数チャレ 第217回(2019年2月)

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。

出典：2009年 千葉大学 医学部

解答

(1) 6で割った余りが $0,\ 2,\ 4$ である整数は2で割り切れ，余りが $0,\ 3$ である整数は3で割り切れる。よって，5以上の素数は6と互いに素であるから，余りは1または5であり，ある自然数 n を用いて $6n+1$ または $6n-1$ の形で表される。

(証明おわり)

(2) $6N-1$ は奇数であるから，素因数はすべて奇数である。

$$3\times 3=9\equiv 3 \pmod 6,\quad 1\times 1\equiv 1 \pmod 6,\quad 1\times 3\equiv 3 \pmod 6$$

より，3および $6n+1$ (n は自然数)の形で表される素数の積は6で割ると1または3余るものに限られる。(1)より，3以外の奇素数は $6n\pm 1$ の形に表されるものしかないから，$6N-1$ の素因数の中に $6n-1$ の形のものがある。　(証明おわり)

(3) $6n-1$ (n は自然数)の形で表される素数が有限個の

$$6n_1-1,\ 6n_2-1,\ \cdots,\ 6n_N-1$$

に限られるとするとき，

$$P=(6n_1-1)(6n_2-1)\cdots(6n_N-1)$$

とおくと，

$$P\equiv 1 \pmod 6 \text{ または } P\equiv -1 \pmod 6$$

(i) $P\equiv 1 \pmod 6$ のとき

$$P+4\equiv -1 \pmod 6$$

であるから，(2)より $P+4$ の素因数の中に $6n-1$ の形の素数 q があるが，

$$gcd(P+4,\ 6n_k-1)=gcd(4,\ 6n_k-1)=1 \quad (k=1,\ 2,\ \cdots,\ N)$$

より，この素数 q は $6n_1-1,\ 6n_2-1,\ \cdots,\ 6n_N-1$ のいずれも一致しないから矛盾する。

(ii) $P \equiv -1 \pmod 6$ のとき

$$P + 6 \equiv -1 \pmod 6$$

であるから，(2) より $P + 6$ の素因数の中に $6n - 1$ の形の素数 q があるが，

$$gcd(P + 6,\ 6n_k - 1) = gcd(6,\ 6n_k - 1) = 1 \quad (k = 1,\ 2,\ \cdots,\ N)$$

より，この素数 q は $6n_1 - 1,\ 6n_2 - 1,\ \cdots,\ 6n_N - 1$ のいずれも一致しないから矛盾する。

以上により，$6n - 1$ (n は自然数) の形で表される素数は無限に多く存在する。

(証明おわり)

(注) 現在の我々から見ると典型的な問題に映るかもしれないが，2009 年の時点では，合同剰余類もユークリッドの互除法も高校の学習範囲外だったので，当時の受験生にとっては，それほど易しくはなかったであろう。