a , b , c はどの２つも１以外の共通な約数をもたない正の整数とする。
a , b , c が

$$a^2+b^2=c^2$$

をみたしているとき，次の問に答えよ。

(1) c は奇数であることを示せ。

(2) a , b の１つは３の倍数であることを示せ。

(3) a , b の１つは４の倍数であることを示せ。

(4) a , b , c の１つは５の倍数であることを示せ。

＜ '04 旭川医科大 改 ＞

【戦略】

(1) **a , b の偶奇のパターンで言えば**

(a , b)=(**偶数，偶数**)，(**偶数，奇数**)，(**奇数，偶数**)，(**奇数，奇数**)

という４パターンあります。

このうち，(a , b)=(偶数，偶数) は条件である a , b が互いに素であるということからありえません。

題意を示すには，(奇数，奇数) を否定すればよいことになります。

方法としては背理法でいきます。

その際ですが，
平方数を何かで割った余り（平方剰余）は限られる
ということが基礎となっているかどうかが差を生みます。

今回は $\begin{cases}(2k)^2=4k^2\\(2k+1)^2=4k^2+4k+1\end{cases}$ **ということから４で割った余りに**

注目していきます。

(2) **引き続き背理法ですが，今度は a , b を３で割った余りで分類します。**

３で割ったときの平方剰余は０，１に限られます。

(3) **a , b を４で割った余りで分類します。**

対称性から a が奇数，b が偶数として考えて一般性を失わないため
$a=4M\pm1$, $b=4N+2$ とおきます。

$a^2+b^2=16M^2\pm8M+16N^2+16N+5$ **という形から何で割った余りに注目すればよいかを考えることになります。**

なるべく数が小さいほうがよいので，最初の候補は４で割った余りを考えたいですが，$a^2+b^2\equiv1\pmod4$ で，矛盾と言えません。

そうなると，次の候補は８で割った余りです。

８で割った平方剰余は調べると０，１，４に限られますから矛盾します。

(4) **a , b , c を５で割った余りで分類します。**

５で割った余りは０，１，４に限られます。
ただ，a , b , c がどれも５の倍数でないという背理法による仮定の下で考えるので，実質的には１，４に限られています。

【解答】

(1) 条件から a , b は互いに素であるので，a , b がともに偶数ということはない。… ①

一般に整数 m , k に対して

$$\begin{aligned}&m=2k\ \text{のとき，}m^2=4k^2\\&m=2k+1\ \text{のとき，}m^2=4(k^2+k)+1\end{aligned}$$

ということから，平方数 m^2 を４で割った余りは０または１ … (*)

ここで，a , b がともに奇数だと仮定する。

このとき，整数 A , B を用いて $\begin{cases}a=2A+1\\b=2B+1\end{cases}$ と表せる。

$$\begin{aligned}c^2&=a^2+b^2\\&=(2A+1)^2+(2B+1)^2\\&=4(A^2+B^2+A+B)+2\end{aligned}$$

となり，c^2 という平方数を４で割った余りが２ということになり，(*) に矛盾する。

ゆえに，a , b がともに奇数となることはない。… ②

①，② より，a , b の偶奇は異なり，c^2 は奇数となるため，
c は奇数となる。

(2) 一般に m , k を整数として

$$\begin{cases}m=3k & \Longrightarrow\quad m^2=9k^2\ (=3\cdot3k^2)\\m=3k\pm1 & \Longrightarrow\quad m^2=9k^2\pm6k+1\ (=3(3k^2\pm2k)+1)\end{cases}$$

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

ということから，平方数 m^2 を３で割った余りは０または１ … (**)

a , b がともに３の倍数でないと仮定すると，(☆) より

a^2+b^2 を３で割った余りは２

$a^2+b^2=c^2$ より，c^2 を３で割った余りも２である。

一方，(**) より平方数 c^2 を３で割った余りは０または１であり，矛盾する。

よって，a , b の１つは３の倍数である。

(3) a , b がともに４の倍数でないと仮定する。

(1) より a , b の偶奇は一致しないため，a , b に関する対称性から
a が奇数，b が偶数として考えて一般性を失わない。

よって，整数 M , N を用いて $\begin{cases}a=4M\pm1\\b=4N+2\end{cases}$ と表せる。

$$\begin{aligned}a^2+b^2&=(16M^2\pm8M+1)+(16N^2+16N+4)\\&=8(2M^2\pm M+N^2+2N)+5\ \cdots③\end{aligned}$$

以下，合同式における法は 8 とする。

一方，一般に m，k を整数として

$$m=8k \text{ のとき } m^2\equiv 0$$

$$m=8k\pm 1 \text{ のとき } m^2\equiv 1$$

$$m=8k\pm 2 \text{ のとき } m^2\equiv 4$$

$$m=8k\pm 3 \text{ のとき } m^2\equiv 1$$

$$m=8k+4 \text{ のとき } m^2\equiv 0$$

であるため，平方数 m^2 を 8 で割った余りは 0 または 1 または 4

ゆえに，c^2 という平方数を 8 で割った余りは 5 とはならない。

③ を考えると $a^2+b^2=c^2$ の両辺を 8 で割った余りが異なることになり矛盾する。

よって，a，b のうち 1 つは 4 の倍数である。

(4) a，b，c がどれも 5 の倍数でないと仮定する。

以下，合同式における法は 5 とする。

一般に m，k を整数として

$$m=5k \text{ のとき } m^2\equiv 0$$

$$m=5k\pm 1 \text{ のとき } m^2\equiv 1$$

$$m=5k\pm 2 \text{ のとき } m^2\equiv 4$$

であるため，平方数 m^2 を 5 で割った余りは 0 または 1 または 4

この仮定の下では，$(a^2,\ b^2)\equiv(1,\ 1),\ (1,\ 4),\ (4,\ 1),\ (4,\ 4)$

つまり，$a^2+b^2\equiv 0$ または 2 または 3

一方，この仮定の下では $c^2\equiv 1$ または 4 であるため，$a^2+b^2=c^2$ の両辺を 5 で割った余りが異なることになり，矛盾する

ゆえに，a，b，c のうち 1 つは 5 の倍数である。

【(3) 戦略 2】

a が奇数，b が偶数として一般性を失わないのですが，このとき b が 4 の倍数であることを示せばよいことになります。

b が 4 の倍数でないと仮定すると，整数 A，B，C を用いて

$$a=2A-1,\ b=4B-2,\ c=2C-1$$

と表せます。

これらを $a^2+b^2=c^2 \Leftrightarrow b^2=(c+a)(c-a)$ に代入して整理すると

$$(2B-1)^2=(A+C-1)(C-A)$$

を得ることになります。

$(A+C-1)+(C-A)=2C-1$（＝奇数）**であることに気が付けば**

$A+C-1$ と $C-A$ の偶奇が異なることになり，右辺が偶数，左辺は奇数となり矛盾します。

【(3) 解 2】

(1) より a，b の偶奇は一致しないため，a，b に関する対称性から
a が奇数，b が偶数として考えて一般性を失わない。

このとき，b が 4 の倍数であることを示せばよい。

b が 4 の倍数とならないと仮定する。

c は奇数であるから，整数 A，B，C を用いて

$$a=2A-1,\ b=4B-2,\ c=2C-1$$

と表せる。

$a^2+b^2=c^2$ より，$b^2=(c+a)(c-a)$ であるため，

$$\{2(2B-1)\}^2=\{(2C-1)+(2A-1)\}\{(2C-1)-(2A-1)\}$$

これを整理すると $(2B-1)^2=(A+C-1)(C-A)$ …(★)

ここで，$(A+C-1)+(C-A)=2C-1$（＝奇数）であるので

$$A+C-1,\ C-A \text{ の偶奇は異なる}$$

ゆえに，(★) の左辺は奇数，(★) の右辺は偶数ということになり矛盾する。

ゆえに，b は 4 の倍数であり，題意は示された。

【総括】

a , b , c のどの 2 つも互いに素であるものとする中で

$$a^2+b^2=c^2$$

を満たす自然数（a , b , c）の組を原始ピタゴラス数と言います。

今回は原始ピタゴラス数の組の中に

必ず 2 の倍数 , 3 の倍数 , 4 の倍数 , 5 の倍数が入っている

という有名事実を証明する問題でした。

入試においても頻出の話題です。

平方剰余（平方数に関する余り）は限られるということは本問に限らずある程度は常識化しておきたいところです。

その際に大切なこととしては

何で割った余りに注目するか

ということです。

これに関しては特効薬的なものがあるわけではないので , 式の形や示すべきことなどからその場において判断することになります。