数チャレ 第226回(2019年11月)

自然数 $m,\ n$ は $m<n$ であり，p は $2^{2^m}+1$ の素因数，q は $2^{2^n}+1$ の素因数であるとする。

(1) $2^{2^n}-1$ は $2^{2^{m+1}}-1$ で割り切れることを示せ。

(2) p と q は異なる素数であることを示せ。

解答

(1) $2^n=2^{m+1}\cdot 2^{n-m-1}$，$n-m-1\geqq 0$ であるから，$N=2^{n-m-1}$ と置いて考えることにより

$$\begin{aligned}2^{2^n}-1&=\left(2^{2^{m+1}}\right)^N-1\\&=\left(2^{2^{m+1}}-1\right)\left(2^{2^{m+1}(N-1)}+2^{2^{m+1}(N-2)}+\cdots+2^{2^{m+1}}+1\right)\end{aligned}$$

は $2^{2^{m+1}}-1$ で割り切れる。 (証明おわり)

(2) $$\left(2^{2^m}+1\right)\left(2^{2^m}-1\right)=2^{2^{m+1}}-1$$

であるから

$$p\,\Big|\,2^{2^m}+1\,\Big|\,2^{2^{m+1}}-1$$

(1)より

p は $2^{2^n}-1$ の素因数

である。pが

$$2^{2^n}+1=\left(2^{2^n}-1\right)+2$$

の素因数でもあるとすれば，pは2の約数ということになるから，$p=2$となって，pが奇素数であることに反する。よって，

p は $2^{2^n}+1$ の素因数ではない。

qは $2^{2^n}+1$ の素因数であるから

$$p\neq q$$

である。 (証明おわり)

(注) $\left\{2^{2^n}+1\right\}$は増加列であるから，本問は「素数が無限個存在する」ことを事実上示したことになる。歴史的には，Fermatが $2^{2^n}+1$はすべて素数であると予想したが，Eulerが $2^{2^5}+1$は素因数541をもつ合成数であること(反例)を示した。