

$n \mid 2^n + 1$ を満たす整数について

ナム 3

2026 年 8 月 3 日

正の整数 n について

$$n \mid 2^n + 1 \quad (1)$$

という条件を考える。最初に見つかるのは 1, 3, 9, 27 で、しばらくは 3 のべきしかないと思っていた。ところが 171 も条件を満たす。

以下では、(1) を満たす数に名前を付け、3 のべきが解になる理由、新しい解を作る方法、解に必ず現れる素因数の順に整理する。完全な分類ではないが、何が分かっているかまでは一つの形にできた。

| という記号

最初に、題名にも使った記号について書いておく。整数 a, b に対して

$$a \mid b$$

と書いたら、「 a は b を割り切る」という意味である。もう少し正確には、ある整数 k を使って

$$b = ak$$

と書けるという意味になる。たとえば $18 = 6 \cdot 3$ だから $6 \mid 18$ であり、 $18 = 5k$ となる整数 k はないので $5 \nmid 18$ である。割り切れないときは、縦線に斜線を重ねた $\nmid$ を使う。

分数の計算をしているわけではないのに、数と数の間へ縦線を一本置くだけで「割った余りが 0」という条件を書ける。この記号を使うと、(1) は「 $2^n + 1$ を n で割った余りが 0 になる n を探す」という問題を一行にできる。

同じ条件を合同式で書けば

$$n \mid 2^n + 1 \iff 2^n \equiv -1 \pmod{n} \quad (2)$$

となる。左側は割り切れることを見たいとき、右側は累乗の余りを計算したいときに使いやすい。このノートでは、同じ条件を場面によって二通りに書く。

1 良い数

定義 1.1. 正の整数 n が

$$2^n \equiv -1 \pmod{n}$$

を満たすとき、ここでは n を**良い数**と呼ぶ。また、良い数全体を $\mathcal{G}$ と書く。

この呼び方はこのノートの中だけのもので、一般に使われている用語ではない。

例 1.2. 1, 3, 9 は良い数である。実際、 $3 \mid 9$ であり、 $9 \mid 513 = 2^9 + 1$ である。一方、5 は $2^5 + 1 = 33$ を割らないので良い数ではない。

命題 1.3. $n > 1$ が良い数なら、 n は奇数である。

証明. n が偶数なら n は 2 で割り切れるが、 $2^n + 1$ は奇数である。したがって $n \mid 2^n + 1$ とはならない。 $\square$

偶数はここで全部除かれる。以下では奇数だけを考える。

2 3のべきが並ぶ理由

$3, 9, 27, \dots$ を一つずつ確かめる代わりに、 $2^m + 1$ が 3 で何回割れるかを数える。

定義 2.1. 素数 p と 0 でない整数 N に対して、 $p^a \mid N$ となる最大の非負整数 a を

$$v_p(N)$$

と書き、 N の p 進付値と呼ぶ。たとえば $72 = 2^3 \cdot 3^2$ なので、 $v_2(72) = 3$, $v_3(72) = 2$ である。

奇数 m について、LTE の補題の $p = 3$ の場合から

$$v_3(2^m + 1) = v_3(2 + 1) + v_3(m) = 1 + v_3(m) \quad (3)$$

となる。

命題 2.2. 任意の $a \geq 1$ について、 3^a は良い数である。

証明. 式 (3) で $m = 3^a$ とすると

$$v_3(2^{3^a} + 1) = a + 1$$

である。よって $2^{3^a} + 1$ は 3^a で割り切れる。 □

実際には 3^a より一つ多い 3 まで因数に含まれている。この余分な因数が、次の解を作るときに関係する。

3 良い数を増やす

$a = 2$ の場合を実際に因数分解すると

$$2^9 + 1 = 513 = 3^3 \cdot 19 \quad (4)$$

となる。9 が必要としている 3^2 のほかに、3 と 19 が余っている。このうち 19 を 9 へ掛けると、別の良い数が得られる。

定理 3.1 (因数を付け足す操作). $n \in \mathcal{G}$ とする。奇数 m が

$$m \mid 2^n + 1, \quad \gcd(m, n) = 1$$

を満たすなら、 $nm \in \mathcal{G}$ である。

証明. n が良い数で、 m は奇数だから

$$2^{nm} = (2^n)^m \equiv (-1)^m = -1 \pmod{n}.$$

また $m \mid 2^n + 1$ から、同じ計算を m を法として行えて

$$2^{nm} = (2^n)^m \equiv (-1)^m = -1 \pmod{m}.$$

n と m は互いに素なので、二つを合わせると $2^{nm} \equiv -1 \pmod{nm}$ となる。 □

例 3.2. $9 \in \mathcal{G}$ であり、式 (4) より $19 \mid 2^9 + 1$ 、また $\gcd(9, 19) = 1$ である。したがって

$$171 = 9 \cdot 19 \in \mathcal{G}.$$

$2^{171} + 1$ を十進数で書かなくても、割り切れることが分かる。

注意. 互いに素という条件は外せない。 $n = 3$ では $2^3 + 1 = 9$ だが、 $m = 9$ は n と共通因数を持つので、この定理から 27 が良い数だとはいえない。3 の指数を増やす部分は、式 (3) で別に扱っている。

4 最小の素因数

次は、良い数にどの素数が入るかを考える。そのために位数を使う。

定義 4.1. 奇素数 p に対して

$$2^r \equiv 1 \pmod{p}$$

となる最小の正の整数 r を、 p を法とする 2 の**位数**と呼び、 $\text{ord}_p(2)$ と書く。

たとえば $2^1 \equiv -1 \pmod{3}$ 、 $2^2 \equiv 1 \pmod{3}$ なので、 $\text{ord}_3(2) = 2$ である。Fermat の小定理から、 $\text{ord}_p(2)$ は $p-1$ の約数になる。

定理 4.2. $n > 1$ が良い数なら、 n の最小の素因数は 3 である。特に、すべての $n \in \mathcal{G} \setminus \{1\}$ は 3 の倍数である。

証明. p を n の最小の素因数とし、 $r = \text{ord}_p(2)$ とおく。 $2^n \equiv -1 \pmod{p}$ だから

$$r \mid 2n, \quad r \nmid n.$$

n は奇数なので、 $r = 2d$ かつ $d \mid n$ となる。一方、 $r \mid p-1$ より

$$2d \leq p-1. \tag{5}$$

もし $d > 1$ なら、 d の素因数は n の素因数でもある。 p がその中で最小だから $d \geq p$ となり、式 (5) と矛盾する。よって $d = 1$ 、したがって $r = 2$ である。

2 の位数が 2 であることから $2 \equiv -1 \pmod{p}$ となるので、 $p \mid 3$ である。ゆえに $p = 3$ である。□

5 二種類の増え方

ここまでの内容から、良い数が増える仕組みは少なくとも二つある。

1. すでに含まれる 3 の指数を、付値を使って増やす。
2. $2^n + 1$ に現れた n と互いに素な奇因数を、定理 3.1 で n へ付け足す。

最初の予想は

$$\mathcal{G} = \{1, 3, 9, 27, \dots\}$$

だったが、171 が反例になった。今分かっている範囲は

$$\{1, 3, 9, 27, 81, \dots\} \subsetneq \mathcal{G}, \quad n \in \mathcal{G}, n > 1 \implies 3 \mid n$$

とまとめられる。

二種類の操作だけですべての良い数が得られるかは分らない。また 171 の先へ同じ方法で進むには、 $2^{171} + 1$ の因数を知る必要がある。完全な一覧より先に、解の作られ方の一部が見えたところで、今回は止めることにした。

参考にしたもの

式 (3) では LTE の補題を使った。位数については、初等整数論の本にある Fermat の小定理と位数の基本性質を参照した。定理 3.1 と、最小素因数を使った定理 4.2 の証明は、この問題について考えたものを整理した。