次の問いに答えよ。

(1) 5以上の素数は，ある自然数 n を用いて $6n+1$ または $6n-1$ の形で表されることを示せ。

(2) N を自然数とする。$6N-1$ は，$6n-1$（n は自然数）の形で表される素数を約数にもつことを示せ。

(3) $6n-1$（n は自然数）の形で表される素数は無限に多く存在することを示せ。

＜ '09 千葉大 ＞

【戦略】

(1) **この世の整数を 6 で割った余りで分類すれば**

$$\begin{cases} 6n & (=2\cdot 3\cdot n) \\ 6n+1 & \\ 6n+2 & (=2(3n+1)) \\ 6n+3 & (=3(2n+1)) \\ 6n+4 & (=2(3n+2)) \\ 6n+5 & \end{cases}$$

という 6 タイプありますが，余り 0，2，3，4 は合成数確定です。

したがって，5 以上の奇素数ということになると，

$6n+1$ **型か** $6n-1$ **型**

しかあり得ないことになります。

※ 6 で割った余りが 5 の数たちは

6 の倍数から見て 1 足りない連中

という捉え方ができ， $6n-1$ **型となります。**

(2) $\begin{cases} 6N-1 \text{ 自体が 5 以上の数である} \\ 6N-1 \text{ は素因数 2，3 をもたない} \end{cases}$ **ということを考えると**

$6N-1$ **を素因数分解したときの各素因数は 5 以上となります。**

この各素因数は (1) から $\begin{cases} 6n+1 \text{ 型} \\ 6n-1 \text{ 型} \end{cases}$ **のいずれかです。**

$6n-1$ **型の素因数を少なくとも 1 つことを示せばよいため，**

$$6N-1=(6n_1+1)(6n_2+1)\cdots(6n_k+1)$$

と，全ての素因数が $6n+1$ **型であると仮定し，背理法で仕留めます。**

(3) **引き続き，** $6n-1$ **型の素数が有限個しかないと仮定するという背理法です。**

$6n-1$ **型の素数が** k **個しかないと仮定し，** p_1，p_2，……，p_k **とおきます。**

このとき，例題の経験が活きてきますが，

$$P=6p_1p_2\cdots p_k-1$$

（P を $6n-1$ 型で設定したいのです。）

というユークリッド先輩のアイデアを活かします。

【解答】

(1) 5 以上の素数は 2 でも 3 でも割り切れず，

6 で割った余りは 1 または 5

である。

これより，5 以上の素数は

$6n+1$，または $6n-1$（n は自然数）

といういずれかの形で表される。

(2) $N=1$，2，… に対して，$6N-1$ は 5 以上であり，2 でも 3 でも割り切れない。

したがって，$6N-1$ を素因数分解したときに現れる素因数はすべて 5 以上の素因数である。

今，$6N-1=p_1p_2\cdots p_k$ と素因数分解できるとする。

p_i（$i=1$，2，…，k）は全て 5 以上なので，(1) から

$p_i=6n_i+1$ または $6n_i-1$

のいずれかの形で表される。

もし，$i=1$，2，…，k の全ての i で，$p_i=6n_i+1$ の形であったと仮定すると

$$6N-1=(6n_1+1)(6n_2+1)\cdots(6n_k+1)$$

であり，このとき

$$(\text{左辺}) \equiv -1 \equiv 5 \pmod 6$$

$$(\text{右辺}) \equiv 1\cdot 1\cdot\cdots\cdot 1 \ (=1) \pmod 6$$

となり，左辺と右辺を 6 で割った余りが異なり矛盾する。

ゆえに，$p_1 \sim p_k$ の中に，$6n_i-1$ という形で表されるものが少なくとも 1 つ存在し，$6N-1$ が $6n-1$ という形の素因数をもつということが示された。

(3) $6n-1$ という形の素数（以下 $6n-1$ 型素数と呼ぶ）が k 個しかないと仮定する。

このとき，その k 個の $6n-1$ 型素数を

p_1，p_2，……，p_k

とおく。

$P=6p_1p_2\cdots p_k-1$ という数 P を考える。

P が素数とすると，P は $6n-1$ 型素数で，
$p_1 \sim p_n$ のどれよりも大きく，これらと相異なる $6n-1$ 型素数であり，k 個しかないことに反する。

したがって，P は合成数ということになる。

P は $6n-1$ 型なので，(2) から $6n-1$ 型素数の素因数をもつ。

今，$6n-1$ 型素数は $p_1 \sim p_k$ しかないと仮定しているため
P は $p_1 \sim p_k$ という $6n-1$ 型素数のどれかで割り切れる。

しかし，P の形から $p_1 \sim p_k$ のどれでも割り切れず，矛盾する。

以上から，$6n-1$ という形の素数は無限に多く存在する。

【総括】

例題の内容をそのまんま運用するというわけではなく，少し一手間を加えて運用します。

このぐらい適度な誘導があった方が入試問題としては適切でしょう。

この誘導も絶妙な難易度で，整数問題としてキッチリと差が付く適度な良問です。

加えて歴史の一端に触れる話題的な面白さもあるでしょう。