2014年 東大数学 文系第4問 理系第5問

(1) a_nをPで割った商を g_n とすると

$$\begin{cases} a_n = pg_n + b_n \\ a_{n+1} = pg_{n+1} + b_{n+1} \\ a_{n+2} = pg_{n+2} + b_{n+2} \end{cases}$$

$a_{n+2} = a_{n+1}(a_n+1)$ より

$$pg_{n+2} + b_{n+2} = (pg_{n+1} + b_{n+1})(pg_n + b_n + 1)$$

$$\Leftrightarrow\ b_{n+2} = p\underbrace{\{g_{n+1}(pg_n + b_n + 1) + g_n b_{n+1}\}}_{何らかの整数} + b_{n+1}(b_n+1)$$

$b_{n+1}(b_n+1)$ は Pより大きい可能性がある。

$b_{n+2} = p(整数) + b_{n+1}(b_n+1)$ なので、
b_{n+2}をPで割った余りは $b_{n+1}(b_n+1)$ をPで割った余りと一致する。
定義より、b_{n+2} をPで割った余りは b_{n+2} そのものである。
よって、b_{n+2} と $b_{n+1}(b_n+1)$ をPで割った余りは等しい。

別解 合同式を使う

$a_{n+2} \equiv b_{n+2} \pmod P$
$a_{n+1} \equiv b_{n+1} \pmod P$
$a_n \equiv b_n \pmod P$ である。

$a_{n+2} = a_{n+1}(a_n+1)$ より、
$a_{n+2} \equiv a_{n+1}(a_n+1) \pmod P$ なので、

$b_{n+2} \equiv b_{n+1}(b_n+1) \pmod P$

この式は、b_{n+2} と $b_{n+1}(b_n+1)$ において、Pで割った余りが等しいことを主張するが、

b_{n+2}をPで割った余りは b_{n+2} であるので、題意は示された。

(2) $a_1 = 2$
$a_2 = 3$ より

同じ余りが出現したので周期性を疑い始める。

$a_3 = 3 \times (2+1) = 9$
$a_4 = 9 \times (3+1) = 36 \equiv 2 \pmod{17}$
$a_5 \equiv 2 \times (9+1) = 20 \equiv 3 \pmod{17}$
$a_6 \equiv 3 \times (2+1) = 9 \pmod{17}$
$a_7 \equiv 9 \times (3+1) = 36 \equiv 2 \pmod{17}$
$a_8 \equiv 2 \times (9+1) = 20 \equiv 3 \pmod{17}$
$a_9 \equiv 3 \times (2+1) = 9 \pmod{17}$
$a_{10} \equiv 9 \times (3+1) = 36 \equiv 2 \pmod{17}$

よって、$b_1 = b_4 = b_7 = b_{10} = 2$
$b_2 = b_5 = b_8 = 3$
$b_3 = b_6 = b_9 = 9$ //

(3)

$\boxed{\begin{array}{l}\text{AとBをPで割った余りが等しい}\\ \text{ことを示すには・・・}\\ A \equiv B \pmod P \text{ でも}\\ A - B \equiv 0 \pmod P \text{ でもOK}\end{array}}$

(1)より $b_{n+2} \equiv b_{n+1}(b_n+1) \pmod P$
$b_{m+2} \equiv b_{m+1}(b_m+1) \pmod P$ である。

ここで $b_{n+2} = b_{m+2}$ なので、
$b_{n+1}(b_n+1) \equiv b_{m+1}(b_m+1) \pmod P$
$b_{n+1} = b_{m+1}$ なので、
$b_{n+1}(b_n+1) \equiv b_{n+1}(b_m+1) \pmod P$
である。

よって
$b_{n+1}(b_n+1) - b_{n+1}(b_m+1) \equiv 0 \pmod P$
$b_{n+1}(b_n - b_m) \equiv 0 \pmod P$

Pは素数なので、$b_{n+1} \equiv 0$ または $b_n - b_m \equiv 0$ であるが、定義から b_{n+1} は $0 < b_{n+1} \leqq p-1$ を満たす整数なので、$b_{n+1} \equiv 0$ は解なし。

よって $b_n - b_m \equiv 0 \Leftrightarrow b_n \equiv b_m$
余りは一致するので、$b_n = b_m$ //