{\alpha_{m,i}\}$  を考える。さらに, 群  $\mathbf{Z}/10\mathbf{Z}$  の部分群  $\langle a \rangle$  の位数  $\#\langle a \rangle$  を  $d$  とすると以下が成り立つ。

- (1)  $\{\alpha_{m,i}\}$  は周期的である。
- (2)  $\{\alpha_{m,i}\}$  の周期の長さは, ある定数  $c, \alpha$  により,  $cd^{m-\alpha}$  となる。