

## 2020 年後期

$a, b$  を正の整数とする.

- (1)  $a$  が  $b$  の倍数ならば,  $2^a - 1$  は  $2^b - 1$  の倍数であることを示せ.
- (2)  $2^a - 1$  が素数ならば,  $a$  は素数であることを示せ.
- (3)  $2^a - 1 = (2a + 1)(8a + 1)$  を満たす  $a$  を求めよ.

**考え方** (1) は「 $a$  が  $b$  の倍数」なので, 例えば  $a = 3b$  などとすると

$$2^a - 1 = 2^{3b} - 1 = (2^b)^3 - 1 = (2^b - 1)((2^b)^2 + 2^b + 1)$$

なので,  $2^a - 1$  は  $2^b - 1$  の倍数であることがわかります. つまり, 「 $a$  は  $b$  の  $n$  倍」とすれば, 要するに,  $x^n - 1$  の有名な因数分解をやるだけのことになります.

(2) ですが, 「素数であること」を証明するのは難しい (ていうか不可能). しかし, 「素数でないこと」を証明するのは簡単です. なぜなら, 「素数でない」= 「1 以外の 2 整数の積で表せる」からです. ということは, 待遇命題を証明するのが良いでしょう. つまり

$$a \text{ が素数でない} \implies 2^a - 1 \text{ は素数でない}$$

を示します. その過程で, (1) の結果を使うことに気づくでしょう.

(3) が「クセモノ」です. 当然ながら, 「(1)(2) の結果を使うのだろう」と思って取り組みますが, 全く糸口が見えません.

実は, 一橋大学の HP には「出題意図」なるものが公開されています (ぜひ一度見てみてください). この問題の主題意図を見てみるとビックリしました. 以下, HP からの抜粋

**1** 整数の性質について、特に  $2^n - 1$  と  $n$  の関係についての問題である。

- (1) は等比級数の和の公式を用いることで解くことができる。
- (2) は (1) の結果を用いることで解くことができる。
- (3) は  $a$  がある程度大きいときには左辺が常に右辺より大きくなることから  $a$  の範囲を限定

し、整数解を求めることができる。

この問題からわかるように、 $2^n - 1$  が素数となるためには  $n$  が素数でなければならないが、逆は必ずしも成り立たない。

整数の剰余の性質について理解しているか、また、解の範囲を限定して整数解を求める等の操作を適切に行うことができるか確認するために出題した。

爆笑ものなの、分かります？

「(2) で

$$2^a - 1 \text{ が素数} \implies a \text{ は素数}$$

を証明しましたが、その逆

$$a \text{ が素数} \implies 2^a - 1 \text{ は素数}$$

は必ずしも成り立ちませんよ. その具体例として (3) を出題しました.  $a$  が素数のときでも,  $2^a - 1$  は素数にならないこともあるんですよ. というだけのようです. つまり, (1)(2) は全く不要 (爆笑).

それだったら, ノーヒントでいきなり (3) を出題した方が正答率は上がったかもしれませんね.

方針としては, 指数関数と 2 次関数のグラフの形状から, 解の個数は 1 個か 2 個, それも, それほど大きくない場所にあるだろうと見越して, 実験していき, 予想して証明します.

2016 年後期の問題も参照してください.

**解**

(1)  $a$  が  $b$  の倍数であるので,  $a = nb$  とおく. このとき,

$$\begin{aligned} & 2^a - 2 \\ &= 2^{nb} - 2 \\ &= (2^b)^n - 2 \\ &= (2^b - 1)((2^b)^{n-1} + (2^b)^{n-2} + \dots + 2^b + 1) \end{aligned}$$

$(2^b)^{n-1} + (2^b)^{n-2} + \dots + 2^b + 1$  は整数であるので、 $2^a - 1$  は  $2^b - 1$  の倍数である。

(2)  $a$  が素数でないを仮定する。

(i)  $a = 1$  のとき、 $2^a - 1 = 1$  は素数ではない。

(ii)  $a \geq 2$  のとき、 $a$  は 2 以上の 2 つの整数の積で表される。つまり、 $a = pq$  とおける。

このとき、 $a$  は  $p$  の倍数になるので、(1) の結果より、 $2^a - 1$  は  $2^p - 1$  の倍数である。 $2^p - 1 \neq 1$  なので、 $2^a - 1$  は素数ではない。

よって、

$$a \text{ が素数でない} \implies 2^a - 1 \text{ は素数でない}$$

が証明されたので、対偶をとって、

$$2^a - 1 \text{ が素数} \implies a \text{ は素数}$$

が示された。

(3)  $2^a - 1 = (2a + 1)(8a + 1)$  より

$$2^a - 1 = 16a^2 + 10a + 1$$

$$2^a = 16a^2 + 10a + 2$$

$$2^{a-1} = 8a^2 + 5a + 1$$

$a$	$2^{a-1}$	$8a^2 + 5a + 1$
1	1	14
2	2	43
3	4	88
4	8	149
5	16	226
6	32	319
7	64	428
8	128	553
9	256	689
10	512	852
11	1024	1024
12	2048	1213
13	4096	1418

よって、 $1 \leq a \leq 11$  で、 $2^{a-1} = 8a^2 + 5a + 1$  となるのは、 $a = 11$  のときのみである。

$a \geq 12$  のとき

$$2^{a-1} > 8a^2 + 5a + 1$$

であることを数学的帰納法で示す。

[I]  $n = 12$  のとき

[II]  $n = k$  のとき成立するとすると

$$2^{k-1} > 8k^2 + 5k + 1$$

$n = k + 1$  のときの差を考えると

$$\begin{aligned} & 2^{(k+1)-1} - \{8(k+1)^2 + 5(k+1) + 1\} \\ &= 2 \cdot 2^{k-1} - \{8(k+1)^2 + 5(k+1) + 1\} \\ &> 2(8k^2 + 5k + 1) - (8k^2 + 16k + 8 + 5k + 5 + 1) \\ &= 8k^2 - 11k - 12 \\ &= 7k^2 + (k+1)(k-12) \geq 0 (\because k \geq 12) \end{aligned}$$

$$\therefore 2^{(k+1)-1} > \{8(k+1)^2 + 5(k+1) + 1\}$$

よって、 $n = k + 1$  のときも成立する。

[I][II] より、 $a \geq 12$  のとき、

$$2^{a-1} > 8k^2 + 5k + 1 \text{ である。}$$

したがって、以上より、 $2^{a-1} = 8a^2 + 5a + 1$  となるのは、 $a = 11$  のときのみである。

$$\therefore a = 11$$

■

**参考**  $2^{a-1} = 8a^2 + 5a + 1$  の式から、 $a$  についてもう少しいろいろなことが分かります。

まず、 $a \geq 1$  なので、(右辺)  $\geq 14$  となるので、 $a \geq 4$  であることが分かります。つまり、**解** で作った表は  $a = 1, 2, 3$  の部分は不要だったわけです。

さらに、 $a \geq 4$  ということは、(左辺) は 8 の倍数になるの、 $5a + 1$  も 8 の倍数であることが分かります。

$$5 \cdot 1 + 1 = 6$$

$$5 \cdot 2 + 1 = 11$$

$$5 \cdot 3 + 1 = 16$$

$$5 \cdot 4 + 1 = 21$$

$$5 \cdot 5 + 1 = 26$$

$$5 \cdot 6 + 1 = 31$$

$$5 \cdot 7 + 1 = 36$$

なので、 $5a + 1$  が 8 の倍数になるのは、

$$a \equiv 3 \pmod{8}$$

です。 $a \geq 4$  なので、等式を満たす最小の  $a$  は 11 であろうと予想できます。