【6】$k$ を 2 以上の自然数, $n$ を自然数とする。$n!$の $k$ 進法表示において、下(しも)の桁から数えて 0 が続く個数を $x_n$ とする。すなわち、

$n! =: [b_M, \cdots, b_1, b_0]_{(k)} \left( := \sum_{i=0}^{M} b_i k^i \right)$ ($b_i$は整数, $0 \leqq b_i \leqq k-1, b_M \neq 0$)

と表示した時、$b_0 = b_1 = \cdots = b_{i-1} = 0, b_i \neq 0$ を満たす $i$ を $x_n$とする。例えば、

$k = 2$ の時、$4! = 24 = [1,1,0,0,0]_{(2)}$より $x_4 = 3$

$k = 5$ の時、$7! = 5040 = [1,3,0,1,3,0]_{(5)}$より $x_7 = 1$

(1) $k$ の最大素因数を $p$ とする。$x_n$を $n, p$ の式で表せ。ただしガウス記号, $\sum$を用いてよい。

(2) $n =: [a_N, \cdots, a_1, a_0]_{(p)}$とする。

$c_n := \sum_{i=0}^{N} a_i$とする。

$x_n = \dfrac{1}{p-1}(n - c_n)$ を示せ。

(3) $\lim_{n\to\infty} \dfrac{x_n}{n}$を求めよ。ただし $\lim_{N\to\infty} \dfrac{N}{p^N} = 0$ を証明なしで用いてよい。

(解)

(1)

$k$ の素因数を大きい順に $p, q, r, \cdots$ とする。

$n!$の素因数分解における $p, q, r$ の指数をそれぞれ $a, b, c, \cdots$ とする。

$$
\begin{aligned}
x_n &= (n! \text{ を } k \text{ で割り切る最大回数}) \\
&= \min\{a, b, c, \cdots\} \\
&= a \\
&= \sum_{j=1}^{l} (n \text{ 以下の } p^j \text{の正の倍数の個数}) \quad (p^l \leqq n < p^{l+1}) \\
&= \sum_{j=1}^{[\log_p n]} \left[ \frac{n}{p^j} \right]
\end{aligned}
$$

(2)

$$
\begin{aligned}
x_n &= \sum_{j=1}^{\infty} \left[ \frac{[a_N, \cdots, a_1, a_0]_{(p)}}{p^j} \right] \quad (\because (1)) \\
&= \sum_{j=1}^{\infty} [a_N, \cdots, a_{j+1}, a_j]_{(p)} \\
&= (p^{N-1} + p^{N-2} + \cdots + 1)a_N + (p^{N-2} + \cdots + 1)a_{N-1} + \cdots + a_1 \\
&= \sum_{i=1}^{N} (1 + p + \cdots + p^{i-1})a_i \\
&= \sum_{i=1}^{N} \frac{p^i - 1}{p-1} a_i \\
&= \frac{1}{p-1} \left( \sum_{i=0}^{N} a_i p^i - \sum_{i=0}^{N} a_i \right) \\
&= \frac{1}{p-1}(n - c_n)
\end{aligned}
$$

(3)

$$\frac{x_n}{n} = \frac{1}{p-1}\left(1 - \frac{c_n}{n}\right)$$

ここで $0 < \dfrac{c_n}{n} \leqq \dfrac{(p-1)(N+1)}{p^N} \to 0 \ (n \to \infty)$

$\therefore \lim_{n\to\infty} \dfrac{x_n}{n} = \dfrac{1}{p-1}$ //

【完全数の決定】

自身以外の正の約数の和に等しくなる自然数を完全数という。

(例) $6=1+2+3, 28=1+2+4+7+14, 496=1+2+4+8+16+31+62+124+248, \cdots$

$=2\times 3$ $=2^2\times 7$ $=2^4\times 31$

以下、$n$ は自然数とする。

$\sigma(n) :=$ ($n$ の正の約数の和)

・$n \leqq \sigma(n) \leqq \dfrac{1}{2}n(n+1)$, 1 つ目の等号成立は $n=1,2$ つ目の等号成立は $n=1,2$ の時。

・$n$ が素数 $\Leftrightarrow \sigma(n)=n+1$

・$n$ が完全数 $\Leftrightarrow \sigma(n)=2n$

$\Leftrightarrow$ ($n$ の正の約数の逆数和) $=2$

・$\sigma(ab) \leqq \sigma(a)\sigma(b)$, 等号成立は $a$ と $b$ が互いに素の時。

定理 1

$2^{n+1}-1$ が素数 $\Leftrightarrow 2^n(2^{n+1}-1)$ は完全数

(pr.)

$$\begin{aligned}\sigma(2^n(2^{n+1}-1)) &= \sigma(2^n)\sigma(2^{n+1}-1) \ (\because 2^n \text{ と } 2^{n+1}-1 \text{ は互いに素}) \\ &\geqq \left(\sum_{i=0}^{n} 2^i\right)\{1+(2^{n+1}-1)\} \\ &= \frac{1(2^{n+1}-1)}{2-1}\cdot 2^{n+1} \\ &= 2\cdot 2^n(2^{n+1}-1)\cdots ①\end{aligned}$$

ここで、

$2^n(2^{n+1}-1)$ が完全数 $\Leftrightarrow$ ①の等号成立

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

$\Leftrightarrow 2^{n+1}-1$ は素数■

定理 2

$p$ : 自然数, $2^p-1$ : 素数 $\Rightarrow p$ は素数

(pr.)

$p=ab$ ($a,b$ は自然数) とする。

$$\begin{aligned}2^p-1 &= 2^{ab}-1 \\ &= (2^a)^b-1 \\ &= (2^a-1)\{2^{a(b-1)}+2^{a(b-2)}+\cdots+2^a+1\}\end{aligned}$$

$2^p-1$ は素数より、$2^a-1=1$ or $2^{a(b-1)}+2^{a(b-2)}+\cdots+2^a+1=1$

$\therefore a=1$ or $b=1$

故に $p$ は素数。■

逆は成り立たない。(反例 : $2^{11}-1=23\times 89, 2^{23}-1=47\times 178481, 2^{29}-1=233\times 1103\times 2089$)

定理 3

偶数の完全数は $2^n(2^{n+1}-1)$ ($n$ : 自然数) の形である。

(pr.)

偶数の完全数を $m$ とする。

$m =: 2^n l$ ($n$ : 自然数, $l$ : 奇数) と表せる。

$$\begin{aligned}\sigma(m) &= \sigma(2^n l) \\ &= \sigma(2^n)\sigma(l) \ (\because 2^n \text{ と } l \text{ は互いに素}) \\ &= (2^{n+1}-1)\sigma(l)\end{aligned}$$

一方、

$$\begin{aligned}\sigma(m) &= 2m \ (\because m \text{ は完全数}) \\ &= 2\cdot 2^n l \\ &= 2^{n+1}l\end{aligned}$$

$\therefore 2^{n+1}l = (2^{n+1}-1)\sigma(l)$
$2^{n+1}$ と $2^{n+1}-1$ は互いに素だから、$l = (2^{n+1}-1)k$ ($k$ : 自然数) と表せる。
この時、
$$\begin{aligned}2^{n+1}k &= \sigma(l)\\ &= \sigma((2^{n+1}-1)k)\\ &\geqq k + (2^{n+1}-1)k \ (\because k < (2^{n+1}-1)k)\\ &= 2^{n+1}k\end{aligned}$$
$\therefore \sigma((2^{n+1}-1)k) = k + (2^{n+1}-1)k$
$\therefore k = 1$
$$\begin{aligned}\therefore m &= 2^n l\\ &= 2^n(2^{n+1}-1)\end{aligned}$$ ■
定理 1 ∼ 定理 3 より、次のことが言える。
「偶数の完全数は $2^{p-1}(2^p-1)$ ($2^p-1$ : 素数, $p$ : 素数) と表せる。」
「素数 $p$ で $M_p := 2^p-1$ が素数 $\Rightarrow 2^{p-1}(2^p-1)$ は完全数」
素数である $M_p$をメルセンヌ素数という。そのような $p$ は以下の素数である。
$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937,$
$21701, 23209, 44497, 86243, \cdots$ (無数に存在するかは未解決問題)
2018 年 12 月 7 日 (金曜日) の時点で 51 個の $p$ が発見されている。小さい順は 48 番目まで確定している。

(奇数の完全数)
奇数の完全数が存在するかどうかは未解決問題である。計算機により次のことが分かっている。
・$10^{300}$以下には存在しない。
・9 個以上の素因数を持つ。
・$10^8$より大きい素因数を持つ。
・重複を込めた素因数の個数は 75 個以上。

定理 4(奇数の完全数の必要条件)
奇数の完全数は (存在すれば) $p^a n^2$ ($p \equiv a \equiv 1 \pmod 4$) と表せる。
(pr.)
奇数の完全数を $n$ とする。
$n =: {p_1}^{a_1} \cdots {p_N}^{a_N}$ (素因数分解) とする。
$$\begin{aligned}\sigma(n) &= \sigma({p_1}^{2a_1} \cdots {p_N}^{2a_N})\\ &= \sigma({p_1}^{a_1}) \cdots \sigma({p_N}^{a_N})\end{aligned}$$
一方、$n$ は完全数より、$\sigma(n) = 2n$
$\therefore 2n = \sigma({p_1}^{a_1}) \cdots \sigma({p_N}^{a_N})$
$\therefore 2 \equiv \sigma({p_1}^{a_1}) \cdots \sigma({p_N}^{a_N}) \pmod 4$, 以下同様) ($\because n$ は奇数)
$1 \sim N$ を適当に並べ替えて$\sigma({p_i}^{a_i}) \equiv \begin{cases} 2 & (i=1) \\ \pm 1 & (2 \leqq i \leqq N) \end{cases}$ としてよい。
ここで、
$$\begin{aligned}\sigma({p_i}^{a_i}) &= 1 + p_i + {p_i}^2 + \cdots + {p_i}^{a_i}\\ &\equiv \begin{cases} 1 + \underbrace{1 + \cdots + 1}_{a_i} & (p_i \equiv 1) \\ 1 + \underbrace{(-1) + 1 + (-1) + 1 + \cdots}_{a_i} & (p_i \equiv -1) \end{cases}\end{aligned}$$

$$\therefore \begin{cases} \sigma({p_1}^{a_1}) \equiv 2 \Rightarrow p_1 \equiv a_1 \equiv 1 \\ \sigma({p_i}^{a_i}) \equiv \pm 1 \Rightarrow a_i \equiv 0, 2 \end{cases}$$

故に成り立つ。■

【ラグランジュの 4 平方定理】

$p$ を 3 以上の素数とする。次を示せ。ただし (5), (6) では以下の恒等式 $(*)$ を用いてよい。

(1) $0^2, 1^2, \cdots, \left(\dfrac{p-1}{2}\right)^2$ を $p$ で割った余りは互いに異なる。

(2) ある整数 $a, b \left(0 \leqq a \leqq \dfrac{p-1}{2}, 0 \leqq b \leqq \dfrac{p-1}{2}\right)$ を取ると、$a^2+b^2+1$ は $p$ の倍数

(3) $a^2+b^2+1 < p^2$

(4) ある自然数 $k$ $(2 \leqq k \leqq p-1)$ を取ると、$pk = \sum_{i=1}^{4} {a_i}^2$ ($a_i$は 0 以上の整数) と表せると仮定する。

$a_i$を $k$ で割った余りを $r_i$ $\left(-\dfrac{k}{2} < r_i \leqq \dfrac{k}{2}\right)$ $(i = 1 \sim 4)$ とする。

$k' := \dfrac{1}{k} \sum_{i=1}^{4} {r_i}^2$

この時、$k'$は $k-1$ 以下の自然数。

(5) $pk' = \sum_{i=1}^{4} {a'_i}^2$ ($a'_i$は 0 以上の整数) と表せる。

(6) 任意の自然数 $n$ は $n = \sum_{i=1}^{4} {a_i}^2$ ($a_i$は 0 以上の整数) と表せる。

$$(*) \quad \sum_{i=1}^{4} {x_i}^2 \sum_{i=1}^{4} {y_i}^2 = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2$$

(pr.)

(1)

$0 \leqq i \leqq \dfrac{p-1}{2}, 0 \leqq j \leqq \dfrac{p-1}{2}, i^2 \equiv j^2 \pmod{p}$ とする。

$0 \equiv i^2 - j^2 = (i+j)(i-j)$

$p$ : 素数より、$i+j \equiv 0$ or $i-j \equiv 0$

$0 \leqq i+j \leqq p-1, |i-j| \leqq \dfrac{p-1}{2}$ より、$i = j$

故に $0^2, 1^2, \cdots, \left(\dfrac{p-1}{2}\right)^2$ を $p$ で割った余りは互いに異なる。

(2)

$\left\{0^2, 1^2, \cdots, \left(\dfrac{p-1}{2}\right)^2\right\}, \left\{-0^2-1, -1^2-1, \cdots, -\left(\dfrac{p-1}{2}\right)^2 - 1\right\}$ において、

和集合の要素の個数は $p+1$, 各集合では要素は互いに合同でない。

故に、部屋割り論法より、ある整数 $a, b \left(0 \leqq a \leqq \dfrac{p-1}{2}, 0 \leqq b \leqq \dfrac{p-1}{2}\right)$ を取ると、

$a^2 \equiv -b^2 - 1$

この時 $a^2+b^2+1 \equiv 0$

故に $a^2+b^2+1$ は $p$ の倍数である。

(3)

$$\begin{aligned} a^2+b^2+1 &\leqq \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 \\ &< 4\left(\frac{p}{2}\right)^2 \\ &= p^2 \end{aligned}$$

$\therefore a^2+b^2+1 < p^2$

(4)

$$\begin{aligned} \sum_{i=1}^{4} {r_i}^2 &\equiv \sum_{i=1}^{4} {a_i}^2 \pmod{k} \\ &= pk \end{aligned}$$

$$\equiv 0 \pmod{k}$$

故に $k'$は整数である。

$$kk' = \sum_{i=1}^{4} {r_i}^2$$
$$\leqq 4\left(\frac{k}{2}\right)^2$$
$$= k^2$$

$\therefore k' \leqq k$

$k' = k$ と仮定する。

$r_i = \dfrac{k}{2}$ $(i = 1 \sim 4)$

故に $a_i = ku_i + \dfrac{k}{2}$ ($u_i$は整数) と表せる。

$$pk = \sum_{i=1}^{4} {a_i}^2$$
$$= \sum_{i=1}^{4} \left(ku_i + \frac{k}{2}\right)^2$$
$$= k^2 \left\{ \sum_{i=1}^{4} ({u_i}^2 + u_i) + 1 \right\}$$

$$\therefore p = k \left\{ \sum_{i=1}^{4} ({u_i}^2 + u_i) + 1 \right\}$$

これは $p$ は奇数, $k$ は偶数に矛盾。

$\therefore k' \leqq k - 1$

$k' = 0$ と仮定する。

$r_i = 0$ $(i = 1 \sim 4)$

故に $a_i = kv_i$ ($v_i$は整数) と表せる。

$$pk = \sum_{i=1}^{4} {a_i}^2$$
$$= \sum_{i=1}^{4} (kv_i)^2$$
$$= k^2 \sum_{i=1}^{4} {v_i}^2$$

$$\therefore p = k \sum_{i=1}^{4} {v_i}^2$$

これは $p$ : 素数, $2 \leqq k \leqq p - 1$ に矛盾。

$\therefore k' \neq 0$

故に $k'$は $k - 1$ 以下の自然数。

(5)

$$\sum_{i=1}^{4} {a_i}^2 \sum_{i=1}^{4} {r_i}^2 = (a_1r_1 + a_2r_2 + a_3r_3 + a_4r_4)^2$$
$$+ (a_1r_2 - a_2r_1 + a_3r_4 - a_4r_3)^2$$
$$+ (a_1r_3 - a_2r_4 - a_3r_1 + a_4r_2)^2$$
$$+ (a_1r_4 + a_2r_3 - a_3r_2 - a_4r_1)^2$$

ここで、

$$a_1r_1 + a_2r_2 + a_3r_3 + a_4r_4 \equiv \sum_{i=1}^{4} {a_i}^2 = pk \equiv 0 \pmod{k}$$
$$a_1r_2 - a_2r_1 + a_3r_4 - a_4r_3 \equiv \cancel{a_1a_2} \cancel{- a_2a_1} \cancel{+ a_3a_4} \cancel{- a_4a_3} = 0 \pmod{k}$$
$$a_1r_3 - a_2r_4 + a_3r_1 - a_4r_2 \equiv \cancel{a_1a_3} \cancel{- a_2a_4} \cancel{+ a_3a_1} \cancel{- a_4a_2} = 0 \pmod{k}$$
$$a_1r_4 + a_2r_3 - a_3r_2 - a_4r_1 \equiv \cancel{a_1a_4} \cancel{- a_2a_3} \cancel{+ a_3a_2} \cancel{- a_4a_1} = 0 \pmod{k}$$

故に $\begin{cases} a_1r_1+a_2r_2+a_3r_3+a_4r_4=:ka_1' \\ a_1r_2-a_2r_1+a_3r_4-a_4r_3=:ka_2' \\ a_1r_3-a_2r_4+a_3r_1-a_4r_2=:ka_3' \\ a_1r_4+a_2r_3-a_3r_2-a_4r_1=:ka_4' \end{cases}$ ($a_i'$は整数) と表せる。

この時、$pk\cdot kk'=(ka_1')^2+(ka_2')^2+(ka_3')^2+(ka_4')^2$

$\therefore pk'=\sum_{i=1}^{4}a_i'^2$

$a_i'<0$ ならば $-a_i'$を改めて $a_i'$とすることより、これは $a_i'\geqq 0$ を満たす。

(6)

$(*)$ より、$n$ が素数の時を示せばよい。

$n=2$ の時は、$2=0^2+0^2+1^2+1^2$より成り立つ。

故に $n=p$ (3 以上の素数) の時を示せばよい。これを示す。

(3) より、$p-1$ 以下のある自然数 $k$ を取ると、$pk=\sum_{i=1}^{4}a_i^2$

(4) より、$k-1$ 以下のある自然数 $k'$を取ると、$pk'=\sum_{i=1}^{4}a_i'^2$

同様にこの操作を繰り返していくと、$1\leqq k'<k$ より、$k^{(p-1)}=1$

$\therefore p=\sum_{i=1}^{4}\left(a_i^{(p-1)}\right)^2$ ■

【素数の逆数和】

素数の逆数和は発散することを、次の手順で示せ。

$n$ 番目の素数を $p_n$ とする。

$\sum_{i=1}^{\infty} \frac{1}{p_i}$ は収束すると仮定する。

$\sum_{i=1}^{\infty} \frac{1}{p_i} - \sum_{i=1}^{N} \frac{1}{p_i} < \frac{1}{2}$ を満たす自然数 $N$ を取る。

$n$ を自然数とする。

$a_n :=$ ($n$ 以下の自然数の内、全ての素因数が $p_N$ 以下のものの個数), $b_n := n - a_n$ とする。

(1) $a_n \leqq 2^N \sqrt{n}$

(2) $b_n < \frac{1}{2} n$

(3) $\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$

(pr.)

(1)

$n$ 以下の自然数の内全ての素因数が $p_N$ 以下のものを $u^2 v$ ($v$ の素因数の指数は全て 1) と表す。

$u^2 \leqq u^2 v \leqq n$ より $u \leqq \sqrt{n}$, 故に $u$ の取り方は高々 $[\sqrt{n}]$ 通り。

$v$ の取り方は高々 $2^N$ 通り。

$\therefore a_n \leqq [\sqrt{n}] 2^N \leqq 2^N \sqrt{n}$

(2)

$$
\begin{aligned}
b_n &< \sum_{i=N+1}^{\infty} \left[ \frac{n}{p_i} \right] \\
&< \sum_{i=N+1}^{\infty} \frac{n}{p_i} \\
&= n \sum_{i=N+1}^{\infty} \frac{1}{p_i} \\
&< \frac{1}{2} n
\end{aligned}
$$

故に成り立つ。

(3)

$$
\begin{aligned}
n &= a_n + b_n \\
&< 2^N \sqrt{n} + \frac{1}{2} n
\end{aligned}
$$

$\frac{1}{2} n < 2^N \sqrt{n}$

$\sqrt{n} < 2^{N+1}$

$\therefore n < 2^{2N+2}$

両辺を $n \to \infty$ とすると矛盾。

$\therefore \sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$ ■

【チェビシェフの定理】

任意の自然数 $n$ に対して、$n < p \leqq 2n$ を満たす素数 $p$ が存在することを、次の手順で示せ。

$x > 0, P(x) :=$ ($x$ 以下の素数の積) とする。

(1) ($x$ 以下の素数の個数) $< \dfrac{1}{3}x + 2$

(2) $\dfrac{P(2n-1)}{P(n)} \leqq {}_{2n-1}\mathrm{C}_n \leqq 2^{2n-2}$

(3) $x \geqq 3$ で $P(x) < 2^{2x-3}$

(4) ${}_{2n}\mathrm{C}_n > \dfrac{2^{2n}}{n}$ $(n \geqq 4)$

(5) $y = \dfrac{\log x}{x}$ は $x \geqq e$ で減少である。

以下、ある自然数 $n \geqq 5$ を取ると、$n < p \leqq 2n$ を満たす素数 $p$ が存在しないと仮定する。

$p$ を ${}_{2n}\mathrm{C}_n$ の素因数, $a_p$ を $p$ の指数とする。

(6) $a_p = \displaystyle\sum_{i=1}^{[\log_p 2n]} \left( \left[ \frac{2n}{p^i} \right] - 2 \left[ \frac{n}{p^i} \right] \right)$

(7) $p \leqq \dfrac{2}{3}n$

(8) ${}_{2n}\mathrm{C}_n < (2n)^{\frac{1}{3}\sqrt{2n}+2} \times 2^{\frac{4}{3}n-5}$

(9) $n < 2^6$

(10) 自然数 $n \leqq 63$ に対して、$n < p \leqq 2n$ を満たす素数 $p$ が存在する。

(pr.)

(1)

($x$ 以下の素数の個数) $\leqq$ ($2, 3$ の倍数でない $x$ 以下の自然数の個数) $+ 1$

$$\leqq \left( \left[ \frac{x}{3} \right] + 1 \right) + 1 \text{ (等号成立は } x \text{ を } 6 \text{ で割った余りが } 1, 2, 5)$$

$$\leqq \frac{1}{3}x + 2 \text{ (等号成立は } x \text{ が } 3 \text{ の倍数)}$$

故に成り立つ。

(2)

$${}_{2n-1}\mathrm{C}_n = \frac{(2n-1) \cdot (2n-2) \cdot \cdots \cdot (n+1) \cdot \cancel{n}}{\cancel{n} \cdot (n-1) \cdot \cdots \cdot 1}$$

この分子には、$n+1$ 以上 $2n-1$ 以下の全ての素数が現れ、それらは分母と約分できない。

$$\therefore \frac{P(2n-1)}{P(n)} = (n+1 \text{ 以上 } 2n-1 \text{ 以下の素数の積}) \leqq {}_{2n-1}\mathrm{C}_n$$

$$\begin{aligned} {}_{2n-1}\mathrm{C}_n &= \frac{1}{2} \cdot 2\, {}_{2n-1}\mathrm{C}_n \\ &\leqq \frac{1}{2} \sum_{i=0}^{2n-1} {}_{2n-1}\mathrm{C}_i \quad (\because {}_{2n-1}\mathrm{C}_{n-1} = {}_{2n-1}\mathrm{C}_n) \\ &= \frac{1}{2}(1+1)^{2n-1} \\ &= 2^{2n-2} \end{aligned}$$

故に成り立つ。

(3)

$x = n$ の時成り立つことを、$n$ に関する数学的帰納法で示す。

$n = 3, 4$ の時、

$P(3) = 6 < 2^3, P(4) = 6 < 2^5$

故に成り立つ。

$3 \leqq n \leqq 2m-2$ の時成り立つと仮定する。$(m \geqq 3)$

$$\begin{aligned} P(2m-1) &= P(m) \cdot \frac{P(2m-1)}{P(m)} \\ &< 2^{2m-3} \cdot 2^{2m-2} \quad (\because \text{仮定}, (2)) \end{aligned}$$

$$= 2^{4m-5} = 2^{2(2m-1)-3}$$

$P(2m) = P(2m-1)$ ($\because 2m$ は素数でない)

$$< 2^{2(2m-1)-3}$$

$$< 2^{2\cdot 2m-3}$$

故に $2m-1, 2m$ の時も成り立つ。

故に $x = n$ の時成り立つ。

$\therefore P(x) = P([x]) < 2^{2[x]-3} \leqq 2^{2x-3}$

(4)

$n$ に関する数学的帰納法で示す。

$n = 4$ の時、

${}_8\mathrm{C}_4 = \dfrac{8\cdot 7\cdot 6\cdot 5}{4\cdot 3\cdot 2\cdot 1} = 70, \dfrac{4^4}{4} = 64$ より成り立つ。

$n-1$ 以下の時成り立つと仮定する。

$${}_{2n}\mathrm{C}_n = \frac{2n\cdot(2n-1)\cdot\cdots\cdot(n+1)}{n\cdot(n-1)\cdot\cdots\cdot 1}$$

$$= \frac{(2n-2)\cdot(2n-3)\cdot\cdots\cdot n}{(n-1)\cdot(n-2)\cdot\cdots\cdot 1}\cdot\frac{2n\cdot(2n-1)}{n\cdot n}$$

$$= 2\cdot\frac{2n-1}{n}\cdot{}_{2(n-1)}\mathrm{C}_{n-1}$$

$$> 2\cdot\frac{2n-1}{n}\cdot\frac{4^{n-1}}{n-1}$$

$$= 2\cdot\frac{2n-1}{n-1}\cdot\frac{4^{n-1}}{n}$$

$$> 2\cdot 2\cdot\frac{4^{n-1}}{n}$$

$$= \frac{4^n}{n}$$

故に $n$ の時も成り立つ。

(5)

$$y' = \frac{1-\log x}{x^2}$$

$x \geqq e$ で $1-\log x < 0$ より $y' < 0$

故に成り立つ。

(6)

$${}_{2n}\mathrm{C}_n = \frac{(2n)!}{n!^2}$$

$\therefore a_p = ((2n)!$の素因数 $p$ の指数$) - 2\times(n!$の素因数 $p$ の指数$)$

$$= \sum_{i=1}^{\infty}(2n \text{ 以下の } p^i \text{の正の倍数の個数}) - 2\sum_{i=1}^{\infty}(n \text{ 以下の } p^i \text{の正の倍数の個数})$$

$$= \sum_{i=1}^{[\log_p 2n]}\left[\frac{2n}{p^i}\right] - 2\sum_{i=1}^{[\log_p n]}\left[\frac{n}{p^i}\right]$$

$$= \sum_{i=1}^{[\log_p 2n]}\left(\left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right]\right)$$

(7)

$p > \dfrac{2}{3}n$ と仮定する。

$p \leqq 2n$ であり、$n < p \leqq 2n$ を満たす $p$ は存在しないから、$\dfrac{2}{3}n < p \leqq n$

一方、$p^2 > \dfrac{4}{9}n^2 > 2n$ ($\because n \geqq 5$) より、$[\log_p 2n] \leqq 1$

$$\therefore a_p \leqq \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \quad (\because [\log_p 2n] \leqq 1)$$

$$= 2 - 2\cdot 1 \quad \left(\because 2 \leqq \frac{2n}{p} < 3, 1 \leqq \frac{n}{p} < \frac{3}{2}\right)$$

$= 0$, これは矛盾。

$\therefore p \leqq \dfrac{2}{3}n$

(8)

$$a_p = \sum_{i=1}^{[\log_p 2n]} \left( \left[ \frac{2n}{p^i} \right] - 2 \left[ \frac{n}{p^i} \right] \right)$$

$$\leqq [\log_p 2n] \quad \left( \because [2x] - 2[x] = \begin{cases} 0 & (x - [x] < 0.5) \\ 1 & (x - [x] \geqq 0.5) \end{cases} \right)$$

$$\leqq \log_p 2n$$

$\therefore p^{a_p} \leqq 2n$

特に、$p > \sqrt{2n} \Rightarrow a_p < \log_p p^2 = 2$

$$\therefore {}_{2n}\mathrm{C}_n = (\text{素因数が}\sqrt{2n}\text{以下の部分}) \cdot \frac{P\left(\frac{2}{3}n\right)}{P\left(\sqrt{2n}\right)}$$

$$< (2n)^{\frac{1}{3}\sqrt{2n}+2} \cdot \frac{2^{2 \cdot \frac{2}{3}n-3}}{2 \cdot 3} \quad (\because (1), (3), \sqrt{2n} > 3)$$

$$< (2n)^{\frac{1}{3}\sqrt{2n}+2} \cdot 2^{\frac{4}{3}n-5}$$

(9)

(4), (8) より $\dfrac{2^{2n}}{n} < {}_{2n}\mathrm{C}_n < (2n)^{\frac{1}{3}\sqrt{2n}+2} \cdot 2^{\frac{4}{3}n-5}$

両辺に log を取ると、$2n\log 2 - \log n < \left(\dfrac{1}{3}\sqrt{2n} + 2\right)(\log 2 + \log n) + \left(\dfrac{4}{3}n - 5\right)\log 2$

整理すると、$\dfrac{2}{3}n\log 2 < \dfrac{1}{3}\sqrt{2n}\log 2n + 3\log\dfrac{n}{2}$

両辺を $\dfrac{3}{n}$ 倍すると、$2\log 2 < \sqrt{\dfrac{2}{n}}\log 2n + \dfrac{9}{n}\log\dfrac{n}{2}$

$\therefore \sqrt{2} \cdot \dfrac{\log\sqrt{n}}{\sqrt{n}} + \dfrac{9}{4} \cdot \dfrac{\log\frac{n}{2}}{\frac{n}{2}} + \dfrac{\log 2}{\sqrt{2n}} > \log 2$

左辺を $f(n)$ とする。

(5) より、$f(n)$ は $n \geqq \max\{e^2, 2e\} = 7.3\cdots$ で減少である。

$2^6 > e^2$ であり、

$$f(2^6) = \sqrt{2} \cdot \frac{3\log 2}{8} + \frac{9}{4} \cdot \frac{5\log 2}{32} + \frac{\log 2}{8\sqrt{2}}$$

$$= \frac{45 + 56\sqrt{2}}{128}\log 2$$

$$< \frac{45 + 56 \times 1.42}{128}\log 2$$

$$= \frac{124.52}{128}\log 2 < \log 2$$

$\therefore n < 2^6 = 64$

(10)

$p = 2 \Rightarrow n = 1$

$p = 3 \Rightarrow n = 2$

$p = 5 \Rightarrow n = 3, 4$

$p = 7 \Rightarrow n = 4 \sim 6$

$p = 13 \Rightarrow n = 7 \sim 12$

$p = 23 \Rightarrow n = 12 \sim 22$

$p = 43 \Rightarrow n = 22 \sim 42$

$p = 83 \Rightarrow n = 42 \sim 82$ ■

【ピタゴラス数】
$x^2+y^2=z^2$の自然数解 $(x,y,z)$ をピタゴラス数という。
特に $x,y,z$ が互いに素のものを原始ピタゴラス数という。
・ピタゴラス数 $(x,y,z)$ が原始的 $\Leftrightarrow$ $x,y,z$ の内のある 2 個が互いに素
$(x,y,z)$ を原始ピタゴラス数とする。
(1) $x-y$ は奇数
(2) 以下、$x$ : 奇数, $y$ : 偶数とする。
$z+x=:2m^2, z-x=:2n^2$ ($m,n$ は互いに素な自然数, $m>n, m-n$ は奇数) と表せる。
(3) $(x,y,z)=(m^2-n^2, 2mn, m^2+n^2)$
(pr.)
(1)
$(x,y,z)$ は原始的より ($x,y$ は互いに素), 故に $x,y$ の少なくとも一方は奇数である。
$x,y$ は奇数と仮定する。
$x\equiv\pm1, y\equiv\pm1 \pmod 4$ (複号任意)
$\therefore z^2=x^2+y^2\equiv 2 \pmod 4$, これは $z^2\equiv\begin{cases}0 & (z:\text{偶数})\\ 1 & (z:\text{奇数})\end{cases} \pmod 4$ に矛盾。
故に $x-y$ は奇数。
(2)
$y=:2y'$ ($y'$は自然数) とする。
$4y'^2=y^2$
$\quad=(z+x)(z-x)$
$z+x$ と $z-x$ の偶奇は一致するから、$z+x=:2a, z-x=:2b$ ($a,b$ : 自然数)
$z=a+b, x=a-b$ は互いに素だから、$a,b$ は互いに素, $a-b$ は奇数。
$4y'^2=2a\cdot 2b, \therefore y'^2=ab$
$a,b$ は互いに素より $a=:m^2, b=:n^2$ ($m,n$ : 自然数)
この時、
$z+x=2m^2, z-x=2n^2$
$a,b$ は互いに素より $m,n$ は互いに素
$0<x=a-b=m^2-n^2$ より $m>n$
$(m+n)(m-n)=a-b$ : 奇数より $m-n$ : 奇数
(3)
$2z=2m^2+2n^2, \therefore z=m^2+n^2$
$2x=2m^2-2n^2, \therefore x=m^2-n^2$
$y^2=(z+x)(z-x)$
$\quad=2m^2\cdot 2n^2$
$\quad=(2mn)^2$
$\therefore y=2mn$ ■
・自然数 $a,b$ ($a>b$) について、$a+b, a-b$ が互いに素 $\Leftrightarrow$ $a,b$ は互いに素, $a-b$ は奇数
(pr.)
($\Rightarrow$)
$a=:ga', b=:gb'$ ($g:=\gcd(a,b)$) とする。
$a+b=g(a'+b'), a-b=g(a'-b')$ は互いに素より $g=1$
故に $a,b$ は互いに素。
$a+b, a-b$ は互いに素で偶奇が一致するから、共に奇数。
($\Leftarrow$)
$a+b=:gu, a-b=:gv$ ($g:=\gcd(a+b, a-b)$) とする。

$2a = g(u+v), 2b = g(u-v)$
ここで、$gv = a - b$ : 奇数より $g$ : 奇数
故に $u+v =: 2k, u-v =: 2l$ ($k, l$ : 自然数) とおける。
この時 $2a = g \cdot 2k, 2b = g \cdot 2l$
$\therefore a = gk, b = gl$
$a, b$ は互いに素より $g = 1$
故に $a+b, a-b$ は互いに素。■
・自然数の組 $(x, y, z)$ が原始ピタゴラス数
$\Leftrightarrow (x, y, z) = (m^2 - n^2, 2mn, m^2 + n^2)$ or $(2mn, m^2 - n^2, m^2 + n^2)$
($m, n$ は互いに素な自然数, $m > n, m - n$ は奇数) と表せる
・$x$ or $y$ は 4 の倍数
・$xy$ は 3 の倍数
・$xyz$ は 5 の倍数
直角 3 角形の面積
$(x, y, z)$ をピタゴラス数とする。
この時、$S := \frac{1}{2}xy$ は平方数でない。
(pr.)
あるピタゴラス数 $(x, y, z)$ を取ると、$S = \frac{1}{2}xy$ は平方数と仮定する。
$(x, y, z)$ の内 $S$ が最小のものを取る。
$x =: gx', y =: gy', z =: gz'$ ($g := \gcd(x, y, z)$)
$(gx')^2 + (gy')^2 = (gz')^2$ より $x'^2 + y'^2 = z'^2$
$S = \frac{1}{2}x'y' \cdot g^2$は平方数より、$S' := \frac{1}{2}x'y'$は平方数, $S = g^2 S' \geqq S'$
故に、$S$ の最小性より $g = 1$
$(x, y, z) =: (m^2 - n^2, 2mn, m^2 + n^2)$ ($m, n$ は互いに素な自然数, $m > n, m - n$ は奇数)
$S = mn(m+n)(m-n)$ は平方数
$m, n, m+n, m-n$ のどの 2 つも互いに素より、
$m =: z'^2, n =: k^2, m+n =: a^2, m-n =: b^2$ ($k, a, b$ : 自然数)
$$\begin{aligned}(a+b)(a-b) &= a^2 - b^2 \\ &= 2n \\ &= 2k^2\end{aligned}$$
$a+b, a-b$ は偶奇が一致するから、$(a+b, a-b) =: (2u^2, 4v^2), (4v^2, 2u^2)$ ($u, v$ : 自然数)
この時、$(a, b) = (u^2 + 2v^2, \pm(u^2 - 2v^2))$
$$\begin{aligned}z'^2 &= m \\ &= \frac{1}{2}(a^2 + b^2) \\ &= \frac{1}{2}\{(u^2 + 2v^2)^2 + (u^2 - 2v^2)^2\} \\ &= (u^2)^2 + (2v^2)^2\end{aligned}$$
故に、$x' := u^2, y' := 2v^2$とすると、$x'^2 + y'^2 = z'^2 \cdots ①$
$$\begin{aligned}S' &:= \frac{1}{2}x'y' \\ &= (uv)^2 \cdots ② \\ &= \frac{1}{8}(a+b)(a-b) \\ &= \frac{1}{8} \cdot 2n \\ &< n \\ &< S \cdots ③\end{aligned}$$
①, ②, ③は $S$ の最小性に矛盾。

故に $S = \frac{1}{2}xy$ は平方数でない。■

4 次のフェルマー最終定理

$x^4 + y^4 = z^4$の自然数解 $(x, y, z)$ は存在しない。

(pr.)

$x^4 + y^4 = z^4$の自然数解 $(x, y, z)$ が存在すると仮定する。

$(x, y, z)$ の内 $z$ が最小のものを取る。この時 $x, y, z$ は互いに素。

$w := z^2$

$(x^2, y^2, w) =: (m^2 - n^2, 2mn, m^2 + n^2)$ ($m, n$ は互いに素な自然数, $m > n, m - n$ は奇数)

$m$ : 偶数, $n$ : 奇数と仮定すると、

$x^2 = m^2 - n^2 \equiv -1 \pmod 4$, これは $x^2 \equiv \begin{cases} 0 & (x : \text{偶数}) \\ 1 & (x : \text{奇数}) \end{cases} \pmod 4$ に矛盾。

$\therefore m$ : 奇数, $n$ : 偶数

$y^2 = 2mn, (m, n$ は互いに素) より、$m =: w'^2, n =: 2v^2$ ($w', v$ : 自然数) の形である。

$x^2 = m^2 - n^2$

$\quad = (w'^2)^2 - (2v^2)^2$

$\therefore x^2 + (2v^2)^2 = (w'^2)^2$

$(x, 2v^2, w'^2) =: (k^2 - l^2, 2kl, k^2 + l^2)$ ($k, l$ は互いに素な自然数, $k > l, k - l$ は奇数)

$v^2 = kl, (k, l$ は互いに素) より、$k =: x'^2, l =: y'^2$ ($x', y'$ : 自然数) の形である。

$w'^2 = k^2 + l^2$

$\quad = x'^4 + y'^4 \cdots ①$

$w = m^2 + n^2$

$\quad > m$

$\quad = w'^2$

$\quad \geqq w' \cdots ②$

①, ②は $w$ の最小性に矛盾。

故に、$x^4 + y^4 = z^4$の自然数解 $(x, y, z)$ は存在しない。■

【$\mathbb{Z}[\sqrt{3}i]$ の一意分解整域性】

本章で登場する文字は全て整数とする。

補題 1

$a, b$ は互いに素とする。

$p = c^2 + 3d^2$は $a^2 + 3b^2$の約数であるとする。

(1) $\dfrac{a^2+3b^2}{p} = \Big(\dfrac{ac \pm 3bd}{p}\Big)^2 + 3\Big(\dfrac{ad \mp bc}{p}\Big)^2$ (複号は同順, and)

(2) $c = d = 1 \Rightarrow \dfrac{ac \pm 3bd}{p}, \dfrac{ad \mp bc}{p}$は整数 (複号同順)

(3) $p$ : 素数 $\Rightarrow \dfrac{ac \pm 3bd}{p}, \dfrac{ad \mp bc}{p}$は整数 (複号同順)

(4) $a^2 + 3b^2 = 4^\delta m$ $((\delta = 0, 1), m$ : 奇数) の形である。

(5) $p$ は$\alpha^2 + 3\beta^2$の形でない奇素因数とする。

この時、$\dfrac{a^2+3b^2}{p}$は$\alpha^2 + 3\beta^2$の形でない奇素因数を持つ。

(pr.)

(1)

$$\begin{aligned}(ac \pm 3bd)^2 + 3(ad \mp bc)^2 &= a^2c^2 \pm 6abcd + 9b^2d^2 + 3(a^2d^2 \mp 2abcd + b^2c^2)\\ &= a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2\\ &= (a^2 + 3b^2)(c^2 + 3d^2)\end{aligned}$$

$$\therefore \frac{a^2+3b^2}{p} = \Big(\frac{ac \pm 3bd}{p}\Big)^2 + 3\Big(\frac{ad \mp bc}{p}\Big)^2$$

(2)

$a, b$ は互いに素, $a^2 + 3b^2$は 4 の倍数より、$a, b$ は奇数。

$\therefore 4 \mid a \mp b$

故に、$\dfrac{a \pm 3b}{4}, \dfrac{a \mp b}{4}$は整数。

(3)

$$(ad + bc)(ad - bc) = d^2(a^2 + 3b^2) - b^2(c^2 + 3d^2)$$

$p = c^2 + 3d^2$は $a^2 + 3b^2$の素因数より、$p \mid (ad \mp bc)$

$$(a^2 + 3b^2)p = (ac \pm 3bd)^2 + 3(ad \mp bc)^2$$

$\therefore p \mid (ac \pm 3bd)$

故に、$\dfrac{ac \pm 3bd}{p}, \dfrac{ad \mp bc}{p}$は整数。

(4)

$(a^2, b^2) \equiv (0, 1), (1, 0), (1, 1) \pmod 4$

$\therefore a^2 + 3b^2 \equiv 0, 1, 3 \pmod 4$

$(a^2, b^2) \equiv (0, 1), (1, 0), (1, 4), (4, 1) \pmod 8$

$\therefore a^2 + 3b^2 \equiv 1, 3 \pmod 8$

故に成り立つ。

(5)

対偶 :「$\dfrac{a^2+3b^2}{p}$の奇素因数は$\alpha^2 + 3\beta^2$の形 $\Rightarrow p = \alpha^2 + 3\beta^2$の形」を示す。

$$\frac{a^2+3b^2}{p} =: 4^\delta p_1 \cdots p_n \quad (p_k = {\alpha_k}^2 + 3{\beta_k}^2 : \text{奇素数})$$

$$\frac{a^2+3b^2}{4^\delta} = pp_1 \cdots p_n$$

(1), (3) より、$pp_2 \cdots p_n = \dfrac{{a_n}^2 + 3{b_n}^2}{p_1} =: {\gamma_1}^2 + 3{\delta_1}^2$

$pp_3 \cdots p_n = \dfrac{{\gamma_1}^2 + 3{\delta_1}^2}{p_2} =: {\gamma_2}^2 + 3{\delta_2}^2$

$\vdots$

$p = \dfrac{{\gamma_{n-1}}^2 + 3{\delta_{n-1}}^2}{p_n} =: {\gamma_n}^2 + 3{\delta_n}^2$ ■

定理 1

$a, b$ は互いに素とする。$p$ を $a^2 + 3b^2$ の奇素因数とする。

(1) $a, b$ を $p$ で割った余りをそれぞれ $r, s$ $\left(|r| < \dfrac{p}{2}, |s| < \dfrac{p}{2}\right)$ とする。

この時、$r^2 + 3s^2$ は $p$ の倍数, $l := \dfrac{r^2 + 3s^2}{p} < p$

(2) $r =: ga', s =: gb'$ $(g := \gcd(r, s)), k' := \dfrac{l}{g^2}$ とする。

この時、${a'}^2 + 3{b'}^2 = pk', k'$ は自然数, $k' < p$

(3) $p = \alpha^2 + 3\beta^2$ の形である。

(4) $a^2 + 3b^2 = ({\alpha_1}^2 + 3{\beta_1}^2) \cdots ({\alpha_n}^2 + 3{\beta_n}^2)$ $({\alpha_k}^2 + 3{\beta_k}^2 = 4$ or 奇素数) の形である。

(pr.)

(1)

$a^2 + 3b^2 =: pk$

$a =: pc + r$

$b =: pd + s$

$$\begin{aligned} r^2 + 3s^2 &= (a - pc)^2 + 3(b - pd)^2 \\ &= (a^2 + 3b^2) - 2p(ac + 3bd) + p^2(c^2 + 3d^2) \\ &= p\{k - 2(ac + 3bd) + p(c^2 + 3d^2)\} \\ &= pl \end{aligned}$$

$$\begin{aligned} pl &= r^2 + 3s^2 \\ &< \left(\frac{p}{2}\right)^2 + 3\left(\frac{p}{2}\right)^2 \\ &= p^2 \end{aligned}$$

$\therefore l < p$

(2)

$g^2 \mid r^2 + 3s^2 = pl$

$p \mid g \Rightarrow p \leqq \gcd(a, b) = 1$ より $p \nmid g$

$\therefore g^2 \mid l$, 故に $k'$ は整数。

$(ga')^2 + 3(gb')^2 = p \cdot g^2 k'$

$\therefore {a'}^2 + 3{b'}^2 = pk', k' \leqq l < p$

(3)

$p$ は $\alpha^2 + 3\beta^2$ の形でないと仮定する。

$a^2 + 3b^2$ の奇素因数 $p$ は $\alpha^2 + 3\beta^2$ の形でない。

${a'}^2 + 3{b'}^2 = pk', (a', b'$ は互いに素), 補題 1(5) より、

$k'$ は $\alpha^2 + 3\beta^2$ の形でない奇素因数 $p'$ を持つ。

ここで、$p' \leqq k' < p$

同様に、$p^{(n)} > p^{(n+1)} > \cdots \geqq 1$, これは矛盾。

故に、$p = \alpha^2 + 3\beta^2$ の形である。

(4)

補題 1(4) より、$a^2 + 3b^2 = 4^\delta p_1 \cdots p_n$ ($p_i$ : 奇素数)

故に、$4 = 1^2 + 3 \cdot 1^2$, (3) より、$a^2 + 3b^2 = ({\alpha_1}^2 + 3{\beta_1}^2) \cdots ({\alpha_n}^2 + 3{\beta_n}^2)$ の形である。■

補題 2

$p = c^2 + 3d^2$ とすると、

$a + \sqrt{3}ib = (c \pm \sqrt{3}id)\left(\dfrac{ac \pm 3bd}{p} + \sqrt{3}i \cdot \dfrac{\mp ad + bc}{p}\right)$ (複号は and, 同順)

(pr.)
$(c \pm \sqrt{3}id)\{(ac \pm 3bd) + \sqrt{3}i(\mp ad + bc)\}$
$= ac^2 \pm 3bcd \pm 3(-1)d(\mp ad + bc) + \sqrt{3}i\{c(\mp ad + bc) \pm d(ac \pm 3bd)\}$
$= ac^2 + 3ad^2 + \sqrt{3}i(bc^2 + 3bd^2)$
$= (a + \sqrt{3}ib)(c^2 + 3d^2)$
$\therefore a + \sqrt{3}ib = (c \pm \sqrt{3}id)\Big(\dfrac{ac \pm 3bd}{p} + \sqrt{3}i \cdot \dfrac{\mp ad + bc}{p}\Big)$

定理 2

$a, b$ は互いに素とする。
$a^2 + 3b^2 =: (\alpha_1{}^2 + 3\beta_1{}^2) \cdots (\alpha_n{}^2 + 3\beta_n{}^2)$ $(\alpha_k{}^2 + 3\beta_k{}^2 = 4$ or 奇素数)
この時、$a + \sqrt{3}ib = \pm(\alpha_1 \pm \sqrt{3}i\beta_1) \cdots (\alpha_n \pm \sqrt{3}i\beta_n)$ (複号任意)
この因数分解は、因数の符号, 順序を除いて一意的である。共役な因数を持たない。
(pr.)
(可能の pr.)
補題 2 より、$a + \sqrt{3}ib =: (\alpha_1 \pm \sqrt{3}i\beta_1)(a_1 + \sqrt{3}ib_1) =: z$ の形である。
$z\overline{z} = a^2 + 3b^2 = (\alpha_1{}^2 + 3\beta_1{}^2)(a_1{}^2 + 3b_1{}^2)$
$\therefore a_1{}^2 + 3b_1{}^2 = (\alpha_2{}^2 + 3\beta_2{}^2) \cdots (\alpha_n{}^2 + 3\beta_n{}^2)$
$\therefore a_1 + \sqrt{3}ib_1 =: (\alpha_2 \pm \sqrt{3}i\beta_2)(a_2 + \sqrt{3}ib_2)$
$\vdots$
$a_{n-1}{}^2 + 3b_{n-1}{}^2 = \alpha_n{}^2 + 3\beta_n{}^2$
$a_{n-1} + \sqrt{3}ib_{n-1} =: (\alpha_n \pm \sqrt{3}i\beta_n)(a_n + \sqrt{3}ib_n)$
$\cancel{a_{n-1}{}^2 + 3b_{n-1}{}^2} = (\cancel{\alpha_n{}^2 + 3\beta_n{}^2})(a_n{}^2 + 3b_n{}^2)$
$\therefore a_n{}^2 + 3b_n{}^2 = 1$
$\therefore a_n = \pm 1, b_n = 0$
$\therefore a + \sqrt{3}ib = \pm(\alpha_1 \pm \sqrt{3}i\beta_1) \cdots (\alpha_n \pm \sqrt{3}i\beta_n)$
(一意性の pr.)
$(\alpha_1 + \sqrt{3}i\beta_1) \cdots (\alpha_n + \sqrt{3}i\beta_n) = (\gamma_1 + \sqrt{3}i\delta_1) \cdots (\gamma_m + \sqrt{3}i\delta_m)$
$(\alpha_j{}^2 + 3\beta_j{}^2, \gamma_k{}^2 + 3\delta_k{}^2 = 4$ or 奇素数) とする。
$(\alpha_1{}^2 + 3\beta_1{}^2) \cdots (\alpha_n{}^2 + 3\beta_n{}^2) = (\gamma_1{}^2 + 3\delta_1{}^2) \cdots (\gamma_m{}^2 + 3\delta_m{}^2)$
素因数分解の一意性より、$n = m$, 因数の順序を適当に並び替えると $\alpha_k{}^2 + 3\beta_k{}^2 = \gamma_k{}^2 + 3\delta_k{}^2$
$\alpha_k, \beta_k$ は互いに素, 補題 2 より、$\alpha_k + \sqrt{3}i\beta_k =: (\gamma_k \pm \sqrt{3}i\delta_k)(e + \sqrt{3}if)$ の形である。
$\cancel{\alpha_k{}^2 + 3\beta_k{}^2} = (\cancel{\gamma_k{}^2 + 3\delta_k{}^2})(e^2 + 3f^2)$
$e^2 + 3f^2 = 1$
$\therefore e = \pm 1, f = 0$
$\therefore \alpha_k + \sqrt{3}i\beta_k = \pm(\gamma_k + \sqrt{3}i\delta_k)$
(非共役の pr.)
$\alpha_k + \sqrt{3}i\beta_k, \alpha_k - \sqrt{3}i\beta_k$ は $a + \sqrt{3}ib$ の因数と仮定する。
$a + \sqrt{3}ib = (\alpha_k{}^2 + 3\beta_k{}^2)(c + \sqrt{3}id)$ の形である。
$\therefore \gcd(a, b) \geqq \alpha_k{}^2 + 3\beta_k{}^2 > 1$, これは ($a, b$ は互いに素) に矛盾。
故に $a + \sqrt{3}ib$ は共役な因数を持たない。■

定理 3

$a, b$ は互いに素, $a^2 + 3b^2$ は立方数
この時、ある $u, v$ をとると、$a + \sqrt{3}ib = (u + \sqrt{3}iv)^3$
(pr.)
$a^2 + 3b^2 =: (\alpha_1{}^2 + 3\beta_1{}^2)^3 \cdots (\alpha_n{}^2 + 3\beta_n{}^2)^3$ $(\alpha_i{}^2 + 3\beta_i{}^2 = 4$ or 奇素数)
この時、$a + \sqrt{3}ib = \pm\{\pm(\alpha_1 \pm \sqrt{3}i\beta_1)^3\} \cdots \{\pm(\alpha_n \pm \sqrt{3}i\beta_n)^3\}$ (複号任意)

$$= \{\pm(\alpha_1 \pm \sqrt{3}i\beta_1)\cdots(\alpha_n \pm \sqrt{3}i\beta_n)\}^3$$
$$=: (u + \sqrt{3}iv)^3 \blacksquare$$

3 次のフェルマー最終定理

$x^3 + y^3 = z^3$の整数解 $(x, y, z)$ $(xyz \neq 0)$ は存在しない。

(pr.)

$x^3 + y^3 = z^3$の整数解 $(x, y, z)$ $(xyz \neq 0)$ が存在すると仮定する。

$(x, y, z)$ の内 $x, y, z$ が互いに素であるものを取る。

$x, y, z$ の内 1 つだけが偶数である。$x^3 + y^3 + (-z)^3 = 0$ より $x, y$ : 奇数, $z$ : 偶数としてよい。

さらに $(x, y, z)$ の内 $|z|$ が最小のものを取る。

$x + y =: 2a, x - y =: 2b$ とする。

$$z^3 = x^3 + y^3$$
$$= (a + b)^3 + (a - b)^3$$
$$= 2a(a^2 + 3b^2)$$

$(x = a + b, y = a - b$ は互いに素$), y = a - b$ は奇数より、$a, b$ は互いに素。

$z^3$は 8 の倍数, $a^2 + 3b^2$は奇数より、$a$ は 4 の倍数, $b$ は奇数。

$$\therefore \gcd(2a, a^2 + 3b^2) = \gcd(a, a^2 + 3b^2)$$
$$= \gcd(a, 3b^2)$$
$$= \gcd(a, 3)$$
$$= 1, 3$$

$1^\circ$ $\gcd(2a, a^2 + 3b^2) = 1$ と仮定する。

$z^3 = 2a(a^2 + 3b^2)$ より、$2a =: s^3, a^2 + 3b^2 =: t^3$の形である。

定理 3 より、ある $u, v$ を取ると、$\begin{cases} a = u(u + 3v)(u - 3v) \\ b = 3v(u + v)(u - v) \end{cases}$

ここで $(u, v$ は互いに素$), u$ : 4 の倍数, $u$ : 3 の倍数でない, $v$ : 奇数

$$s^3 = 2u(u + 3v)(u - 3v)$$
$$\gcd(2u, u \pm 3v) = \gcd(u, u \pm 3v)$$
$$= \gcd(u, 3v)$$
$$= \gcd(u, 3)$$
$$= 1$$
$$\gcd(u + 3v, u - 3v) = \gcd(6v, u + 3v)$$
$$= \gcd(3v, u + 3v)$$
$$= \gcd(u, 3v)$$
$$= 1$$

故に、$2u =: z'^3, u + 3v =: y'^3, u - 3v =: x'^3$の形である。

$$x'^3 + y'^3 + (-z')^3 = (u - 3v) + (u + 3v) + (-2u) = 0 \cdots ①$$
$$|z|^3 = 2|a|(a^2 + 3b^2)$$
$$= 2|u||u + 3v||u - 3v|(a^2 + 3b^2)$$
$$= |z'^3||u + 3v||u - 3v|(a^2 + 3b^2)$$
$$\geqq 3|z'|^3$$
$$> |z'|^3$$
$$\therefore |z| > |z'| \cdots ②$$

①, ②は $|z|$ の最小性に矛盾。

$\therefore \gcd(2a, a^2 + 3b^2) \neq 1$

$2^\circ$ $\gcd(2a, a^2 + 3b^2) = 3$ と仮定する。

$a =: 3a'$とする。$(a', b$ : 互いに素$), a'$ : 4 の倍数, $b$ : 3 の倍数でない。

$$z^3 = 2(a^2 + 3b^2)$$

$= 18a'(3a'^2 + b^2)$

$18a', 3a'^2 + b^2$は互いに素より、$18a' =: s^3, 3a'^2 + b^2 =: t^3$の形である。

定理 3 より、ある $u, v$ を取ると、$\begin{cases} b = u(u+3v)(u-3v) \\ a' = 3v(u+v)(u-v) \end{cases}$

ここで ($u, v$ は互いに素), $u$ : 奇数, $u$ : 3 の倍数でない, $v$ : 4 の倍数

$$2v(u+v)(u-v) = \frac{2}{3}a'$$
$$= \left(\frac{s}{3}\right)^3$$

ここで

$$\gcd(2v, u \pm v) = \gcd(v, u \pm v)$$
$$= \gcd(u, v)$$
$$= 1$$
$$\gcd(u+v, u-v) = \gcd(2v, u+v)$$
$$= \gcd(v, u+v)$$
$$= \gcd(u, v)$$
$$= 1$$

故に、$2v =: z'^3, u+v =: y'^3, u-v =: x'^3$の形である。

$x'^3 + y'^3 + (-z')^3 = (u-v) + (u+v) + (-2u) = 0 \cdots ①$

$|z|^3 = 18|a'|(3a'^2 + b^2)$

$= 18 \cdot 3|v||u+v||u-v|(a^2 + 3b^2)$

$= 27|z'^3||u+v||u-v|(a^2 + 3b^2)$

$\geqq 27 \cdot 3|z'|^3$

$> |z'|^3$

$\therefore |z| > |z'| \cdots ②$

①, ②は $|z|$ の最小性に矛盾。

$\therefore \gcd(2a, a^2 + 3b^2) \neq 3$

故に、$x^3 + y^3 = z^3$の整数解 $(x, y, z)$ は存在しない。■

【原始ピタゴラス数の分類】
原始ピタゴラス数 $(x,y,z)$ は
$(x,y,z)=(m^2-n^2,2mn,m^2+n^2)$ ($m,n$ は互いに素な自然数, $m>n$, $m-n$ は奇数)
で表せることは分かった。これにより, 原始ピタゴラス数全体を分類したい。
そこで, $(m,n)\fallingdotseq(2,1)$ の「退化」を次で定義する :
2 辺が $n,m$ の長方形と 2 辺が $n,2n$ の長方形の内, 含む方から含まれる方を除いてできる長方形 (対称差) の短辺を $n'$, 長辺を $m'$ とする。
具体的には, 次の通りである :

$$(m',n'):=\begin{cases}(2n-m,n) & \left(\frac{m}{n}<2\right)\\ (m-2n,n) & \left(2<\frac{m}{n}<3\right)\\ (n,m-2n) & \left(\frac{m}{n}>3\right)\end{cases}$$

(1) $m',n'$ は互いに素な自然数, $m'>n'$, $m'-n'$ は奇数
(2) $m'<m$
(3) $(m,n)$ に「退化」を繰り返していくと, 有限回で $(2,1)$ になる。
(4) 「退化」の $\left(\frac{m}{n}<2\right),\left(2<\frac{m}{n}<3\right),\left(\frac{m}{n}>3\right)$ への制限は, 全単射である。
(証明)
(1) はユークリッドの互除法, 仮定より, (2) は $m>n$ より成り立つ。
(3) $m>n$ より有限回で $n=1$ になる。
このとき偶奇性より $(2k,1)$ ($k$ は自然数) である。故に成り立つ。
(4) $(m',n')=(2n-m,n)$ の逆写像は $(m,n)=(2m'-n',m')$ で, これは $\frac{m}{n}<2$ などを満たす。
$(m',n')=(m-2n,n)$ の逆写像は $(m,n)=(2m'+n',m')$ で, これは $2<\frac{m}{n}<3$ などを満たす。
$(m',n')=(n,m-2n)$ の逆写像は $(m,n)=(m'+2n',n')$ で, これは $\frac{m}{n}>3$ などを満たす。■
故に, 全ての $(m,n)$ は, $(2,1)$ に「退化」の逆写像「添加」を有限回施すことで, 重複なく得られる。
このことを原始ピタゴラス数 $(x,y,z)$ で表示すると次の通りである :
全ての原始ピタゴラス数 ${}^t(x,y,z)$ は, ${}^t(3,4,5)$ に次の行列を左から有限回掛けることで, 重複なく得られる :

$$U=\begin{pmatrix}1&-2&2\\2&-1&2\\2&-2&3\end{pmatrix},A=\begin{pmatrix}1&2&2\\2&1&2\\2&2&3\end{pmatrix},D=\begin{pmatrix}-1&2&2\\-2&1&2\\-2&2&3\end{pmatrix}\quad //$$

・「添加」$u$ は 斜辺 $-$ (偶数の辺) を保つ
・「添加」$a$ は直角をはさむ 2 辺の差を $(-1)$ 倍にする
・「添加」$d$ は 斜辺 $-$ (他の奇数の辺) を保つ

(操作の分数表示)
$(m,n)$ の操作は, 既約分数 $\frac{m}{n}$ に対応させると, 簡単な計算で求められる。

$$u^{-1}:\frac{m}{n}\mapsto\frac{1}{2-\frac{m}{n}}\ \left(\frac{m}{n}<2\right)$$
$$a^{-1}:\frac{m}{n}\mapsto\frac{1}{\frac{m}{n}-2}\ \left(2<\frac{m}{n}<3\right)$$
$$d^{-1}:\frac{m}{n}\mapsto\frac{m}{n}-2\ \left(\frac{m}{n}>3\right)$$

$<$ 例 $>$
$(a,b,c)=(115,252,277)$ への $(3,4,5)$ からの「添加」列を求める。

$$(m,n)=\left(\sqrt{\frac{277+115}{2}},\sqrt{\frac{277-115}{2}}\right)=(14,9)$$
$$\frac{14}{9}\overset{u^{-1}}{\mapsto}\frac{1}{2-\frac{14}{9}}=\frac{9}{4}$$

$$\overset{a^{-1}}{\mapsto} \frac{1}{\frac{9}{4}-2} = \frac{4}{1}$$

$$\overset{d^{-1}}{\mapsto} \frac{4}{1} - 2 = \frac{2}{1}$$

$\therefore (2,1) \overset{d}{\mapsto} (4,1) \overset{a}{\mapsto} (9,4) \overset{u}{\mapsto} (14,9)$

$\therefore (3,4,5) \overset{d}{\mapsto} (15,8,17) \overset{a}{\mapsto} (65,72,97) \overset{u}{\mapsto} (115,252,277) \quad //$

＜原始ピタゴラス数の三分木＞