[東京大学 2014 年前期 理科 5]

r を 0 以上の整数とし，数列$\{a_n\}$を次のように定める。

$$a_1 = r,\ a_2 = r+1,\ a_{n+2} = a_{n+1}(a_n+1) \quad (n = 1, 2, 3, \cdots)$$

また，素数 p を 1 つとり，a_n を p で割った余りをb_n とする。

ただし，0 を p で割った余りは 0 とする。

(1) 自然数nに対し，b_{n+2}は $b_{n+1}(b_n+1)$ を p で割った余りと一致することを示せ。

(2) $r = 2,\ p = 17$ の場合に，10以下のすべての自然数nに対して，b_n を求めよ。

(3) ある 2 つの相異なる自然数n, mに対して，

$$b_{n+1} = b_{m+1} > 0,\ b_{n+2} = b_{m+2}$$

が成り立ったとする。このとき，$b_n = b_m$ が成り立つことを示せ。

(4) $a_2, a_3, a_4, \cdots$に p で割り切れる数が現れないとする。このとき，a_1 も p で割り切れないことを示せ。

(1) a_n を p で割ったときの商をc_n とおくと

$$\begin{cases} a_{n+2} = pc_{n+2} + b_{n+2} \\ a_{n+1} = pc_{n+1} + b_{n+1} \\ a_n = pc_n + b_n \end{cases}$$ となる。

したがって $a_{n+2} = a_{n+1}(a_n+1)$

$$= \left(pc_{n+1} + b_{n+1}\right)\left(pc_n + b_n + 1\right)$$

$$= p^2 c_{n+1}c_n + pb_n c_{n+1} + pb_{n+1}c_n + b_{n+1}(b_n+1)$$

$$= p\left(pc_{n+1}c_n + b_n c_{n+1} + b_{n+1}c_n\right) + b_{n+1}(b_n+1) \quad \cdots①$$

a_{n+2} を p で割った余りがb_{n+2} であり，

①よりそれは$b_{n+1}(b_n+1)$ を p で割った余りと一致する。

よって題意は示された。

(2) $r=2$ より $a_1=2$, $a_2=3$ である。

$p=17$ であるから $b_1=2, b_2=3$ であり,

$b_2\left(b_1+1\right)=3(2+1)=9$ より $b_3=9$

$b_3\left(b_2+1\right)=9(3+1)=36$ より $b_4=2$

$b_4\left(b_5+1\right)=2(9+1)=20$ より $b_5=3$

以下同様であり, $b_n=\begin{cases}2 & (n=1,\,4,\,7,\,10)\\ 3 & (n=2,\,5,\,8)\\ 9 & (n=3,\,6,\,9)\end{cases}$

(3)(1)より b_{n+2} は $b_{n+1}(b_n+1)$ を p で割った余りと一致するので,

$b_{n+1}(b_n+1)=pd_n+b_{n+2}$ …②, $b_{m+1}(b_m+1)=pd_m+b_{m+2}$ …③ （d_n, d_m は整数）

と表すことができる。

$b_{n+1}=b_{m+1}, b_{n+2}=b_{m+2}$ であるから, ②−③より $b_{n+1}(b_n-b_m)=p(d_n-d_m)$

ここで, 右辺は素数 p の倍数であり, $0<b_{n+1}<p$, $-p<b_n-b_m<p$ であるから

$b_n-b_m=0$ でなければならない。

したがって $b_n=b_m$ が成り立つ。

(4) $b_1\neq 0$ であることを示せばよい。

$a_2, a_3, a_4, \cdots$ に p で割り切れる数が現れないことから $n\geqq 2$ に対し, $0<b_n<p$ である。

(b_{n+1}, b_{n+2}) の組を考えると, 組の総数は $(p-1)^2$ 以下である。

したがって, $2\leqq k<\ell$ かつ $(b_{k+1}, b_{k+2})=(b_{\ell+1}, b_{\ell+2})$ を満たす自然数 k, ℓ が存在する。

このとき, (3)より $b_k=b_\ell$ が成立する。

したがって, 帰納的に $b_1=b_{\ell-k+1}$ となるが,

$\ell-k>0$ より $\ell-k+1\geqq 2$ なので, $b_{\ell-k+1}>0$ すなわち $b_{\ell-k+1}\neq 0$

よって, $b_1>0$ すなわち $b_1\neq 0$ となるから, a_1 は p で割り切れない。