桑野耕一様

熊野さんから先週，お年玉講座資料最終節にあった誤りを指摘されました．より詳しく言いますと「$5^m+3=2^n$ が成立するような正の整数 $m,\ n$ は $(m,n)=(3,7)$ に限る」とあるが，「$5^m+3=2^n$ が成立するような正の整数 $m,\ n$ は $(m,n)=(1,3),(3,7)$ に限る」を Kneser が示していたことが飯高茂「数学の研究をはじめよう I」に書いてあるとの教示をいただきました．確かにその通りで，$m=1,2$ の場合を点検しなかったのは迂闊でした．講座資料では説明が足りませんでしたので，以下を熊野さんに送り，検討をお願いしたところ，論証には納得していただけました．ご参考までに桑野さんにもお送りします．

観察 1．$5^m+3=2^n$ が成立するような正の整数 $m,\ n$ は $(m,n)=(1,3),(3,7)$ に限る．

証明．m,n を $2^n=5^m+3$ が成立するような正の整数とし，$m>3$ と仮定する．このとき，$2^n>5^3+3=2^7$ なので，$n>7$．このとき，$2^n=5^m+3,\ 2^7=5^3+3$ の辺々を差し引いて

$$2^7(2^{n-7}-1)=5^3(5^{m-3}-1)$$

を得る．ここで，$(2^7,2^{n-7}-1)=1,\ (5^3,5^{m-3}-1)=1$ なので，

$$\mathrm{ord}_5(2^{n-7}-1)=3,\ \mathrm{ord}_2(5^{m-3}-1)=7,\ \mathrm{ord}_p(2^{n-7}-1)=\mathrm{ord}_p(5^{m-3}-1)\ (p\text{ は素数}\neq 2,5)$$

さらに，乗法群 $(\mathbb{Z}/5^3\mathbb{Z})^\times$ における 2 の位数が $4\cdot 5^2$，乗法群 $(\mathbb{Z}/5^4\mathbb{Z})^\times$ における 2 の位数が $4\cdot 5^3$ なので，

$$4\cdot 5^2|(n-7),\ 4\cdot 5^3\nmid(n-7)$$

一方，乗法群 $(\mathbb{Z}/2^7\mathbb{Z})^\times$ における 5 の位数が 32 なので，$32|(m-3)$．したがって，

$$(5^{32}-1)|(5^{m-3}-1)$$

ここで，

$$(5^2+1)|(5^{32}-1),\ 5^2+1=2\cdot 13$$

なので，

$$13|(5^{m-3}-1)\ \Rightarrow\ 13|(2^{n-7}-1)$$

さらに，乗法群 $(\mathbb{Z}/13\mathbb{Z})^\times$ における 2 の位数が 12 なので，$12|(n-7)$．したがって，

$$(2^{12}-1)|(2^{n-7}-1)$$

ここで，

$$(2^3-1)|(2^{12}-1),\ 2^3-1=7$$

なので，

$$7|(2^{n-7}-1)\ \Rightarrow\ 7|(5^{m-3}-1)$$

さらに，乗法群 $(\mathbb{Z}/7\mathbb{Z})^\times$ における 5 の位数が 6 なので，$6|(m-3)$．ここで，$32|(m-3)$ なので，$96|(m-3)$．したがって，

$$(5^{96}-1)|(5^{m-3}-1)$$

ここで，

$$(5^8-5^4+1)|(5^{96}-1),\ 5^8-5^4+1=390001$$

なので，

$$390001|(5^{m-3}-1)\ \Rightarrow\ 390001|(2^{n-7}-1)$$

さらに，乗法群 $(\mathbb{Z}/390001\mathbb{Z})^\times$ における 2 の位数が $2\cdot 5^4\cdot 13$ なので，$5^4|(n-7)$．これは，$4\cdot 5^2|(n-7)$, $4\cdot 5^3\nmid(n-7)$ に反する．

以上のことから結論を得る．

追記２．議論を「$2^n=5^m+3$, $2^3=5^1+3$ の辺々を差し引いて」と始めますと，

$$2^3(2^{n-3}-1)=5(5^{m-1}-1)$$

を得る．ここで，$(2^3,2^{n-3}-1)=1$, $(5,5^{m-1}-1)=1$ なので，

$$\mathrm{ord}_5(2^{n-3}-1)=1,\ \mathrm{ord}_2(5^{m-1}-1)=3,\ \mathrm{ord}_p(2^{n-3}-1)=\mathrm{ord}_p(5^{m-1}-1)\ (p\text{ は素数}\neq 2,5)$$

さらに，乗法群 $(\mathbb{Z}/5\mathbb{Z})^\times$ における 2 の位数が 4，乗法群 $(\mathbb{Z}/5^2\mathbb{Z})^\times$ における 2 の位数が 20 なので，

$$4|(n-3),\ 20\nmid(n-3)$$

一方，乗法群 $(\mathbb{Z}/2^3\mathbb{Z})^\times$ における 5 の位数が 2 なので，

$$2|(m-1)$$

したがって，

$$(5^2-1)|(5^{m-1}-1)$$

と $(m,n)=(3,7)$ が規制をかいくぐって現れます．油断も隙もありません．

訂正３．資料 p27 補足 2 の最後の節で

ここで，$(5^4-5^2+1)|(5^{24}-1)$, $5^4-5^2+1=601$ なので，$601|(2^{n-1}-1)$．さらに，乗法群 $(\mathbb{Z}/601\mathbb{Z})^\times$ における 2 の位数が 25 なので，$25|(n-1)$．これは，$20|(n-1)$, $100\nmid(n-1)$ に反する．

とあるのは

ここで，$(5^4-5^2+1)|(5^{24}-1)$, $5^4-5^2+1=601$ なので，$601|(2^{n-5}-1)$．さらに，乗法群 $(\mathbb{Z}/601\mathbb{Z})^\times$ における 2 の位数が 25 なので，$25|(n-5)$．これは，$20|(n-5)$, $100\nmid(n-5)$ に反する．

とすべきでした．また，補足 5 に続く節の中で

「乗法群 $(\mathbb{Z}/390001\mathbb{Z})^\times$ における 5 の位数が $16250=2\cdot 5^4\cdot 13$ である」ことを利用して，

とあるのは

「乗法群 $(\mathbb{Z}/390001\mathbb{Z})^\times$ における 2 の位数が $16250=2\cdot 5^4\cdot 13$ である」ことを利用して，

とすべきでした．なかなか訂正が収束しません．訂正した資料を改めて添付します．なお，熊野さんにご指摘いただいた点については，誤記ではなくて読み抜けでしたので，敢えてそのままにしてあります．

補足４．「乗法群 $(\mathbb{Z}/390001\mathbb{Z})^\times$ における 2 の位数が $16250=2\cdot 5^4\cdot 13$ である」ことは

$$\begin{aligned}2^{16250}&\equiv 1 \mod 390001,\\ 2^{16250/2}&\equiv 390000 \mod 390001,\\ 2^{16250/5}&\equiv 281908 \mod 390001,\\ 2^{16250/13}&\equiv 9811 \mod 390001\end{aligned}$$

から従います．また，観察 1 での議論で

$$\Phi_{16}(5)=5^8+1,\ \Phi_{32}(5)=5^{16}+1,\ \Phi_{48}(5)=5^{16}-5^8+1,\ \Phi_{96}(5)=5^{32}-5^{16}+1$$

の素因数分解は必要ではありませんでしたので，ほったらかしにしていますが，円分多項式に整数を代入して得られる整数の素因数分解について研究している一群の人たちがいます．

１９年２月１５日　諏訪紀幸