(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。

＜ '15 九州大 ＞

【戦略 1】

(1) **$2^{2k}-1$，すなわち 4^k-1 が 3 の倍数であることを示すわけですが $(3+1)^k-1$ と見て，二項展開をかますのが常套手段の一つです。**

$$\begin{aligned}&(3^k+{}_kC_1\,3^{k-1}+{}_kC_2\,3^{k-2}+\cdots+{}_kC_{k-1}\,3^1+1)-1\\&=3^k+{}_kC_1\,3^{k-1}+{}_kC_2\,3^{k-2}+\cdots+{}_kC_{k-1}\,3^1\\&=(3\text{ の倍数})\end{aligned}$$

ですが，解答では 3 で括れる部分は無視して余りだけを見る記号である合同式を用いて記述することにします。

(2) **2^n+1，2^n-1 の最大公約数が 1 であることを示せばよいわけですが，そうなると最大公約数に迫る手立てとしてユークリッドの互除法をインスピレーションするのが自然でしょうか。**

$2^n+1=(2^n-1)\cdot1+2$ **より**

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

ということが分かり，ほとんどオシマイです。

(3) **前までの設問を活かそうと思うと，p の偶奇が気になります。**

素数の偶奇については，2 か奇素数かで場合分けするのが普通です。

$p=2$ のときはさっさと片づけてしまい，$p\geqq3$ のときに集中します。

このとき，$2^{p-1}-1$ は $2^{\text{偶数}}-1$ という形であり，(1) から 3 の倍数ということになります。

したがって，pq^2 も 3 の倍数ということになり，

$$p=3 \text{ または } q=3$$

のいずれかが成立します。

$p=3$ のときは個別検証でオシマイです。

$q=3$ のときは，$2^{p-1}-1=9p$ という形を得ます。

ここから複数方針が考えられますが，(2) を活かす方針で言えば

偶数である $p-1$ を $p-1=2m$ とおくと，$2^{2m}-1=9p$

すなわち $(2^m+1)(2^m-1)=9p$ となります。

(2) より，2^m+1，2^m-1 は互いに素であるため，このあとの

約数の拾い上げが簡単になります。

【解 1】

(1) 条件より $n=2k$ $(k=1,\ 2,\ \cdots)$ とおける。

このとき，$\begin{aligned}2^n-1&=2^{2k}-1\\&=4^k-1\\&=(3+1)^k-1\\&\equiv1^k-1\pmod3\\&=0\end{aligned}$

ゆえに，2^n-1 は 3 の倍数である。

(2) 2 つの整数 M，N の最大公約数を $G(M,\ N)$ と表す。

$2^n+1=(2^n-1)\cdot1+2$ より，ユークリッドの互除法から

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

n は自然数なので，2^n-1 は奇数となり，2^n-1，2 は互いに素。

ゆえに，$G(2^n-1,\ 2)=1$ となり，$G(2^n+1,\ 2^n-1)=1$ が成り立つ。

以上から，2^n+1，2^n-1 は互いに素である。

(3) $p=2$ のとき，$2^1-1=2q^2$ より，$q^2=\dfrac{1}{2}$ となり，これを満たす素数 q は存在しない。

$p\geqq3$ のとき p は奇素数。

よって，$2^{p-1}-1$ は $2^{\text{偶数}}-1$ という形となり，(1) より 3 の倍数

したがって，pq^2 も 3 の倍数となる。

p，q は素数なので，$p=3$ または $q=3$

(i) $p=3$ のとき

$2^2-1=3q^2$ で，$q^2=1$ を得るが，これを満たす素数 q は存在しない。

(ii) $q=3$ のとき $2^{p-1}-1=9p$

p は奇素数ゆえ，$p-1$ は偶数となり，$p-1=2m$ とおける。

このとき，$2^{2m}-1=9p$ すなわち

$$(2^m+1)(2^m-1)=9p$$

$p=3$ は不適であったので，$p\geqq5$ であり，$m\geqq2$

$0<2^m-1<2^m+1$，及び (2) より 2^m-1，2^m+1 が互いに素であることに注意すると

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

$\begin{cases} 2^m+1=9 \\ 2^m-1=p \end{cases}$ のとき $\begin{cases} 2^{\frac{p-1}{2}}+1=9 \cdots ① \\ 2^{\frac{p-1}{2}}-1=p \cdots ② \end{cases}$

① を満たすのは $\dfrac{p-1}{2}=3$，すなわち $p=7$ のとき
このとき ② も満たす。

$\begin{cases} 2^m+1=p \\ 2^m-1=9 \end{cases}$ のとき $\begin{cases} 2^{\frac{p-1}{2}}+1=p \cdots ③ \\ 2^{\frac{p-1}{2}}-1=9 \cdots ④ \end{cases}$

④ について $2^{\frac{p-1}{2}}=10$ であり，これを満たす素数 (整数) p が存在しないため，不合理。

以上から，求める p，q の値の組は $(p, q)=(7, 3)$ …㊀

【戦略 2】(1) について

$n=2k$ として，4^k-1 を考える際

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

と因数分解も常套手段の一つです。

【解 2】(1) について

条件より $n=2k$ ($k=1, 2, \cdots$) とおける。

このとき，$2^n-1=2^{2k}-1$
$=4^k-1$
$=(4-1)(4^{k-1}+4^{k-2}+\cdots\cdots+4+1)$
$=3\cdot$(整数)

ゆえに，2^n-1 は 3 の倍数である。

【戦略 3】(2) について

「互いに素」というのは「1 以外の公約数をもたない」という否定的な概念なので 背理法という方針も有力です。

【解 3】(2) について

2^n+1，2^n-1 の最大公約数を G として，$G \geqq 2$ と仮定する。

このとき

$\begin{cases} 2^n+1=G\alpha \cdots ① \\ 2^n-1=G\beta \cdots ② \end{cases}$ ($G \geqq 2$ α，β は $\alpha>\beta$ である正の整数)

①−② より，$G(\alpha-\beta)=2$

$G>2$ のとき　$\alpha-\beta$ は正の整数なので，(左辺)>(右辺) となり不合理。

$G=2$ のとき　$\alpha-\beta=1$ …③

①+② より $2\cdot 2^n=2(\alpha+\beta)$ であり，$\alpha+\beta=2^n$ …④

③，④ より，$\alpha=\dfrac{2^n+1}{2}$，$\beta=\dfrac{2^n-1}{2}$

n が自然数であるとき，α，β はともに $\dfrac{\text{奇数}}{2}$ という形となり，整数とならず不合理。

したがって，$G=1$ であるため，2^n+1，2^n-1 は互いに素である。

【戦略 4】(3) について

$p=3$ **または** $q=3$ **を得る部分までは同じです。**

$q=3$ **のときに現れる** $2^{p-1}-1=9p$ **という形ですが**

左辺は指数関数的に増加し，右辺は 1 次

ですから， p **が大きくなると** (左辺)＞(右辺) **であることが考えられます。**

とりあえず， $2^{p-1}=9p+1$ **という形に直して実験してみると**

$$\begin{aligned} p&=3 \quad \cdots\ 2^2<9\cdot3+1\\ p&=5 \quad \cdots\ 2^4<9\cdot5+1\\ p&=7 \quad \cdots\ 2^6=9\cdot7+1\\ p&=11 \quad \cdots\ 2^{10}>9\cdot11+1 \end{aligned}$$

とここから先は左辺の方が爆発的に大きくなりそうです。

あとはこれを帰納法で裏付けます。

この帰納法は素数というよりも 8 以上の自然数 N **に対して** $2^{N-1}>9N+1$ **が成立することを示すようなニュアンスです。**

【解 4】(3) $p=3$ **または** $q=3$ **を得る部分までは【解 1】と同じ**

(i) $p=3$ のとき

$2^2-1=3q^2$ で，$q^2=1$ を得るが，これを満たす素数 q は存在しない。

(ii) $q=3$ のとき

$2^{p-1}-1=9p$，すなわち $2^{p-1}=9p+1$

p が素数であることは一旦おいておき，$p\geqq8$ で

$$2^{p-1}>9p+1 \quad \cdots(*)$$

であることを数学的帰納法で示す。

(ii−1) $p=8$ のとき $2^{8-1}>9\cdot8+1$（$128>73$）で (*) は成立

(ii−2) $p=k$ ($k=8$，9，…) のとき $2^{k-1}>9k+1$ と仮定する。

$$\begin{aligned} 2^k-9(k+1)-1&=2\cdot2^{k-1}-9k-10\\ &>2(9k+1)-9k-10\\ &=9k-8\\ &>0 \quad (\because\ k\geqq8) \end{aligned}$$

よって，$p=k+1$ のときも (*) は成立する。

ゆえに，11 以上の素数 p に対して $2^{p-1}=9p+1$ が成立することはない。

$p=3$ のとき，$2^{3-1}<9\cdot3+1$

$p=5$ のとき，$2^{5-1}<9\cdot5+1$

$p=7$ のとき，$2^{7-1}=9\cdot7+1$

以上から，$(p,\ q)=(7,\ 3)$ … 答

【総括】

a^n-1 というタイプの整数問題は色々なものの見方が出来る反面，迷いが生じる部分もあります。

整数問題の３大手法として

① 積の形から約数を拾う
② 余りで分類する
③ 範囲を絞る (評価する)

というのがあります。

これは常に意識しておくことが大切です。

(2) を活かす方針【解 1】は ① を，指数関数と 1 次式が等しいということはある程度小さな p であるということを睨んだ【解 4】は ③ を意識しています。