フェルマーの定理を巡って（Ｉ）解答

問題 原始ピタゴラス数 (x, y, z) は，必ず

$$(x, y, z)=(m^2-n^2, 2mn, m^2+n^2) \qquad \cdots\cdots（*）$$

の形で表すことができる．

【補題１】　原始ピタゴラス数 (x, y, z) の x, y は，一方が奇数で，もう一方は偶数である．

【補題２】　原始ピタゴラス数 (x, y, z) に対して，$\dfrac{z \pm x}{2}$ はともに整数であり，互いに素である．

【補題１】<u>（証明）</u>

x, y の偶奇の場合分けで考える．$(3, 4, 5), (5, 12, 13)$ など補題１の条件で成立する x, y は存在するから，x, y の偶奇が一致するときを確認すれば十分である．

(i)　x, y がともに偶数のとき

仮定から，$x=2k, y=2l$（k, l は自然数）とすると，

$$\begin{aligned} z^2 &= x^2+y^2 \\ &= (2k)^2+(2l)^2 \\ &= 2^2(k^2+l^2) \end{aligned}$$

となり，z も偶数となる．これは互いに素であることに矛盾する．

(ii)　x, y がともに奇数のとき

まずは，平方数は必ず 4 で割った余りが 0 か 1 となることを確認する．

自然数 s, t に対して，$t=2s-1$ と表すと t は奇数である．

$$\begin{aligned} t^2 &= (2s-1)^2 \\ &= 4(s^2-s)+1 \end{aligned}$$

よって，4 で割った余りは 1 である．次に，$t=2s$ とすると，

$$\begin{aligned} t^2 &= (2s)^2 \\ &= 4s^2 \end{aligned}$$

よって，4 で割った余りは 0 である．

したがって，すべての平方数は 4 で割った余りが 0 か 1 となる．

仮定から，$x=2k-1, y=2l-1$ とすると，

$$\begin{aligned} z^2 &= x^2+y^2 \\ &= (2k-1)^2+(2l-1)^2 \\ &= 4(k^2+l^2-k-l)+2 \end{aligned}$$

したがって，自然数 z の平方数は 4 で割った余りが 2 となるが，これは上記のことから矛盾する．

以上 (i)　(ii) より，原始ピタゴラス数 (x, y, z) の x, y の偶奇は異なる．

（今回，$(x, y)=(m^2-n^2, 2mn)$ としたが，もちろん $(x, y)=(2mn, m^2-n^2)$ のように入れ替えても全く問題はないです．）

（証明終わり）

【補題２】 (証明)

条件から $x^2+y^2=z^2$ であり，これを変形すると， $y^2=(z-x)(z+x)$ となる．今， x, z の最大公約数を g とすると， $x=gx', z=gz'$ （x', z' は互いに素）とできて，

$$
\begin{aligned}
y^2&=(gz'-gx')(gz'+gx')\\
&=g^2(z'-x')(z'+x')
\end{aligned}
$$

よって， y も g を約数にもつが，条件から x, y, z は互いに素であり，$g=1$ でないとならないから，x, z は互いに素である．（ x, y, z が互いに素であるから，一見すると x, z が互いに素であることは当たり前のように思えますが，これは間違いである．※１）

x, z が互いに素であるとき，その和と差は互いに素である．

（実際に，上段の解法とほとんど同じ論法で証明ができるので，ぜひチャレンジしてみてください．）

さらに，補題１から x は奇数， y は偶数としてよく， $x^2+y^2=z^2$ より， z は奇数となる．

したがって， $z\pm x$ は(奇数)±(奇数) となり，偶数である．ゆえに， $\dfrac{z\pm x}{2}$ は整数となる．

（証明終わり）

問題 (証明)

補題１から $y=2k$ （ k は自然数）としてよく，

$$
\begin{aligned}
(2k)^2&=(z-x)(z+x)\\
k^2&=\frac{z-x}{2}\cdot\frac{z+x}{2}
\end{aligned}
$$

補題２より， $\dfrac{z\pm x}{2}$ は互いに素であるから，共通素因数をもたない．つまり， $\dfrac{z\pm x}{2}$ はどちらも平方数である．そこで，

$$
m^2=\frac{z+x}{2}>\frac{z-x}{2}=n^2
$$

とすると， $x=m^2-n^2, z=m^2+n^2$ となる．さらに， $z-x=2n^2, z+x=2m^2$ であるから，

$$
\begin{aligned}
y^2&=(z-x)(z+x)\\
&=2n^2\cdot 2m^2\\
&=(2mn)^2
\end{aligned}
$$

したがって， $y=2mn$ となる．

（証明終わり）

※１　一般に３数で互いに素だからといって，そのうちの２数が互いに素だとは限りません．
例えば， $(x, y, z)=(15, 6, 10)$ は３数で見ると互いに素であるが， ２数ずつ見るとどの２数も互いに素ではありません．実際に， $(15, 6, 10)=(3\cdot5, 2\cdot3, 2\cdot5)$ より， 15, 6, 10 は３数すべてに共通する因数はありませんが， 15, 10 は共通因数５をもちます．

しかしながら，実は原始ピタゴラス数 (a, b, c) の場合は a, b, c のどの２数をとっても互いに素となります．これを， (a, b, c) は各対で互いに素と言います．