強者の戦略

それでは，前回の解答です．

第１問（ⅠＡⅡＢ）

p，q は互いに素な自然数とする．以下の問いに答えよ．

(1)　p，q がともに奇数であるとき，p^4+q^4 は自然数の 2 乗にならないことを示せ．

(2)　q は奇数とする．次の手順にしたがって，$(2p)^4+q^4$ が自然数の 2 乗にならないことを背理法を用いて示せ．

(ｉ)　次の仮定 (H) が成り立つものとして，以下の問い (A)～(D) に答えよ．

仮定 (H)：

$(2p)^4+q^4=r^2$ となる自然数 r が存在する．

(A)　$2p$ と r は互いに素になることを示せ．

(B)　互いに素な自然数 m，n があって，

$$r+(2p)^2=m^4,\ r-(2p)^2=n^4$$

と表されることを示せ．

(C)　(B) の m，n について，

$$m+n=2a,\ m-n=2b$$

とおく．p^2 を a，b を用いて表せ．

(D)　$2p_1$ と q_1 が互いに素になり，$p=2p_1q_1r_1$ かつ $(2p_1)^4+(q_1)^4=(r_1)^2$ となる自然数 p_1，q_1，r_1 が存在することを示せ．

(ⅱ)　(ｉ) の仮定 (H) が成り立たないことを示せ．

【2010 年度　福島県立医科大学　第 4 問】

(解答)

以下，自然数全体の集合を $\mathbb{N}$ で表す．

(1)　$n\in\mathbb{N}$ に対して，n が偶数のとき n^2 を 4 で割った余りは 0 であり，n が奇数のとき $n=2k-1$ $(k\in\mathbb{N})$ とおくと $n^2=4(k^2-k)+1$ より n^2 を 4 で割った余りは 1 である．

p，$q\in\mathbb{N}$ が奇数のとき，p^2，q^2 も奇数なので，$p^4=(p^2)^2$，$q^4=(q^2)^2$ を 4 で割った余りはどちらも 1 で，これから p^4+q^4 を 4 で割った余りは 2 である．ところが，自然数の 2 乗を 4 で割った余りは 0 または 1 なので，p^4+q^4 は自然数の 2 乗にならない．

(2)

(ｉ)　(A)　q は奇数より，r も奇数である．$2p$ と r が互いに素でないと仮定すると，$2p$ と r をともに割り切る奇素数 d が存在する．

$$(2p)^4+q^4=r^2 \iff q^4=r^2-(2p)^4$$

より，d は q^4 を割り切り，従って q を割り切る．ところが，p，q は互いに素な自然数なので，$2p$ と q をともに割り切る奇素数は存在せず．矛盾する．よって，$2p$ と r は互いに素になる．

(B)

$$\begin{aligned}&(2p)^4+q^4=r^2\\ \iff\ & q^4=r^2-(2p)^4\\ \iff\ & q^4=\{r+(2p)^2\}\{r-(2p)^2\}\quad\cdots\cdots①\end{aligned}$$

ここで，$r+(2p)^2$ と $r-(2p)^2$ が互いに素になることを示す．これらの公約数の 1 つを d とすると，d は

$$\{r+(2p)^2\}+\{r-(2p)^2\}=2r$$

$$\{r+(2p)^2\}-\{r-(2p)^2\}=2\cdot(2p)^2$$

をともに割り切り，これと (A) から $d=1$ または 2 である．さらに，$r+(2p)^2$，$r-(2p)^2$ はともに奇数であることから，d は奇数であり $d=1$ となる．すなわち．$r+(2p)^2$ と $r-(2p)^2$ は互いに素になる．

これと，① より $r+(2p)^2$ と $r-(2p)^2$ のどちらも自然数の 4 乗になるので，互いに素な自然数 m，n があって

$$r+(2p)^2=m^4,\ r-(2p)^2=n^4\quad\cdots\cdots②$$

と表される．

(C)　② の 2 式を辺々引いて

$$\begin{aligned}8p^2&=m^4-n^4\\ &=(m+n)(m-n)(m^2+n^2)\quad\cdots\cdots③\end{aligned}$$

が成り立つ．

② から m，n は奇数で，$m>n$ なので

$$m+n=2a,\ m-n=2b\ (a,\ b\in\mathbb{N})$$

とおけ

$$m=a+b,\ n=a-b\quad\cdots\cdots④$$

となる．よって

$$m^2+n^2=(a+b)^2+(a-b)^2=2(a^2+b^2)$$

なので，③ から

$$8p^2 = 2a \cdot 2b \cdot 2(a^2+b^2)$$
$$\iff \quad p^2 = ab(a^2+b^2) \quad \cdots\cdots ⑤$$

である．

(D)　m，n が互いに素であることと ④ から，a，b も互いに素になる．すると，a と a^2+b^2 の公約数 (の 1 つ) を d とすると，d は a^2 を割り切るので $(a^2+b^2)-a^2=b^2$ も d で割り切れ，$d=1$ となる．よって a と a^2+b^2 は互いに素．同様にして，b と a^2+b^2 も互いに素になる．すると，⑤ から a，b，a^2+b^2 はどれも自然数の平方となる．

さらに，m，n が奇数であることから，a，b の偶奇は異なるので，偶数のものを α，奇数のものを β とおくと

$$\alpha = (2p_1)^2,\ \beta = {q_1}^2,\ \alpha^2+\beta^2 = {r_1}^2$$
$$(p_1,\ q_1,\ r_1 \in \mathbb{N},\ 2p_1 \text{ と } q_1 \text{ は互いに素})$$

となる p_1，q_1，r_1 がとれて，これらは

$$p^2 = \alpha\beta(\alpha^2+\beta^2) = (2p_1)^2{q_1}^2{r_1}^2$$
$$\iff \quad p = 2p_1q_1r_1$$
$$\alpha^2+\beta^2 = {r_1}^2$$
$$\iff \quad (2p_1)^4 + {q_1}^4 = {r_1}^2$$

を満たす．ゆえに，題意を満たす自然数 p_1，q_1，r_1 が存在する．

(ii)　仮定 (H) が成立すると仮定すると，(i) で示したことから $2p_1$ と q_1 が互いに素になり

$$p = 2p_1q_1r_1 \quad \text{かつ} \quad (2p_1)^4 + (q_1)^4 = (r_1)^2$$

となる自然数 p_1，q_1，r_1 が存在する．このとき $p_1 < p$ なので，(i) の (D) の手順を繰り返していくと，方程式 $x^4+y^4=z^2$ の自然数解 $(x,\ y,\ z)$ で，x がいくらでも小さいものが作れることになり，これは矛盾である. よって. 仮定 (H) は成立しない.

□

（コメント）

数学科の川崎です．今回は，前回に引き続き，フェルマーの最終定理をテーマにした問題を扱いました．使った議論は前回の証明と重複するところもありますので，前回の証明と合わせて見ると，理解も深まるのではと思います．

以下，解答についての補足です．

まず，この問題をもとにフェルマーの最終定理の $n=4$ の場合の証明ができることを確認しましょう．フェルマーの最終定理とは

“n が 3 以上の自然数のとき，$x^n+y^n=z^n$ を満たす自然数 x，y，z は存在しない”

というものです．x，y が偶数であれば，z も偶数ですので，両辺を 2^n で割ることにより，x，y は

（ア）　どちらも奇数

（イ）　どちらかが偶数でどちらかは奇数

の 2 つの場合を考えれば十分になります．（ア）の場合を証明したのが (1)，（イ）の場合を証明したのが (2) です．

(1)　これは有名な問題で，類題をやったことがある人も多いでしょう．ポイントになるのは整数を 1 つの整数で割った

「余りで分類する」

という発想です．これにより，整数を有限のカテゴリーに分けることができるので，議論が有限回で済みます．特に平方数に関しては

・平方数を 3 で割った余りは 0 または 1

・平方数を 4 で割った余りは 0 または 1

・平方数を 5 で割った余りは 0 または 1 または 4

などは，頭に入れておきましょう．簡単に示せますので，証明しておいてください．

今回は, p，q に奇数という条件がありますので，2^k で割った余りを考えるのが良く，2^2 で割った余りを考えればうまくいきます．

(2)(i)

(A)　$2p$ と r の 1 以外の公約数があるとして，その 1 つをとると，与えられた関係式からそれが q^4 を割り切ることが分かります．p と q が互いに素を使いたいので，この公約数が q を割り切ると言うために “素数” という条件をつけました（このような素数がないと言えれば十分です）．さらに，r が奇数なのでこの公約数は奇数で，p の前に 2 がついていても問題ありません．

(B)　与えられた式から ① の因数分解に気づきま

しょう．左辺が自然数の 4 乗なので，あとは右辺の 2 数が互いに素であることを示せば OK です．

2 数が互いに素であることを証明するとき，公約数をおいて，2 数の和・差を考え，その公約数は 1 であるともっていく証明はよく使いますので是非マスターしておいてください．

(C)　p^2 を表すので, (B) の 2 式から r を消去します．m，n を a，b で表せますので，それを代入すれば求められます．これは易しいですね．一つ注意することとしては，m，n はどちらも奇数なので

$$m=2k-1,\ n=2l-1\ (k,\ l\in\mathbb{N})$$

とおくと

$$a=k+l-1,\ b=k-l$$

となり

$$m>n \iff k>l$$

より a，b は自然数です．さらに，$k+l$ と $k-l$ の偶奇は一致するので, a，b の偶奇は異なります．これは (D) で必要になる事柄です．

(D)　本問でもっとも難しい部分がここです．条件を満たす p_1，q_1，r_1 を自分で作らなければならないのですが，自力で作るのは至難の業です．誘導に乗りましょう．(C) の

$$p^2=ab(a^2+b^2)\cdots\cdots(*)$$

が大きなヒントで，右辺の a，b，a^2+b^2 がどれも平方数になれば (a，b のどちらかは偶数であることに注意して)，a，b の一方を $(2p_1)^2$，他方を $q_1{}^2$，a^2+b^2 を $r_1{}^2$ とおくことができ，この p_1，q_1，r_1 が題意を満たします．平方数になることを示すには，$(*)$ の左辺が平方数であることから a，b，a^2+b^2 が互いに素であることが言えればよく，(B) がヒントになっています．

(ii)　(i) から何をさせたいか分かりますか？今年私が担当している記事をもらさず読んでくれている人はピンとくると思います．そうです，

「無限降下法」

です．存在を仮定すると，それよりも小さいものがどんどん作れてしまい，矛盾が導かれるのでした．

(i) の (D) を見て，この手法に気づけるようにしましょう．意外とこの方法を知らない人もいるのではないでしょうか．使えるようにしてライバルに差をつけてください．

それでは今回はここまでにしたいと思います．寒くなってきましたが体調など崩さないように．この冬に頑張っていい春を迎えましょう．ではまた次回．

（数学科　川﨑）