整数問題の攻略（基礎編）

『整数問題攻略のための５つの原則』では，整数特有の性質や考え方の基本姿勢を紹介しました．ここからは，もう少し具体的に学んでいきたいと思います．

1　余りで分類する

すべての整数は n で割ったときの余りによって n 個のグループに分類されます．例えば，3 で割った余りが 0，1，2 のいずれであるかによって，全整数は 3 つのグループに分類され，その各グループに含まれる数を k を整数として，

$$3k,\quad 3k+1,\quad 3k+2$$

と表します（場合によっては，$3k$，$3k\pm1$ ととることもあり，この方が計算が楽になることが多い）．全ての整数は，この 3 つのグループのいずれか 1 つに必ず属します．この考え方は，**無限個ある整数をグループ分けし，そのグループに属する数をまとめて扱う，という点において非常に重要な考え方で，多くの整数問題を解くときの基本となります．**

➪**注**　合同式の言葉で言えば，

$$n\equiv 0,\ 1,\ 2\ \ (\mathrm{mod}\ 3)$$

ということです．もちろん

$$n\equiv 0,\ \pm 1\ \ (\mathrm{mod}\ 3)$$

としても同じことです．

例題　n を整数とするとき，$2n^3-3n^2+n$ は 6 の倍数であることを示せ．

考え方　言うまでもなく，6 の倍数とは 2 の倍数かつ 3 の倍数のことです．

解　$2n^3-3n^2+n=n(n-1)(2n-1)$ より，連続 2 整数の積 $n(n-1)$ を含むから，必ず 2 の倍数である．あとは，これが 3 の倍数でもあることを示せばよい．よって 3 で割った余りで分類する．

$n=3k$ のとき，n が 3 の倍数．

$n=3k+1$ のとき，$n-1=3k$ より，$n-1$ が 3 の倍数．

$n=3k+2$ のとき，$2n-1=6k+3$ より，$2n-1$ が 3 の倍数．

よって，$n(n-1)(2n-1)$ は 3 の倍数になる．

$\therefore$ $2n^3-3n^2+n$ は 6 の倍数である．

■

➪**注**　3 の倍数になる部分の証明を合同式を用いれば次のようになります．

$n\equiv 0\ (\mathrm{mod}\ 3)$ のとき，

$2n^3-3n^2+n\equiv 0\ (\mathrm{mod}\ 3)$.

$n\equiv 1\ (\mathrm{mod}\ 3)$ のとき，

$2n^3-3n^2+n\equiv 2-3+1\equiv 0\ (\mathrm{mod}\ 3)$.

$n\equiv 2\ (\mathrm{mod}\ 3)$ のとき，

$2n^3-3n^2+n\equiv 16-12+2\equiv 6\equiv 0\ (\mathrm{mod}\ 3)$.

よって，$2n^3-3n^2+n$ は 3 の倍数である．

➪**注**　6 の倍数であることを示すのだから，いきなり（mod 6）で考えてもできますが，計算が結構大変になるのであまりおススメしません．

➪**注**　式変形でも 6 の倍数であることがわかります．

$$\begin{aligned}&n(n-1)(2n-1)\\=&n(n-1)(2(n-2)+3)\\=&2n(n-1)(n-2)+3n(n-1)\end{aligned}$$

$n(n-1)(n+1)$ は連続 3 整数の積なので 6 の倍数．また，$n(n-1)$ は連続する 2 整数の積なので 2 の倍数だから $3n(n-1)$ も 6 の倍数．

よって，$n(n-1)(2n-1)$ は 6 の倍数．■

例題　自然数 P が 2 でも 3 でも割り切れないとき，P^2-1 は 24 で割り切れることを示せ

考え方　まずは，6 で割った余りで分類します．

	2 で割れるか	3 で割れるか
$6k$	割れる	割れる
$6k+1$	割れない	割れない
$6k+2$	割れる	割れない
$6k+3$	割れない	割れる
$6k+4$	割れる	割れない
$6k+5$	割れない	割れない

よって，「2 でも 3 でも割り切れない」とは「$P = 6k+1$ または $P = 6k+5$」の場合になります．また，今回の場合，$P = 6k+1$, $6k+5$ を代入するだけではダメで，もう一手間かかります．

解

$P = 6k+1$ のとき，

$$P^2 - 1 = 36k^2 + 12k = 12k(3k+1)$$

k が偶数のとき $12k$ が 24 の倍数になり，k が奇数のとき，$3k+1$ は偶数になるので $12(3k+1)$ が 24 の倍数になる．よって，P^2-1 は 24 の倍数．

$P = 6k+5$ のとき，

$$P^2-1 = 36k^2+60k+24 = 12(3k+2)(k+1)$$

k が偶数のとき，$12k$ が $3k+2$ は偶数になるので $12(3k+2)$ が 24 の倍数になる．k が奇数のとき，$k+1$ は偶数になるので $12(k+1)$ が 24 の倍数になる．よって，P^2-1 は 24 の倍数．

■

➪注　次章で学習する「平方数の分類」を知っていれば，もっとアッサリ解決します．後ほど紹介します．

➪注　もし合同式を用いるならば，「24 の倍数」を「3 の倍数かつ 8 の倍数」と解釈します．3 の倍数になることの証明は P が 3 の倍数ではないので，$P \equiv \pm 1 \pmod 3$ のときだけを考えればよく，

$$P^2 - 1 \equiv 1 - 1 \equiv 0 \pmod 3$$

と一瞬で証明できますが，8 の倍数であることの証明がヤッカイです (これも後ほど紹介します)．

このように，先ほどの **例題** と違って，合同式で解くほうが難しい場合もあるので，どちらの方法でも解けるようになっておこう．

➪注　式変形でも解けます．$P = 6k+1$ の場合だけ紹介すると，

$$\begin{aligned} P^2 - 1 &= 12k(3k+1) \\ &= 12k(2k+k+1) \\ &= 24k^2 + 12k(k+1) \end{aligned}$$

と解釈すれば，$k(k+1)$ が連続 2 整数の積になっているので，24 の倍数になるのは明らかです．

$P = 6k+5$ のときも同様に解釈できるので，これは各自への宿題としましょう．

2　平方数の分類

平方数 (1，4，9，16，25，…) を 3，4，5，8 で割った余りについて下の表にまとめてみよう．

n	1	2	3	4	5	6	7	8	9	10
n^2	1	4	9	16	25	36	49	64	81	100
n^2 を 3 で割った余り	1	1	0	1	1	0	1	1	0	1
n^2 を 4 で割った余り	1	0	1	0	1	0	1	0	1	0
n^2 を 5 で割った余り	1	4	4	1	0	1	4	4	1	0
n^2 を 8 で割った余り	1	4	1	0	1	4	1	0	1	4

この表から次のことがわかります．

平方数を 3 で割った余りは，0 か 1 である．
平方数を 4 で割った余りは，0 か 1 である．
平方数を 5 で割った余りは，0 か 1 か 4 である．
平方数を 8 で割った余りは，0 か 1 か 4 である．

このように平方数を 3，4，5，8 割った余りは極めて特徴的です．

➪注　したがって，次のような式は全て**あり得ない**ので矛盾です．m，n を整数とするとき，

$m^2 = 3n+2 \implies$ 矛盾
(平方数を 3 で割って余り 2 にはならないから．)
$m^2 = 5n+3 \implies$ 矛盾
(平方数を 5 で割って余り 3 にはならないから．)

それでは，それぞれの状況を証明しよう．

2.1　平方数の 3，5 による分類

合同式を用いた証明が明解です．

▷Point◁(平方数を 3 で割った余り)

n が 3 で割り切れるとき，
　　n^2 を 3 で割ると余り 0
n が 3 で割り切れないとき，
　　n^2 を 3 で割ると余り 1

証明

$n \equiv 0 \pmod 3$ のとき，$n^2 \equiv 0 \pmod 3$
$n \equiv \pm 1 \pmod 3$ のとき，

$$n^2 \equiv (\pm 1)^2 \equiv 1 \pmod 3$$

■

➪注 合同式を用いないなら次のようになります．
$n = 3k$ のとき，$n^2 = (3k)^2 = 9k^2 = 3\cdot 3k^2$ となり，n^2 は 3 で割り切れる．
$n = 3k \pm 1$ のとき，

$$n^2 = (3k \pm 1)^2 = 9k^2 \pm 6k + 1 = 3(3k^2 \pm 2k) + 1$$

となり，n^2 は 3 で割ると 1 余る．

■

➪注 もちろん，$n = 3k$，$3k+1$，$3k+2$ としても構いません．

▷Point◁(平方数を 5 で割った余り)

n が 5 で割り切れるとき，
　　n^2 を 5 で割ると余り 0
n を 5 で割って余りが 1 または 4 のとき，
　　n^2 を 5 で割ると余り 1
n を 5 で割って余りが 2 または 3 のとき，
　　n^2 を 5 で割ると余り 4

証明

$n \equiv 0 \pmod 5$ のとき，$n^2 \equiv 0 \pmod 5$
$n \equiv \pm 1 \pmod 5$ のとき，$n^2 \equiv 1 \pmod 5$
$n \equiv \pm 2 \pmod 5$ のとき，$n^2 \equiv 4 \pmod 5$

■

➪注 合同式を用いないなら，$n = 5k$，$5k \pm 1$，$5k \pm 2$ として n^2 に代入して計算します ($n = 5k$，$5k+1$，$5k+2$，$5k+3$，$5k+4$ としても構いません)．3 で割った場合と全く同じなので，各自でやっといてください．

次の問題は超有名問題です．

例題 自然数 a，b，c が $a^2 + b^2 = c^2$ を満たすとき，
(1) a，b のうち少なくとも 1 つは 3 の倍数があることを示せ．
(2) a，b，c のうち少なくとも 1 つは 5 の倍数があることを示せ．

解

(1) a も b も 3 の倍数でないとすると，a^2，b^2 を 3 で割った余りはそれぞれ 1 なので，$a^2 + b^2$ を 3 で割った余りは 2 である．
また，平方数 c^2 を 3 で割った余りは 0 か 1 なので，$a^2 + b^2 \neq c^2$ となり矛盾する．
よって，a，b のうち少なくとも 1 つは 3 の倍数である．

(2) a，b，c がすべて 5 の倍数でないとすると，a^2，b^2，c^2 を 5 で割った余りは 1 か 4 である．$a^2 + b^2$ を 5 で割った余りは，1＋1 か 1＋4 か 4＋4 を 5 で割った余り，すなわち，2 か 0 か 3 でるので，$a^2 + b^2 \neq c^2$ となり矛盾する．
よって，a，b，c のうち少なくとも 1 つは 5 の倍数である．

■

➪注 今回は「平方数の分類」を知ってるものとして解答しましたが，やはり実際の試験では何も書かないわけにはいかないので，答案の最初に「平方数の分類」の証明をしておいた方が良いでしょう．

2.2　平方数の 4，8 による分類

合同式を使わないほうが明解です．

▷Point◁(平方数を 4 で割った余り)

n が偶数のとき，n^2 を 4 で割ると余り 0
n が奇数のとき，n^2 を 4 で割ると余り 1

証明

$n=2k$ のとき，$n^2=(2k)^2=4k^2$ となり， n^2 は 4 で割り切れる．

$n=2k+1$ のとき，

$n^2=(2k+1)^2=4k^2+4k+1$

となり，n^2 は 4 で割ると 1 余る．

■

▷Point◁(平方数を 8 で割った余り)

n が 4 で割り切れるとき，

n^2 を 8 で割ると余り 0

n を 4 で割ると 2 余るとき，

n^2 を 8 で割ると余り 4

n が奇数 (つまり n を 4 で割ると余り 1， 3) のとき，

n^2 を 8 で割ると余り 1

証明

$n=4k$ のとき，$n^2=(4k)^2=16k^2=8\cdot 2k^2$ となり， n^2 は 8 で割り切れる．

$n=4k+2$ のとき，

$$n^2=(4k+2)^2=16k^2+16k+4=8(2k^2+2k)+4$$

となり，n^2 は 8 で割ると 4 余る．

$n=2k+1$ のとき，

$$n^2=(2k+1)^2=4k^2+4k+1=4k(k+1)+1$$

$k(k+1)$ は連続する 2 整数の積だから偶数．つまり，$4k(k+1)$ は 8 の倍数となり，n^2 は 8 で割ると 1 余る．

■

➪注 特に最後の結果

(奇数)^{2}は 8 で割ると余りが 1 である

は，かなり頻繁に登場するので，これはこれで単独で覚えておいたほうが良いでしょう．

最初に紹介した 例題 はこのことが背景にあります．

例題 自然数 P が 2 でも 3 でも割り切れないとき，P^2-1 は 24 で割り切れることを示せ

解 P が 2 の倍数でない (つまり奇数) のとき，P^2 は 8 で割ると余り 1 なので，P^2-1 は 8 で割り切れる．

P が 3 の倍数でないとき，P^2 は 3 で割ると余り 1 なので，P^2-1 は 3 で割り切れる．

よって，P^2-1 は 3 でも 8 でも割り切れるので 24 の倍数である．

■

最後にもう一度，平方数の分類をまとめておこう．

▷Point◁(平方数の分類)

平方数を 3 で割った余りは，0 か 1 である．

平方数を 4 で割った余りは，0 か 1 である．

平方数を 5 で割った余りは，0 か 1 か 4 である．

平方数を 8 で割った余りは，0 か 1 か 4 である．

平方数の分類結果は，知っていると証明の見通しが立ってとても便利なので，まずは結果を覚えてください．なお，入試では証明なしで用いることは避けたほうが良いでしょう．そんなに大変な証明じゃないので，いつでもすぐにできるようにしておこう．

3　指数型

2^n や 3^n のような指数型の整数を割った余りを考えよう．3 通りの方法があります．次の 例題 をそれぞれの方法で解き比べてみよう．

例題

(1) すべての自然数 n に対して 4^n-1 が 3 で割り切れることを示せ．

(2) 2^n+1 が 3 で割り切れるような自然数 n の満たすべき条件を求めよ．

3.1　合同式の利用

おそらく，この方法が最も簡単でベストな解法です．

解

(1) $4\equiv 1\pmod 3$ なので，

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

よって，$4^n-1\equiv 0\pmod 3$.

(2) $2 \equiv -1 \pmod 3$ なので,

$$2^n + 1 \equiv (-1)^n + 1 \pmod 3$$

n が偶数のとき,

$$(-1)^n + 1 \equiv 1 + 1 \equiv 2 \pmod 3$$

n が奇数のとき,

$$(-1)^n + 1 \equiv -1 + 1 \equiv 0 \pmod 3$$

よって, $2^n + 1$ が 3 で割り切れるための条件は, n が奇数であることである.

■

3.2　二項定理の利用

整数問題でも二項定理を利用することが多々あります.

▷Point◁(二項定理)

$$(a+b)^n = \sum_{k=0}^{n} {}_n\mathrm{C}_k a^{n-k} b^k$$

✍注　二項定理より,

$$\begin{aligned}(a+b)^n &= {}_n\mathrm{C}_0 a^n b^0 + {}_n\mathrm{C}_1 a^{n-1} b^1 + \cdots \\ &\qquad \cdots + {}_n\mathrm{C}_{n-1} a^1 b^{n-1} + {}_n\mathrm{C}_n a^0 b^n \\ &= (a \text{ の倍数}) + b^n\end{aligned}$$

となるので, $(a+b)^n$ を a で割った余りは, b^n を a で割った余りに等しいことがわかります. つまり, 合同式で書けば

$$(a+b)^n \equiv b^n \pmod a$$

解　(1) 二項定理より,

$$\begin{aligned}4^n &= (3+1)^n \\ &= \sum_{k=0}^{n} {}_n\mathrm{C}_k 3^{n-k} 1^k \\ &= {}_n\mathrm{C}_0 3^n 1^0 + {}_n\mathrm{C}_1 3^{n-1} 1^1 + \cdots \\ &\qquad \cdots + {}_n\mathrm{C}_{n-1} 3^1 1^{n-1} + {}_n\mathrm{C}_n 3^0 1^n \\ &= (3 \text{ の倍数}) + 1\end{aligned}$$

なので, $4^n - 1$ は 3 の倍数である.

(2) 二項定理より,

$$\begin{aligned}2^n + 1 &= (3-1)^n + 1 \\ &= \sum_{k=0}^{n} {}_n\mathrm{C}_k 3^{n-k} (-1)^k \\ &= {}_n\mathrm{C}_0 3^n (-1)^0 + {}_n\mathrm{C}_1 3^{n-1} (-1)^1 + \cdots \\ &\quad \cdots + {}_n\mathrm{C}_{n-1} 3^1 (-1)^{n-1} + {}_n\mathrm{C}_n 3^0 (-1)^n + 1 \\ &= (3 \text{ の倍数}) + (-1)^n + 1\end{aligned}$$

なので, これが 3 の倍数になるためには, $(-1)^n + 1 = 0$ でなければならないので, n は奇数である.

■

✍注　うすうす気づいているかもしれませんが, 上の解法において, 二項定理で展開して出てきた項のうちで, 3 の倍数の項を除外し, 3 の倍数以外の項だけに注目して考えるのが最初に紹介した「合同式を用いた解法」に他なりません. つまり, 合同式とは二項定理による解法を簡略化しただけのことです.

3.3　因数分解の利用

次の因数分解は整数問題に限らず重要な公式でいろんなところで登場します.

▷Point◁(因数分解の公式)

公式 ①　n を自然数とするとき,

$$\begin{aligned}&a^n - b^n \\ =&(a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \\ &\qquad \cdots + a^2 b^{n-3} + ab^{n-2} + b^{n-1})\end{aligned}$$

公式 ②　n が奇数のとき,

$$\begin{aligned}&a^n + b^n \\ =&(a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \\ &\qquad \cdots + a^2 b^{n-3} - ab^{n-2} + b^{n-1})\end{aligned}$$

この因数分解は指数の形の式を「積の形に変形する」ことができるという点でとても重要です.

$a^n - b^n$ は全ての自然数 n で $a - b$ を因数にもち, $a^n + b^n$ は n が奇数のときだけ $a + b$ を因数にもつことに注意しよう.

解

(1) $4^n-1=4^n-1^n$ となるので，前問と同様に，公式①で $a=4$，$b=1$ とすれば，

$$\begin{aligned}4^n-1^n&=(4-1)(4^{n-1}+\cdots+1^{n-1})\\&=3(4^{n-1}+\cdots+1^{n-1})\end{aligned}$$

となり，3 の倍数になることがわかる．

(2) $n=2m$ のとき，

$$2^n+1=2^{2m}+1=4^m+1=(4^m-1)+2$$

となり，(1) より，4^m-1 は 3 の倍数だから，2^n+1 は 3 で割ると 2 余る．

$n=2m+1$ のとき，

$$2^n+1=2^{2m+1}+1=4^m\times2+1=2(4^m-1)+3$$

となり，(1) より，4^m-1 は 3 の倍数だから，2^n+1 は 3 で割り切れる．

よって，2^n+1 が 3 で割り切れるような自然数 n は n が奇数であることである．

■

➪**注** (2) で，なぜいきなり n が偶数か奇数かで場合分けしたのでしょう．それは公式②が背景にあります．「いつ 2^n+1 が 3 で割り切れるか」と問われたとき，公式②をイメージして，「n が奇数なら $2^n+1=(2+1)(\cdots\cdots)$ と因数分解できるので 3 で割り切れるはずだ」と考えたからです．

解答では，(2) は (1) の結果を利用しているので，因数分解の公式を直接的に使っていませんが，場合分けを考える際に (間接的に) 因数分解の公式を考えているのです．

以上，3 通りの解法を紹介しましたが，圧倒的に合同式を利用した解法が簡単なのがわかります．しかし，二項定理や因数分解も重要な解法なので，今回だけは 3 通り全てマスターしておきましょう．

例題　2^n を 7 で割ったときの余りが 1 であることの必要十分条件は，n が 3 の倍数であることを証明せよ．

考え方　必要十分条件なので，双方向の証明が必要です．もちろん合同式を利用しましょう．

解

「n が 3 の倍数

$\Longrightarrow 2^n$ を 7 で割ったときの余りが 1」の証明

$n=3k$ とおく．

$$2^n\equiv2^{3k}\equiv8^k\equiv1^k\equiv1\pmod 7$$

よって，2^n を 7 で割ると余り 1 である．

「2^n を 7 で割ったときの余りが 1

$\Longrightarrow n$ が 3 の倍数」の証明

n が 3 の倍数ではないと仮定する．

$n=3k+1$ のとき，

$$2^n\equiv2^{3k+1}\equiv2\cdot8^k\equiv2\cdot1^k\equiv2\pmod 7$$

$n=3k+2$ のとき，

$$2^n\equiv2^{3k+2}\equiv4\cdot8^k\equiv4\cdot1^k\equiv4\pmod 7$$

いずれの場合も 2^n を 7 で割ると余り 1 ではない．

よって，対偶命題が証明されたのでもとの命題は正しい．

■

➪**注**　合同式を利用しないなら，

$8^k=(7+1)^k$ と解釈して二項定理で展開する

$8^k-1=8^k-1^k$ と解釈して因数分解を利用する

ことになります．さっきと全く同じなので各自で勝手にやっといてください．

4　素数 p の性質

まずは素数について確認しておこう．

> 1 以外の自然数で，1 と自分自身以外に正の約数をもたない数を**素数**という．

さて，「素数の問題は難しい」と先入観を持っている人が多いようです．確かに，素数に関する研究者レベルの本格的な問題は非常に難しく，世界中のプロの数学者の頭脳を結集しても歯が立たない状況ですが，高校生を対象にした大学入試で扱う程度の素数の問題は，そんなに高級な手段を用いなくても解けるようになっているわけで，恐れる必要は全くありません．

たいていは次の性質を考えるだけで，簡単に見つかるように作問されています．いずれにしてもポイントは因数分解です．

▷Point◁(素数の性質)

p を素数とするとき，次の性質が成り立つ．

性質 ①　ab が p で割り切れる
$\Longrightarrow$ a または b が p で割り切れる

性質 ②　$p=ab$
$\Longrightarrow (a,\ b)=(1,\ p)$ or $(p,\ 1)$

次の【例】もわりと重要です．

【例】
素数 p は $a\ (1\leqq a\leqq p-1)$ と互いに素．
したがって，p は $(p-1)!$ とも互いに素．

「素数になることの証明」と「素数にならないことの証明」を紹介します．

例題　n を 2 以上の自然数とするとき，n^4+4 は素数にはならないことを示せ．

考え方　「素数にならない＝合成数である」ことから積の形に変形できればいのです．因数分解できることに気づきますか？

解

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

と因数分解できる．$n\geqq 2$ だから，

$$n^2-2n+2=(n-1)^2+1\geqq 2$$
$$n^2+2n+2=(n+1)^2+1\geqq 10$$

となるので，n^4+4 は素数にはならない．

■

例題　n^4+n^2+1 が素数になるような自然数 n を全て求めよ．

考え方　本来，素数になることの証明は非常に難しいのですが，高校生で扱える問題はほぼ間違いなく因数分解できるようになっています．

解　$n^4+n^2+1=(n^2+1)^2-n^2$
$$=(n^2+n+1)(n^2-n+1)$$

だから，n^4+n^2+1 が素数 p になるとき，

$(n^2+n+1,\ n^2-n+1)=(p,\ 1),(1,\ p)$

の組み合わせが考えられるが，n は自然数なので，$n^2+n+1\geqq 3$ だから，$(n^2+n+1,\ n^2-n+1)=(p,\ 1)$ の場合しかない．このとき，$n^2-n+1=1$ より $n=1$ となり，$n^2+n+1=3$ は素数である．
よって，求める自然数は $n=1$.

■

例題　$3p+1$ が平方数になるような素数 p は $p=5$ のときに限ることを証明せよ．

考え方　全ての素数をチェックするのは不可能です．とりあえず，$3p+1=m^2$ とでもおいて，この式をみたす素数が $p=5$ しかないことを示そう．

解　$3p+1=m^2$ とすると，
$3p=(m+1)(m-1)$ だから，

$m+1$	1	3	p	$3p$
$m-1$	$3p$	p	3	1

これらの各場合を検証し，$p=5$ を得る．

■

また「素数 p を求めよ」という問題もありますが，素数を見つけることはプロの数学者でも難しいことなので．高校生が入試問題で素数を求めることができるのは，かなり特別な場合です．まずは

実験して規則性を予想 $\Longrightarrow$ 証明

という流れが基本．

例題　n を自然数とする．
整数 $a_n=19^n+(-1)^{n-1}2^{4n-3}$ の全てを割りきる素数を求めよ．

考え方　僕が高校時代に解いた印象的な問題 (1986 年東工大)．先ほども述べたように「素数を見つける」なんて神の領域の作業なので，高校生が見つけられる素数は身近なところに転がっています．まずは n にいろいろ代入すれば……

解　$a_1 = 19 + 2 = 21 = 3 \times 7$

$a_2 = 19^2 - 2^5 = 329 = 7 \times 47$

となるので，a_n の全てを割り切る素数は 7 であると予想できる．よって「a_n が 7 で割り切れること」を証明すればよい．

合同式を利用して証明する．

$$\begin{aligned} a_n &= 19^n + (-1)^{n-1}2^{4n-3} \\ &\equiv 5^n + (-1)^{n-1}2^{4(n-1)} \cdot 2 \quad (\mathrm{mod}\ 7) \\ &\equiv 5^n + (-1)^{n-1}16^{n-1} \cdot 2 \quad (\mathrm{mod}\ 7) \\ &\equiv 5^n + (-16)^{n-1} \cdot 2 \quad (\mathrm{mod}\ 7) \\ &\equiv 5^{n-1} \cdot 5 + 5^{n-1} \cdot 2 \quad (\mathrm{mod}\ 7) \\ &\equiv 5^{n-1}(5+2) \quad (\mathrm{mod}\ 7) \\ &\equiv 5^{n-1} \cdot 7 \quad (\mathrm{mod}\ 7) \\ &\equiv 0 \quad (\mathrm{mod}\ 7) \end{aligned}$$

■

➪注　$-16 \equiv 5\ (\mathrm{mod}\ 7)$ と考えることがポイントです．実にうまい方法ですが，かなり技巧的でなかなか思いつかないでしょう．その場合は「数学的帰納法」を利用してください．各自でやっとこう．

5　互いに素

5.1　約数の性質

また，次のことは整数問題のほとんど全てに関係するといっても過言ではありません．なお，**互いに素**とは**最大公約数が 1 または共通の素因数を持たない**という意味で後ほど詳しく解説します．

▷Point◁

自然数 a，b，c について，a，b が互いに素であるとする．このとき，

ac が b で割り切れる $\Longleftrightarrow$ c が b で割り切れる．

である．

簡単に説明すると，ac が b で割り切れるとき，$\dfrac{ac}{b}$ は整数になるが，a と b が互いに素なので約分できないから，c が b で割り切れなければならないということです．

まずは「互いに素」の意味を確認しよう．一般的には次のような定義になるでしょう．

▷Point◁(「互いに素」の性質)

a，b が互いに素であるとは，…

定義 ①　a，b が 1 以外の公約数をもたない

定義 ②　a，b の最大公約数が 1 である

➪注　「互いに素」を「互いに素数」と勘違いしている人が意外と多いです．「a，b が互いに素である」と「a，b が素数である」は全く違う意味です．しかし「2 つの異なる素数は互いに素である」は正しいので注意しよう．

互いに素の定義として，これらは数学的に完全に正しいのですが，この定義に従うとなかなか証明問題が解けないことが多いので，次の定義で憶えておきましょう．

▷Point◁(「互いに素」の定義)

a，b が互いに素であるとは，a，b **が共通の素因数 p をもたないこと**である．

「互いに素であることを証明せよ」という問題では，たいてい背理法で証明します．つまり互いに素ではないと仮定して矛盾を導くのです．互いに素であることを共通の素因数をもたないこと，と定義したんだから，「共通の素因数 p をもつと仮定すると」と話が始まります．**素数の力を借りて証明する**わけです．

例題　a，b が互いに素であるとき，$a+b$，ab は互いに素であることを示せ．

考え方　背理法によります．つまり，$a+b$，ab が共通の素数 p で割り切れると仮定して矛盾を示そう．

解　$a+b$，ab が互いに素でないと仮定すると，共通の素因数 p が存在し，

$$a + b = pm \cdots ①$$
$$ab = pn \cdots ②$$

となる．② より，a または b が素数 p で割り切れる．a が p で割り切れるとき，① より $b = pm - a$ だから，b も p で割り切れることになり，a，b が互いに素であることに矛盾する．b が p で割り切れる場合も同様である．

したがって，$a+b$，ab は互いに素である．

■

⇛注 上の 例題 は逆も成立します．

$a+b$，ab が互いに素 $\Longleftrightarrow$ a，b は互いに素

証明は対偶をとることで簡単に示せます．

例題 a を 2 以上の自然数とするとき，a と a^2+1 は互いに素であることを示せ．

考え方 共通の素因数 p をもつと仮定して矛盾を示します．具体的に共通の素因数がないことを実際に示す方法もあります．

解 a，a^2+1 が共通の素因数 p をもつと仮定すると，$a=p\alpha$，$a^2+1=p\beta$ とおける．このとき $p^2\alpha^2+1=p\beta$ より，$p(\beta-p\alpha^2)=1$ となるので矛盾．よって，a，a^2+1 は互いに素である．

■

別解 a の素因数を小さいほうから順番に，p_1，p_2，…，p_n とすると，これら全ての素因数で a^2+1 を割ると，いずれの場合も割っても 1 余る．よって，a と a^2+1 に共通の素因数は存在しない．

■

「互いに素」であるときに成立する重要性質として，忘れてはならないのが次の性質です．平方数であることの証明に利用されます．

▷Point◁(「互いに素」の性質)

a，b を互いに素とする．ab が平方数のとき，a も b も平方数である

感覚的に明らかですが，証明しておこう．

証明

まず，a または b が 1 のときは明らか．それ以外の場合を考えると，a が平方数でなければ，a を素因数分解したとき，ある素数 p で「p の奇数乗」という因数が現れるはずである．ところが，a，b が互いに素だから，b は p を因数にもつことはなく，結局，ab を素因数分解したときも，やはり p の指数は奇数のはず．これは右辺が平方数（全ての指数が偶数）であることに矛盾．よって a は平方数．同様に b も平方数．

■

例題 連続する 2 つの自然数の積は平方数にはならないことを示せ．

考え方 連続する 2 つの自然数の積 $n(n+1)$ が平方数になったと仮定して矛盾を導くのですが，まずは連続する 2 つの自然数は互いに素であることを示す必要があります．

解 連続する 2 つの自然数 n，$n+1$ が互いに素であることを示す．n，$n+1$ が共通の素因数 p をもつと仮定し，$n=p\alpha$，$n+1=p\beta$ とおく．このとき，$p(\beta-\alpha)=1$ となるので $p\geqq 2$ より矛盾．よって，連続する 2 つの自然数は互いに素である．

したがって，それらの積 $n(n+1)$ が平方数になるとき，n も $n+1$ 平方数になる．しかし，2 つの自然数の平方の差は $k^2-l^2=(k+l)(k-l)\geqq 2$ なので，平方数が連続する 2 整数になることはない．よって，n と $n+1$ がともに平方数になることはない．

したがって，連続する 2 つの自然数の積は平方数にはならない．

■

参考 なお，連続する 3 つ以上の自然数の積も平方数にはなりませんが，証明はかなり難しいです．また，2012 年の東大理系第 4 問で類題が出題されています．興味のある人はぜひ挑戦してみてください．

6　偶奇性

整数の問題を考えるとき，その数の偶奇性（その数が偶数なのか奇数なのか）があらかじめわかっていると，かなり手間が省けて都合が良いです．いきなり問題を解き始める前に，その数の偶奇性がどうなっているのか，まず考えるクセをつけよう．

偶奇性が判定できるのは，次のように和，差，積の偶奇がわかっている場合がほとんどです．

▷Point◁(整数の偶奇性)

2 つの整数 m，n について次の偶奇性が成り

立つ.

$m+n$が偶数 $\Longleftrightarrow$ m, nの偶奇は一致する
$m-n$が偶数 $\Longleftrightarrow$ m, nの偶奇は一致する
$m+n$が奇数 $\Longleftrightarrow$ m, nの偶奇は一致しない
$m-n$が奇数 $\Longleftrightarrow$ m, nの偶奇は一致しない
mnが奇数 $\Longleftrightarrow$ m, nは共に奇数

例題　a, bを整数とし，2次方程式$x^2+ax+b=0$を考える．この方程式の判別式Dが平方数であるならば，解は全て整数であることを示せ.

考え方　$D=a^2-4b=m^2$とおけば，解は$x=\dfrac{-a\pm\sqrt{D}}{2}=\dfrac{-a\pm m}{2}$．これが整数になるには，$-a\pm m$が偶数になればよいことがわかります．このとき，$a$, mの偶奇性はどうなればよいのでしょうか.

解　$D=a^2-4b=m^2$とおけば，解は

$$x=\frac{-a\pm\sqrt{D}}{2}=\frac{-a\pm m}{2}$$

となる．$D=a^2-4b=m^2$より，
$(a+m)(a-m)=4b=$偶数 となる．また，$(a+m)+(a-m)=2a=$偶数 ともなるので，
$a+m$と$a-m$は共に偶数である.
したがって，解の分子部分$-a+m$と$-a-m$が偶数だから，解は整数になる.

■

例題　p, qを整数とし，$f(x)=x^2+px+q$とおく．$f(1)$も$f(2)$も2で割り切れないとき，方程式$f(x)=0$は整数の解をもたないことを示せ.

考え方　$f(1)$も$f(2)$も2で割り切れないことから，pとqの偶奇性が決まります.

解　$f(1)=1+p+q$が2で割り切れないことから，$p+q$は偶数．$f(2)=4+2p+q$が2で割り切れないことから，qは奇数．したがって，pもqも奇数となる.

方程式$f(x)=0$が整数の解$x=m$をもつと仮定すると，$f(m)=0$より，

$$m^2+pm+q=0$$
$$m(m+p)+q=0$$

$(m+p)-m=p$(奇数)だから，$m+p$とmの偶奇性は一致しないので，積$m(m+p)$は偶数である.
したがって，$m(m+p)+q=$(偶数)+(奇数)が0になることはない
つまり，方程式$f(x)=0$は整数の解をもたない.

■

7　周期性

ある状態が繰り返しおこっているとき「周期性をもつ」といいます．整数問題に限らず，数学においては周期性を考えることは重要です．周期性を見つける方法はただ一つ，**ひたすら実験すること**です.
次の問題でも，まずは，3^1, 3^2, 3^3, 3^4, 3^5, …の1の位を順に調べて，規則性を予測するしかありません.

例題　3^{1000}の一の位の数字を求めよ.

解　3^1, 3^2, 3^3, 3^4, 3^5, …の一の位を順に調べると，3, 9, 7, 1, 3, 9, 7, 1, …と周期4で繰り返す．1000は4で割り切れるから，3^{1000}の一の位の数字は1である.

■

注　おそらく上の解答で問題ないと思いますが，「上の解答は単なる予想に過ぎず，厳密性に欠ける」と思う人は．周期が4であることを証明してください．証明方法は，3^1, 3^2, 3^3, 3^4の一の位の数字が異なることを確認した上で，3^{n+4}と3^nの1の位の数字が等しいこと，つまり，$3^{n+4}-3^n$が10の倍数であることを示せばよいでしょう.

例題　2000^nを7で割った余りをa_nとし，$S_n=a_1+a_2+\cdots+a_n$とおく．このとき，S_n

が 7 で割り切れる最小の n を求めよ.

考え方　まずは実験して a_n を予測しますが，実際に，2000^1，2000^2，2000^3，2000^4，2000^5，… を計算してから 7 で割るでしょうか．こんなときこそ合同式です.

解　$2000 \equiv 5 \pmod 7$ であるので,

$2000^2 \equiv 5^2 \equiv 4 \pmod 7$

$2000^3 \equiv 5^3 \equiv 5 \cdot 5^2 \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod 7$

$2000^4 \equiv 5^4 \equiv (5^2)^2 \equiv 4^2 \equiv 2 \pmod 7$

$2000^5 \equiv 5^5 \equiv 5^2 \cdot 5^3 \equiv 4 \cdot 6 \equiv 24 \equiv 3 \pmod 7$

$2000^6 \equiv 5^6 \equiv (5^3)^2 \equiv 6^2 \equiv 36 \equiv 1 \pmod 7$

$2000^7 \equiv 5^7 \equiv 5^1 \cdot 5^6 \equiv 5^1 \equiv 5 \pmod 7$

以後，5, 4, 6, 2, 3, 1 を繰り返していく．したがって,

$$5 + 4 + 6 + 2 + 3 + 1 = 21$$

ではじめて 7 で割り切れるから, 最小の n は $n = 6$.

■