21 （'15 九州大） **【難易度】** … 標準

以下の問いに答えよ．

（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．$2^{p-1}-1=pq^2$ を満たす p, q の組をすべて求めよ．

【テーマ】：整数問題

方針

(1) は，二項定理や合同式を用いて証明をします．(2) は，最大公約数を g として式を作ります．(3) は，(1) から p, q は奇数の素数であることがわかるので，これを利用して p, q の値を求めます．

♣ ♠

解答

（1） **【証明】**

n は偶数なので，$n=2k$（k は自然数）とおける．よって，二項定理を用いると，

$$\begin{aligned}2^n-1&=2^{2k}-1\\&=4^k-1\\&=(3+1)^k-1\\&={}_kC_0\cdot3^k+{}_kC_1\cdot3^{k-1}+\cdots\cdots+{}_kC_{k-1}\cdot3+{}_kC_k-1\\&=3\left({}_kC_0\cdot3^{k-1}+{}_kC_1\cdot3^{k-2}+\cdots\cdots+{}_kC_{k-1}\right)\end{aligned}$$

${}_kC_0\cdot3^{k-1}+{}_kC_1\cdot3^{k-2}+\cdots\cdots+{}_kC_{k-1}$ は自然数であるから，2^n-1 は 3 の倍数である．

ゆえに，示された． **（証明終）**

（2） **【証明】**

2^n+1, 2^n-1 の最大公約数を g とすると，

$$\begin{cases}2^n+1=ga' & \cdots\cdots\ ①\\ 2^n-1=gb' & \cdots\cdots\ ②\end{cases}\quad（a', b' \text{ は互いに素}）$$

とおくことができる．① − ② より，

$$2=g(a'-b')$$

となる．このとき，$(g, a'-b')=(1, 2), (2, 1)$ であるが，2^n+1, 2^n-1 はともに奇数であるから，$g=2$ は不適．したがって，$g=1$, $a'-b'=2$ である．よって，2^n+1, 2^n-1 は互いに素であることが示された．

（証明終）

（3） $2^{p-1}-1=pq^2$ …… ①

$p-1\geqq1$ であるから，$2^{p-1}-1$ は奇数であるから，p, q は 3 以上の素数である．よって，$p-1$ は正の偶数となるので，(1) の結果から，$2^{p-1}-1$ は 3 の倍数である．ゆえに，pq^2 が 3 の倍数となるので，p または q のいずれかが 3 である．

(i) $p=3$ のとき，① は $2^2-1=3q^2$ となるので，$q^2=1$ となるので不適．

(ii) $q=3$ のとき，$p=2m+1$（m は自然数）とすると，① は，

$$2^{2m}-1=9(2m+1) \iff (2^m+1)(2^m-1)=9(2m+1)$$

である．(2) より，2^m+1，2^m-1 は互いに素であるから，

$$(2^m+1,\ 2^m-1)=(9,\ 2m+1),\ (2m+1,\ 9)$$

を得る．ここで，$2^m-1=9$ となる自然数 m は存在しない．一方，$2^m+1=9$ のとき，$m=3$ である．このとき，$p=2\cdot3+1=7$ であり，題意を満たす．

ゆえに，求める p, q の組は，

$$\boldsymbol{(p,\ q)=(7,\ 3)}\cdots\cdots(\textbf{答})$$

♢ ♡

解説

(1) は，合同式を用いて示すこともできます．

別解

(1) **【証明】**

n は偶数なので，$n=2k$（k は自然数）とおける．よって，

$$\begin{aligned}2^n-1&=2^{2k}-1\\&=4^k-1\\&=(3+1)^k-1\\&\equiv 1^k-1 \pmod 3\\&=0\end{aligned}$$

である．ゆえに，2^n-1 は 3 の倍数であることが示された． **（証明終）**

(2) は，互いに素であることを示すため，最大公約数を設定して，それが 1 であることを示します．

(3) は，(1), (2) の結果を利用します．まずは，p, q が 3 以上の素数であることを示します．$2^{p-1}-1=pq^2$ は，$2^{p-1}-1$ を素因数分解すると pq^2 となることを述べています．つまり，$2^{p-1}-1$ が 3 の倍数であることを述べれば，p, q のいずれかが 3 であることがわかります．あとは，$p-1$ が偶数であることから，(2) の結果を用いて p, q の値を求めます．