連続する数について

5 年 C 組　古宮　昌典
指導教員　川口　慎二

１．要約

サイエンス研究会数学班 5 年生は数論について研究している。今回は、ある条件を満たす連続する整数について自ら課題を設定し、それらの問題を解くことを目標とした。また、その目標のために数論における有名な定理について学習した。

キーワード　　素数、不足数、完全数、過剰数、原始過剰数、累乗数

２．研究の背景と目的

参考文献[1]に、「2 以上の任意の整数 n において、連続する n 個の合成数が存在することを示せ」という問題が記載されていた。では、他の特徴をもつ数について、連続するものは存在するのか、あるいは存在しないのかについて考え、本稿にまとめることにした。

３．研究内容

３－１．素数

先ほど挙げた問題は以下のように証明できる。

<u>定理１</u>

2 以上の任意の整数 n において、連続する n 個の合成数が存在する。

（証明）

$n \geqq 2$ において、連続する n 個の整数 $(n+1)!+2,\ (n+1)!+3,\ \cdots,\ (n+1)!+(n+1)$ はすべて合成数である。 (Q. E. D.)

定理１は、「素数とその次の素数の差はいくらでも大きい値をとりえる」と言い換えることができる。

次に、素数の分布について、2, 3 以外の素数はすべて $6n-1$ または $6n+1$ とかける。そこで、次の命題について考えた。

<u>命題１</u>

正の整数 n について、$6n-1$ または $6n+1$ は素数である。

この命題は、$n=1, 2, \cdots, 19$ で条件を満たすが、$n=20$ に対して、$121=11^2$, $119=7\times17$ であるので、偽である。

では、$n=20$ のときのように $6n-1$ と $6n+1$ がどちらも合成数となるような n はどれだけ存在するのかについて考えたところ、以下の定理を得た。

<u>定理２</u>

正の整数 n であって、$6n-1$ と $6n+1$ がともに合成数であるようなものが無数に存在する。

（証明）

任意の非負整数kについて、

$$6(20+77\mathrm{k})-1=119+6\times 77k$$
$$=7(17+66k)$$
$$6(20+77\mathrm{k})+1=121+6\times 77k$$
$$=11(11+42k)$$

より、$n=20+77k$とすれば条件を満たすので、求めるnは無数に存在する。

(Q. E. D.)

また、$6n-1$と$6n+1$のうち一方だけが素数であるようなnについても以下の結果を得た。

定理３

正の整数nであって、$6n-1$と$6n+1$のうち一方だけが素数であるようなものが無数に存在する。

この証明には、以下の補題を用いる。

補題１（ディリクレの算術級数定理）

初項a, 公差d（aとdは互いに素)の等差数列には素数が無数に含まれる。

（証明）

いま、任意の非負整数kについて、

$$6(20+7k)-1=119+6\times 7k$$
$$=7(17+6k)$$

は合成数である。このとき、

$$6(20+7k)+1=121+42k$$

となる。補題より、数列$\{121+42k\}$には素数が無数に現れるので、$n=20+7k$とすれば、一方だけが素数であるようなものが無数に存在することがわかる。 (Q. E. D.)

では、$6n-1$と$6n+1$がともに素数となる場合を考えると、これらは双子素数であるため、双子素数予想(未解決)と同値である。

３－２．不足数、完全数、過剰数

不足数、完全数、過剰数については以下の定理が成り立つことがわかった。

定理４

(1) 連続するa個の不足数が存在するようなaの最大値は５である。

(2) 連続するb個の完全数が存在するようなbは存在しない。

(3) 2以上の任意の整数cについて、連続するc個の過剰数が存在する。

（証明）

(1) まず、以下の補題が成り立つ（参考文献[2]参照）。

補題２

過剰数の倍数は過剰数であり、完全数の倍数は自身を除いて過剰数である。

（補題２の証明）

過剰数Nの約数を

$$1=d_0,d_1,d_2,\cdots,d_m=N$$

とする。このとき、以下が成り立つ。

$$d_0+d_1+d_2+\cdots+d_m>2N$$

両辺をk倍(kは自然数)して、

$$kd_0+kd_1+kd_2+\cdots+kd_m>2kN$$

いま、$0\leqq i\leqq m$においてd_iはNを割り切るので、正の整数kにおいてkd_iはkNを割り切る。すなわちkd_iはkNの約数であるから、kNの約数の総和は$2kN$より大きい。つまり、過剰数の倍数kNは過剰数である。

完全数については、

$$kd_0 + kd_1 + kd_2 + \cdots + kd_m = 2kN$$

となるが、$k \geqq 2$ のとき、$kd_0 = k \neq 1$ であるから、$kd_0, kd_1, kd_2, \cdots, kd_m$ の中に kN の約数である 1 は含まれていない。よって、kN の約数の総和は $2kN$ よりも大きいので完全数の倍数(自身を除く)は過剰数である。

(Q. E. D.)

6 が完全数であることは容易に確認できるので、補題２より、6 以外の 6 の倍数はすべて過剰数である。6 の倍数は連続する 6 個の数の中に 1 つだけ含まれるので、a は 5 以下である。実際、7, 8, 9, 10, 11 は連続する 5 個の不足数である。つまり a の最大値は 5 である。 (Q. E. D.)

(2) まず、以下の補題が成り立つ（参考文献[3]参照)。

<u>補題３</u>

偶数の完全数はすべて $2^{m-1}\left(2^m - 1\right)$ （ただし、$2^m - 1$ は素数)の形で表される。

（補題３の証明）

偶数の完全数 N において 2 以上の整数 m と 3 以上の奇数 k が存在して、

$$N = 2^{m-1}k$$

とかける。また、正の整数 n の正の約数の総和を $\sigma(n)$ と表すことにすると、N は完全数であるから、

$$2N = \sigma(N)$$

$$= \sigma\left(2^{m-1}\right)\sigma(k) = \left(2^m - 1\right)\sigma(k)$$

が成り立つ。ゆえに、

$$2 \cdot 2^{m-1}k = \left(2^m - 1\right)\sigma(k)$$

$$\sigma(k) = k + \frac{k}{2^m - 1}$$

を得る。ここで、$\sigma(k)$ と k はどちらも整数なので、$\dfrac{k}{2^m - 1}$ は整数である。つまり、$2^m - 1$ は k の約数であることがわかるので、$\dfrac{k}{2^m - 1}$ も k の約数である。したがって、k の約数は k と $\dfrac{k}{2^m - 1}$ だけである。よって $\dfrac{k}{2^m - 1} = 1$, すなわち $N = 2^{m-1}(2^m - 1)$ とかける。さらに、$k = 2^m - 1$ は 1 と自身以外の約数を持たないので、$2^m - 1$ は素数である。 (Q. E. D.)

連続する完全数が存在しないことを背理法で示す。それには $b = 2$ のときを考えれば十分である。いま、連続する 2 つの完全数が存在したと仮定すると、補題３より、ある正の整数 p が存在し、

$$2^{p-1}\left(2^p - 1\right) + 1 \quad \text{または} \quad 2^{p-1}\left(2^p - 1\right) - 1$$

が完全数である。

(Ⅰ) $2^{p-1}\left(2^p - 1\right) + 1$ が完全数である場合

$2^{p-1}\left(2^p - 1\right) + 1 = A$ とおく。補題３より、$2^p - 1$ は素数である。いま、p が合成数であると仮定すると、2 以上の整数 d, e によって $p = de$ と表すことができる。すると、

$$2^p-1=2^{de}-1=\left(2^d\right)^e-1$$

が成り立つが、これは$2^d-1>1$で割り切れるので矛盾が生じる。つまり p は素数でなくてはならない。

$p=2$ のとき、$2^{p-1}\left(2^p-1\right)=6$ であるが、$A=7$ は完全数でない。

p が奇素数であるとき、

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

$$\equiv(-1)^{p-1}\left\{(-1)^p-1\right\}+1$$

$$\equiv 1 \pmod 3 \quad \cdots①$$

が成り立つ。

いま、A の正の約数を $f_1<f_2<\cdots<f_\alpha$ とおく。A は奇数であるから、$f_1, f_2, \cdots, f_\alpha$ はすべて奇数である。

ここで、A が平方数であると仮定すると、α は奇数であるから、約数の総和は奇数となる。しかし A は完全数であるから約数の総和は $2A$ に等しくなければならず、これは矛盾である。

よって A は平方数ではなく、α は偶数である。ここで、$\dfrac{\alpha}{2}=t$ とおくと

$$A=f_1f_\alpha=f_2f_{\alpha-1}=\cdots=f_tf_{t+1}$$

が成り立つ。いま、$1≦j≦t$ の任意の整数 j において、$\left(f_j, f_{\alpha+1-j}\right)$ という組合せは mod 3において(1, 1), (1, −1), (−1, −1)のいずれかと等しいが、①より、2 数の積は−1 と合同である必要があり、それは(1, −1)でのみ実現されるので$\left(f_j, f_{\alpha+1-j}\right)$の組合せは(1, −1)と等しい。ゆえに、

$$f_j+f_{\alpha+1-j}\equiv 1-1=0 \pmod 3$$

が成り立つので、A の約数の総和

$$f_1+f_2+f_3+\cdots+f_\alpha$$

は 3 の倍数となる。これは①に矛盾する。ゆえに、A は完全数でない。

(Ⅱ) $2^{p-1}\left(2^p-1\right)-1$ が完全数である場合

$2^{p-1}\left(2^p-1\right)-1=B$ とおく。(Ⅰ)と同様の議論により、p が奇素数である場合を考えればよい。このとき、$p≧3$ であるから

$$B=2^{p-1}\left(2^p-1\right)-1$$

$$\equiv -1 \pmod 4 \quad \cdots②$$

が成り立つ。

B の正の約数を

$$g_1<g_2<g_3<\cdots<g_\beta$$

とする。再び(Ⅰ)と同じ議論により B は平方数ではなく、β は偶数であることがわかる。$\dfrac{\beta}{2}=s$ とおくと、

$$B=g_1g_\beta=g_2g_{\beta-1}=\cdots=g_sg_{s+1}$$

が成り立つ。

いま、$1≦u≦s$ の任意の整数 u において、$\left(g_u, g_{\beta+1-u}\right)$ という組合せは、mod 4 において、(1, 1), (1, −1), (−1, −1)のいずれかと等しいが、①より、2 数の積は−1と合同である必要があり、それは(1, −1)でのみ実現されるので、$\left(g_u, g_{\beta+1-u}\right)$ の組合せは(1, −1)と等しい。ゆえに、

$$g_u + g_{\beta+1-u} \equiv 1-1 = 0 \pmod 4$$

が成り立つので、B の約数の総和

$$g_1 + g_2 + g_3 + \cdots + g_\beta$$

は 4 の倍数となる。これは②に矛盾する。ゆえに B は完全数でない。

（Ⅰ），（Ⅱ）より、連続する完全数は存在しない。（Q. E. D.）

(3) まず、以下の補題を示す。

補題４

任意の正の整数 n において、n と互いに素な過剰数が存在する。

（補題４の証明）

i 番目の素数を p_i とかくことにする。n の最大の素因数を p_m とする。ここで、$m+1$ 以上の整数 N において、

$$T_N = \prod_{k=m+1}^{N} p_k$$

とおくと、T_N の正の約数の総和は

$$\sigma(T_N) = \prod_{k=m+1}^{N} (p_k + 1)$$

となるので、T_N がもし過剰数であるとすると、次が成り立つ。

$$2T_N < \prod_{k=m+1}^{N} (p_k + 1)$$

両辺を $T_N = \prod_{k=m+1}^{N} p_k$ で割って、

$$2 < \prod_{k=m+1}^{N} \left(1 + \frac{1}{p_k}\right)$$

を得る。逆に、

$2 < \prod_{k=m+1}^{N} \left(1 + \frac{1}{p_k}\right)$ を満たすような整数 N が存在することを示せば、n と互いに素な過剰数 T_N が存在することが導かれる。

さらに、これは

$$\prod_{k=1}^{\infty} \left(1 + \frac{1}{p_k}\right) = \infty$$

となることを示せば十分である。なぜなら、

$\prod_{k=1}^{\infty} \left(1 + \frac{1}{p_k}\right) = \infty$ であるとき、

$$\prod_{k=m+1}^{\infty} \left(1 + \frac{1}{p_k}\right) = \infty$$

が成り立つので、$2 < \prod_{k=m+1}^{N} \left(1 + \frac{1}{p_k}\right)$ を満たすような整数 N が存在することが示されるからである。

まず、素因数分解の一意性により以下が成り立つ（参考文献[3]を参照）。

$$\prod_{k=1}^{\infty} \left(1 + \frac{1}{p_k} + \frac{1}{{p_k}^2} \cdots\right) > 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p_n}$$

ここで、左辺は等比級数の和の公式より

$$\prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k}} = \prod_{k=1}^{\infty} \left(1 + \frac{1}{p_k - 1}\right)$$

と変形できる。一方、素数は無限にあるため、右辺は限りなく大きくなる。ゆえに、

$$\prod_{k=1}^{\infty} \left(1 + \frac{1}{p_k - 1}\right) = \infty$$

が成り立つので、

$$\prod_{k=2}^{\infty}\left(1+\frac{1}{p_k-1}\right)=\infty \quad \cdots ③$$

を得る。ここで、任意の正の整数dにおいて$p_{d+1}-1 \geqq p_d$が成り立つので、

$$\prod_{k=2}^{n+1}\left(1+\frac{1}{p_k-1}\right) \leqq \prod_{k=1}^{n}\left(1+\frac{1}{p_k}\right)$$

である。よって、③より$\displaystyle\prod_{k=1}^{\infty}\left(1+\frac{1}{p_k}\right)=\infty$が成り立つことが示された。したがって題意は示された。（Q. E. D.）

88と945がどちらも過剰数であることは容易に確かめられる。また、88の素因数は2と11であり、945の素因数は3と5と7であるからこの2数は互いに素である。ここで、不定方程式

$$88x-945y=1$$

を考える。この等式を満たす整数の組(x, y)は無数に存在するが、そのうちの1つを求めると、$(x, y)=(247, 23)$という組が得られる。このとき、

$$88x=21736,\ 945y=21735$$

である。(1)の補題２より、それぞれは過剰数であるから、21735, 21736は連続する2つの過剰数である。

2以上の任意の整数cについて、連続するc個の過剰数が存在することを数学的帰納法により示す。

$c=2$の場合は先に示した通りである。

$c=k$のとき、条件を満たすk個の過剰数$a, a+1, a+2, \cdots, a+k-1$が存在したと仮定する。

ここで、$a+k$が過剰数であれば、それを含めた$k+1$個が$k+1$個の連続する過剰数となる。

$a+k$が過剰数でないとき、

$$\mathrm{LCM}(a,\ a+1,\ a+2,\ \cdots,\ a+k-1)=A$$

とする。このとき、任意の正の整数nにおいて(1)の補題２より

$$a+nA,\ a+nA+1,\ \cdots,\ a+nA+k-1$$

はk個の連続する過剰数となっている。

いま、補題４よりAと互いに素な過剰数が存在し、そのうちの１つをBとする。ここで、B個の数

$$a+k+A,\ a+k+2A,\ \cdots,\ a+k+BA$$

を考える。

この中にBの倍数が存在しないと仮定すると、鳩の巣原理よりこのB個の数の中にBで割った余りが等しい２数

$$a+k+iA,\ a+k+jA \quad (i<j)$$

が存在する。すると

$$(a+k+jA)-(a+k+iA)=(j-i)A$$

はBの倍数となるはずだが、$0<j-i<B$であり、BはAと互いに素であるから、$(j-i)A$はBの倍数でない。これは矛盾である。

よってB個の数

$$a+k+A,\ a+k+2A,\ \cdots,\ a+k+BA$$

の中にBの倍数が存在し、それを$a+k+tA$とする。すると

$$a+tA,\ a+tA+1,\ \cdots,\ a+tA+k$$

の$k+1$個の数は連続する$k+1$個の過剰数となっている。

よって、数学的帰納法より2以上の任意の整数cにおいて連続するc個の過剰数が存在することが示された。（Q. E. D.）

定理４から、以下がわかる。

定理５

(1) 不足数とその次の不足数の差に上限はない。

(2) 完全数とその次の完全数の差に上限はない。

(3) 他の過剰数の倍数でも、完全数の倍数でもない過剰数を「原始過剰数」([2])とよぶとき、原始過剰数とその次の原始過剰数の差に上限はない。

（証明）

(1)および(2)は、定理４の(3)より、明らかに成り立つ。

(3) 任意の正の整数dについて、連続するd個の正の整数であって、そのいずれも原始過剰数でないものが存在することを示せばよい。定理４より、連続するd個の過剰数が存在し、それらを$a_1,\ a_2, \cdots, a_d$とおく。ここで、$a_1,\ a_2, \cdots, a_d$の総乗をAとおくと、$A+a_1, A+a_2, \cdots, A+a_d$はそれぞれ$a_1,\ a_2, \cdots, a_d$の倍数（自身でない）であるため原始過剰数でない。

よって、$A+a_1, A+a_2, \cdots, A+a_d$は原始過剰数でない$d$個の連続する整数である。よって、原始過剰数とその次の原始過剰数の差に上限はないことが示された。

(Q. E. D.)

原始過剰数についてさらに調べると、以下が成り立つことがわかった。

定理６

互いに素な正の整数a, dについて、初項a，公差dの等差数列には原始過剰数が無数に現れる。

（証明）

ディリクレの算術級数定理（補題１）より、初項a，公差dの等差数列には素数が無数に現れる。そのうちの１つをp_0とする。また、初項1, 公差dの等差数列について、p_0よりも大きい素数を小さい順に並べたものを$p_1, p_2, \cdots$とする。いま、ディリクレの算術級数定理において、現れる素数の逆数和は発散するので、

$$\frac{1}{p_0}+\frac{1}{p_1}+\frac{1}{p_2}+\cdots=\infty$$

が成り立つ。よって、

$$\prod_{i=0}^{\infty}\left(1+\frac{1}{p_i}\right)>\sum_{i=0}^{\infty}\frac{1}{p_i}=\infty$$

が成り立つので、ある正の整数Nが存在して、

$$\prod_{i=0}^{N-1}\frac{p_i+1}{p_i}<2 \quad \text{かつ} \quad \prod_{i=0}^{N}\frac{p_i+1}{p_i}>2$$

を満たす。すなわち、$\prod_{i=0}^{N-1}p_i$は不足数であり、$\prod_{i=0}^{N}p_i$は過剰数であるから、参考文献[2]の命題８より、$\prod_{i=0}^{N}p_i$は原始過剰数である。また、

$$\prod_{i=0}^{N}p_i\equiv a\cdot1\cdot1\cdot\cdots\cdot1=a \pmod d$$

より、$\prod_{i=0}^{N}p_i$は初項a，公差dの等差数列に含まれる。いま、p_0の選び方は無数にあるので、同様の議論により、初項a，公差dの等差数列には原始過剰数が無数に含まれることが示された。 (Q. E. D.)

定理６において、$a=1$，dを過剰数とす

ることで、過剰数と原始過剰数が連続するようなものが無数に存在することがわかる。

３－３．累乗数

累乗数（$k≧2$ を用いて m^k とかける数）が連続するかどうかについて、参考文献[4], [5]を参考にして以下の結果を得た。

定理 7

$x^t = y^2+1$ を満たす自然数 x, t, y $(t≧2)$ は存在しない。

（証明）

t を 4 で割った余りで場合分けをする。

（ⅰ）$t \equiv 0, 2 \pmod 4$ のとき

このとき、t は偶数であるから、x^t は平方数である。すると 2 つの平方数の差が 1 となるが、これはありえない。

（ⅱ）$t \equiv 3 \pmod 4$ のとき

$t = 4n+3$ $(n≧0)$ とかける。条件式の右辺を変形して、以下を得る。

$$x^t = (y+i)(y-i)$$

ここで、ガウス整数環における 2 つのガウス整数 $y+i,\ y-i$ について、それらの最大公約数を g とすると、g は

$$(y+i)-(y-i) = 2i$$

を割り切るので、g としてあり得る数は $1, i, 2, 2i$ である。いま、g が 2 または $2i$ に等しいとすると、$y^2+1=(y+i)(y-i)$ が 4 の倍数となるが、$y^2+1 \equiv 1, 2 \pmod 4$ であるため、矛盾する。ゆえに、g は 1 または i であるから、$y+i$ と $y-i$ は互いに素である。ここで、任意のガウス整数はガウス素数の積で一意に表されることから、ある整数 a, b によって

$$y+i = (a+bi)^{4n+3}$$

とかける。右辺を展開して整理すると、

$$\begin{aligned} y+i &= \sum_{k=0}^{4n+3} {}_{4n+3}C_k a^{4n+3-k}(bi)^k \\ &= \sum_{k=0}^{2n+1} (-1)^k {}_{4n+3}C_{2k} a^{4n+3-2k} b^{2k} \\ &\quad + \left(\sum_{k=0}^{2n+1} (-1)^k {}_{4n+3}C_{2k+1} a^{4n+2-2k} b^{2k+1} \right) i \end{aligned}$$

となるので、

$$\sum_{k=0}^{2n+1} (-1)^k {}_{4n+3}C_{2k+1} a^{4n+2-2k} b^{2k+1} = 1$$

得る。この式の左辺は b で割り切れることから、b は 1 または -1 である。また、

$$\sum_{k=0}^{2n+1} (-1)^k {}_{4n+3}C_{2k+1} a^{4n+2-2k} b^{2k} = \pm 1$$

であり、$b^{2k}=1$ なので、

$$\sum_{k=0}^{2n} (-1)^k {}_{4n+3}C_{2k+1} a^{4n+2-2k} = 0,\ 2 \quad \cdots①$$

を得る。ここで、a を奇数と仮定すると、mod 2 において、

$$\begin{aligned} &\sum_{k=0}^{2n} (-1)^k {}_{4n+3}C_{2k+1} a^{4n+2-2k} \\ &\equiv \sum_{k=0}^{2n} {}_{4n+3}C_{2k+1} \\ &= \sum_{k=0}^{n} {}_{4n+3}C_{2k+1} + \sum_{k=n+1}^{2n} {}_{4n+3}C_{2k+1} \\ &= \sum_{k=0}^{n} {}_{4n+3}C_{2k+1} + \sum_{k=1}^{n} {}_{4n+3}C_{2k} \\ &= \sum_{k=1}^{2n+1} {}_{4n+3}C_k = \frac{2^{4n+3}-2}{2} \\ &= 2^{4n+2}-1 \equiv 1 \end{aligned}$$

となり矛盾する。ゆえに a は偶数である。すると①の左辺は 4 で割り切れるので、

$$\sum_{k=0}^{2n}(-1)^k {}_{4n+3}C_{2k+1}a^{4n+2-2k}=0$$

を得る。

$n=0$ のとき、${}_3C_1a^2=0$ より $a=0$ であるので、$y=0$ となるが、これは y が自然数であることに反する。

$n≧1$ のとき、

$$\sum_{k=0}^{2n}(-1)^k {}_{4n+3}C_{2k+1}a^{4n+2-2k}=0$$

の両辺を $a^2\neq 0$ で割って、

$$\sum_{k=0}^{2n}(-1)^k {}_{4n+3}C_{2k+1}a^{4n-2k}=0$$

ゆえに、

$$\begin{aligned}\sum_{k=0}^{2n-1}(-1)^k {}_{4n+3}C_{2k+1}a^{4n-2k} &= -{}_{4n+3}C_{4n+1}\\ &= -\frac{(4n+3)(4n+2)}{2}\\ &= -(4n+3)(2n+1)\end{aligned}$$

ここで、a は偶数なので左辺は偶数であるが、右辺は奇数であるから矛盾する。以上より、条件を満たす整数 a,b は存在しないので、x,y も存在しない。

(ⅲ) $t\equiv 1 \pmod 4$ のとき

$t=4m+1$（m は自然数)とかける。(ⅱ)と同様の議論により、$y+i=(c+di)^{4m+1}$ とかくことができる。また、d は1または-1であり、

$$\sum_{k=0}^{2m-1}(-1)^k {}_{4n+1}C_{2k+1}c^{4m-2k}=0$$

が成り立つので、

$$\sum_{k=0}^{2m}(-1)^k {}_{4n+1}C_{2k+1}c^{4m-2k}d^{2k}=1$$

を得る。いま、

$$d\sum_{k=0}^{2m}(-1)^k {}_{4n+1}C_{2k+1}c^{4m-2k}d^{2k}=1$$

が成り立つので、$d=1$ である。ゆえに、

$$y+i=(c+i)^{4m+1}$$

が成り立つ。よって、

$$|y+i|=\left|(c+i)^{4m+1}\right|$$

したがって、

$$\sqrt{y^2+1}=\left(\sqrt{c^2+1}\right)^{4m+1}=\sqrt{\left(c^2+1\right)^{4m+1}}.$$

両辺を 2 乗して、

$$y^2+1=\left(c^2+1\right)^{4m+1} \quad \cdots②$$

を得る。

いま、t が合成数であるとすると、ある素数 p が存在して、$t=ps$ とかける。すると、$y^2+1=x^t=\left(x^s\right)^p$ となるので、結局 t が素数である場合に条件を満たす x,y が存在しないことを示せば十分である。$t\equiv 3 \pmod 4$ のときはすでに示されているので、$4m+1$ が素数である場合を考えれば十分である。

$4m+1=q$ とおく。また、(ⅱ)の議論により、c は偶数であるから、$c=2u$ とかける。②にこれらを代入して、

$$y^2+1=\left(4u^2+1\right)^q$$

右辺を展開して、$y^2+1=\sum_{k=0}^{q}{}_qC_k\left(4u^2\right)^k$

である。ゆえに、

$$y^2=\sum_{k=1}^{q}{}_qC_k\left(4u^2\right)^k \quad \cdots③$$

ここで、q は素数であるから、${}_qC_k$ は q で割り切れる。よって、y^2 は q で割り切れる

ので、y は q で割り切れる。すると、②において、

$$(\text{左辺}) \equiv 1 \pmod{q}$$

$$(\text{右辺}) \equiv 4u^2 + 1 \pmod{q}$$

（ここで、フェルマーの小定理を用いた）が成り立つので、$4u^2 \equiv 0 \pmod{q}$ を得る。q は奇数であるから、u は q で割り切れる。いま、u は q で r 回割り切れるとする。ここで、③を

$$\begin{aligned} y^2 &= \sum_{k=1}^{q} {}_qC_k \left(4u^2\right)^k \\ &= \sum_{k=2}^{q} {}_qC_k \left(4u^2\right)^k + q \cdot 4u^2 \end{aligned}$$

と変形すると、$\sum_{k=2}^{q} {}_qC_k \left(4u^2\right)^k$ は q で $4r+1$ 回以上割り切れるが、$q \cdot 4u^2$ は q でちょうど $2r+1$ 回割り切れるので、右辺は q でちょうど $2r+1$ 回割り切れることがわかる。しかし、左辺は q で偶数回割り切れる必要があるので矛盾している。ゆえに、条件を満たす自然数 x, y は存在しない。

(ｉ), (ⅱ), (ⅲ)より、条件を満たす自然数 x, t, y は存在しないことが示された。

(Q. E. D.)

定理７の一般化として次が成り立つことが知られている。

カタラン予想

以下の式を満たす正の整数 x, a, y, b は $(x, a, y, b) = (3, 2, 2, 3)$ のみである。

$$x^a - y^b = 1$$

４．今後の課題

今回は素数、不足数、完全数、過剰数、原始過剰数、累乗数について調べたが、階乗数など、他の整数にも注目していきたい。また、今回の研究において、「連続する原始過剰数は存在するか」という問題について考えたが解くことはできなかったので、すでに知られている定理を調べながら、解決の糸口を探っていきたい。

５．参考文献

[1]「数論の精選104問」、Titu Andreescu, Dorin Andrica, Zuming Feng 著、小林一章、鈴木晋一 監訳、清水俊宏、西本将樹 訳(朝倉書店)

[2] 「約数の総和についてⅡ」、小椋晃一、奈良女子大学附属中等教育学校平成 28 年度 SSH 生徒研究論文集、p.68－78

[3] web サイト「高校数学の美しい物語」, https://mathtrain.jp/perfectnumber

[4] web サイト「IMOmath」, http://www.imomath.com/index.php?options=375&lmm=0

[5] web サイト「高校数学の美しい物語」, https://mathtrain.jp/gaussianint

６．謝辞

今回の研究にあたり、ご指導くださいました顧問の川口先生ありがとうございました。