2014 年東大理 5

(1)

a_n を p で割った商を c_n とし、$a_n = pc_n + b_n$ と表すと

$$a_{n+2} = a_{n+1}(a_n + 1) = (pc_{n+1} + b_{n+1})(pc_n + b_n + 1) = p\{pc_{n+1}c_n + c_{n+1}(b_n + 1) + c_n b_{n+1}\} + b_{n+1}(b_n + 1)$$

したがって、a_{n+2} を p で割った余りは $b_{n+1}(b_n + 1)$ を p で割った余りに一致する。

すなわち、b_{n+2} は $b_{n+1}(b_n + 1)$ を p で割った余りに一致する。(証明終)

(2)

$a_1 = 2,\ a_2 = 3$ より　$\therefore b_1 = 2,\ b_2 = 3$　$b_2(b_1 + 1) = 9$ より　$\therefore b_3 = 9$

$b_3(b_2 + 1) = 36 = 17 \times 2 + 2$ より　$\therefore b_4 = 2$　$b_4(b_3 + 1) = 20 = 17 + 3$ より　$\therefore b_5 = 3$

以下繰り返しであり、

$$\therefore b_1 = 2,\ b_2 = 3,\ b_3 = 9,\ b_4 = 2,\ b_5 = 3,\ b_6 = 9,\ b_7 = 2,\ b_8 = 3,\ b_9 = 9,\ b_{10} = 2$$ ……(答)

(3)

$b_{n+2} = b_{m+2}$ より、$b_{n+1}(b_n + 1)$ を p で割った余りと $b_{m+1}(b_m + 1)$ を p で割った余りは一致する。

すなわち、$b_{n+2} - b_{m+2} = b_{n+1}(b_n + 1) - b_{m+1}(b_m + 1)$ は p で割り切れる。

$b_{n+1} = b_{m+1} > 0$ より、$b_{n+2} - b_{m+2} = b_{n+1}(b_n - b_m)$ は p で割り切れる。

$1 \leqq b_{n+1} \leqq p - 1$ より、b_{n+1} は p で割り切れず、$b_n - b_m$ が p で割り切れる必要がある。

$0 \leqq b_n \leqq p - 1,\ 0 \leqq b_m \leqq p - 1$ より、$-(p-1) \leqq b_n - b_m \leqq p - 1$ であるから、$b_n - b_m = 0$ しかあり得ない。

したがって、$b_n = b_m$ が示された。(証明終)

(4)

$a_2, a_3, a_4, \cdots$ に p で割り切れる数が現れないとき、$b_2, b_3, b_4, \cdots$ に 0 が現れない。

$b_2, b_3, b_4, \cdots$ に現れる数は、$1, 2, \cdots, p-1$ の $p-1$ 個の数のいずれかである。

数列 $b_2, b_3, b_4, \cdots$ を無限に並べると、隣接する 2 数の並び方は $(p-1)^2$ 通りしかなく、隣接する 2 数の並びが一致する箇所が必ず存在する。

今、$1 \leqq m < n$ であり、$b_{n+1} = b_{m+1} > 0$、$b_{n+2} = b_{m+2}$ とする。このとき、(3)および $b_2, b_3, b_4, \cdots$ に 0 が現れないことから、$b_n = b_m > 0$ が成り立つ。

以下、順次 $b_{n-1} = b_{m-1} > 0,\ b_{n-2} = b_{m-2} > 0, \cdots, b_{n-m+1} = b_1 > 0$ がわかる。

したがって、$b_1 \neq 0$ であるから、a_1 は p で割り切れない。(証明終)

(注)

$b_n = p - 1$ とすると、$b_{n+1}(b_n + 1) = pb_{n+1}$ となり、$b_{n+2} = 0$ となる。以下、$b_{n+3} = 0,\ b_{n+4} = 0, \cdots$ となる。

$b_2, b_3, b_4, \cdots$ に 0 が現れないとき、$b_2, b_3, b_4, \cdots$ に現れる数は、正確には $1, 2, \cdots, p-2$ のいずれかである。