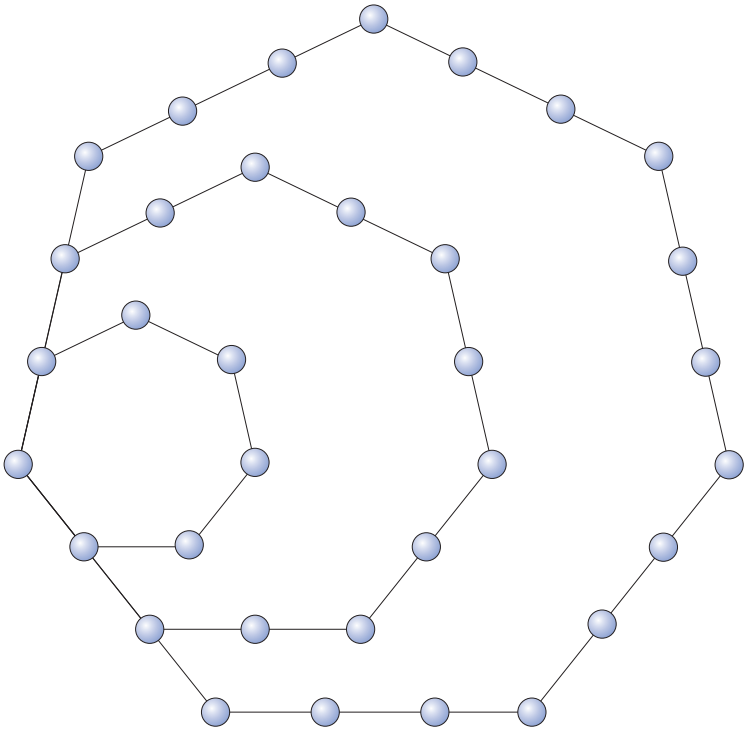
多角数に関する３つの定理



寺垣内　政一（広島大学大学院教育学研究科）

はじめに

本稿は，広島大学大学院教育学研究科リサーチオフィス経費プロジェクトの一環として，発展的な内容に意欲をもつ高校生，高等学校数学科教員を目指す大学生あるいは現職の高等学校教員を対象に，多角数に関する 3 つの著名な定理を，その証明も含めて紹介することにある．

多角数とは，正多角形にそって，たとえば碁石を並べた際の碁石の総数として定義される数である．中でも，三角形状に碁石を並べて得られる三角数は有名であり，ドイツの詩人ハンス・エンツェンスベルガーの著書「数の悪魔」第五夜にも登場する．算数・数学嫌いの少年ロバートの夢の中に夜な夜な「数の悪魔」が出現し，ロバートに数学の講義をするという物語だが，驚くべきことにその第五夜において，どんな自然数も高々 3 つの三角数の和として表せることが言及されている．この事実は，一般に Gauss の定理として知られており，本稿の §4 でその証明を紹介するのだが，やさしいといえるような証明は今日にいたっても知られていない．Gauss の証明は，3 元 2 次形式とよばれるものを用いたものだと聞くが，§4 で述べる証明は，Ankeny によって 1957 年に発表されたもので，Fermat の二平方定理，Dirichlet の算術級数定理および Minkowski の凸体定理を利用する．そのため，§4 の準備として，§2 では，Legendre symbol および Jacobi symbol の基本性質を証明無しに紹介し，中国剰余定理および Minkowski の定理を証明する．節を変えて §3 で Fermat の二平方定理の証明を与える．残念ながら，Dirichlet の算術級数定理の証明は困難であり，収録できない．これらは，三角数に関する Gauss の定理の証明にのみ必要となるものであり，§5 および §6 は独立に読むことができる．

§5 では，Lagrange の四平方定理を扱う．四角数とは平方数に他ならず，四平方定理とは，任意の自然数が高々 4 つの平方数の和として表されることを主張する．現在では，様々な証明が知られているが，ここで紹介するものは剰余類を用いる程度の初等的な証明である．

最後に §6 では，Cauchy の多角数定理を紹介する．任意の自然数は，m 角数の高々 m 個の和として表されることを主張するもので，Fermat が証明は残さず，見つけたとのみ書き残し，後に Cauchy が証明を与えたものである．ここでは，1987 年に Nathanson が発表した短い証明を紹介する．

本稿で扱った 3 つの定理は，いずれも著名なものであり，現職の教員の中でも耳にされたことのある方々は多いと思われる．しかし，その証明となると接する機会は少なく，と

りわけ Gauss の定理と Cauchy の定理については証明の掲載された文献へのアクセスすら容易ではないと思われ，そのことが本稿作成の動機となった．

本稿の作成にあたって，広島大学大学院理学研究科の山内卓也氏から関連文献の教示や助言をいただいた．ここに感謝の意を表したい．なお，本文中に誤りがあるとすれば，筆者の責任であることはいうまでもない．

2007 年 1 月　寺垣内　政一

追記（2008 年 4 月 24 日）．授業で何度か使用しているうちに，タイプミス等が散見されたので，修正を行った．

目次

1　多角数

三角数とは，図 1 のように，たとえば碁石を三角形状に並べたときの碁石の総数として現れる整数である．三角数のなす数列は

$$1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, \ldots$$

となる．ちなみに，36 番目の三角数は，黙示録に記された獣の数 666 である．

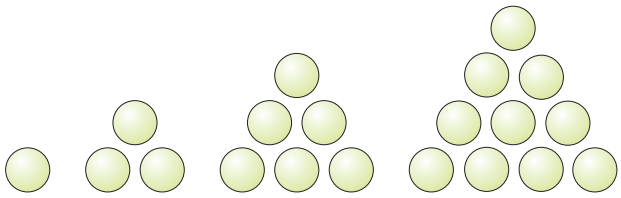


図 1　三角数

同様に，四角数は，図 2 のように正方形状に碁石を並べたときの碁石の総数であり，四角数のなす数列は，

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$$

となり，平方数のなす数列に他ならない．

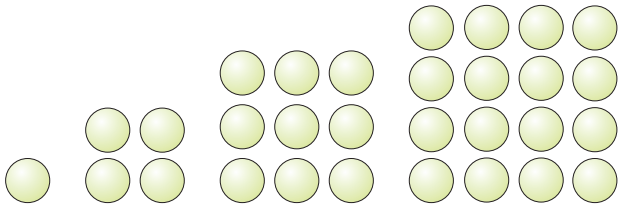


図 2　四角数

さらに，五角数とは，正五角形にそって碁石を並べたときの碁石の総数であり (図 3)，

$$1, 5, 12, 22, 35, 51, 70, 92, 117, 145, \ldots$$

となる．

一般に，整数 $m \geq 1$ に対して，$m+2$ 角数とは，順次拡大していく正 $m+2$ 角形にそって碁石を並べたときの碁石の総数として定義される．従って，階差数列が初項 $m+1$，公

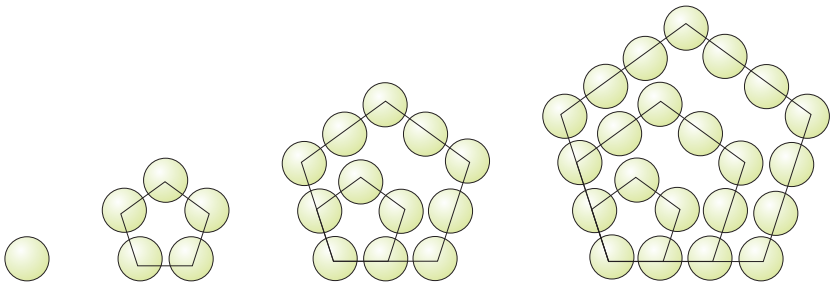


図 3　五角数

差 m の等差数列であるような数列を形成するので，k 番目の $m+2$ 角数を $p_m(k)$ で表せば，

$$\begin{aligned} p_m(k) &= 1 + (m+1) + (2m+1) + \cdots + ((k-1)m+1) \\ &= \frac{mk(k-1)}{2} + k \end{aligned}$$

となる．なお，$p_m(0) = 0$ なので，0 も $m+2$ 角数として解釈することとする．

2　整数論からの準備

この節では，§4 において必要となる整数論の事項をまとめる．

まず，自然数 m および整数 a, b に対して，合同式

$$a \equiv b \pmod{m}$$

とは，$a-b$ が m で割り切れることを意味する．

a が m で割り切れるとき，

$$m|a$$

と書く．割り切れないときは，

$$m \not| a$$

と書く．

また，a の素因数 p に対して，

$$p^n|a \quad \text{だが} \quad p^{n+1} \not| a$$

のとき，

$$p||a$$

と表す.

奇素数 p および p で割り切れない整数 a に対して，合同式

$$x^2 \equiv a \pmod{p}$$

を満たす整数 x が存在するのであれば，a を p に関する平方剰余といい，x が存在しないのであれば，a を p に関する平方非剰余という.

Legendre symbol とは，a が p で割り切れる場合も便宜上含めて，次のように表記するものである.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ が } p \text{ に関する平方剰余のとき}) \\ -1 & (a \text{ が } p \text{ に関する平方非剰余のとき}) \\ 0 & (a \text{ が } p \text{ で割り切れるとき}) \end{cases}$$

Legendre symbol の基本的な性質をまとめておく．これらについては，整数論の教科書に証明が載っているので，ここでは証明を省略する.

定理 2.1. p，q を異なる奇素数，a，b を整数とする.

(1) $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$

(2) (第 1 補充法則) $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(3) (第 2 補充法則) $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

(4) (平方剰余の相互法則) $\left(\dfrac{q}{p}\right)\left(\dfrac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Legendre symbol を一般化したものが，Jacobi symbol である.

奇数 N の素因数分解を

$$N = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

とするとき，整数 a に対して，Jacobi symbol を

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

と定める．Legendre symbol の性質と同様に，次が成り立つ.

定理 2.2. N を奇数，a，b を整数とする.

(1) $\left(\dfrac{ab}{N}\right) = \left(\dfrac{a}{N}\right)\left(\dfrac{b}{N}\right)$

(2) (第 1 補充法則) $\left(\dfrac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}$

(3) (第 2 補充法則) $\left(\dfrac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$

定理 2.3 (中国剰余定理)**.** $k \geq 2$ とする．整数 $a_1, a_2, \ldots, a_k$ と互いに素な自然数 $m_1, m_2, \ldots, m_k$ に対して,

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_k \pmod{m_k} \tag{2.1}$$

を満たす整数 x が存在する．しかも，x および y が (2.1) の解であるならば,

$$x \equiv y \pmod{m_1 m_2 \ldots m_k}$$

が成り立つ.

証明. k に関する帰納法で証明する．まず，$k = 2$ とする．$\gcd(m_1, m_2) = 1$ だから,

$$pm_1 + qm_2 = 1$$

となる整数 p, q が存在する．そこで,

$$x = a_1(1 - pm_1) + a_2(1 - qm_2)$$

とおくと,

$$x \equiv a_1 \pmod{m_1} \text{ かつ } x \equiv a_2 \pmod{m_2}$$

を満たしている.

次に, $k \geq 3$ とし, $k-1$ のときに正しいと仮定する．つまり, $i = 1, 2, \ldots, k-1$ に対して, $y \equiv a_i \pmod{m_i}$ を満たす整数 z が存在している．ここで，$\gcd(m_1 m_2 \ldots m_{k-1}, m_k) = 1$ だから，$k = 2$ の場合を適用して,

$$\begin{aligned} &x \equiv z \pmod{m_1 m_2 \ldots m_{k-1}}, \\ &x \equiv a_k \pmod{m_k} \end{aligned}$$

を満たす整数 x が存在する．この x が求める解である.

さて，x および y が連立合同式 (2.1) の解とすると，全ての i に対して，$x - y$ は m_i で割り切れる．m_i は互いに素なので，$x - y$ は $m_1 m_2 \ldots m_k$ で割り切れる． □

定理 2.4 (Dirichlet の算術級数定理)**.** 互いに素な自然数 a および d が与えられたとき, 初項 a，交差 d の等差数列の中には，素数が無限に多く現れる.

この定理は非常に強力である．素数が無限に多く存在することについては，Euclid の証明が有名だが，Dirichet の定理を使えば，4 で割って 3 余る素数や 6 で割って 5 余る素数が無限に多く存在することが従う．初等的な証明は知られておらず，通常，Dirichlet の L 関数とよばれるものが使われる．[5, 附録] や [10] には証明が掲載されている．

定理 2.5 (Minkowiski 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．

一般に，Minkowski の定理は，n 次元空間における原点対称かつ凸な領域に対しても正しく，その場合，原点以外の格子点を含むための条件は体積が 2^n を超えることである．[5] には 2 次元の場合の証明が載っている．n 次元の場合には，[8] などに証明がある．ここでは，[8] の証明を $n = 3$ として示しておく．

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

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

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

$$C(P) = \left\{ (x, y, z) \mid \frac{2p}{t} \leq x \leq \frac{2(p+1)}{t},\ \frac{2q}{t} \leq y \leq \frac{2(q+1)}{t},\ \frac{2r}{t} \leq z \leq \frac{2(r+1)}{t} \right\}$$

が対応するものとする．このとき，P を立方体 $C(P)$ の角とよぶ．

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．$V > 8$ だから，十分大きい t に対しては $N(t) > t^3$ が成立する．

さて，整数の組 (p, q, r) を $\bmod t$ でみるとき，t^3 通りしか可能性がないことから，$\mathcal{B}$ 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，

$$p_1 - p_2 \equiv 0 \pmod{t},\ q_1 - q_2 \equiv 0 \pmod{t},\ r_1 - r_2 \equiv 0 \pmod{t}$$

を満たすものが見つかる．

領域 $\mathcal{B}$ は原点対称だから，P_2 の対称点 $P_2' = (-2p_2/t, -2q_2/t, -2r_2/t)$ も $\mathcal{B}$ に含まれ，さらに凸性より，2 点 P_1，P_2' の中点 M は $\mathcal{B}$ に含まれる．しかし，

$$M = \left(\frac{p_1 - p_2}{t}, \frac{q_1 - q_2}{t}, \frac{r_1 - r_2}{t}\right)$$

ゆえ，M が求める格子点である． □

3 Fermat の二平方定理

定理 3.1 (Fermat)**.** 素数 p が $p \equiv 1 \pmod 4$ を満たすならば，p は平方数 2 つの和として表される．

Zagier [11] による「one-sentence proof」を紹介したい．それは [1] にも収録されている．

証明. $p = 4m + 1$ とおく．集合

$$S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$$

を考えると，S は有限集合である．また，$(1, 1, m) \in S$ より，$S \neq \emptyset$ である．

さて，写像 $\varphi : S \to S$ を次のように定義する．

$$\varphi((x, y, z)) = \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } 2y < x \end{cases}$$

すると，φ^2 が恒等写像であることが確認できる．さらに，φ の固定点は，$(1, 1, m)$ のみであることがわかる．こうして，S は奇数個の点からなる．

さて，写像 $h : S \to S$ を

$$h(x, y, z) = (x, z, y)$$

で定義すると，h は固定点を持たねばならない．そこで，$(a, b, b) \in S$ を固定点とすると，S の条件から

$$a^2 + 4b^2 = p$$

を満たし，p が平方数 2 つの和にかけている． □

集合 S に作用する位数 2 の写像 φ を利用するというのは，もともと，Heath-Brown のアイデアによるのだが，残念ながらその文献は入手できない．

定理 3.2. 自然数 N が平方数 2 つの和に表されるための必要十分条件は，N の素因数分解において，$4m + 3$ の形の素数は必ず偶数べきをもつことである．

証明. $N = x^2 + y^2$ とする．$p = 4m + 3$ を N の素因数とする．

主張 3.1. $\gcd(x,y) > 1$.

主張 3.1 の証明. $\gcd(x,y) = 1$ としよう．もし $p|x$ ならば，$p|N$ とあわせて，$p|y$ となってしまう．よって，$p \not| x$ であり，同様に $p \not| y$.

$\gcd(p,x) = 1$ なので，$ap + bx = 1$ となる整数 a, b が存在する．両辺に y をかけて，$apy + bxy = y$．よって，$y \equiv \ell x \pmod{p}$ を得る．こうして，$x^2(1+\ell^2) \equiv x^2 + y^2 \equiv 0 \pmod{p}$ より，$1 + \ell^2 \equiv 0 \pmod{p}$.

これは，-1 が p に関する平方剰余であることを意味するが，第 1 補充法則 $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$ に矛盾する． □

そこで，$\gcd(x,y) = d > 1$ とおこう．$x = Xd$，$y = Yd$ (ただし，$\gcd(X,Y) = 1$) とかける．$X^2 + Y^2 = M$ とすれば，$N = Md^2$．もし p が M を割り切れば，主張 3.1 を $M = X^2 + Y^2$ に適用して矛盾を生じる．よって，$p \not| M$．こうして，p は d^2 を割り切ることになり，偶数べきまで含まれることがわかる．

逆に，N の素因数分解において，$4m+3$ の形の素数は全て偶数べきをもつとしよう．よって，$4m+3$ の形の素因数をもたない N_2 を用いて，$N = N_1^2 N_2$ をかける．

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - y_1x_2)^2$$

なので，平方数 2 つの和にかける整数の積は，平方数 2 つの和にかける．$2 = 1^2 + 1^2$ であり，Fermat の二平方定理 (定理 3.1) より，N_2 は平方数 2 つの和にかけることがわかる．

よって，$N_2 = a^2 + b^2$ とすれば，

$$N = N_1^2 N_2 = N_1^2(a^2 + b^2) = (N_1 a)^2 + (N_1 b)^2$$

となって，N が平方数 2 つの和にかける． □

4 Gauss の定理

Gauss は，1796 年 7 月 10 日付けの日記 (このとき Gauss は 19 歳) に，Archimedes のエピソードに因んで，

$$\text{EΥPHKA! num} = \triangle + \triangle + \triangle$$

と記した．すなわち，

定理 4.1 (Gauss)**.** 任意の自然数は，3 つの三角数の和として表される．

表 1 は，1 から 20 までの自然数を三角数の和として示したものである．表中で，三角数は太字で示してある．

$\mathbf{1} = 1+0+0$	$\mathbf{6} = 6+0+0$	$11 = 10+1+0$	$16 = 15+1+0$
$2 = 1+1+0$	$7 = 6+1+0$	$12 = 10+1+1$	$17 = 15+1+1$
$\mathbf{3} = 3+0+0$	$8 = 6+1+1$	$13 = 10+3+0$	$18 = 15+3+0$
$4 = 3+1+0$	$9 = 6+3+0$	$14 = 10+3+1$	$19 = 15+3+1$
$5 = 3+1+1$	$\mathbf{10} = 10+0+0$	$\mathbf{15} = 15+0+0$	$20 = 10+10+0$

表 1

証明. 任意の自然数 N に対して，$8N+3$ を考える．次に示す定理 4.2 より，非負整数 k_1, k_2, k_3 を用いて，

$$8N+3 = (2k_1+1)^2 + (2k_2+1)^2 + (2k_3+1)^2$$

と表される．これを変形して，

$$\begin{aligned} N &= \frac{k_1(k_1+1)}{2} + \frac{k_2(k_2+1)}{2} + \frac{k_3(k_3+1)}{2} \\ &= p_1(k_1) + p_1(k_2) + p_1(k_3) \end{aligned}$$

を得る． □

定理 4.2 (Gauss)**.** 自然数 N が，$N \equiv 3 \pmod 8$ を満たすならば，N は奇数の平方数 3 つの和として表される．

証明. もし $N = p^2M$ (p は素数) とかけるならば，p は奇数であり，$p^2 \equiv 1 \pmod 8$. よって，$N \equiv M \pmod 8$ であり，M が奇数の平方数 3 つの和として書ければ，N もそういう形にかけることになる．従って，以降，$N = p_1p_2 \dots p_r$，ただし p_i は互いに異なる奇素数，として素因数分解されているとしてよい．

主張 4.1. 素数 q で，$q \equiv 1 \pmod 4$ かつ $i = 1, 2, \dots, r$ に対して

$$\left(\frac{-2q}{p_i}\right) = 1$$

を満たすものが存在する．

主張 4.1 の証明. 各 p_i に対して，$p_i - 2$ と p_i は互いに素であるから，合同式

$$-2x \equiv 1 \pmod{p_i}$$

は解 a_i をもつ.

中国剰余定理 (定理 2.3) より,

$$\begin{aligned} X &\equiv 1 \pmod{4} \\ X &\equiv a_1 \pmod{p_1} \\ &\vdots \\ X &\equiv a_r \pmod{p_r} \end{aligned}$$

を満たす整数 X が存在する.

このとき，$\gcd(X, 4N) = 1$ に注意する．Dirichlet の算術級数定理 (定理 2.4) より，初項 X，交差 $4N$ の等差数列の中で，素数 q が見つかる．つまり，$q \equiv X \pmod{4N}$ を満たす.

そこで, $q = X + 4Nk$ と表せば, $q \equiv 1 \pmod 4$ かつ, 各 i に対して, $q \equiv a_i \pmod{p_i}$ である．特に,

$$-2q \equiv -2a_i \equiv 1^2 \pmod{p_i} \tag{4.1}$$

なので,

$$\left(\frac{-2q}{p_i}\right) = 1$$

を満たす. □

(4.1) と中国剰余定理より,

$$-2q \equiv 1 \pmod{N} \tag{4.2}$$

であることに注意しておく.

さて，素数 q に対して次が成立する.

主張 4.2.

$$\left(\frac{-N}{q}\right) = 1$$

主張 4.2 の証明. Legendre symbol, Jacobi symbol の性質から,

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

ここで, 平方剰余の相互法則から

$$\left(\frac{q}{p_i}\right) = \left(\frac{p_i}{q}\right)$$

なので,

$$\prod_{i=1}^{r} \left(\frac{q}{p_i}\right) = \prod_{i=1}^{r} \left(\frac{p_i}{q}\right) = \left(\frac{N}{q}\right).$$

従って,

$$\left(\frac{-2}{N}\right)\left(\frac{N}{q}\right) = 1$$

を得る.

一方, Jacobi symbol の性質より,

$$\left(\frac{-2}{N}\right) = \left(\frac{-1}{N}\right)\left(\frac{2}{N}\right) = (-1)^{\frac{N-1}{2}}(-1)^{\frac{N^2-1}{8}} = 1$$

だから,

$$\left(\frac{N}{q}\right) = 1$$

を得る.

以上より,

$$\left(\frac{-N}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{N}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = 1.$$

□

従って, $b^2 \equiv -N \pmod{q}$ となる整数 b が存在する. いいかえれば, 整数 h_1 を用いて

$$b^2 - qh_1 = -N$$

と表すことができる. このとき, $(q-b)^2 \equiv -N \pmod{q}$ であり, 必要があれば, b と $q-b$ を入れ替えることで, b は奇数であると仮定してよい. (q は奇数なので, b と $q-b$ の偶奇性は一致しない.)

そうすると，$b^2 - qh_1 = -N$ を mod 4 でみると，

$$1 - h_1 \equiv -3 \pmod 4$$

となり，$h_1 \equiv 0 \pmod 4$ がわかる．そこで，$h_1 = 4h$ と書き直せば

$$b^2 - 4qh = -N$$

を得る．

さて，(R, S, T) 空間において，原点を中心とし，半径 $\sqrt{2N}$ の球領域

$$\mathcal{B} = \{(R, S, T) \mid R^2 + S^2 + T^2 < 2N\}$$

を考える．1 次変換

$$\begin{pmatrix} R \\ S \\ T \end{pmatrix} = \begin{pmatrix} 2q & b & N \\ \sqrt{2q} & \frac{b}{\sqrt{2q}} & 0 \\ 0 & \frac{\sqrt{N}}{\sqrt{2q}} & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

によって，領域 $\mathcal{B}$ は，(x, y, z) 空間内の領域 $\mathcal{S}$ に対応する．明らかに，$\mathcal{B}$ は原点対称かつ凸であり，対応する領域 $\mathcal{S}$ も同じ性質をもつ．しかも，$\mathcal{S}$ の体積は，$\mathcal{B}$ の体積 $\frac{4}{3}\pi\sqrt{2N}^3$ を 1 次変換の行列の行列式 $N\sqrt{N}$ で割ったものに一致するので，

$$\text{Volume of } \mathcal{S} = \frac{\frac{4}{3}\pi\sqrt{2N}^3}{N\sqrt{N}} = \frac{4}{3}\pi\sqrt{2}^3 = \frac{8\sqrt{2}}{3}\pi > 8$$

を満たす．

従って，Minkowski の凸体定理 (定理 2.5) より，$\mathcal{S}$ は原点以外の格子点 (x_1, y_1, z_1) を含む．これに対応した $\mathcal{B}$ 内の点を (R_1, S_1, T_1) とする．すると，

$$\begin{aligned} S_1^2 + T_1^2 &= (\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1)^2 + \frac{N}{2q}y_1^2 \\ &= 2qx_1^2 + 2bx_1y_1 + \frac{b^2 + N}{2q}y_1^2 \\ &= 2qx_1^2 + 2bx_1y_1 + 2hy_1^2 \\ &= 2(qx_1^2 + bx_1y_1 + hy_1^2) \in \mathbb{Z} \end{aligned}$$

とわかる．そこで，$v = qx_1^2 + bx_1y_1 + hy_1^2$ とおくと，

$$R_1^2 + S_1^2 + T_1^2 = R_1^2 + 2v \in \mathbb{Z}$$

となる．

一方，(4.2) を利用すると

$$\begin{aligned} 2q(R_1^2+S_1^2+T_1^2) &= 2q(2qx_1+by_1+Nz_1)^2+(2qx_1+by_1)^2+Ny_1^2 \\ &\equiv 2q(2qx_1+by_1)^2+(2qx_1+by_1)^2 \\ &\equiv (2q+1)(2qx_1+by_1)^2 \\ &\equiv 0 \pmod{N} \end{aligned}$$

であり，N は $2q$ と互いに素であるから，

$$R_1^2+S_1^2+T_1^2 \equiv 0 \pmod{N}$$

となる．つまり，$N \mid R_1^2+2v$．また，領域 $\mathcal{B}$ の定義より，$R_1^2+2v<2N$ である．

主張 4.3. $R_1^2+2v=N$

主張 4.3 の証明. 整数 R_1^2+2v は，N で割り切れ，$R_1^2+2v<2N$ であることがわかっている．よって，$R_1^2+2v>0$ であることさえいえば十分.

$$\begin{aligned} v &= q\left(x_1+\frac{b}{2q}y_1\right)^2+\left(h-\frac{b^2}{4q}\right)y_1^2 \\ &= q\left(x_1+\frac{b}{2q}y_1\right)^2+\frac{N}{4q}y_1^2 \end{aligned}$$

だから，$v \geq 0$ であり，$x_1=y_1=0$ のときに限り，$v=0$ となる．

もし $v>0$ ならば，$R_1^2+2v>0$ を得る．もし $v=0$ ならば，$x_1=y_1=0$ であるが，$(x_1,y_1,z_1) \neq (0,0,0)$ だから，$R_1=Nz_1 \neq 0$. □

あとは，v を奇数べきまで割り切る奇素数 p が，必ず $p \equiv 1 \pmod{4}$ を満たすことをいえば，定理 3.2 によって，$2v$ は平方数 2 つの和に表せ，よって N が 3 つの平方数の和として表されることになる．

そこで，p を奇素数とし，$p^{2n+1}||v$ とする．2 つの場合に分けて考える．

Case 1. p が N を割り切らない場合.

$R_1^2+2v=N$ より，$R_1^2 \equiv N \pmod{p}$．つまり，

$$\left(\frac{N}{p}\right)=1$$

である．

もし $p|q$ ならば，$b^2 - 4qh = -N$ より，

$$\left(\frac{-N}{p}\right) = 1$$

となる．もし $p \not| q$ ならば，

$$4qv = 4q(qx_1^2 + bx_1y_1 + hy_1^2) = (2qx_1 + by_1)^2 + Ny_1^2$$

より，$p^{2n+1} || (2qx_1 + by_1)^2 + Ny_1^2$ となる．Jacobi symbol を用いれば，

$$\left(\frac{-Ny_1^2}{p^{2n+1}}\right) = 1$$

となるが，Jacobi symbol の定義および性質により，

$$\begin{aligned}\left(\frac{-Ny_1^2}{p^{2n+1}}\right) &= \left(\frac{-N}{p}\right)^{2n+1}\left(\frac{y_1}{p^{2n+1}}\right)^2 \\ &= \left(\frac{-N}{p}\right)^{2n+1}\end{aligned}$$

となり，

$$\left(\frac{-N}{p}\right) = 1$$

を得る．

Legendre symbol の性質から，

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

となり，$p \equiv 1 \pmod 4$ でなければならない．

Case 2. p が N を割り切る場合．

$N = R_1^2 + 2v$ で，$p|v$ なので，$p|R_1$ となる．さて

$$2qN = 2q(R_1^2 + 2v) = 2qR_1^2 + \{(2qx_1 + by_1)^2 + Ny_1^2\} \tag{4.3}$$

なので，$p \mid 2qx_1 + by_1$ である．

(4.3) の両辺を p で割って，さらに mod p で読むと，

$$2q\frac{N}{p} \equiv \frac{N}{p}y_1^2 \pmod p$$

となる．$\dfrac{N}{p} \not\equiv 0 \pmod{p}$ なので，$y_1^2 \equiv 2q \pmod{p}$ を得る．つまり，

$$\left(\frac{2q}{p}\right) = 1.$$

一方，

$$\left(\frac{-2q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2q}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

であるが，p は N の素因数のうちの 1 つであるから，主張 4.1 より，$(-1)^{\frac{p-1}{2}} = 1$ となる．従って，$p \equiv 1 \pmod{4}$ を得た．

最後に，$N = a^2 + b^2 + c^2$ とするとき，N は奇数なので，a, b, c のうち奇数は 1 つか 3 つのいずれかである．もし 1 つだけが奇数だとすると，$N \equiv 1, 5 \pmod{8}$ となり矛盾する．こうして，N は奇数の平方数 3 つの和として表されている． □

Gauss は実際には，定理 4.2 よりも強い次の定理を証明している．

定理 4.3. 自然数 N が 3 つの平方数の和として表されるための必要十分条件は，N が $4^a(8k+7)$ の形をしていないことである．

証明. 必要性だけなら，初等的に証明できる．背理法で証明しよう．$N = 4^a(8k+7) = x^2 + y^2 + z^2$ と書けているとする．

もし $a = 0$ ならば，$8k + 7$ が 3 つの平方数の和として表されることになり，不可能である．(平方数は，mod 8 で $0, 1, 4$ の値しかとらないため．)

$a > 0$ ならば，x, y, z はいずれも偶数である．(もしも奇数が混ざっているならば，2 つだけが奇数ということになるが，そのとき，両辺を mod 4 でみると不合理．) そこで，

$$\frac{N}{4} = 4^{a-1}(8k+7) = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$$

となり，これを続ければ，やがて $8k + 7$ が 3 つの平方数の和として表されることになり，矛盾にいたる． □

Gauss の証明は入手できないので，詳細はわからないが，おそらく正定値な整数係数の 3 元 2 次形式が discriminant 1 をもてば，標準形 $x_1^2 + x_2^2 + x_3^2$ と同値であるという事実を使うと思われる．この方針に沿った証明は，[10] に収録されている．

5 Lagrange の四平方定理

どんな自然数も高々 4 つの平方数 (四角数) の和として表されることを主張するのが, Lagrange の四平方定理である．$0^2 = 0$ なので，0 も平方数として捉えていることに注意する．

定理 5.1 (Lagrange)**.** 任意の自然数は，4 つの平方数の和として表される．

表 2 は，1 から 20 までの自然数を平方数の和として示したものである．

$1 = 1^2 + 0 + 0 + 0$	$6 = 2^2 + 1^2 + 1^2 + 0$	$11 = 3^2 + 1^2 + 1^2 + 0$
$2 = 1^2 + 1^2 + 0 + 0$	$7 = 2^2 + 1^2 + 1^2 + 1^2$	$12 = 3^2 + 1^2 + 1^2 + 1^2$
$3 = 1^2 + 1^2 + 1^2 + 0$	$8 = 2^2 + 2^2 + 0 + 0$	$13 = 3^2 + 2^2 + 0 + 0$
$4 = 2^2 + 0 + 0 + 0$	$9 = 3^2 + 0 + 0 + 0$	$14 = 3^2 + 2^2 + 1^2 + 0$
$5 = 2^2 + 1^2 + 0 + 0$	$10 = 3^2 + 1^2 + 0 + 0$	$15 = 3^2 + 2^2 + 1^2 + 1^2$

表 2

ちなみに，$2007 = 42^2 + 15^2 + 3^2 + 3^2$，$2008 = 42^2 + 12^2 + 10^2$ である．

証明. まず,

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

ただし,

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \end{aligned} \tag{5.1}$$

により, 4 つの平方数の和として表される数 2 つの積は, 再び 4 つの平方数の和として表される．従って, 素数 p に対して, 主張を証明すれば十分である．また, $2 = 1^2+1^2+0^2+0^2$ なので，p は奇素数としてよい．

平方数の集合

$$R = \left\{ x^2 \mid x = 0, 1, 2, \ldots, \frac{p-1}{2} \right\}$$

は, $\mathrm{mod}\ p$ においては互いに異なる $(p+1)/2$ 個の剰余類を代表する．なぜなら, $x^2, y^2 \in R$ $(x > y)$ に対して，$x^2 - y^2 = (x+y)(x-y)$ で，$0 < x \pm y < p-1$ ゆえ，$x^2 - y^2 \not\equiv 0 \pmod{p}$ だからである．

同様に，整数の集合

$$S = \left\{ -y^2 - 1 \mid y = 0, 1, 2, \ldots, \frac{p-1}{2} \right\}$$

も，$\mathrm{mod}\ p$ においては互いに異なる $(p+1)/2$ 個の剰余類を代表する．

$\mathrm{mod}\ p$ の剰余類は，p 個しか存在しないから，

$$x^2 \equiv -y^2 - 1 \pmod{p}$$

を満たす $0 \leq x, y \leq (p-1)/2$ が存在する．つまり，

$$x^2 + y^2 + 1 = mp$$

を満たす自然数 m が存在する．特に，

$$mp \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < \frac{p^2}{2} + 1 < p^2$$

より，$m < p$ である．

さて，自然数 n は，np が 4 つの平方数の和として表されるような最小のものとする．（そういう n が存在する理由は，自然数全体の集合が通常の大小関係に対して，整列集合をなすからである．）つまり，

$$np = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

となる $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ が存在し，

$$1 \leq n \leq m < p$$

を満たす．以下，$n = 1$ であることを証明する．

x_1, x_2, x_3, x_4 のうち，偶奇性の一致するものがある．仮に，x_1, x_2 としよう．もし n が偶数ならば，残る x_3, x_4 の偶奇性も一致する．つまり，

$$\frac{x_1 \pm x_2}{2}, \frac{x_3 \pm x_4}{2} \in \mathbb{Z}$$

であり，

$$\left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2 = \frac{x_1^2+x_2^2+x_3^2+x_4^2}{2} = \frac{n}{2}p$$

となって，n の最小性に反する．従って，n は奇数でなければならない．

さて，各 x_i に対して

$$y_i \equiv x_i \pmod{n}$$

となる y_i を，$-n/2 < y_i < n/2$ に選ぶ．このとき，

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = np \equiv 0 \pmod{n}$$

だから，非負整数 q によって，

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = nq$$

とかける．しかも，

$$nq = y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{n}{2}\right)^2 = n^2$$

より，$q < n$ である．

ここで，

$$\begin{aligned} n^2pq &= (np)(nq) \\ &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= z_1^2 + z_2^2 + z_3^2 + z_4^2 \end{aligned}$$

ただし，z_i は (5.1) によって定義されたものとする．

$x_i \equiv y_i \pmod{n}$ より，$z_i \equiv 0 \pmod{n}$ がわかる．そこで，$w_i = z_i/n$ とおくと，

$$w_1^2 + w_2^2 + w_3^2 + w_4^2 = pq.$$

n の最小性から，$q = 0$ でなければならない．

すると，$y_1^2 + y_2^2 + y_3^2 + y_4^2 = 0$ より，各 $y_i = 0$ であり，$x_i \equiv 0 \pmod{n}$ となる．よって，$x_1^2 + x_2^2 + x_3^2 + x_4^2$ が n^2 で割り切れることになり，p は n で割り切れる．しかし，$1 \leq n < p$ で，p は素数であったことから，$n = 1$ を得る． □

なお，平方数は，mod 8 で $0, 1, 4$ のいずれかにしかならないため，自然数 N が $N \equiv 7 \pmod{8}$ を満たすならば，3 個以下の平方数の和としては表現できない．また，Jacobi によって，自然数 N を 4 個の平方数の和として表す方法の総数を求める式が与えられている．

6 Cauchy の多角数定理

多角数定理とは，どんな自然数も $m+2$ 個の $m+2$ 角数の和として表わされることを主張する．つまり，どんな自然数も 3 個の三角数の和，4 個の四角数の和，5 個の五角数の和というように表現できるということである．これを最初に主張したのは，Fermat であり，Diophantus の著書「算術 (Arithmetica)」の翻訳本の余白に書き込みを残している．ただし，証明は書かれていない．$m=1$ の場合に相当するのが §4 で紹介した Gauss の定理 (定理 4.1) であり，$m=2$ の場合に相当するのが §5 で述べた Lagrange の四平方定理 (定理 5.1) に他ならない．$m \geq 3$ の場合の証明を最初に示したのは，Cauchy であり，1813 年のことだった．残念ながら，Cauchy の証明がどういうものであったのか，文献を入手できない．この節の目的は，Nathanson によって 1987 年に発表された，多角数定理の短くかつ初等的な証明 [9] を紹介することにある．(ただし，証明に必要な Cauchy's Lemma (補題 6.1) の証明において，Gauss の定理 (定理 4.1) を用いている．)

定理 6.1 (Cauchy's polygonal number theorem)**.** $m \geq 3$ とする．任意の自然数は，$m+2$ 個の $m+2$ 角数の和として表される．

Nathanson による証明のポイントは，与えられた m (≥ 3) および自然数 N に対して，N/m の値が小さい場合を先に除外しておくことにある．

k 番目の $m+2$ 角数は

$$p_m(k) = \frac{mk(k-1)}{2} + k$$

であった．ここで，$p_m(0)=0$，$p_m(1)=1$ に注意しておく．

$k_1, k_2, \ldots, k_s$ を自然数とすると，$r = 0, 1, 2, \ldots, m+2-s$ に対して，

$$p_m(k_1) + p_m(k_2) + \cdots + p_m(k_s) + r p_m(1) \tag{6.1}$$

という形の整数は，$m+3-s$ 個の連続した整数を与えている．しかも，それぞれ高々 $m+2$ 個の $m+2$ 角数の和として，よって $p_m(0)=0$ を利用すれば，$m+2$ 個の $m+2$ 角数の和として表現できることがわかる．

表 3 は，(6.1) の形として，表現できる整数の範囲を示している．

このように，$108m$ までの整数を具体的に，$m+2$ 角数の和として表現しておくことは可能である．(実際，Pepin と Dickson がそのような表を出版したとのことだが，19 世紀末から 20 世紀初頭にかけてのことであり，文献は入手できない．) そして，$N \geq 108m$

$rp_m(1)$	0	$m+2$
$p_m(2)+rp_m(1)$	$m+2$	$2m+3$
$2p_m(2)+rp_m(1)$	$2m+4$	$3m+4$
$p_m(3)+rp_m(1)$	$3m+3$	$4m+4$
$p_m(3)+p_m(2)+rp_m(1)$	$4m+5$	$5m+5$
$4p_m(2)+rp_m(1)$	$4m+8$	$5m+6$
$p_m(3)+2p_m(2)+rp_m(1)$	$5m+7$	$6m+6$
$p_m(4)+rp_m(1)$	$6m+4$	$7m+5$
$p_m(4)+p_m(2)+rp_m(1)$	$7m+6$	$8m+6$
$2p_m(3)+p_m(2)+rp_m(1)$	$7m+8$	$8m+7$
$p_m(4)+2p_m(2)+rp_m(1)$	$8m+8$	$9m+7$
$p_m(4)+p_m(3)+rp_m(1)$	$9m+7$	$10m+7$
$p_m(5)+rp_m(1)$	$10m+5$	$11m+6$
$p_m(5)+p_m(2)+rp_m(1)$	$11m+7$	$12m+7$
$2p_m(4)+rp_m(1)$	$12m+8$	$13m+8$
$p_m(5)+p_m(3)+rp_m(1)$	$13m+8$	$14m+8$
$p_m(5)+2p_m(2)+rp_m(1)$	$14m+9$	$15m+8$
$p_m(6)+rp_m(1)$	$15m+6$	$16m+7$
$p_m(6)+p_m(2)+rp_m(1)$	$16m+8$	$17m+8$
$p_m(5)+p_m(4)+rp_m(1)$	$16m+9$	$17m+9$
$p_m(6)+2p_m(2)+rp_m(1)$	$17m+10$	$18m+9$
$p_m(6)+p_m(3)+rp_m(1)$	$18m+9$	$19m+9$
$p_m(6)+3p_m(2)+rp_m(1)$	$18m+12$	$19m+10$
$p_m(6)+p_m(3)+p_m(2)+rp_m(1)$	$19m+11$	$20m+10$
$2p_m(5)+rp_m(1)$	$20m+10$	$21m+10$
$p_m(7)+rp_m(1)$	$21m+7$	$22m+8$
$p_m(7)+p_m(2)+rp_m(1)$	$22m+9$	$23m+9$
$2p_m(5)+2p_m(2)+rp_m(1)$	$22m+14$	$23m+12$
$p_m(7)+2p_m(2)+rp_m(1)$	$23m+11$	$24m+10$
$p_m(7)+p_m(3)+rp_m(1)$	$24m+10$	$25m+10$

表 3

を満たす自然数 N に対しては，定理 6.2 で，Cauchy's polygonal theorem (定理 6.1) よりは少し強い主張を証明する．

補題 6.1 (Cauchy's Lemma)**.** a, b (> 0) を奇数とする．もし，$b^2 < 4a$ かつ $3a < b^2 + 2b + 4$ ならば，

$$\begin{aligned} a &= s^2 + t^2 + u^2 + v^2 \\ b &= s + t + u + v \end{aligned}$$

を満たす非負整数 s, t, u, v が存在する．

証明. a, b は奇数だから，$a = 2a' + 1$，$b = 2b' + 1$ として，

$$\begin{aligned} 4a - b^2 &= 4(2a' + 1) - (2b' + 1)^2 \\ &= (8a' + 4) - (4b'^2 + 4b' + 1) \\ &= 8a' - 4b'(b' + 1) + 3 \equiv 3 \pmod 8. \end{aligned}$$

定理 4.2 より，奇数 $x \geq y \geq z > 0$ を用いて，

$$4a - b^2 = x^2 + y^2 + z^2 \tag{6.2}$$

と表せる．

ここで，b, x, y, z はすべて奇数だから，mod 4 で ± 1 である．従って

$$b + x + y \equiv \pm 1 \pmod 4$$

であり，

$$b + x + y \pm z \equiv 0 \pmod 4 \tag{6.3}$$

を満たすように，z の前の符号を選んでおくことができる．

さて，

$$\begin{aligned} s &= \frac{b + x + y \pm z}{4} \\ t &= \frac{b + x}{2} - s = \frac{b + x - y \mp z}{4} \\ u &= \frac{b + y}{2} - s = \frac{b - x + y \mp z}{4} \\ v &= \frac{b \pm z}{2} - s = \frac{b - x - y \pm z}{4} \end{aligned}$$

とおく．$s \in \mathbb{Z}$ は等式 (6.3) より従う．b, x は奇数だから，$t \in \mathbb{Z}$ であり，u, v についても同様である．

あとは，これら s, t, u, v が求めるものであることを確認するだけである．

まず，

$$\begin{aligned} s+t+u+v &= s + \left(\frac{b+x}{2} - s\right) + \left(\frac{b+y}{2} - s\right) + \left(\frac{b \pm z}{2} - s\right) \\ &= b + \frac{b+x+y \pm z}{2} - 2s \\ &= b. \end{aligned}$$

次に，

$$\begin{aligned} s^2+t^2+u^2+v^2 &= s^2 + \frac{(b+x)^2}{4} - s(b+x) + s^2 \\ &\quad + \frac{(b+y)^2}{4} - s(b+y) + s^2 \\ &\quad + \frac{(b \pm z)^2}{4} - s(b \pm z) + s^2 \\ &= 4s^2 + \frac{(b+x)^2 + (b+y)^2 + (b \pm z)^2}{4} - s(b+x+y \pm z) - 2sb \\ &= \frac{3b^2 + x^2 + y^2 + z^2 + 2b(x+y \pm z)}{4} - 2sb \\ &= \frac{b^2 + x^2 + y^2 + z^2}{4} + \frac{2b(b+x+y \pm z)}{4} - 2sb \\ &= \frac{b^2 + x^2 + y^2 + z^2}{4} = a. \end{aligned}$$

残るのは，非負性だけであるが，

$$\begin{aligned} s - t &= \frac{y \pm z - (-y \mp z)}{4} = \frac{2y \pm 2z}{4} = \frac{y \pm z}{2} \geq 0 \\ t - u &= \frac{x-y}{2} \geq 0 \\ u - v &= \frac{y \mp z}{2} \geq 0 \end{aligned}$$

だから，$v > -1$ さえいえば，v は整数だから $v \geq 0$ といえる．実際，$v \geq \dfrac{b-x-y-z}{4}$ であるので，$b-x-y-z > -4$ をいう．さらに言い換えて，$x+y+z < b+4$ を示す．

これは，条件式 (6.2) のもとで，$x+y+z$ の最大値を評価することで解ける．3 次元ユークリッド空間において，原点を中心とする半径 $\sqrt{4a-b^2}$ の球面上の点で，$x = y = z$

のときに $x+y+z$ は最大値をとる．このとき，$3x^2 = 4a - b^2$ より，$x = \sqrt{\dfrac{4a-b^2}{3}}$. 従って，

$$x+y+z \leq 3\sqrt{\frac{4a-b^2}{3}} = \sqrt{3(4a-b^2)} < \sqrt{4(b^2+2b+4)-3b^2} = b+4.$$

□

補題 6.2. m, N を自然数とし，$m \geq 3$ とする．区間

$$I = \left(\frac{1}{2} + \sqrt{\frac{6N}{m} - 3}, \quad \frac{2}{3} + \sqrt{\frac{8N}{m} - 8} \right)$$

の長さを L とすると，$N \geq 108m$ ならば $L > 4$ である．

証明. $x = \dfrac{N}{m}$ とおくと，

$$L = \sqrt{8x-8} - \sqrt{6x-3} + \frac{1}{6}.$$

従って，$L > 4$ を示すには，

$$\sqrt{8x-8} > \sqrt{6x-3} + \frac{23}{6} \tag{6.4}$$

をいえばよい．記述が煩雑になるので，$\ell = \dfrac{23}{6}$ とおくと，不等式 (6.4) は，2 乗して整理すると，

$$4x(x - (5+7\ell^2)) + (5+\ell^2)^2 + 12\ell^2 > 0$$

と同値である．これは，

$$x \geq 5 + 7\ell^2 = 5 + 7\left(\frac{23}{6}\right)^2 = 107.86111\ldots$$

のときには成立するので，$N \geq 108m$ では $L > 4$ となる． □

補題 6.3. m, N を自然数とし，$m \geq 3$，$N \geq 108m$ とする．非負整数 a, b, r が，

$$0 \leq r < m$$

および

$$N = \frac{m}{2}(a-b) + b + r$$

を満たすとする．区間

$$I = \left(\frac{1}{2} + \sqrt{\frac{6N}{m} - 3}, \quad \frac{2}{3} + \sqrt{\frac{8N}{m} - 8} \right)$$

に対して，$b \in I$ ならば，$b^2 < 4a$ かつ $3a < b^2 + 2b + 4$ が成立する．

証明.

$$a = \left(1 - \frac{2}{m}\right) b + 2 \left(\frac{N-r}{m}\right)$$

なので，

$$f(b) = b^2 - 4a = b^2 - 4 \left(1 - \frac{2}{m}\right) b - 8 \left(\frac{N-r}{m}\right)$$

とおくと，$f(0) = -8 \left(\frac{N-r}{m}\right) < 0$ より，

$$0 \leq b < 2 \left(1 - \frac{2}{m}\right) + \sqrt{4 \left(1 - \frac{2}{m}\right)^2 + 8 \left(\frac{N-r}{m}\right)}$$

のとき，$f(b) < 0$ となる．

しかし，$b \in I$ なので，

$$\begin{aligned} 0 < b &< \frac{2}{3} + \sqrt{\frac{8N}{m} - 8} \\ &< 2 \left(1 - \frac{2}{m}\right) + \sqrt{8 \left(\frac{N-r}{m}\right)} \\ &< 2 \left(1 - \frac{2}{m}\right) + \sqrt{4 \left(1 - \frac{2}{m}\right)^2 + 8 \left(\frac{N-r}{m}\right)} \end{aligned}$$

が成立している．以上から，$b^2 < 4a$ を得る．

次に，

$$g(b) = b^2 + 2b + 4 - 3a = b^2 - \left(1 - \frac{6}{m}\right) b - \left(6 \left(\frac{N-r}{m}\right) - 4\right)$$

は，

$$b > \left(\frac{1}{2} - \frac{3}{m}\right) + \sqrt{\left(\frac{1}{2} - \frac{3}{m}\right)^2 + 6 \left(\frac{N-r}{m}\right) - 4}$$

ならば，$g(b) > 0$ となる．

しかし，$b \in I$ なので，

$$\begin{aligned} b &> \frac{1}{2} + \sqrt{\frac{6N}{m} - 3} \\ &> \left(\frac{1}{2} - \frac{3}{m}\right) + \sqrt{\left(\frac{1}{2} - \frac{3}{m}\right)^2 + \frac{6N}{m} - 4} \\ &> \left(\frac{1}{2} - \frac{3}{m}\right) + \sqrt{\left(\frac{1}{2} - \frac{3}{m}\right)^2 + 6\left(\frac{N-r}{m}\right) - 4} \end{aligned}$$

が成立している．以上から，$b^2 + 2b + 4 + 4 > 3a$ を得る． □

定理 6.2. $m \geq 4$ とする．自然数 N が $N \geq 108m$ を満たすならば，N は $m+1$ 個の $m+2$ 角数の和として表される．しかも，$0, 1$ 以外の値をとるのは，そのうち高々 4 つにできる．また，$N \geq 324$ ならば，N は 5 個の 5 角数の和として表され，そのうちの少なくとも 1 つは 0 か 1 である．

証明. 補題 6.2 より，区間

$$I = \left(\frac{1}{2} + \sqrt{\frac{6N}{m} - 3}, \quad \frac{2}{3} + \sqrt{\frac{8N}{m} - 8}\right)$$

の長さは 4 よりも大きい．従って，I は連続した 4 つの整数を含み，特に，連続した奇数 b_1, b_2 を含む．

$b \in \{b_1, b_2\}$ とし，$r \in \{0, 1, 2, \ldots, m-3\}$ ($m \geq 4$ のとき)，あるいは $\{0, 1\}$ ($m = 3$ のとき) として走らせると，$b + r$ は，$\bmod m$ で全ての剰余類を与える．従って，$N \equiv b + r \pmod{m}$ となる b, r を見つけることができる．

ここで，

$$a = 2\left(\frac{N-b-r}{m}\right) + b = \left(1 - \frac{2}{m}\right)b + 2\left(\frac{N-r}{m}\right) \ (> 0)$$

とおく．a は奇数であり，

$$N = \frac{m}{2}(a-b) + b + r$$

に注意する．

$b \in I$ だから，補題 6.3 より，$b^2 < 4a$ かつ $3a < b^2 + 2b + 4$ が成立する．従って，Cauchy's Lemma (補題 6.1) より，

$$a = s^2 + t^2 + u^2 + v^2$$

かつ

$$b = s + t + u + v$$

を満たす非負整数 s, t, u, v が見つかる．このとき，

$$\begin{aligned} N &= \frac{m}{2}(a-b) + b + r \\ &= \frac{m}{2}(s^2 - s + t^2 - t + u^2 - u + v^2 - v) + (s + t + u + v) + r \\ &= \frac{m}{2}(s^2 - s) + s + \frac{m}{2}(t^2 - t) + t + \frac{m}{2}(u^2 - u) + u + \frac{m}{2}(v^2 - v) + v + r \\ &= p_m(s) + p_m(t) + p_m(u) + p_m(v) + r \end{aligned}$$

となる．

こうして，$m \geq 4$ のときには，$0 \leq r \leq m-3$ ゆえ，$r = 1 + 1 + \cdots + 1$ として高々 $m-3$ 個の $m+2$ 角数の和として表されることから，N を $m+1$ 個の $m+2$ 角数の和として表現できる．(0 も $m+2$ 角数であることに注意．)

$m = 3$ のときには，$r = 0$ あるいは 1 であり，N は 5 個の 5 角数の和として表現でき，そのうちの少なくとも 1 つは 0 か 1 である． □

補足. 上記の証明は，もともと，Nathanson [9] によるものを，[10] において Nathanson 自身が修正したものをもとにしている．発表論文である [9] では，定理 6.2 において，$m = 3$ の場合を分けて扱わざるをえないことが欠落していた．

参考文献

[1] M. アイグナー, G. ツィグナー (蟹江幸博　訳), 天書の証明, シュプリンガー・フェアラーク東京, 2002.

[2] H. エンツェンスベルガー (丘沢静也　訳), 数の悪魔, 晶文社, 1998.

[3] 小林昭七, なっとくするオイラーとフェルマー, 講談社, 2003.

[4] 小野孝, 2 次形式, 現代数学の土壌 (上野健爾, 志賀浩二, 砂田利一編), 日本評論社, 2000.

[5] 高木貞治, 初等整数論講義, 第 2 版, 共立出版, 1971.

[6] 山本芳彦, 数論入門, 岩波書店, 2003.

[7] N. Ankeny, *Sums of three squares*, Proc. Amer. Math. Soc. **8** (1957), 316–319.

[8] G. Hardy and E. Wright, An introduction to the theory of numbers, Fifth edition, The Clarendon Press, Oxford University Press, New York, 1979.

[9] M. Nathanson, *A short proof of Cauchy's polygonal number theorem*, Proc. Amer. Math. Soc. **99** (1987), 22–24.

[10] M. Nathanson, Additive number theory; The Classical Bases, Graduate Texts in Mathematics, **164**, Springer-Verlag, New York, 1996.

[11] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), 144.