

- (1) $100!$ の末尾には0が連続して何個並ぶか。
 (2) 2つの正の整数の和は54で、その最小公倍数は231である。各数を求めよ。
 (3) $\frac{5561}{6059}$ を既約分数に直せ。

(1)

1 ~ 100 の中に

$$\begin{cases} 5 \text{ の倍数} & \text{は} & 20 \\ 5^2 \text{ の倍数} & \text{は} & 4 \\ 5^3 \text{ の倍数} & \text{は} & 0 \end{cases}$$

よって $100!$ は 5 で 24 回割り切れる。

2 で は、さらに多くの回数で割り切れる。

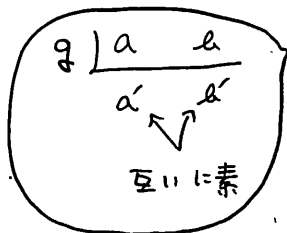
つまり

$100!$ は 10 で 24 回割り切れるから

$100!$ の末尾には 0 が 24 個連続して並ぶ。

(2) 解法1

2つの正の整数を a, b ($a \leq b$) とおく。



a と b の最大公約数
 を g とおくと、互いに
 素な自然数 a', b'
 ($a' \leq b'$) を用いて

$$a = ga', \quad b = gb'$$

と置き

題意より

$$\begin{cases} ga' + gb' = 54 & \text{--- ①} \\ ga'b' = 231 & \text{--- ②} \end{cases}$$

g, a', b' は ② より 0 ではないから

② ÷ ① とし

$$\frac{ga'b'}{g(a'+b')} = \frac{231}{54}$$

$$\frac{a'b'}{a'+b'} = \frac{77}{18}$$

$$18a'b' = 77a' + 77b'$$

$$18a'b' - 77a' - 77b' = 0$$

$$\begin{pmatrix} & b' & -\frac{77}{18} \\ 18a' & 18a'b' & -77a' \\ -77b' & & \frac{77^2}{18} \end{pmatrix} + \frac{77^2}{18} - 77 \quad + \frac{77^2}{18}$$

$$(18a' - 77)(b' - \frac{77}{18}) = \frac{77^2}{18}$$

$$(18a' - 77)(18b' - 77) = 77^2 \times 11^2$$

$1 \leq a' \leq b'$ より

$$-59 \leq 18a' - 77 \leq 18b' - 77$$

$18a' - 77$	1	7	11	7^2	7×11
$18b' - 77$	$7^2 \times 11^2$	7×11^2	$7^2 \times 11$	11^2	7×11
$18a'$	78	84	88	126	154
$18b'$	77×78	77×84	77×88	198	154
	X	X	X		X

よって

$$a' = 7, \quad b' = 11$$

(互いに素であることを満たす)

よって ② より

$$77g = 231$$

$$g = 3$$

よって

$$a = 21, \quad b = 33$$

つまり、2数は、21 と 33

(3) a と b の最大公約数を (a, b) とする。

$$(5561, 6059) = (498, 5561)$$

$$= (83, 498) = 83$$

よって

$$\frac{5561}{6059} = \frac{67}{73}$$

(裏に続く)

(2) 解法2

$$\begin{cases} g(a'+b') - 54 = 2 \times 3^3 \\ g a' b' = 231 = 3 \times 7 \times 11 \end{cases}$$

$a' + b'$ と $a' b'$ は互いに素な数

$$g = 3, a' + b' = 18, a' b' = 77$$

a' と b' を解にもつ 2次方程式は

$$t^2 - 18t + 77 = 0$$

$$(t-7)(t-11) = 0$$

$$t = 7, 11$$

$$a' \leq b' \text{ より}$$

$$a' = 7, b' = 11$$

よって

$$a = 21, b = 33$$

つまり、

求める2数は 21 と 33

a, b, c は、それぞれ5で割った余りが1, 2, 3となる正の整数である。 $a+2b+3c, abc$ を5で割った余りをそれぞれ求めよ。

解法1

a, b, c はそれぞれ5で割った

商を a', b', c' とおくと

$$\begin{cases} a = 5a' + 1 \\ b = 5b' + 2 \\ c = 5c' + 3 \end{cases}$$

と置き

$$\begin{aligned} a+2b+3c &= (5a'+1) + 2(5b'+2) + 3(5c'+3) \\ &= 5a' + 1 + 10b' + 4 + 15c' + 9 \\ &= 5a' + 10b' + 15c' + 14 \\ &= 5(a' + 2b' + 3c' + 2) + 4 \end{aligned}$$

よって、余り 4

$$abc = (5a'+1)(5b'+2)(5c'+3)$$

$$= (5a' \text{ 倍数}) + 6$$

$$= (5a' \text{ 倍数}) + 1$$

よって、余り 1

解法2

(mod 5 で考える.)

$$a \equiv 1, b \equiv 2, c \equiv 3$$

よって

$$\begin{aligned} a+2b+3c &\equiv 1+4+9 \\ &\equiv 14 \\ &\equiv \underline{4} \end{aligned}$$

$$abc \equiv 1 \times 2 \times 3$$

$$\equiv 6$$

$$\equiv \underline{1}$$

- (1) n が奇数ならば, n^2-1 は 8 で割り切れることを示せ。
 (2) 整数 n に対して, $2n^3-3n^2+n$ が 6 の倍数であることを示せ。

(1) (証明)

$$n = 2k-1 \quad (k \in \mathbb{Z}) \text{ とおく.}$$

このとき

$$\begin{aligned} n^2-1 &= (2k-1)^2-1 \\ &= 4k^2-4k \\ &= 4k(k-1) \end{aligned}$$

ここで

$k(k-1)$ は 連続 2 整数の積
 であるので 2 の倍数 である。

よって

n^2-1 は 8 で割り切れる。 ■

(2) (証明)

$$\begin{aligned} 2n^3-3n^2+n &= n(2n^2-3n+1) \\ &= n(2n-1)(n-1) \\ &= (n-1)n \{(n+1)+(n-2)\} \\ &= (n-1)n(n+1) + (n-2)(n-1)n \end{aligned}$$

$(n-1)n(n+1)$ も $(n-2)(n-1)n$ も

ともに、連続 3 整数の積 であるので

$3! = 6$ の倍数 である。

よって

$2n^3-3n^2+n$ は 6 の倍数 である。 ■

(1) a, b を自然数とする。 $4a+3b$ を 7 で割った余りが 3 で、 $3a+2b$ を 7 で割った余りが 5 であるとき、 a, b を 7 で割った余りをそれぞれ求めよ。

(2) m, n を整数とする。 $m-n$ を 3 で割った余りが k のとき、 m^3-n^3 を 3 で割った余りも k であることを示せ。

(1) 2013 名古屋学院大

(2) 2014 愛媛大

(1) 解法1

$4a+3b, 3a+2b$ を 7 で割った商をそれぞれ k_1, k_2 とおくと

$$\begin{cases} 4a+3b = 7k_1 + 3 & \text{--- ①} \\ 3a+2b = 7k_2 + 5 & \text{--- ②} \end{cases}$$

$$\text{①} \times 2 \quad 8a+6b = 14k_1+6$$

$$\text{②} \times 3 \quad 9a+6b = 21k_2+15 \quad (-)$$

$$-a = 14k_1 - 21k_2 - 9$$

$$a = 7(-2k_1 + 3k_2) + 9$$

$$= 7(-2k_1 + 3k_2 + 1) + 2$$

$$\text{①} \times 3 \quad 12a+9b = 21k_1+9$$

$$\text{②} \times 4 \quad 12a+8b = 28k_2+20 \quad (-)$$

$$b = 21k_1 - 28k_2 - 11$$

$$= 7(k_1 - 4k_2) - 11$$

$$= 7(k_1 - 4k_2 - 2) + 3$$

よって

a, b を 7 で割った余りはそれぞれ 2, 3

解法2

(mod 7 で考える)

$$\begin{cases} 4a+3b \equiv 3 & \text{--- ①} \\ 3a+2b \equiv 5 & \text{--- ②} \end{cases}$$

①+②

$$7a+5b \equiv 8$$

$$5b \equiv 1$$

$$15b \equiv 3$$

$$b \equiv 3$$

よって ① より

$$4a+9 \equiv 3$$

$$4a \equiv -6$$

$$4a \equiv 1$$

$$36a \equiv 9$$

$$a \equiv 2$$

よって $a \equiv 2, b \equiv 3$

(2) 証明1

$m-n$ を 3 で割った商を q とおくと

$$m-n = 3q + k$$

よって

$$m^3-n^3 = (m-n)(m^2+mn+n^2)$$

$$= (m-n)\{(m-n)^2+3mn\}$$

$$= (m-n)^3+3mn(m-n)$$

$$= (3q+k)^3+3mn(m-n)$$

$$= 27q^3+27q^2k+9qk^2+k^3+3mn(m-n)$$

$$= (3\alpha\text{倍数}) + k^3$$

($\therefore k^3 \pmod 3$ を考える)

k	0	1	2
k^3	0	1	8 ≡ 2

$$k^3 \equiv k \pmod 3$$

m^3-n^3 を 3 で割った余りも k である。

証明2

$$(m^3-n^3) - (m-n)$$

$$= (m^3-m) - (n^3-n)$$

$$= (m-1)m(m+1) - (n-1)n(n+1)$$

$(m-1)m(m+1), (n-1)n(n+1)$ とともに

連続3整数の積なので 3α 倍数

よって

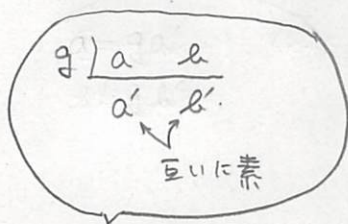
$$m^3-n^3 \text{ と } m-n \text{ を } 3 \text{ で割った余りは等しい。}$$

つまり

$$m^3-n^3 \text{ を } 3 \text{ で割った余りは } k \text{ である。}$$

2つの自然数 a, b ($a < b$) について, $a + b = 8075$ で, a, b の最小公倍数 l を最大公約数 g で割ったときの商が 84 である. このような a, b の組をすべて求めよ.

(東邦大)



$$a = ga', b = gb'$$

$\exists$ 満たす a', b' ($a' < b'$, a' と b' は互いに素) が存在する.

題意より

$$\begin{cases} ga' + gb' = 8075 \\ \frac{ga'b'}{g} = 84 \end{cases}$$

$$\Leftrightarrow \begin{cases} g(a' + b') = 8075 & \text{--- ①} \\ a'b' = 84 & \text{--- ②} \end{cases}$$

②より $(a', b') = (1, 84), (3, 28), (4, 21), (7, 12)$

(i) $(a', b') = (1, 84)$ のとき

①は

$$85g = 8075$$

$$g = 95$$

このとき

$$a = 95, b = 7980$$

(ii) $(a', b') = (3, 28)$ のとき

①は

$$31g = 8075$$

これを満たす $g \in \mathbb{Z}$ は存在しない.

(iii) $(a', b') = (4, 21)$ のとき

①は

$$25g = 8075$$

$$g = 323$$

このとき

$$a = 1292, b = 6783$$

(iv) $(a, b) = (7, 12)$ のとき

①は

$$19g = 8075$$

$$g = 425$$

このとき

$$a = 2975, b = 5100$$

(i) ~ (iv) より

$$(a, b) = (95, 7980), (1292, 6783), (2975, 5100)$$

自然数 P が 2 でも 3 でも割り切れないとき, $P^2 - 1$ が 24 で割り切れることを証明せよ。(1998 1-4492 清心女子大)

証明1

$$P = 6k+1, 6k+5 \quad (k \in \mathbb{Z})$$

で表される.

(i) $P = 6k+1$ のとき

$$P^2 - 1 = (P+1)(P-1)$$

$$= (6k+2) \cdot 6k$$

$$= 12k(k+1)$$

$k(k+1)$ は連続2整数の積なので

2の倍数である.

よって

$P^2 - 1$ は 24 で割り切れる.

(ii) $P = 6k+5$ のとき

$$P^2 - 1 = (P+1)(P-1)$$

$$= (6k+6)(6k+4)$$

$$= 6(k+1) \times 2(3k+2)$$

$$= 12(k+1) \{2k + (k+2)\}$$

$$= 24k(k+1) + 12(k+1)(k+2)$$

$(k+1)(k+2)$ は連続2整数の積なので

2の倍数である.

よって

$P^2 - 1$ は 24 で割り切れる.

(i), (ii) より

$P^2 - 1$ は 24 で割り切れる. ■

証明2

$$P^2 - 1 = (P+1)(P-1) \text{ であり}$$

$P-1, P, P+1$ は連続3整数で

P は 3の倍数ではないので

$P+1$ と $P-1$ のいずれかは

3の倍数である.

また, P は 2の倍数ではないので

$P+1$ と $P-1$ はともに 2の倍数で

あり. かつ, いずれかは 4の倍数である.

よって

$P^2 - 1$ は $3 \times 2 \times 4 = 24$ の倍数.

つまり

$P^2 - 1$ は 24 で割り切れる. ■

- (1) y が整数のとき, y^2+2 は5で割り切れないことを示せ。
 (2) $5x^2-2y^2=4$ を満たす整数 x, y の組は存在しないことを示せ。

(東京静大)

(1) (証明)

mod 5 で考えると

$$y \equiv 0 \text{ のとき } y^2+2 \equiv 2$$

$$y \equiv 1 \text{ のとき } y^2+2 \equiv 3$$

$$y \equiv 2 \text{ のとき } y^2+2 \equiv 6 \equiv 1$$

$$y \equiv 3 \text{ のとき } y^2+2 \equiv 11 \equiv 1$$

$$y \equiv 4 \text{ のとき } y^2+2 \equiv 18 \equiv 3$$

$$\text{よって } y^2+2 \not\equiv 0$$

■

(2) (証明)

$$5x^2-2y^2=4 \quad \text{より}$$

$$5x^2=2(y^2+2) \quad \text{————— ①}$$

ここで (1) より

$$y^2+2 \not\equiv 0 \pmod{5}$$

よって

① を満たす $x, y \in \mathbb{Z}$ は
 存在しない。

■

4個の整数 $n+1$, n^3+3 , n^5+5 , n^7+7 がすべて素数となるような正の整数 n は存在しない。これを証明せよ。

(2013 大阪大)

n	$n+1$	n^3+3	n^5+5	n^7+7
1	2	4	6	8
2	3	11	37	135
4	5	67	1029	16391
6	7	219		

$n=1, 2$ のときはすべて素数とはならないので

$n \geq 3$ で考えるとよい。

$n+1$ が素数となるためには

n が偶数であることが必要

このとき
 $\text{mod } 6$ とは

$n \equiv 0, 2, 4 \pmod{6}$ のいずれかである。

(i) $n \equiv 0 \pmod{6}$ のとき

$$n^3+3 \equiv 3$$

となり、これは3の倍数であることを示す。

さらに、上表より $n^3+3 > 3$

(ii) $n \equiv 2 \pmod{6}$ のとき

$$n^7+7 \equiv 128+7$$

$$\equiv 135$$

$$\equiv 3$$

となり、これは3の倍数であることを示す。

さらに、上表より $n^7+7 > 3$

(iii) $n \equiv 4 \pmod{6}$ のとき

$$n^5+5 \equiv 1024+5$$

$$\equiv 1029$$

$$\equiv 3$$

となり、これは3の倍数であることを示す。

さらに、上表より $n^5+5 > 3$

(i) ~ (iii) より

$n+1$, n^3+3 , n^5+5 , n^7+7 がすべて

素数となるような正の整数 n は存在しない。

n を正の整数とする。(1) n^2 と $2n+1$ は互いに素であることを示せ。(2) n^2+2 が $2n+1$ の倍数になる n を求めよ。

(一橋大)

(1) (証明)

 n^2 と $2n+1$ の最大公約数 g (>0) とおく。

$$\begin{cases} n^2 = ga & \text{--- ①} \\ 2n+1 = gb & \text{--- ②} \end{cases} \quad \left(\begin{array}{l} a, b \text{ は互いに素} \\ \text{な自然数} \end{array} \right)$$

と表すことができる。

① $\times 2$ $2n^2 = 2ga$

② $\times n$ $2n^2 + n = gbn$ (-
 $-n = g(2a - 2n) \text{ --- ③}$

② $2n+1 = ga$

③ $\times 2$ $-2n = g(4a - 2n) \text{ (+}$
 $1 = g(4a - 2n + n)$

$g, 4a - 2n + n \in \mathbb{Z}$ である。

$g = 1$

つまり、 n^2 と $2n+1$ は互いに素である。

(2)

n	n^2+2	$2n+1$
①	3	3
2	6	5
3	11	7
④	18	9
5	27	11
6	38	13
7	51	15
8	66	17
9	83	19
10	102	21
11	123	23
12	146	25
13	171	27

$n^2+2 = k(2n+1)$

を満たす $k \in \mathbb{Z}$ が存在するとい。

$2n+1 \neq 0$ である。

$$k = \frac{n^2+2}{2n+1}$$

$$= \frac{(n+\frac{1}{2})(n-\frac{1}{2}) + \frac{9}{4}}{2n+1}$$

$$= \frac{(2n+1)(2n-1) + 9}{4(2n+1)}$$

$$= \frac{1}{4} \left(2n+1 + \frac{9}{2n+1} \right)$$

よって k が整数 となるには $2n+1$ が 9 の約数 となること

が必要

$n \geq 1$ である $2n+1 \geq 3$

よって

$2n+1 = 3, 9$

つまり

$n = 1, 4$

逆にこのとき

$n=1$ とすると

$n^2+2=3, 2n+1=3$

となり 題意を満たす。

$n=4$ とすると

$n^2+2=18, 2n+1=9$

となり 題意を満たす。

よって

$n = 1, 4$

自然数 n に対して、 $3n^3+n$ と n^3+1 の最大公約数を g とする。

(1) すべての n について、 $g \neq 5$ であることを示せ。

(2) $g=14$ となるような n の最小値を求めよ。

(2017 学習院大)

(1) **証明1**

$g=5$ と仮定すると

$$\begin{cases} 3n^3+n = 5a & \text{--- ①} \\ n^3+1 = 5b & \text{--- ②} \end{cases} \quad (a, b \text{ は互いに素な自然数})$$

とできる。

$$\text{①} \quad 3n^3+n = 5a$$

$$\text{②} \times 3 \quad 3n^3+3 = 15b \quad (-)$$

$$n-3 = 5(a-3b)$$

$$n = 5(a-3b) + 3.$$

$$\therefore n \equiv 3 \pmod{5}$$

よって $n \equiv 3 \pmod{5}$ のとき

$$\begin{cases} 3n^3+n \equiv 81+3 \\ \equiv 84 \\ \equiv 4 \\ 5a \equiv 0 \end{cases}$$

これは ① に反する。

よって $g \neq 5$ である。

証明2

$$3n^3+n = (n^3+1) \times 3 + (n-3)$$

$$\left(\begin{array}{r|rrrrr} 3 & 1 & 0 & 0 & 1 \\ & 3 & 9 & 27 & \\ \hline & 1 & 3 & 9 & 28 \end{array} \right)$$

$$n^3+1 = (n-3)(n^2+3n+9) + 28$$

互除法の原理により

$$(3n^3+n, n^3+1) = (n^3+1, n-3)$$

$$= (n-3, 28)$$

$$= (n-3, 2^2 \times 7)$$

$$\neq 5$$

$$\therefore g \neq 5$$

(2)

$$g=14 \text{ のとき}$$

$$\begin{cases} 3n^3+n = 14a & \text{--- ③} \\ n^3+1 = 14b & \text{--- ④} \end{cases} \quad (a, b \text{ は互いに素な自然数})$$

とできる

$$\text{③} \quad 3n^3+n = 14a$$

$$\text{④} \times 3 \quad 3n^3+3 = 42b \quad (-)$$

$$n-3 = 14(a-3b)$$

$$n = 14(a-3b) + 3$$

$$\therefore n \equiv 3 \pmod{14}$$

$$n = 3 \text{ のとき}$$

$$\begin{cases} 3n^3+n = 81+3 = 84 \\ n^3+1 = 27+1 = 28 \end{cases}$$

$$\therefore \text{このとき } g = 28 \text{ となり不合理}$$

$$n = 17 \text{ のとき}$$

$$\begin{cases} 3n^3+n = 14739+17 = 14756 \\ n^3+1 = 4913+1 = 4914 \end{cases}$$

$$\therefore \text{このとき } g = 14 \text{ となり適する。}$$

$$\therefore \min n = 17$$

- (1) 任意の自然数 a に対し, a^2 を 3 で割った余りは 0 か 1 であることを証明せよ。
 (2) 自然数 a, b, c が $a^2 + b^2 = 3c^2$ を満たすと仮定すると, a, b, c はすべて 3 で割り切れなければならないことを証明せよ。
 (3) $a^2 + b^2 = 3c^2$ を満たす自然数 a, b, c の組は存在しないことを証明せよ。 (2014 九州大)

(1) (証明)

mod 3 で考える

$$\begin{cases} a \equiv 0 & a \text{ とき} & a^2 \equiv 0 \\ a \equiv 1 & a \text{ とき} & a^2 \equiv 1 \\ a \equiv 2 & a \text{ とき} & a^2 \equiv 4 \equiv 1 \end{cases}$$

よて,

 a^2 は 3 で割った余りは 0 か 1 である。

(2) (証明)

mod 3 で考える

$$3c^2 \equiv 0 \quad \text{より}$$

$$a^2 + b^2 \equiv 0$$

これを満たすとき, (1) より

$$a \equiv 0, b \equiv 0$$

このとき

$$a = 3k, b = 3l \quad (k, l \text{ は自然数})$$

とてき

$$3c^2 = 9k^2 + 9l^2$$

$$c^2 = 3k^2 + 3l^2$$

$$= 3(k^2 + l^2) \equiv 0$$

$$\text{よて } c \equiv 0$$

つまり,

 a, b, c はすべて 3 で割り切れなければならない。

(3) 証明 1

$$a^2 + b^2 = 3c^2 \quad \text{を満たすとき}$$

(2) より 自然数 a', b', c' を用いて

$$a = 3a', b = 3b', c = 3c'$$

とてき

$$9a'^2 + 9b'^2 = 27c'^2$$

$$a'^2 + b'^2 = 3c'^2$$

(2) より 自然数 a'', b'', c'' を用いて

$$a' = 3a'', b' = 3b'', c' = 3c''$$

とてき

$$9a''^2 + 9b''^2 = 27c''^2$$

$$a''^2 + b''^2 = 3c''^2$$

この操作は無限に繰り返される。

つまり,

 a, b, c は何度でも 3 で割れることが

でき, そのような自然数は存在しない。

証明 2

$$a^2 + b^2 = 3c^2 \quad \text{を満たす自然数 } a, b, c$$

の組のうち, a が最小となるような組を a_1, b_1, c_1 とする。(2) より, 自然数 a_2, b_2, c_2 を用いて

$$a_1 = 3a_2, b_1 = 3b_2, c_1 = 3c_2$$

とてき,

$$9a_2^2 + 9b_2^2 = 27c_2^2$$

$$a_2^2 + b_2^2 = 3c_2^2$$

したがって, a_2, b_2, c_2 は $a^2 + b^2 = 3c^2$ を満たす。(しかし, $a_2 < a_1$ となり, これは a_1 が最小であることに矛盾する。

よて,

 $a^2 + b^2 = 3c^2$ を満たす自然数 a, b, c は存在しない。

a, b は2以上の整数とする。

(1) $a^b - 1$ が素数ならば、 $a=2$ であり、かつ b は素数であることを証明せよ。

(2) $a^b + 1$ が素数ならば、 $b=2^c$ (c は整数) と表せることを証明せよ。

(2007 千葉大)

(1) (証明)

$$a^b - 1 = (a-1)(a^{b-1} + a^{b-2} + \dots + a + 1)$$

が素数 であるとき

$$a-1 < a^{b-1} + a^{b-2} + \dots + a + 1 \quad \text{なので}$$

$$a-1 = 1$$

$$\text{つまり } a = 2$$

このとき、 b が素数 でない と仮定すると、

$$b = pq \quad (p, q \text{ は } 2 \text{ 以上の整数}) \text{ とでき、}$$

$$2^{pq} - 1 = (2^p)^q - 1$$

$$= (2^p - 1) \left((2^p)^{q-1} + (2^p)^{q-2} + \dots + 2^p + 1 \right)$$

$$\text{となり } 2^p - 1 > 1, \quad (2^p)^{q-1} + (2^p)^{q-2} + \dots + 2^p + 1 > 1$$

なので、 $2^{pq} - 1$ が素数 であることに矛盾。

よって

$$a = 2, \text{ かつ } b \text{ は素数 である。}$$

(2) (証明)

$$b = 2^c \text{ と表せたり と仮定する。}$$

$$\text{つまり } b = 2^c k \quad (k \text{ は } 3 \text{ 以上の奇数}) \text{ である。}$$

このとき

$$a^b + 1 = a^{2^c k} + 1 = 1 + (a^{2^c})^k$$

$$\left(\begin{array}{l} \text{ここで} \\ n \text{ は奇数 として} \\ 1 - x + x^2 - x^3 + \dots + x^{n-1} = \frac{1 - (-x)^n}{1 - (-x)} \\ (1+x)(1-x+x^2-x^3+\dots+x^{n-1}) = 1+x^n \end{array} \right)$$

$$a^b + 1 = (1 + a^{2^c}) \left(1 - a^{2^c} + (a^{2^c})^2 - (a^{2^c})^3 + \dots + (a^{2^c})^{k-1} \right)$$

であり、

$$1 + a^{2^c} > 1, \quad 1 - a^{2^c} + (a^{2^c})^2 - (a^{2^c})^3 + \dots + (a^{2^c})^{k-1} > 1$$

なので、 $a^b + 1$ が素数 であることに矛盾

よって

$$b = 2^c \text{ と表せる。}$$