互いに素(Part.2)

ちょっとムズイけど がんばろう

オー

大学入試においては，互いに素であることを証明する問題よりも，互いに素であることを利用する問題が多く見受けられます．少し難しいですが，いくつか紹介しよう．

まずは記念すべき新課程入試1年目に出題された問題から．整数問題の基本的な考え方の多くを含んでいる良問だと思います．

> **例題 3.**
> (1) n が正の偶数のとき，2^n-1 は3の倍数であることを示せ．
> (2) n を自然数とする．2^n+1 と 2^n-1 は互いに素であることを示せ．
> (3) p，q を異なる素数とするとき，
> $$2^{p-1}-1=pq^2$$
> を満たす p，q の組をすべて求めよ．
> ［九州大学 2015 年前期理系］

こんな問題が出たんか

フ〜ン

考え方 (1)(2) は基本問題．これまでにも何度も紹介しました．(3) は当然 (1)(2) の結果を使いますが，特に (2) の結果をどのように使うのかがポイントでしょう．

解 (1) $n=2m$ (m は正の整数) とおけて，

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

よって，2^n-1 は3の倍数である．

重要な因数分解です

(2) 2^n+1 と 2^n-1 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，

$$2^n+1=p\alpha \quad 2^n-1=p\beta$$

となる．2^n+1 と 2^n-1 は共に奇数なので，p も奇数である．

基本的な証明スタイル

このとき，$p(\beta-\alpha)=2$．p は奇素数なので $p\geqq 3$ より矛盾．よって，2^n+1 と 2^n-1 は互いに素である．

(1)(2)は大丈夫

(3) $2^{p-1}-1=pq^2$ … ①

$p-1\geqq 1$ なので ① の左辺は奇数．よって p，q はともに奇数になる．

まずこれがポイント

このとき $p-1$ は偶数なので (1) より，① の左辺 $2^{p-1}-1$ は3の倍数になるので，$p=3$ または $q=3$ である．

(i) $p=3$ のとき

① より，$2^2-1=3p^2$ となるが，この式を満たす素数 p は存在しない．

(ii) $q=3$ のとき

① より，$2^{p-1}-1=9p$．$p-1$ は偶数なので，

pは奇数だからね

$$(2^{\frac{p-1}{2}}+1)(2^{\frac{p-1}{2}}-1)=3^2p$$

この因数分解ポイントやね

(2) より，$2^{\frac{p-1}{2}}+1$ と $2^{\frac{p-1}{2}}-1$ は互いに素で，p は3でない素数だから，

(ア) $2^{\frac{p-1}{2}}+1=3^2$，$2^{\frac{p-1}{2}}-1=p$ のとき．
このとき，$p=7$ である．

(イ) $2^{\frac{p-1}{2}}+1=p$，$2^{\frac{p-1}{2}}-1=3^2$ のとき．
このとき，この式をみたす素数 p は存在しない．

したがって (i)(ii) より，求める p，q の組は，$(p,\ q)=(7,\ 3)$．

なかなかの良問ネ

■

注 (1) は合同式を用いるともっとスッキリ示せます．

別解 $2^n\equiv 4^m\equiv 1^m\equiv 1 \pmod 3$

よって，2^n-1 は3の倍数である．

■

> **例題 4.** 3以上 9999 以下の奇数 a で，a^2-a が 10000 で割り切れるものをすべて求めよ．
> ［東京大学 2005 年前期理系］

考え方 $a^2-a=a(a-1)$ と因数分解すれば，連続する2整数の積になります．「連続する2整数は互いに素」を思い出そう．

これは憶えておこう

解 $a^2-a=a(a-1)$ が $10000=2^4\cdot 5^4$ で割り切れるとき，a と $a-1$ は互いに素であるから，

a と $a-1$ の一方のみが素因数2をもち，

a と $a-1$ の一方のみが素因数5をもつ．

まず，a は奇数なので $a-1$ は偶数．よって $a-1$ が 2^4 の倍数である．

$a-1$ が 5^4 の倍数だとすると，$a-1$ は 2^4 かつ 5^4 の倍数つまり 10000 の倍数になるので，$a-1 \geqq 10000$ で，$3 \leqq a \leqq 9999$ に反する．

つまり，a が $5^4=625$ の倍数である．

$a=625n$ とおくことができる．$3 \leqq a \leqq 9999$ より，$3 \leqq 625n \leqq 9999$．よって，$0<n<16$

この中で $a-1$ が 2^4 の倍数になるような奇数 n を求めればよい．

$a-1=625n-1=16\cdot 39n+n-1$

であるから，$n-1$ が 16 の倍数にならねばならない．つまり $n=1$ に限られる．

このとき a は $a=625$．

■

注　まず，連続する 2 整数が互いに素であることを知っていないとどうしようもありません．これは必ず覚えておこう．試験では時間と解答スペースに余裕があれば証明もしておこう．

例題 5.　a，b，p，q はすべて自然数で，$\dfrac{p^2+q^2}{a}=\dfrac{pq}{b}$ を満たしている．a と b の最大公約数が 1 のとき以下の問に答えよ．

(1) pq は b で割り切れることを示せ．

(2) $\sqrt{a+2b}$ は自然数であることを示せ．

［京都大学 1998 年後期文系］

これはムズイ

文系の出題だなんて…

ひ〜

考え方　(1) は問題ないと思いますが，(2) がとても難しい．こんなときは具体例で考えます．

例えば，$p=6$, $q=8$ としてみよう．このとき，$p^2+q^2=100$，$pq=48$ なので，$\dfrac{100}{a}=\dfrac{48}{b}$ をみたす，互いに素な a と b を求めればよく，少し計算すれば，$a=25$，$b=12$ と見つかります．確かに，$\sqrt{a+2b}=\sqrt{25+24}=\sqrt{49}=7$ となります．

次に，$p=5$，$q=8$ としてみよう．このとき，$p^2+q^2=89$，$pq=40$ なので，$\dfrac{89}{a}=\dfrac{40}{b}$ をみたす，互いに素な a と b を求めればよく，少し計算すれば，$a=89$，$b=40$ と見つかります．確かに，$\sqrt{a+2b}=\sqrt{89+80}=\sqrt{169}=13$ となります．

さて，a や b はどういう数なのでしょうか．p と q が互いに素な場合は $b=pq$ らしいですが，p と q が互いに素でない場合は・・・・ここがポイントです．

解　(1)　$\dfrac{p^2+q^2}{a}=\dfrac{pq}{b}$　… ①

① より，$apq=b(p^2+q^2)$．

よって，a，b が互いに素だから，pq が b で割り切れる．

(2) (1) より，$\dfrac{p^2+q^2}{a}=\dfrac{pq}{b}=m$　… ②

とおける (m は自然数)．p と q の最大公約数を g とおくと，

$$p=gp',\quad q=gq'\ (p' \text{と} q' \text{は互いに素})$$

となり，これを ② に代入して，

$$\frac{n^2(p'^2+q'^2)}{a}=\frac{n^2p'q'}{b}=m$$

$$\frac{p'^2+q'^2}{a}=\frac{p'q'}{b}=\frac{m}{n^2}\ \cdots③$$

① と同じ形になるので，(1) より，

$p'q'$ は b で割り切れる．… ④

③ より，

$$b\frac{q'^2}{p'}=aq'-bp'\quad b\frac{p'^2}{q'}=ap'-bq'$$

であり，p' と q' が互いに素なので，b は p' でも q' でも割り切れる．つまり，

b は $p'q'$ で割り切れる．… ⑤

したがって，④，⑤ より，$b=p'q'$．

結局，コレ!! これがポイント

なかなか気付かんよ

よって，③ より $\dfrac{m}{n^2}=1$ になるので，

$a=p'^2+q'^2$

したがって，

$$\sqrt{a+2b}=\sqrt{p'^2+q'^2+2p'q'}=\sqrt{(p'+q')^2}=p'+q'$$

となり，$\sqrt{a+2b}$ は自然数である．

■

「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．

当たり前…かな？

証明