

生徒のための復習・自学教材

【整数編】

合同式の活用（中国の剰余定理）

助問 1

7 で割ると 2 余り, 8 で割ると 5 余る 2 桁の自然数をすべて求めよ。

助問 2

自然数 n が条件

(*) $n+5$ は 7 の倍数で, $n+7$ は 5 の倍数を満たすとき, 次の問いに答えよ。

- (1) $n+12$ を 35 で割った余りを求めよ。
- (2) (*) の条件を満たす最小の n を求めよ。

['09 中央大学]

ボス問 1

- (1) 2016 と $2^{2016}+1$ は互いに素であることを証明せよ。
- (2) $2^{2016}+1$ を 2016 で割った余りを求めよ。
- (3) $2^{2016}(2^{2016}+1)(2^{2016}+2)\cdots(2^{2016}+m)$ が 2016 の倍数となる最小の自然数 m を求めよ。

['16 九州大学・後]

助問 1

7 で割ると 2 余り, 8 で割ると 5 余る 2 桁の自然数をすべて求めよ。

$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 5 \pmod{8} \end{cases}$$

$$x = 8a + 7b$$

$$\begin{cases} 8a \equiv 2 \pmod{7} \\ 7b \equiv 5 \pmod{8} \end{cases} \text{ を解く}$$

$$8a \equiv 2 \pmod{7} \text{ より } 7b \equiv 5 \pmod{8} \text{ より}$$

$$a \equiv 2 \pmod{7} \quad -b \equiv 5 \pmod{8}$$

$$b \equiv -5 \pmod{8}$$

$$\therefore b \equiv 3 \pmod{8}$$

$$8a \equiv 16 \pmod{56}, \quad 7b \equiv 21 \pmod{56}$$

$$8a + 7b \equiv 37 \pmod{56}$$

$$\therefore x \equiv 37 \pmod{56}$$

$$x = 56k + 37 \quad (k: \text{整数}) \text{ と書ける。}$$

2 桁の自然数となるのは $k=0, 1$ のときのみ。

$$\underline{37, 93}$$

助問 2

自然数 n が条件

(*) $n+5$ は 7 の倍数で, $n+7$ は 5 の倍数を満たすとき, 次の問いに答えよ。

(1) $n+12$ を 35 で割った余りを求めよ。

(2) (*) の条件を満たす最小の n を求めよ。

['09 中央大学]

$$(1) \begin{cases} n+5 \equiv 0 \pmod{7} \\ n+7 \equiv 0 \pmod{5} \end{cases}$$

$$\therefore \begin{cases} n \equiv -5 \equiv 2 \pmod{7} \\ n \equiv -7 \equiv 3 \pmod{5} \end{cases}$$

$$\therefore \begin{cases} n+12 \equiv 14 \equiv 0 \pmod{7} \\ n+12 \equiv 15 \equiv 0 \pmod{5} \end{cases}$$

より, $n+12$ は 7 の倍数かつ 5 の倍数であり,

7 と 5 は互いに素なので, 35 の倍数となる。

つまり, 35 で割った余りは 0 となる。

$$(2) (1)より \begin{cases} n \equiv 2 \pmod{7} \\ n \equiv 3 \pmod{5} \end{cases}$$

$$n = 5a + 7b$$

$$\begin{cases} 5a \equiv 2 \pmod{7} \\ 7b \equiv 3 \pmod{5} \end{cases} \quad \text{各解く}$$

$$5a \equiv 2 \pmod{7} \text{ より}$$

$$-2a \equiv 2 \pmod{7}$$

2 と 7 は互いに素だから

$$a \equiv -1 \equiv 6 \pmod{7}$$

$$5a \equiv 30 \pmod{35}$$

$$7b \equiv 3 \pmod{5} \text{ より}$$

$$2b \equiv 8 \pmod{5}$$

2 と 5 は互いに素だから

$$b \equiv 4 \pmod{5}$$

$$7b \equiv 28 \pmod{35}$$

$$5a + 7b \equiv 30 + 28 \equiv 58 \equiv 23 \pmod{35}$$

$$\therefore n \equiv 23 \pmod{35}$$

より, 求める最小の n は 23

ボス問 1

- (1) 2016 と $2^{2016} + 1$ は互いに素であることを証明せよ。
 (2) $2^{2016} + 1$ を 2016 で割った余りを求めよ。
 (3) $2^{2016}(2^{2016} + 1)(2^{2016} + 2) \cdots (2^{2016} + m)$ が 2016 の倍数となる最小の自然数 m を求めよ。

['16 九州大学・後]

(1) $2016 = 2^5 \cdot 3^2 \cdot 7$

$$\begin{cases} 2^{2016} + 1 \equiv 1 \pmod{2} \\ 2^{2016} + 1 \equiv (2^2)^{672} + 1 \equiv 8^{672} + 1 \equiv (-1)^{672} + 1 \equiv 2 \pmod{3} \\ 2^{2016} + 1 \equiv 8^{672} + 1 \equiv 1^{672} + 1 \equiv 2 \pmod{7} \end{cases}$$

よって、 $2^{2016} + 1$ は $2, 3, 7$ のいずれも素因数にもたないの
 2016 と互いに素である。

(2)

$$\begin{cases} 2^{2016} + 1 \equiv (2^3)^{672} + 1 \equiv 8^{672} + 1 \equiv (-1)^{672} + 1 \equiv 2 \pmod{9} \\ 2^{2016} + 1 \equiv (2^5)^{403} \cdot 2 + 1 \equiv 1 \pmod{32} \\ 2^{2016} + 1 \equiv 2 \pmod{7} \end{cases}$$

$x = 2^{2016} + 1$ とおいて

$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 2 \pmod{9} \end{cases} \text{ を解く}$$

7 と 9 は互いに素なので $x \equiv 2 \pmod{63}$

次に

$$\begin{cases} x \equiv 2 \pmod{63} \\ x \equiv 1 \pmod{32} \end{cases} \text{ を解く}$$

$x \equiv 32a + 63b$

$$\begin{cases} 32a \equiv 2 \pmod{63} \\ 63b \equiv 1 \pmod{32} \end{cases} \text{ を解く}$$

$32a \equiv 2 \pmod{63}$ より $63b \equiv 1 \pmod{32}$ より

$64a \equiv 4 \pmod{63}$, $-b \equiv 1 \pmod{32}$

$a \equiv 4 \pmod{63}$, $b \equiv -1 \pmod{32}$

$32a \equiv 128 \pmod{2016}$, $63b \equiv -63 \pmod{2016}$

$\therefore 32a + 63b \equiv 65 \pmod{2016}$

$x \equiv 65 \pmod{2016}$

$2^{2016} + 1 \equiv 65 \pmod{2016}$

したがって $2^{2016} + 1$ を 2016 で割った余りは 65

(3) (1), (2) より

$x = 2^{2016}$ とおくと

$$\begin{cases} x \equiv 1 \pmod{3} \quad \therefore x+2 \equiv 0 \pmod{3}, x+5 \pmod{3} \\ x \equiv 1 \pmod{7} \quad \therefore x+6 \equiv 0 \pmod{7} \\ x \equiv 0 \pmod{32} \end{cases}$$

よって $x(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)$

において、 x は 2^5 の倍数、 $x+2$, $x+5$ は 3 の倍数、 $x+6$ は 7 の倍数となる。

ゆえに $x(x+1)(x+2) \cdots (x+6)$ は $2^5 \cdot 3^2 \cdot 7 = 2016$ の倍数である。

つまり、求める最小の自然数 m は 6 である。