

素数の累乗と約数の総和の関係について ～倍積完全数に迫る～

愛媛県立松山南高等学校 数学班

村上和馬

指導教諭 福澤純治 笹岡慎太郎

1. 背景・目的

整数は日常にあふれ、特別な意味を持つようには見えない。だが数学的な考察を試みればその整数には、4は平方数、5は素数等と、個々に違った特徴があることが分かる。私はこのような整数の不思議な性質に興味を持ったため、数論の研究を始めた。数論の中でも私は完全数に着目した。完全数とは、その正の約数の総和が元の数の2倍になる数のことである。完全数について調べるうちに倍積完全数というものを見つけた。これは完全数が元の数の2倍であるのに対し、それを自然数倍まで拡張したものである。倍積完全数の中でも2倍完全数は完全数のことである。そこで、倍積完全数で一般的な理論が完成すればそれが完全数にも適応でき、間接的に完全数を研究できると考え、倍積完全数を研究することにした。

2. 方法

「素数の累乗」とその「約数の総和の素因数分解」の対応表を独自に作成し、倍積完全数の性質を探る。特に、「素数の累乗」とその「約数の総和の素因数分解」の関連性を探る。

3. 倍積完全数の性質

「素数の累乗」とその「約数の総和の素因数分解」の対応表（表1）のA列から数を選択し、選んだA列に対応するB列の数をすべて掛け合わせることで倍積完全数を作ることができる。

表1 「素数の累乗（A）」とその「約数の総和の素因数分解（B）」

| A ₁ | B ₁ | A ₂ | B ₂ | A ₃ | B ₃ | A ₄ | B ₄ |
|----------------|-------------------|----------------|----------------------|----------------|--------------------------|----------------|--------------------------------------|
| 2 | 3 | 3 | 2 ² | 5 | 2×3 | 7 | 2 ³ |
| 2 ² | 7 | 3 ² | 13 | 5 ² | 31 | 7 ² | 3×19 |
| 2 ³ | 3×5 | 3 ³ | 2 ³ ×5 | 5 ³ | 2 ² ×3×13 | 7 ³ | 2 ⁴ ×5 ² |
| 2 ⁴ | 31 | 3 ⁴ | 11 ² | 5 ⁴ | 11×17 | 7 ⁴ | 2801 |
| 2 ⁵ | 3 ² ×7 | 3 ⁵ | 2 ² ×3×7 | 5 ⁵ | 2×3 ² ×7×31 | 7 ⁵ | 2 ³ ×3×19×43 |
| 2 ⁶ | 127 | 3 ⁶ | 1093 | 5 ⁶ | 19531 | 7 ⁶ | 29×4733 |
| 2 ⁷ | 3×5×17 | 3 ⁷ | 2 ⁴ ×5×41 | 5 ⁷ | 2 ³ ×3×13×313 | 7 ⁷ | 2 ⁵ ×5 ² ×1201 |
| 2 ⁸ | 7×73 | 3 ⁸ | 13×757 | 5 ⁸ | 19×31×829 | 7 ⁸ | 3 ² ×19×37×1063 |

(nを自然数、 $\sigma(n)$ をnの約数の総和、 $k = \frac{\sigma(n)}{n}$ として、k倍完全数とする。)

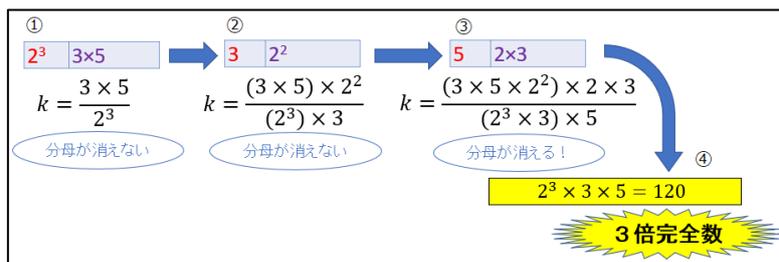


図1 表を用いた倍積完全数の作り方

例として、3倍完全数120を作る過程を示す。

4. 主張と整理

以上のことを踏まえて、以下に主張としてまとめる。

表3の素因数5の列について、指数が規則的に現れるということは「素数の累乗の約数の総和が5の倍数であるものが規則的に現れている」と言い換えられる。ここで逆に、素数2の累乗の約数の総和が5の倍数であるための必要十分条件を考えてみる。

$$\sigma(2^n) = 1 + 2^2 + 2^3 + \dots + 2^n + 2^{n+1}$$

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

つまり、 $2^{n+1} - 1 \equiv 0 \pmod{5}$ であればよい。

$$2^{n+1} \equiv 1 \pmod{5}$$

ここで2の累乗が5で割って1余るとき、その指数を1ずつ増やすとその余りは

$$1, 2, 4, 3, 1, 2, 4, \dots$$

というように4つずつ循環することがわかる(図2)。

つまり、 $\sigma(2^n)$ (n は自然数)が5の倍数であるような自然数 n は4個の連続する自然数の中に1個ずつ定期的に表れることがわかる。実際に表3で確認すると4個に1個ずつ素因数5が現れることが確認された。

これを合同式で表現すると、約数の総和が5の倍数になるような最小の2の累乗は 2^3 で、ここから指数が4ずつ増えるから、 $\sigma(2^{4n-1}) \equiv 0 \pmod{5}$ となる。

この例から、素数の累乗をそれと異なる素数で割った余りの周期は、表3にみられる周期に密接に関係しているのではないかと考えた。

ここで、先ほどの式を一般化した主張を次のようにまとめた。

p, a を相異なる素数、 n を自然数とする。 s を、 p で a の累乗を割った余りの循環の周期であるとする。

このとき、 $\sigma(a^{sn-1}) \equiv 0 \pmod{p}$

別の表現をすると

$$\sigma(a^{sn-1}) = a^{sn} - 1 \equiv 0 \pmod{p}$$

$$a^{sn} \equiv 1 \pmod{p}$$

ここで、 p, a は相異なる素数であるから互いに素、フェルマーの小定理より

$$a^{p-1} \equiv 1 \pmod{p}$$

つまり

$$a^{p-1} \equiv a^{sn} \pmod{p}$$

底 a が両辺で共通で、素数 p で割った余りが等しいから、指数について、 $p-1$ と sn は s を法として合同となる。(∵ s は a の累乗を素数 p で割った余りの周期)つまり

$$p-1 \equiv sn \pmod{s}$$

$$p-1 \equiv 0 \pmod{s}$$

つまり、 s は $p-1$ の約数となる。

これによって、周期 s が $p-1$ の約数であることを示せば、 s と表3にみられる周期が密接に関係しているといえる。実際に表で確認したところ確認できる範囲内のすべての場所で s は $p-1$ の約数

となった。また、 $\frac{p-1}{s}$ を実際に求めてみたが(表4)そこに法則性のようなものは今のところ見出すことができなかった。

| |
|--------------------------------------|
| $2^{n+1} \equiv 1 \pmod{5}$ |
| $2^{n+2} \equiv 2 \pmod{5}$ |
| $2^{n+3} \equiv 4 \pmod{5}$ |
| $2^{n+4} \equiv 8 \equiv 3 \pmod{5}$ |
| $2^{n+5} \equiv 6 \equiv 1 \pmod{5}$ |

図2 5で割った余りの進行

表4 a = 2の場合の $\frac{p-1}{s}$

| | | | | | | | | | | |
|-----------------|---|---|---|----|----|----|----|----|----|----|
| p | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
| s | 2 | 4 | 3 | 10 | 12 | 8 | 18 | 11 | 28 | 5 |
| $\frac{p-1}{s}$ | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 6 |

5. 今後の課題

表1でA列から選んだ数がどのような条件をみたすべきかについては明らかになっている。ここでB列に該当する素数の累乗の約数の総和に規則性や法則性が見つかれば、素数の累乗の約数の総和をある程度予測することができるようになるため、A列から数を選ぶ手順を推察することができる。また、今まではそれぞれの表を作るときに、

[素数の累乗を計算→その約数の総和を求める→それを素因数分解する]

という時間のかかる手順を踏んでいた。素数の累乗を順に計算するということは等比数列を1つずつ順に求めているようなもので数が非常に大きなものになりやすく、計算に時間が掛かる上、コンピュータでは処理できないほど大きな数になってしまうことがよくあり、パソコンがフリーズするという事態もしばしば見られたため、作業の効率化を図りたい。

主張をある程度まとめることはできたが、証明しようと思うと難解であった。だが、これを証明することができれば、表3の規則性と4.主張と整理で用いたsが完全に結びつくことになり、問題になっていることを別の角度から見つめることができるようになるので、この主張の証明を進めるとともに、素数の累乗をそれと異なる素数で割った時のあまりの周期についても調べていきたいと思う。

6. 参考文献

- ・ The Multiply Perfect Numbers Page 「<http://www.homes.uni-bielefeld.de/achim/mpn.html>」
- ・ オンライン整数列大辞典 「<https://oeis.org/>」