自然数 a , b , c , d が $a^2+b^2+c^2=d^2$ を満たしている。
次の問に答えよ。
(1) d が 3 で割り切れるならば，a , b , c は全て 3 で割り切れるか，a , b , c のどれも 3 で割り切れないかのどちらかであることを示せ。
(2) a , b , c のうち偶数が少なくとも 2 つあることを示せ。

＜ ’00 横浜国立大 ＞

【戦略】

(1) は 3 で割った余りについて考察するので，a , b , c を3 で割った余りで分類することになります。

その際，$3k$, $3k+1$, $3k+2$ と分類してもよいですが，余り 2 の整数というのは

3 の倍数から見て 1 足りない連中

と見ることもできますから，$3k$, $3k\pm1$ と分類すると手際がいいですね。

すると，一般に

$$\begin{cases} m \text{ が3の倍数} \iff m^2 \text{ を 3 で割った余りは} 0 \\ m \text{ が3の倍数でない} \iff m^2 \text{ を 3 で割った余りは} 1 \end{cases}$$

ということが言えます。3 で割った平方剰余が 0 か 1 かで，元々の数が 3 の倍数かどうかが判定できるという結果です。

a^2, b^2, c^2 を 3 で割った余りのパターン数は，それぞれ 0 か 1 の 2 通りずつあるので，$2^3=8$ 【通り】あります。

条件から $d^2\equiv 0 \pmod 3$ なので，$a^2+b^2+c^2\equiv 0 \pmod 3$ となる (a^2, b^2, c^2) のパターンを考えますが，8 パターンであれば個別検証してもたかが知れていますので，正面突破できるでしょう。

(2) は偶奇についての考察を考えるので，$2k$, $2k+1$ と分類して考えます。

これにより，
$$\begin{cases} m \text{ が 偶数} \iff m^2 \text{ を 4 で割った余りは} 0 \\ m \text{ が 奇数} \iff m^2 \text{ を 4 で割った余りは} 1 \end{cases}$$

と，4 で割った平方剰余が 0 か 1 かで，元々の数の偶奇を判定できることになります。

これより (1) 同様，a^2, b^2, c^2 を 4 で割った余りのパターン数は 8 通りということになります。

今回は d の偶奇については条件で与えられていないので，自分で場合分けをして考察していくことになります。

要領は (1) と同じでよいでしょう。

【解答】

一般に m , k を整数として

$$\begin{cases} m=3k \implies m^2=9k^2 (=3\cdot 3k^2) \\ m=3k\pm1 \implies m^2=9k^2\pm6k+1 \ (=3(3k^2\pm2k)+1) \end{cases}$$

なので，
$$\begin{cases} m \text{ が3の倍数} \iff m^2 \text{ を 3 で割った余りは} 0 \\ m \text{ が3の倍数でない} \iff m^2 \text{ を 3 で割った余りは} 1 \end{cases} \cdots (*)$$

整数 A , B , C を整数 n で割ったときの余りがそれぞれ r_1 , r_2 , r_3 であるとき $(A, B, C)\equiv(r_1, r_2, r_3) \pmod n$ と表す。

$$\begin{aligned}(a^2, b^2, c^2) \equiv\ &(0,0,0), (0,0,1), (0,1,0), (0,1,1) \\ &(1,0,0), (1,0,1), (1,1,0), (1,1,1) \pmod 3\end{aligned}$$

条件より d は 3 で割り切れるので，$d^2\equiv 0 \pmod 3$

ゆえに，$a^2+b^2+c^2=d^2$ が成立しているとき，

$$a^2+b^2+c^2\equiv 0 \pmod 3$$

が成立する。

上記 8 通りのうち，これを満たすのは

$$(a^2, b^2, c^2)\equiv(0,0,0), (1,1,1) \pmod 3$$

のときのみである。

$(*)$ より，これは a^2, b^2, c^2 がすべて 3 で割り切れるか，a^2, b^2, c^2 のどれも 3 で割り切れないということを意味する。

(2) 一般に m , k を整数として

$$\begin{cases} m=2k \implies m^2=4k^2 \\ m=2k+1 \implies m^2=4k^2+4k+1 \ (=4(k^2+k)+1) \end{cases}$$

なので，
$$\begin{cases} m \text{ が 偶数} \iff m^2 \text{ を 4 で割った余りは} 0 \\ m \text{ が 奇数} \iff m^2 \text{ を 4 で割った余りは} 1 \end{cases} \cdots (**)$$

$$\begin{aligned}(a^2, b^2, c^2) \equiv\ &(0,0,0), (0,0,1), (0,1,0), (0,1,1) \\ &(1,0,0), (1,0,1), (1,1,0), (1,1,1) \pmod 4\end{aligned}$$

d が偶数のとき $(**)$ より $d^2\equiv 0 \pmod 4$

上記 8 通りのうち，$a^2+b^2+c^2\equiv 0 \pmod 4$ を満たすのは

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

このとき，$(**)$ より，a , b , c の 3 つが偶数であることが言える。

d が奇数のとき $(**)$ より $d^2\equiv 1 \pmod 4$

上記 8 通りのうち，$a^2+b^2+c^2\equiv 1 \pmod 4$ を満たすのは

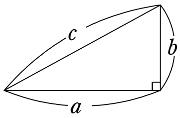
$$(a^2, b^2, c^2)\equiv(0,0,1), (0,1,0), (1,0,0) \pmod 4$$

このとき，$(**)$ より，a , b , c のうち 2 つが偶数であることを意味する。

【総括】

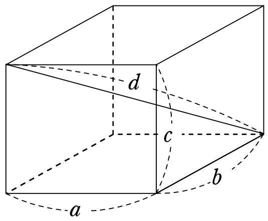
ピタゴラス数の拡張版のような等式です。

$a^2+b^2=c^2$ が



という直角三角形とリンクしているのに対して

$a^2+b^2+c^2=d^2$ は



という直方体とリンクしています。

第 1 講で扱ったピタゴラス数に関する典型問題と要領や着眼点は似通っていると感じたことでしょう。

繰り返しになりますが，

平方数を何かで割った余りは限られる

ということは常識としておきましょう。

余りで分類と口で言うのは簡単ですが，結局は「何で割った余りを考えるか」ということが大切であり，難しい部分です。

余りを扱う記号である合同式の扱いについてもある程度の練習は積んでおきたいところです。

$(A, B, C)\equiv(r_1, r_2, r_3)\ (\mathrm{mod}\ n)$ という記号の使い方に市民権があるかどうか分からないので，誰が読むか分からない答案では説明をつけておく方がよいと思います。

【復習用問題】

正の整数 a，b，c，d が等式 $a^2+b^2+c^2=d^2$ を満たすとする。

(1) d が 3 の倍数でないならば，a，b，c の中に 3 の倍数がちょうど 2 つあることを示せ。

(2) d が 2 の倍数でも 3 の倍数でもないならば，a，b，c のうち少なくとも 1 つは 6 の倍数であることを示せ。

＜ '94 一橋大 ＞

【略解】

(1) 整数 A，B，C を整数 n で割ったときの余りがそれぞれ r_1，r_2，r_3 であるとき $(A, B, C)\equiv(r_1, r_2, r_3)\ (\mathrm{mod}\ n)$ と表す。

条件より，$d^2\equiv 1\ (\mathrm{mod}\ 3)$

これより，$a^2+b^2+c^2\equiv 1\ (\mathrm{mod}\ 3)$ となり，これを満たすのは

$$(a^2, b^2, c^2)\equiv(0, 0, 1), (0, 1, 0), (1, 0, 0)\ (\mathrm{mod}\ 3)$$

のときであり，a，b，c の中に 3 の倍数が 2 つ含まれている。… ①

(2) d が 2 の倍数でないとき，$d^2\equiv 1\ (\mathrm{mod}\ 4)$

これより，$a^2+b^2+c^2\equiv 1\ (\mathrm{mod}\ 4)$ となり，これを満たすのは

$$(a^2, b^2, c^2)\equiv(0, 0, 1), (0, 1, 0), (1, 0, 0)\ (\mathrm{mod}\ 4)$$

のときであり，a，b，c の中に 2 の倍数が 2 つ含まれている。… ②

①，② より，a，b，c の中に少なくとも 1 つは
2 の倍数かつ 3 の倍数，すなわち 6 の倍数であるものが含まれる。

【余談】

ちなみに，本問のような

$a^2+b^2+c^2=d^2$ を満たす自然数 a，b，c，d を探そうと思うと

$$3^2+4^2=5^2$$

$$5^2+12^2=13^2$$

というようにつながっていれば，$3^2+4^2+12^2=13^2$ と見つけることができます。（あくまで探せる程度のもので，全て出てくるとは言っていません）

ちなみに $13^2+84^2=85^2$ ですから，$3^2+4^2+12^2+84^2=85^2$

というように，$a^2+b^2+c^2+d^2=e^2$ を満たす自然数 a，b，c，d，e を見つけることができます。

$(3, 4, 5)$，$(5, 12, 13)$，$(13, 84, 85)$ …… のようなピタゴラス数の並びを「ピタゴラスしりとり」とでも呼ぶことにします。

この「ピタゴラスしりとり」はいくらでも続きます。

それを証明してみます。

【ピタゴラスしりとりが任意の長さで継続可能であることの証明】

以下，使用する文字は全て整数とする。

a が奇数，b が偶数としても一般性を失わない。

ゆえに，$a=2k+1$ と表せる。

唐突においていますが，種明かしは後でします。

このとき，$b=2k^2+2k\ (=2k(k+1))$，$c=2k^2+2k+1$ とおくと，

左辺は $(2k+1)^2+4k^2(k+1)^2=4k^4+8k^3+8k^2+4k+1$

右辺は，

$(2k^2+2k+1)^2=4k^4+4k^2+1+8k^3+4k+4k^2=4k^4+8k^3+8k^2+4k+1$

となり，$a^2+b^2=c^2$ が成立する。

以上から，$a=2k+1$ としたとき，b，c を $\begin{cases} b=2k(k+1) \\ c=2k(k+1)+1 \end{cases}$ と設定すれば，(a, b, c) はピタゴラス数

$2k+1$ と k の最大公約数はユークリッドの互除法により，k と 1 の最大公約数に等しく 1 である。

$2k+1=k\cdot 2+1$

また，$2k+1$ と $k+1$ の最大公約数は ユークリッドの互除法により，

$2k+1=(k+1)+k$

$k+1$ と k の最大公約数に等しく 1 である。… $(*)$
(なぜなら，k，$k+1$ は連続 2 整数なので互いに素)

これより，a と b は互いに素

b，c は連続 2 整数なので互いに素

$2k(k+1)+1$ と $2k+1$ の最大公約数はユークリッドの互除法により，

$2k+1$，$k+1$ の最大公約数と等しく，$(*)$ よりそれは 1 である。

$2k(k+1)+1=(2k+1)\cdot k+k+1$

これより，c と a は互いに素

以上から，(a, b, c) は原始ピタゴラス数である。

ゆえに，(a, b, c) が原始ピタゴラス数のとき，c は奇数で，$c=2\ell+1$ と表せ，このとき，

$$d=2\ell(\ell+1),\ e=2\ell(\ell+1)+1$$

とすれば，(c, d, e) も原始ピタゴラス数である

これより，ピタゴラスしりとりを継続することが可能であることが示された。

補足

原始ピタゴラス数の一般解

一般解については第２講を参照してください。

$$(a,\ b,\ c)=(m^2-n^2,\ 2mn,\ m^2+n^2)$$

において，$m=k+1$，$n=k$ という連続２整数で設定してやると

$$a=(k+1)^2-k^2=2k+1$$

$$b=2k(k+1)$$

$$c=(k+1)^2+k^2=2k^2+2k+1$$

が得られることを利用しています。

ピタゴラスしりとりが任意の長さで継続するということは

$$a_1{}^2+a_2{}^2+\cdots\cdots+a_n{}^2=b^2$$

を満たす自然数 $(a_1,\ a_2,\ \cdots\cdots,\ a_n,\ b)$ が存在することを意味します。