平方数の和

中学 3 年 3 組 32 番　平山楓馬

2017 年 5 月 2, 3 日　第 71 回灘校文化祭

本日は第 71 回灘校文化祭にお越し頂きありがとうございます。この記事では主に 2〜4 つの平方数の和について考察します。是非お読み下さい。平方剰余を含む基本的な数論の知識を前提とします。単に平方数と書いた場合は 0 を含みます。

1　二つの平方数の和

まずは素数の場合について以下の定理を示す。

定理 1 (Fermat の二平方定理)**.** p を奇素数としたとき、以下の二つの条件は同値である。
(1)　$p \equiv 1 \pmod 4$
(2)　p は 2 つの平方数の和で表される

証明. (2) → (1)　これは平方数が偶数と奇数の時それぞれ mod 4 で 0 と 1 と合同であることからわかる。
(1) → (2)　平方剰余の相互法則の第一補充法則より、$u^2 \equiv -1 \pmod p$ なる自然数 u が存在する。$0 \le x_i, y_j < \sqrt{p}$ とすると、$\left(x_i, y_j\right)$ の組み合わせの数は $\left(\left\lfloor \sqrt{p} \right\rfloor + 1\right)^2 > p$ である。従って、$(x_1, y_1) \neq (x_2, y_2)$ で $x_1 - uy_1 \equiv x_2 - uy_2 \pmod p$ なるものが存在する。$x = |x_1 - x_2|, y = |y_1 - y_2|$ とすると、$x^2 \equiv u^2y^2 \equiv -y^2 \pmod p$ ここから $x^2 + y^2 \equiv 0 \pmod p$ である。$x, y < \sqrt{p}$ より $0 < x^2 + y^2 < 2p$ なので、$x^2 + y^2 = p$ である。 □

またアメリカの Zagier は以下の「Zagier の一文証明」と呼ばれる本当に一文の証明を残している。これは簡潔なだけでなく、平方剰余の知識を一切必要としないという点で特別である。

証明. 有限集合 $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$（ただし p は mod 4 で 1 に合同な素数) 上の対合

$$(x, y, z) \to \begin{cases} (x + 2z,\ z,\ y - x - z) & x < y - z \\ (2y - x,\ y,\ x - y + z) & y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & x > 2y \end{cases}$$

はちょうど一つの固定点を持つので、$\#S$ は奇数であり、対合 $(x, y, z) \to (x, z, y)$ は固定点を持つ。 □

あまりに簡潔なので少し解説を加える必要があるだろう。対合とは 2 回施すと元に戻るような写像のことで、証明中の写像が対合であることは容易に確認できる。またこの写像の固定点は $(x, y, z) = (2y - x,\ y,\ x - y + z)$ より $x = y$ の場合のみであり、この時 $x(x + 4z) = p$ より $(x, y, z) = \left(1, 1, \frac{p-1}{4}\right)$。この対合の固定点が一つなので S の位数 $\#S$ は奇数である。逆に考えて対合 $(x, y, z) \to (x, z, y)$ は固定点を少なくとも一つは持たねばならず、これを (x, y, y) とすれば $x^2 + (2y)^2 = p$ を得る。

これらにより証明された定理 1 を利用し、一般の場合について次の定理 2 を示す。

定理 2. 自然数 n について以下の二つの条件は同値である。
(1)　n を素因数分解した時、mod 4 で 3 に合同な素数がすべて偶数乗である
(2)　n は 2 つの平方数の和で表される

証明. (1) → (2)　mod 4 で 1 に合同な素数、mod 4 で 3 に合同な素数の偶数乗、そして 2 はいずれも二平方数の和で表されるので、恒等式 $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac \pm bd)^2 + (ad \mp bc)^2$（複号同順）より示される。
(2) → (1)　以下の命題を示せば (2) → (1) を得る。

命題. n は 4 で割って 3 余る素数 q で割り切れるものとする。n が、$n=a^2+b^2$ というように二平方数の和で表されていれば、a,b はともに q で割り切れる。

a が q で割り切れないと仮定する。a と q は互いに素であるから、合同方程式 $ax\equiv 1 \pmod q$ は解を持つ。これを s とする。$1+s^2b^2\equiv s^2a^2+s^2b^2\equiv 0 \pmod q$ より、合同方程式 $x^2+1\equiv 0 \pmod q$ は $x=sb$ という解を持つ。しかし、この合同方程式が解を持つには q を 4 で割った余りが 1 か 2 である必要がある。しかしこれは矛盾。よって a は q で割り切れる。b の場合も同様である。 □

2　二つの平方数の和で表す方法は何通りあるか

定理 3. p が $4k+1$ の形の素数である時、p は二つの平方数の和として（順序と符号を無視して）ちょうど 1 通りに表される。

証明. 素数 p について表し方は高々 1 通りであることを示せばよい。p が二つの平方数の和として 2 通りに表せるとして $p=a^2+b^2=c^2+d^2$ とおく。$(ac+bd)(ac-bd)=a^2c^2-b^2d^2=\left(p-b^2\right)\left(p-d^2\right)-b^2d^2=p\left(p-b^2-d^2\right)$ より $ac\pm bd$ のいずれかは p で割り切れる。また $p^2=\left(a^2+b^2\right)\left(c^2+d^2\right)=(ac+bd)^2+(ad-bc)^2=(ac-bd)^2+(ad+bc)^2$ であることに留意する。$ac+bd$ が p で割り切れる時、$ac+bd\geq p$ より $ac+bd=p,\ ad-bc=0$。ゆえに $\dfrac{a}{b}=\dfrac{c}{d}=k$ とおけるが、この時 $a=c=k\sqrt{\dfrac{p}{k^2+1}},\ b=d=\sqrt{\dfrac{p}{k^2+1}}$ となり矛盾。$ac-bd$ が p で割り切れる場合も同様である。 □

以下、自然数 n を二つの平方数の和として表す表し方の個数を $N(n)$ とおく。ここから先では順序や符号の違いを考える。例えば $N(5)=8$ である。

補題 1. q を 2 または $4k+3$ の形の素数とし、$n=q^2m$ とすると、$N(n)=N(m)$ である。

証明. m を二つの平方数の和で表す方法の一つを $m=a^2+b^2$ とおくと、$n=q^2m=(qa)^2+(qb)^2$ だから $N(n)\geq N(m)$。
逆に n を二つの平方数の和で表す方法の一つを $n=x^2+y^2$ とおく。
(1)　$q=2$ の場合　n は 4 で割り切れるから x,y はともに偶数でなければならない。したがって $m=\left(\dfrac{x}{2}\right)^2+\left(\dfrac{y}{2}\right)^2$ を得る。
(2)　q が $4k+3$ の形の素数の場合　定理 2 の証明の命題より $x,y,$ はともに q で割り切れる。$x=qx_1, y=qy_1$ とおくと $m=x_1^2+y_1^2$ を得る。
(1) と (2) より $N(n)\leq N(m)$ で、$N(n)\geq N(m)$ と合わせて $N(n)=N(m)$ となる。 □

補題 2. m を奇数とし、$n=2m$ とすると $N(n)=N(m)$ である。

証明. m を二つの平方数の和で表す方法の一つを $m=a^2+b^2$ とおくと、$n=(1^2+1^2)(a^2+b^2)=(a+b)^2+(a-b)^2$ より $N(n)\geq N(m)$。逆に n を二つの平方数の和で表す方法の一つを $n=x^2+y^2$ とおくと、$m=\dfrac{1}{2}(x^2+y^2)=\dfrac{1}{4}\left((x+y)^2+(x-y)^2\right)=\left(\dfrac{x+y}{2}\right)^2+\left(\dfrac{x-y}{2}\right)^2$ より $N(n)\leq N(m)$。よって $N(n)=N(m)$。 □

補題 3. 自然数 n の異なる素因数の個数を $\omega(n)$ とすると、n の正の約数の個数 $d(n)=\displaystyle\sum_{d^2\mid n}2^{\omega\left(\frac{n}{d^2}\right)}$ が成り立つ。

証明. まず以下の命題を示す。

命題. 積が n で最大公約数が d である自然数の組 (x,y) の個数は $2^{\omega\left(\frac{n}{d^2}\right)}$ である。

$x=dx',\ y=dy'$ と表せる。ただし x' と y' は互いに素である。$xy=n$ にこれを代入して $x'y'=\dfrac{n}{d^2}$。$\dfrac{n}{d^2}=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ と素因数分解されるとし、この時互いに素な整数の組 (x',y') は、$p_i^{a_i}$ がどちらに含まれるかでそれぞれ 2 通りだから $2^k=2^{\omega\left(\frac{n}{d^2}\right)}$ である。これにより命題は示された。
$xy=n$ を満たす組 (x,y) の個数は $d(n)$ に等しい。x と y の最大公約数として考えられる値を $d_1,d_2,\cdots,d_l$ とすると、$xy=n$ かつ最大公約数が d_i であるような組はそれぞれ $2^{\omega\left(\frac{n}{d_i^2}\right)}$ だから $d(n)=2^{\omega\left(\frac{n}{d_1^2}\right)}+2^{\omega\left(\frac{n}{d_2^2}\right)}+\cdots+2^{\omega\left(\frac{n}{d_l^2}\right)}$。よって題意は示された。 □

定理 4. $n=2^a\left(p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}\right)\left(q_1^{b_1}q_2^{b_2}\cdots q_t^{b_t}\right)$ と素因数分解されるとする。ただし各 p_i は $4k+1$ の形の素数、q_i は $4k+3$ の形の素数、b_i はすべて偶数とする。この時、$N(n)=4(a_1+1)(a_2+1)\cdots(a_s+1)$ である。

証明. $m=p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ とおき、$m=x^2+y^2$ となるすべての組 (x,y) を考える。x と y の最大公約数を d とすると、$\dfrac{m}{d^2}$ も $4k+1$ の形の素因子のみを持つ整数なので、定理 2 より $\dfrac{m}{d^2}=X^2+Y^2$ とおける。$x=dX,\ y=dY$ であり X と Y は互いに素である。定理 3 と恒等式 $\left(a^2+b^2\right)\left(c^2+d^2\right)=(ac+bd)^2+(ad-bc)^2=(ac-bd)^2+(ad+bc)^2$ より、$\dfrac{m}{d^2}$ の異なる素因子の数を s とすれば (X,Y) の組は順序と符号を無視すれば 2^{s-1} 通りである。順序と符号を考えれば $8\times2^{s-1}=2^{s+2}=2^{\omega\left(\frac{n}{d^2}\right)+2}=4\cdot2^{\omega\left(\frac{n}{d^2}\right)}$ 通りであるから $N(m)=4\displaystyle\sum_{d^2|n}2^{\omega\left(\frac{n}{d^2}\right)}$。定理 3 より $N(m)=4d(m)=4(a_1+1)(a_2+1)\cdots(a_s+1)$ である。
$N(n)$ について考える。補題 1 及び 2 より $N(n)=N(2^am)=N(m)=4(a_1+1)(a_2+1)\cdots(a_s+1)$ となる。 □

これで $N(n)$ の値が得られたが、以下のような異なる表記も知られている。これを示す。

定理 5. $D_1(n),D_3(n)$ はそれぞれ n の正の約数のうち $4k+1,\ 4k+3$ の形のものの個数とする。このとき $N(n)=4(D_1(n)-D_3(n))$ である。

補題 4. $f(n)=D_1(n)-D_3(n)$ とおくと、互いに素な自然数 a,b に対して $f(ab)=f(a)f(b)$

証明. mod 4 での積を考えると $D_1(ab)=D_1(a)D_1(b)+D_3(a)D_3(b)$, $D_3(ab)=D_1(a)D_3(b)+D_3(a)D_1(b)$ を得る。よって

$$\begin{aligned}f(ab)&=D_1(ab)-D_3(ab)=(D_1(a)D_1(b)+D_3(a)D_3(b))-(D_1(a)D_3(b)+D_3(a)D_1(b))\\&=(D_1(a)-D_3(a))(D_1(b)-D_3(b))=f(a)f(b)\end{aligned}$$

□

補題 5. $g(n)=\dfrac{N(n)}{4}$ とおくと、互いに素な自然数 a,b に対して $g(ab)=g(a)g(b)$

証明. a と b が互いに素であることを踏まえてそれぞれを素因数分解した形を考えれば容易に示される。 □

定理 5 を示そう。

証明. $f(n)=g(n)$ を示せばよい。p を $4k+1$ の形の素数、q を $4k+3$ の形の素数とする。
(1) $n=2^a$ の時 $f(2^a)=D_1(2^a)-D_3(2^a)=1-0=1$、$g(2^a)=\dfrac{N(2^a)}{4}=\dfrac{4}{4}=1$ より $f(n)=g(n)$
(2) $n=p^a$ の時 p^a の約数はすべて $4k+1$ の形なので $f(p^a)=D_1(p^a)-D_3(p^a)=(a+1)-0=a+1$。また $g(p^a)=\dfrac{N(p^a)}{4}=\dfrac{4(a+1)}{4}=a+1$ より $f(n)=g(n)$
(3) $n=q^a$ の時 約数のうち $4k+1$ の形のものは $1,q^2,q^4,\cdots$、$4k+3$ の形のものは $q,q^3,q^5,\cdots$ である。したがって a が偶数の時は $f(q^a)=1$ で $g(q^a)=\dfrac{4(0+1)}{4}=1$ で $f(n)=g(n)$。また a が奇数の時は $f(q^a)=0$ で $g(q^a)=0$ より $f(n)=g(n)$。
以下 $n=2^a\left(p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}\right)\left(q_1^{b_1}q_2^{b_2}\cdots q_t^{b_t}\right)$ と素因数分解されるとする。補題 4 より $f(n)=f(2^a)f\left(p_1^{a_1}\right)\cdots f(p_s^{a_s})f\left(q_1^{b_1}\right)\cdots f\left(q_t^{b_t}\right)$ で、補題 5 より $g(n)=g(2^a)g\left(p_1^{a_1}\right)\cdots g(p_s^{a_s})g\left(q_1^{b_1}\right)\cdots g\left(q_t^{b_t}\right)$ となるから、(1)〜(3) より $f(n)=g(n)$ を得る。よって題意は示された。 □

3　三つの平方数の和

3 つの場合の証明は 2 つや 4 つの場合とは異なり簡潔ではない。大筋は文献 [2] による。

定理 6. 自然数 n が 3 つの平方数の和であるための必要十分条件は、n が $4^m(8k+7)$ の形でないことである。

証明. まず、$4^m(8k+7)$ の形の自然数は 3 つの平方数の和でないことを m についての数学的帰納法で示す。
(1) $m=0$ の場合 $8k+7$ の形の自然数が三平方数の和でないことは、$4k+3$ の形の自然数が二平方数の和でないことの証明と同様にできる。
(2) $m=l\ (l\geq0)$ の場合に主張が正しいと仮定する。$4^{l+1}(8k+7)=a^2+b^2+c^2\cdots\cdots(1)$ と表せたと仮定する。この時、a,b,c は三つとも偶数か一つのみが偶数のいずれかである。一つのみが偶数の時、a のみが偶数と仮定しても一般性を失わな

い。ここから $a^2 \equiv 0 \pmod 4$, $b^2 \equiv c^2 \equiv 1 \pmod 4$ で、$a^2+b^2+c^2 \equiv 2 \pmod 4$ となるが、左辺は 4 の倍数だからこれは矛盾。ゆえに、a,b,c はすべて偶数でなければならない。(1) の両辺を 4 で割って $4^l(8k+7) = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2$ で、$\frac{a}{2}, \frac{b}{2}, \frac{c}{2}$ はすべて整数となるが、これは帰納法の仮定に矛盾する。よって $m = l+1$ の場合も主張は正しく、数学的帰納法により示された。
逆を示す。n は平方因子を持たないとして良く、$n \equiv 1,2,3,5,6 \pmod 8$ の時に示せば良い。まず以下の補題を示す。

補題 6 (Minkowski の凸体定理)**.** 3 次元空間内の領域 $\mathcal{B}$ は原点対称かつ凸とする。もし $\mathcal{B}$ の体積が 8 よりも大きいのであれば $\mathcal{B}$ は原点以外の格子点を含む。

証明. t を自然数とする。yz 平面、xz 平面、zx 平面とそれぞれ平行な平面

$$x = \frac{2p}{t}\ ,\ y = \frac{2p}{t}\ ,\ z = \frac{2p}{t}\ \ (p \in \mathbb{Z})$$

を考える。これらによって 3 次元空間は 1 辺の長さが $2/t$ の立方体に分割される。頂点 $P = (2p/t, 2q/t, 2r/t)$ と立方体

$$C(P) = \left\{ (x,y,z) \;\middle|\; \frac{2p}{t} \le x \le \frac{2(p+1)}{t},\ \frac{2q}{t} \le y \le \frac{2(q+1)}{t},\ \frac{2r}{t} \le z \le \frac{2(r+1)}{t} \right\}$$

を対応させる。この時 P を $C(P)$ の角と呼ぶ。領域 $\mathcal{B}$ に含まれる角の総数を $N(t)$ とすれば、$\mathcal{B}$ の体積 V に対して

$$\lim_{t\to\infty} \left(\frac{2}{t}\right)^3 N(t) = V$$

が成立する。$V > 8$ より、十分大きい t に対しては $N(t) > t^3$ が成立する。
整数の組 (p,q,r) を $\bmod t$ で見ると t^3 通りしか可能性が無いことから、$\mathcal{B}$ に含まれる 2 つの角 $P_1 = (2p_1/t,\ 2q_1/t,\ 2r_1/t)$, $P_2 = (2p_2/t,\ 2q_2/t,\ 2r_2/t)$ で $\bmod t$ で見て合同なものが存在する。$\mathcal{B}$ は原点対称だから P_2 の対称点 P_2' も $\mathcal{B}$ に含まれ、また $\mathcal{B}$ は凸だから P_1 と P_2' の中点 M も $\mathcal{B}$ に含まれる。P_1, P_2 の定義より M は格子点だから、題意は示された。 □

奇数 $p = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$（$p_1, p_2 \cdots$ は素数) について Lagrange 記号を拡張して Jacobi 記号を次の様に定義する。Lagrange 記号の場合を前提とし、相互法則や補充法則を含む同様の関係が成り立つことの証明を是非考えてみてほしい。この記事の最後に掲載している。

$$\left(\frac{n}{p}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)^{k_i}$$

(1) $n \equiv 1,3,5 \pmod 8$ の場合 $n = p_1 p_2 \cdots p_r$ と素因数分解されるとする。$\bmod 4n$ で考えると、Dirichlet の算術級数定理より以下を満たす素数 q が存在する。

$$q \equiv 1 \pmod 4\,, \quad \left(\frac{-2q}{p_i}\right) = 1 \ \ (j = 1,2,\cdots,r)$$

これより

$$1 = \prod_{i=1}^{r} \left(\frac{-2q}{p_i}\right) = \prod_{i=1}^{r} \left(\frac{-2}{p_i}\right)\left(\frac{q}{p_i}\right) = \left(\frac{-2}{n}\right) \prod_{i=1}^{r} \left(\frac{p_i}{q}\right) = \left(\frac{-2}{n}\right)\left(\frac{n}{q}\right) = \left(\frac{n}{q}\right) = \left(\frac{-n}{q}\right)$$

q は奇素数なので $b^2 \equiv -n \pmod q$ を満たす奇数 b が存在する。$b^2 - qh_1 = -n$ とする。この式を $\bmod 4$ で考えると $1 - h_1 \equiv 1 \pmod 4$ なので $h_1 = 4h$ とおける。また、q の定義より $t^2 \equiv -1/(2q) \pmod n$ を満たす整数 t が存在する。
今、領域 $\mathcal{B} : X^2 + Y^2 + Z^2 < 2n$ を考える。ただし (X,Y,Z) は以下の (x,y,z) の一次変換で得られるものとする。

$$X = 2tqx + tby + nz \quad Y = (2q)^{1/2}x + \frac{b}{(2q)^{1/2}}y \quad Z = \frac{n^{1/2}}{(2q)^{1/2}}y$$

(X,Y,Z) 空間において $\mathcal{B}$ は凸かつ原点対称で体積は $4\pi(2n)^{3/2}/3$ である。(x,y,z) 空間においても $\mathcal{B}$ は凸かつ原点対称で、上の一次変換の行列式は $n^{3/2}$ だから体積は $4\pi(2n)^{3/2}/3 \div n^{3/2} = 2^{7/2}\pi/3$。これは明らかに 8 より大きいので、Minkowski の凸

体定理より $\mathcal{B}$ は原点以外の格子点 (x_1, y_1, z_1) を含む。一次変換で (x_1, y_1, z_1) が移る先を (X_1, Y_1, Z_1) とする。

$$\begin{aligned} X_1^2 + Y_1^2 + Z_1^2 &= (2tqx_1 + tby_1 + nz_1)^2 + \left((2q)^{1/2}x_1 + \frac{b}{(2q)^{1/2}}y_1\right)^2 + \left(\frac{n^{1/2}}{(2q)^{1/2}}y_1\right)^2 \\ &\equiv t^2(2qx_1 + by_1)^2 + \frac{1}{2q}(2qx_1 + by_1)^2 \\ &\equiv 0 \pmod{n} \end{aligned}$$

$$\begin{aligned} X_1^2 + Y_1^2 + Z_1^2 &= X_1^2 + \left((2q)^{1/2}x_1 + \frac{b}{(2q)^{1/2}}y_1\right)^2 + \left(\frac{n^{1/2}}{(2q)^{1/2}}y_1\right)^2 \\ &= X_1^2 + \frac{1}{2q}(2qx_1 + by_1)^2 + \frac{n}{2q}y_1^2 \\ &= X_1^2 + 2(qx_1^2 + bx_1y_1 + hy_1^2) \end{aligned}$$

$v = (qx_1^2 + bx_1y_1 + hy_1^2)$ とおくと、上の 2 つの式より $n \mid X_1^2 + 2v$。定義より $X_1^2 + Y_1^2 + Z_1^2 = X_1^2 + 2v < 2n$ で、また (X_1, Y_1, Z_1) は原点ではないので $X_1^2 + 2v \neq 0$、ゆえに $X_1^2 + 2v = n$。

v は奇素数 p で奇数回割り切れる、すなわち $p^{2m+1} \parallel v$ であるとする。

(i) $p \nmid n$ の時 $X_1^2 + 2v = n$ より $(n/q) = 1$。$p \mid q$ の時、$b^2 - 4qh = -n$ より $(-n/q) = 1$。$p \nmid q$ の時、$4qv = (2qx_1 + by_1)^2 + ny_1^2$ より $p^{2m+1} \parallel (2qx_1 + by_1)^2 + ny_1^2$ で以下より $(-n/p) = 1$。いずれの場合も $(-n/p) = 1$ だから $(-1/p) = 1$ で $p \equiv 1 \pmod 4$。

$$1 = \left(\frac{-ny_1^2}{p^{2n+1}}\right) = \left(\frac{-n}{p}\right)^{2n+1}\left(\frac{y_1}{p^{2n+1}}\right)^2 = \left(\frac{-n}{p}\right)^{2n+1}$$

(ii) $p \mid n$ の時 $X_1^2 + 2v = n$ と $X_1^2 + \left((2qx_1 + by_1)^2 + ny_1^2\right)/2q = n$ より $p \mid X_1$ かつ $p \mid (2qx_1 + by_1)$ で、これより $y_1^2 \equiv 2q \pmod p$ だから $(2q/p) = 1$。q の定義より $(-2q/p) = 1$ だから $(-1/p) = 1$ で $p \equiv 1 \pmod 4$。

ゆえに v を奇数回割り切る素数 p はすべて $p \equiv 1 \pmod 4$ だから、定理 2 より $2v$ は二つの平方数の和で表される。よって $n = X_1^2 + 2v$ より $n \equiv 3 \pmod 8$ の時 n は三つの平方数の和で表される。

(2) $n \equiv 2, 6 \pmod 8$ の場合は以下のように (1) の証明を置き換える。n を割り切るすべての奇素数 p_j に対して $\left(\frac{-2q}{p_i}\right) = 1$ を満たす素数 $q \equiv 1 \pmod 4$ が存在する。$n = 2n_1$ とおけば

$$1 = \prod_{i=1}^{r}\left(\frac{-2q}{p_i}\right) = \prod_{i=1}^{r}\left(\frac{-2}{p_i}\right)\left(\frac{q}{p_i}\right) = \left(\frac{-2}{n_1}\right)\prod_{i=1}^{r}\left(\frac{p_i}{q}\right) = \left(\frac{-2}{n_1}\right)\left(\frac{n_1}{q}\right) = \left(\frac{n_1}{q}\right) = \left(\frac{-n_1}{q}\right)$$

より $b^2 - qh = -m$ とおける。また同様に $t^2 \equiv -1/q \pmod n$ を満たす整数 t が存在する。(x, y, z) の一次変換を以下のように定める。

$$X = tqx + tby + nz \quad Y = q^{1/2}x + \frac{b}{q^{1/2}}y \quad Z = \frac{n^{1/2}}{q^{1/2}}y$$

これらを用いれば (1) と同様の証明が成立し、(1) と (2) を合わせて証明が完了する。 □

4 四つの平方数の和

まず必要ないくつかの補題を示す。

補題 7. $3m$ が 4 つの平方数の和なら、m 自身もまた 4 つの平方数の和である。

証明. $3m = a^2 + b^2 + c^2 + d^2$ とおく。平方数を 3 で割った余りは 0 か 1 である。$a^2 + b^2 + c^2 + d^2$ は 3 の倍数だから、a, b, c, d はすべて 3 の倍数か、一つだけが 3 の倍数かどちらかである。

(1) a, b, c, d がすべて 3 の倍数の時

$A = \dfrac{b + c + d}{3}$, $B = \dfrac{a + c - d}{3}$, $C = \dfrac{a - b + d}{3}$, $D = \dfrac{a + b - c}{3}$ とおくと、A, B, C, D はすべて整数である。

$$\begin{aligned} 9A^2 &= b^2 + c^2 + d^2 + 2bc + 2cd + 2bd \\ 9B^2 &= a^2 + c^2 + d^2 + 2ac - 2cd - 2ad \\ 9C^2 &= a^2 + b^2 + d^2 - 2ab + 2ad - 2bd \\ 9D^2 &= a^2 + b^2 + c^2 + 2ab - 2ac - 2bc \end{aligned}$$

この四つの式を辺々加えると $9(A^2+B^2+C^2+D^2)=3(a^2+b^2+c^2+d^2)=9m$。よって m も 4 つの平方数の和である。
(2)　一つだけが 3 の倍数の時
$a\equiv 0 \pmod 3$, $b\equiv c\equiv d\equiv 1 \pmod 3$ としても一般性を失わない。例えば $b\equiv -1 \pmod 3$ だとしたら $-b$ を b に置き換えればよいからである。あとは、(1) と同様の手順により示すことができる。 □

補題 8. n が平方因子を含まない自然数である時、適当な整数 a,b を選べば a^2+b^2+1 が p で割り切れるようにできる。

証明. まず n が素数の時を示す。$n=2$ の場合、$a=1,b=0$ などとすればよい。n が奇素数の場合、$q=\frac{n-1}{2}$ とおくと、q は整数。集合 A,B を $A=\left\{0^2,1^2,\cdots,q^2\right\}$, $B=\left\{-1-0^2,-1-1^2,\cdots,-1-q^2\right\}$ とすると、A,B のそれぞれ $q+1$ 個の要素は法 n で合同でない。$\#A+\#B=2(q+1)=n+1>n$ だから $a^2\equiv -1-b^2 \pmod n$ となる $a^2\in A$ と $-1-b^2\in B$ を取ることができ、$a^2+b^2+1\equiv 0 \pmod n$ となる。
次に n の異なる素因数が 2 つの時を示す。$n=p_1p_2$ とおく。素数 p_1,p_2 について主張は成り立つので、$a_1^2+b_1^2+1\equiv 0 \pmod{p_1}$ 及び $a_2^2+b_2^2+1\equiv 0 \pmod{p_2}$ となる整数 a_1,a_2,b_1,b_2 が存在する。これらについて次の 2 つの連立合同式を考えると、中国剰余定理によりこれらはそれぞれ解を持つ。

$$\begin{cases} x_1\equiv a_1 \pmod{p_1} \\ x_1\equiv a_2 \pmod{p_2} \end{cases} \qquad \begin{cases} x_2\equiv b_1 \pmod{p_1} \\ x_2\equiv b_2 \pmod{p_2} \end{cases}$$

それぞれの解を a,b とおくと a と b は $a^2+b^2+1\equiv 0 \pmod{p_1}$ かつ $a^2+b^2+1\equiv 0 \pmod{p_2}$ を満たすため、$a^2+b^2+1\equiv 0 \pmod n$ となる。n の異なる素因数の数が 3 つ以上でも同様の議論を繰り返せば良い。 □

これらを利用すると以下の非常に簡潔な結論に達する。これを示そう。

定理 7 (Lagrange の四平方和定理)**.** すべての自然数は、4 つの平方数の和である。

証明. 任意の自然数は平方数と平方因子を含まない自然数の積なので、平方因子を含まない自然数 n の場合に示せば十分である。補題 8 より $a^2+b^2+1\equiv 0 \pmod n$ となる整数 a,b が存在する。s,t,u,v が 0 から $[\sqrt{n}\,]$ までのすべての整数値を取る時、2 つの整数の組 $(as+bt-u,bs-at-v)$ を考える。この組は全部で $([\sqrt{n}\,]+1)^4$ 通りあるが、$\bmod n$ で考えると n^2 通りで、$([\sqrt{n}\,]+1)^4>\sqrt{n}^{\,4}=n^2$ より

$$\begin{cases} as_1+bt_1-u_1\equiv as_2+bt_2-u_2 \pmod n \\ bs_1-at_1-v_1\equiv bs_2-at_2-v_2 \pmod n \end{cases}$$

を満たす異なる組 (s_1,t_1,u_1,v_1) と (s_2,t_2,u_2,v_2) が存在する。ここで s,t,u,v を $s=s_1-s_2$ のようにおけば、以下の様に表せる。

$$\begin{cases} as+bt\equiv u \pmod n \\ bs-at\equiv v \pmod n \end{cases}$$

各式を 2 乗して加えると $u^2+v^2\equiv (as+bt)^2+(bs-at)^2=(a^2+b^2)(s^2+t^2)\equiv -(s^2+t^2) \pmod n$ を得るので、整数 l を用いて $s^2+t^2+u^2+v^2=l\cdot n$ と書ける。$-[\sqrt{n}\,]<s,t,u,v<[\sqrt{n}\,]$ かつ $s,t,u,v\neq 0$ より $0<s^2+t^2+u^2+v^2=l\cdot n\le 4[\sqrt{n}\,]^2<4n$ なので $l=1,2,3$ を得る。
$l=1$ ならば明らかに成り立つ。$l=3$ の時は補題 7 より成り立つ。
$l=2$ の時 $s^2+t^2+u^2+v^2=2n$ より s,t,u,v のうち偶数は偶数個。s,t の偶奇が一致するとして良い。この時 $\frac{s+t}{2},\frac{s-t}{2},\frac{u+v}{2},\frac{u-v}{2}$ はいずれも整数で、これらの平方の和は $\frac{1}{2}\left(s^2+t^2+u^2+v^2\right)=n$ である。 □

5　正の平方数の和

第 4 章ではすべての自然数は 4 つの平方数の和であることを示したが、この「平方数」から 0 を取り除くと結論はどのようになるか考察する。

補題 9. 自然数 n について、$2n$ が 4 つの正の平方数の和で表されることと、$8n$ が 4 つの正の平方数の和で表されることは同値である。

証明. 左から右は明らかなので右から左を示す。すべての平方数は mod 8 で 0,1,4 に合同だから、和が $8n$ になる 4 つの平方数はすべて mod 8 で 0 か 4 に合同である。両辺を 4 で割ることで $2n$ を 4 つの正の平方数の和として表すことができる。 □

例えば 6 は 4 つの正の平方数の和ではないが、補題 9 より $6\times4=24$ も 4 つの正の平方数の和でなく、同様に 4 つの正の平方数の和でない自然数が無限に存在することがわかる。これを 5 つ以上に増やすとどうなるだろうか。

定理 8. 170 以上のすべての自然数 n は 5 つの正の平方数の和かつ 6 つの正の平方数の和として表せる。

証明. $169=13^2=5^2+13^2=3^2+4^2+12^2=1^2+2^2+8^2+10^2=2^2+2^2+2^2+6^2+11^2$ である。定理 4 より $n-169$ は高々 4 つの正の平方数の和で表されるから、例えば $n-169$ が 4 つの正の平方数の和 $a^2+b^2+c^2+d^2$ として表される場合は、$n=a^2+b^2+c^2+d^2+13^2=a^2+b^2+c^2+d^2+5^2+12^2$ とすれば良く、3 つ以下の場合も同様である。 □

おわりに　ウェアリングの問題

この記事では 2〜4 つの平方数の和について様々な主張を示しました。すべての自然数は 4 つの平方数の和で表せるという事実は驚くべきものでしょう。この「平方数」の部分を「立方数」や一般に「k 乗数」へ拡張したらどうなるのか、という問題をウェアリングの問題といいます。すべての自然数を 0 以上の k 乗数の和として表すのに必要な最低限の個数を $g(k)$ とおきます。これを用いると $g(2)=4$ です。$k=3$ と 4 の場合はそれぞれ $23=2^3\times2+1^3\times7$ と $79=2^4\times4+1^4\times15$ が最善であることがわかるので $g(3)\geq9$ と $g(4)\geq19$ がわかります。実際にはそれぞれで等号が成り立ちます。これらについてはまた考察してみたいと思います。一般に k 乗数の場合は $g(k)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2$ が成り立つと予想されてされておりこれは未解決問題です。この等号を不等号に緩めた以下の主張を示してこの記事の終わりとしたいと思います。この記事をお読み頂きありがとうございました。引き続き灘校文化祭をお楽しみ下さい。

定理 9. $g(k)\geq2^k+\left[\left(\frac{3}{2}\right)^k\right]-2$

証明. $q=\left[\left(\frac{3}{2}\right)^k\right]$, $n=2^kq-1$ とおくと、$n\leq2^k\cdot\left(\frac{3}{2}\right)^k-1=3^k-1<3^k$ より n を k 乗数の和で表す時には 2^k と 1^k しか使えない。n を 2^k と 1^k で表す最善の方法は $n=2^k(q-1)+1^k\left(2^k-1\right)$ であるから、$g(k)\geq(q-1)+\left(2^k-1\right)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2$ □

補足　Jacobi 記号への拡張

第 3 章で Jacobi 記号を定義した際、「相互法則や補充法則を含む同様の関係が成り立つことの証明を是非考えてみてほしい」と書いた。ここでは Lagrange 記号における第一・二補充法則と相互法則を前提とし、Jacobi 記号でも同様の法則が成り立つことを導く。$\prod_{p\mid n}$ は n の素因子 p すべてについて積を取ることを表す。下に何も書いていない場合も同様である。

定理 10 (第一補充法則)**.** 正の奇数 n について、$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$

証明. a,b を奇数とすると、$(a-1)(b-1)\equiv0\pmod4$ より $ab-1\equiv(a-1)+(b-1)\pmod4$ で $\frac{ab-1}{2}\equiv\frac{a-1}{2}+\frac{b-1}{2}\pmod2$。これを奇数 3 つ以上に増やしても同じだから、

$$\left(\frac{-1}{n}\right)=\prod_{p\mid n}\left(\frac{-1}{p}\right)=\prod_{p\mid n}(-1)^{\frac{p-1}{2}}=(-1)^{\sum\frac{p-1}{2}}=(-1)^{\frac{n-1}{2}}$$

□

定理 11 (第二補充法則)**.** 正の奇数 n について、$\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$

証明. a,b を奇数とすると、$(a^2-1)(b^2-1)\equiv0\pmod{16}$ より $a^2b^2-1\equiv(a^2-1)+(b^2-1)\pmod{16}$ で $\frac{a^2b^2-1}{8}\equiv$

$\frac{a^2-1}{8}+\frac{b^2-1}{8} \pmod 2$。これを奇数 3 つ以上に増やしても同じだから、

$$\left(\frac{2}{n}\right)=\prod_{p\mid n}\left(\frac{2}{p}\right)=\prod_{p\mid n}(-1)^{\frac{p^2-1}{8}}=(-1)^{\sum\frac{p^2-1}{8}}=(-1)^{\frac{n^2-1}{8}}$$

□

定理 12 (相互法則)**.** 正の奇数 m,n について、$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$

証明.

$$\left(\frac{m}{n}\right)=\prod_{p\mid n}\left(\frac{m}{p}\right)=\prod_{p\mid n}\prod_{q\mid m}\left(\frac{q}{p}\right)$$

m と n を入れ替えても同じだから、

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{q\mid m}\prod_{p\mid n}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\prod_{q\mid m}\prod_{p\mid n}(-1)^{\frac{m-1}{2}\frac{n-1}{2}}=(-1)^{\sum\sum\frac{p-1}{2}\frac{q-1}{2}}=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

□

参考文献

[1] 水上勉・黒川信重、『チャレンジ！整数の問題 199』、日本評論社、2005

[2] N. C. Ankeny, “SUMS OF THREE SQUARES”, 1957

[3] 寺垣内政一、『多角数に関する 3 つの定理』、2007