強者の戦略

それでは，前回の解答です．

第 1 問（数 IAIIB）

[1] 自然数 a で，a^4+4 が素数となるものをすべて求めよ．

[2] p が素数ならば，p^4+14 は素数ではないことを示せ．

＜解答＞

[1] $$a^4+4=(a^4+4a^2+4)-4a^2$$
$$=(a^2+2)^2-4a^2$$
$$=(a^2+2a+2)(a^2-2a+2)$$

である．a が自然数であることから

$$a^2+2a+2>a^2-2a+2$$

であり

$$a^2-2a+2=(a-1)^2+1\geqq 1$$

であることに注意すると，a^4+4 が素数である条件は

$$a^2-2a+2=1 \quad \text{かつ} \quad a^2+2a+2 \text{ が素数}$$

となることである．

$$a^2-2a+2=1$$
$$(a-1)^2=0$$
$$a=1$$

であり，$a=1$ のとき

$$a^2+2a+2=5$$

は素数であるから適する．

以上より

$$a=1$$

である．

[2] 合同式の法を 3 とする．

$p=3$ のとき

$$p^4+14=95=5\cdot 19$$

であるから，これは素数ではない．

$p\neq 3$ のとき，p は素数であるから 3 の倍数ではない．よって

$$p\equiv 1 \quad \text{または} \quad p\equiv 2$$

である．いずれの場合も

$$p^2\equiv 1,\ p^4\equiv 1$$

が成り立つので

$$p^4+14\equiv 15\equiv 0$$

である．すなわち，p^4+14 は 3 の倍数である．さらに

$$p^4+14>14>3$$

であるから，p^4+14 は 3 ではない．よって，このときも p^4+14 は素数ではない．

以上で示せた．

□

＜別解＞

[2] 合同式の法を 5 とする．

$p=5$ のとき

$$p^4+14=639=3^2\cdot 71$$

であるから，これは素数ではない．

$p\neq 5$ のとき，p は素数であるから 5 の倍数ではない．よって

$$p\equiv 1,\ 2,\ 3,\ 4$$

のいずれかが成り立つ．それぞれの場合に対して p^2，p^4 を 5 で割った余りを求めると下表のようになる．

$p \pmod 5$	1	2	3	4
$p^2 \pmod 5$	1	4	4	1
$p^4 \pmod 5$	1	1	1	1

よって，いずれの場合も

$$p^4\equiv 1$$

であるから

$$p^4+14\equiv 15\equiv 0$$

である．すなわち，p^4+15 は 5 の倍数である．さらに

$$p^4+14>14>5$$

であるから，p^4+14 は 5 ではない．よって，このときも p^2+14 は素数ではない．

以上で示せた．

□

強者の戦略

＜参考＞

[2] は p が素数という条件を外すと成り立ちません．数字は大きいのですが，例えば

$165^4+14=741200639$

は素数になります．

＜コメント＞

数学科の川﨑です．今年度もこのページを担当させていただきます．よろしくお願いします．

1 回目は整数問題から，素数に関する問題を出題しました．[2] はこの春に京大の文系で出題された問題です．素数は整数を扱う基本となりますので，考え方をしっかりマスターしてください．

以下，設問ごとに補足を述べます．

まず，素数の扱いとして，いつも授業では次の 3 つを頭に置いておくように指導します．

＜*point*＞
① 素数の中で 2 は特別 (唯一の偶数)
② 積の形を作れ
③ 素数 p に対して，p の倍数で素数は p だけ

[1] 実験してみましょう．

$1^4+4=5$ （素数）
$2^4+4=20=4\cdot5$
$3^4+4=85=5\cdot17$
$4^4+4=260=2^2\cdot5\cdot13$
$5^4+4=629=17\cdot37$

となって，$a=1$ 以外は素数にならなさそうな雰囲気が漂ってきます．少なくとも a が偶数だと a^4+4 は 2 より大きい偶数ですので，素数にはなりませんね (＜*point*＞の ①，③ です)

$a=2$，3，4 のとき，与式が 5 より大きい 5 の倍数となることから素数でないと分かります．これが解決の糸口になるのか？と期待しますが，

$a=5$ のときは 5 の倍数にはならないので違うようです (実は，a が 5 の倍数でなければ a^4+4 は 5 より大きい 5 の倍数となるので素数になりません．これは [2] で使う考え方です)．

方針を変えてみましょう．a^4+4 の式の形をよく見ます．a^4 も 4 も平方数ですね．ここで

$a^4+4=(a^2+2)^2-4a^2$

という形が見えたらしめたものです．実は a^4+4 は因数分解できるのです (＜*point*＞の ②)．有名問題ですが，気付かないと厳しいので

「素数」→「積の形が作れないか」

と考える習慣をつけるようにしましょう．

$a^4+4=(a^2+2a+2)(a^2-2a+2)$

と因数分解できれば，右辺の両因数は自然数であることに注意して

$a^2-2a+2=1$

が必要であることが分かります．これを解いて $a=1$ が決まり，このとき与式は 5 (素数) なので十分となります．

$a=1$ と出せただけの人もいると思いますが，**「他に解がないこと」**を示す部分がこの問題の最重要ポイント（最も難しいところ）ですので，答えが見つかっただけで満足しないようにしましょう．

[2] 今度は p^4+14 で，14 が平方数でないので整数係数の範囲で因数分解することはできません．というわけで実験してみます．

$2^4+14=30=2\cdot3\cdot5$
$3^4+14=95=5\cdot17$
$5^4+14=639=3^2\cdot71$
$7^4+14=2415=3\cdot5\cdot161$

となり，素因数に 3 や 5 が並ぶことが分かるはずです．ただし，$p=3$ のときは与式は 3 の倍数ではなく，$p=5$ のときは与式は 5 の倍数ではないことに注意しましょう．

すると，p^4+14 が 3 や 5 で割り切れるかどうかを調べることになるので，整数問題の必須手法の

一つである

「余りで分類」

をしていくことになります．＜解答＞は 3 で割った余りを．＜別解＞では 5 で割った余りを考えました．どちらも同様の考え方ですので，3 で割った余りを考える方で説明します．

素数を 3 で割った余りは，0，1，2 のいずれかですが，＜*point*＞③ にあるように素数のなかで 3 の倍数は 3 だけです．したがって，p が 3 以外の素数のとき，p を 3 で割った余りは 1 または 2 になります．これを 4 乗すると

$$p\equiv 1 \ \Rightarrow \ p^4\equiv 1$$
$$p\equiv 2 \ \Rightarrow \ p^4\equiv 16\equiv 1$$

となり (合同式の法は 3)，余りはいずれも 1 になるので，p^4+14 は 3 の倍数になります．p^4+14 は 3 より大きいので，再び＜*point*＞③ を用いることで素数ではないことが示せます．

5 で割った余りで分類しても同様に，(p が 5 でなければ) p^4 を 5 で割った余りが 1 となることから p^4+14 が 5 より大きい 5 の倍数となり素数でないことが示せます．

証明の鍵となる事実

$$p^4\equiv 1 \pmod 3 \quad (p\not\equiv 3)$$
$$p^4\equiv 1 \pmod 5 \quad (p\not\equiv 5)$$

の背景には次の有名な定理があります．

＜定理＞ フェルマーの小定理

p を素数とし，a を p の倍数ではない自然数とする．このとき

$$a^{p-1}\equiv 1 \pmod p$$

が成り立つ．

＜証明＞

$$a\cdot 1,\ a\cdot 2,\ \cdots\cdots,\ a\cdot(p-1)$$

を p で割った余りはすべて異なることを背理法で示す．

以下，合同式の法を p とする．

$$a\cdot i\equiv a\cdot j \quad (1\leqq i<j\leqq p-1)$$

となる i, j が存在すると仮定すると

$$a(j-i)\equiv 0 \quad \cdots\cdots(*)$$

となる．ところが，a は p の倍数ではなく

$$1\leqq j-i<p-1$$

であるから，$j-i$ も p の倍数ではない．よって (*) は矛盾である．

したがって

$$a\cdot 1,\ a\cdot 2,\ \cdots\cdots,\ a\cdot(p-1)$$

を p で割った余りはすべて異なり，さらに，この中に p の倍数は存在しないから，余りには

$$1,\ 2,\ \cdots\cdots,\ p-1$$

が 1 つずつ現れる．すると, これらの積を p で割った余りを考えると

$$(a\cdot 1)\cdot(a\cdot 2)\cdot\cdots\cdots\cdot\{a\cdot(p-1)\}\equiv(p-1)!$$
$$a^{p-1}\cdot(p-1)!\equiv(p-1)!$$

であり，p が素数であることから $(p-1)!$ は p の倍数ではないので

$$a^{p-1}\equiv 1$$

である．

＜証明終＞

この定理から，p が 3 以外の素数のとき

$$p^{3-1}\equiv 1 \pmod 3$$

であり，これを 2 乗すると

$$p^4\equiv 1 \pmod 3$$

であることや，p が 5 以外の素数のとき

$$p^{5-1}\equiv 1 \pmod 5$$

などが直ちに分かります．フェルマーの小定理を知らなくても，実験することで解答の方針を立てることは可能ですが，知識としてもっておくと問題に取り組みやすくなります．

それでは，1 問練習問題をつけておきます．『強者の戦略』の冊子内で合格者が「伝説の問題」と書いていたこともある有名な問題です．特に (2) の出題形式が独特で素晴らしいです．

強者の戦略

問

自然数 n の関数 $f(n)$，$g(n)$ を

$f(n)=$(n を 7 で割った余り)

$$g(n)=3f\left(\sum_{k=1}^{7}k^n\right)$$

によって定める．

(1)　すべての自然数 n に対して，$f(n^7)=f(n)$ を示せ．

(2)　あなたの好きな自然数 n を 1 つ決めて $g(n)$ を求めよ．その $g(n)$ の値をこの設問 (2) におけるあなたの得点とする．

＜解答＞

(1)　n^7-n

$=n(n^3-1)(n^3+1)$

$=n(n-1)(n+1)(n^2+n+1)(n^2-n+1)$

が 7 の倍数であることを示す．

n を 7 で割った余りで分類して

・余りが 0 のとき　→　n が 7 の倍数

・余りが 1 のとき　→　$n-1$ が 7 の倍数

・余りが 2 のとき　→　n^2+n+1 が 7 の倍数

・余りが 3 のとき　→　n^2-n+1 が 7 の倍数

・余りが 4 のとき　→　n^2+n+1 が 7 の倍数

・余りが 5 のとき　→　n^2-n+1 が 7 の倍数

・余りが 6 のとき　→　$n+1$ が 7 の倍数

となり，いずれの場合も

$$n(n-1)(n+1)(n^2+n+1)(n^2-n+1)$$

は 7 の倍数である．

よって

$$f(n^7)=f(n)$$

が成り立つ．

(2)　$f\left(\sum_{k=1}^{7}k^n\right)$

$=f(1^n+2^n+3^n+\cdots\cdots+6^n+7^n)$

$=f(f(1^n)+f(2^n)+\cdots\cdots+f(6^n))$

$(\because\ f(7^n)=0)$

である．これと (1) より $1\leqq n\leqq 6$ で考えればよい．

$1\leqq k\leqq 6$ に対して，$k^n\,(1\leqq n\leqq 6)$ を 7 で割った余りは次の表のようになる．

k \ n	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

よって，$n=6$ とすれば

$g(6)=3(1+1+1+1+1+1)=18$

であり，これがこの問題で得られる最高点になる．

＜解答終＞

ちょっと実験をすると

$g(1)=0$，$g(2)=0$，$g(3)=0$

となることから，簡単には正の得点がもらえないことが分かります．あなたは何点取れましたか？

この問題も，k が 7 の倍数ではないとき，フェルマーの小定理から

$$k^6\equiv 1\pmod 7$$

であることが分かっていると $g(6)$ の値が計算しやすくなります．

それでは今回はここまでにしたいと思います．また次回．

（数学科　川﨑）