数列 $\{a_n\}$ を次のように定める。

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

(1) 正の整数 n が 3 の倍数のとき，a_n は 5 の倍数であることを示せ。

(2) k，n を正の整数とする。a_n が a_k の倍数となるための必要十分条件を k，n を用いて表せ。

(3) a_{2022} と $(a_{8091})^2$ の最大公約数を求めよ。

＜ '22 東京大 ＞

【戦略】

(1) **実験をしてみると，**

$a_1=1$　　$a_2=1^2+1=2$　　$a_3=2^2+1=5$

$a_4=5^2+1=26$　　$a_5=26^2+1=677$

というように，確かに題意は言えそうなのですが，数が大きくなっていくにつれ，合同式で処理したくなります。

$a_1=1$　　$a_2=2$　　$a_3\equiv 0$

$a_4\equiv 0^2+1=1$　　$a_5\equiv 1^2+1=2$　　$a_6\equiv 2^2+1\equiv 0$

と要領もつかめてきますし，ここまでくると帰納的な構造も目に付きます。

したがって，数学的帰納法で示すことにします。

(2) **a_1 の倍数を全て書き出してみると**

$$a_1,\ a_2,\ a_3,\ \cdots\cdots$$

$a_2(=2)$ の倍数を書き出してみると

$$a_2,\ a_4,\ a_6,\ \cdots\cdots$$

$a_3(=5)$ の倍数を書き出してみると (1) より

$$a_3,\ a_6,\ a_9,\ \cdots\cdots$$

このあたりから，a_k の倍数を書き出してみると

$$a_k,\ a_{2k},\ a_{3k},\ \cdots\cdots$$

となるんじゃないかいう予想が立ちます。

つまり，$n=mk$ と表せる，すなわち n が k の倍数であることが求める必要十分条件でないかという予想が立ちます。

(1) で周期 3 をもっていたことなどから $a_{n+k}\equiv a_n\pmod{a_k}$ であることも予想が立ちます。

つまり，これは a_n を a_k で割った余りを考えたければ，添え字からどんどん k を引いていって，添え字を小さくしても構わないということを意味します。

これにより，$n=kq+r$ としたとき，

a_n を a_k で割った余りと，a_r を a_k で割った余りは等しい

ということになります。

(3) $a_{8091}\equiv a_{8091-2022}\equiv a_{8091-2\cdot 2022}\equiv\cdots\cdots\equiv a_3\pmod{a_{2022}}$ **です。**

このことから，$a_{8091}=a_{2022}q+5$ ということが言えるため

$$(a_{8091})^2={a_{2022}}^2q^2+10a_{2022}q+25$$

となるわけですが，ユークリッドの互除法から

$$G((a_{8091})^2,\ a_{2022})=G(a_{2022},\ 25)$$

なので，結局は a_{2022} と 25 の最大公約数が求めるものです。

(1) から a_{2022} が 5 の倍数であることは分かりますから，残る問題はさらにもう一つ素因数 5 をもつかどうかです。

(1) 同様にこの数列を 25 で割った余りの中に 0 が入るかどうかをチェックしてみると

$a_1\equiv 1$　　$a_2\equiv 1^2+1=2$　　$a_3\equiv 2^2+1=5$

$a_4\equiv 5^2+1\equiv 1$　　$a_5\equiv 1^2+1=2$　　$a_6\equiv 2^2+1=5$

と，今度は 25 で割った余りが 1，2，5 という周期性をもちそうです。

あとはこれを (1) と同じ要領で片づければ解決です。

【解答】

(1) $a_1=1$　　$a_2=1^2+1=2$　　$a_3=2^2+1=5$
$a_4=5^2+1=26$　　$a_5=26^2+1=677$

以下，合同式の法を 5 として，全ての正の整数 N に対して

$$\begin{cases} a_{3N-2}\equiv 1 \\ a_{3N-1}\equiv 2 \quad \cdots ① \\ a_{3N}\equiv 0 \end{cases}$$

であることを N についての数学的帰納法で示す。

[1] $N=1$ のとき，上記実験から $\begin{cases} a_1\equiv 1 \\ a_2\equiv 2 \\ a_3\equiv 0 \end{cases}$ であり，① は正しい。

[2] $N=M$ $(M=1,\ 2,\ \cdots)$ のとき

$$\begin{cases} a_{3M-2}\equiv 1 \\ a_{3M-1}\equiv 2 \\ a_{3M}\equiv 0 \end{cases}$$ であると仮定する。

このとき，

$$a_{3M+1}={a_{3M}}^2+1\equiv 0^2+1=1$$
$$a_{3M+2}={a_{3M+1}}^2+1\equiv 1^2+1=2$$
$$a_{3M+3}={a_{3M+2}}^2+1\equiv 2^2+1\equiv 0$$

であり，$n=M+1$ のときも ① は正しい。

以上から，$N=1,\ 2,\ \cdots$ に対して $\begin{cases} a_{3N-2}\equiv 1 \\ a_{3N-1}\equiv 2 \\ a_{3N}\equiv 0 \end{cases}$

が成立するため，$\begin{cases} a_1\equiv 1 \\ a_2\equiv 2 \\ a_3\equiv 0 \end{cases}$ と併せると，n が 3 の倍数であるとき

a_n は 5 の倍数である。

(2) $a_{n+k}\equiv a_n \pmod{a_k}$ …(☆) であることを n に関する数学的帰納法で示す。

(i) $n=1$ のとき $a_{1+k}-a_1=a_{k+1}-1\equiv 0 \pmod 1$ より
(☆) は成立する。

(ii) $n=m$ $(m=1,\ 2,\ \cdots)$ のとき，$a_{m+k}\equiv a_m \pmod{a_k}$ と仮定する。

$$\begin{aligned} a_{m+1+k}-a_{m+1} &=({a_{m+k}}^2+1)-({a_m}^2+1) \\ &={a_{m+k}}^2-{a_m}^2 \\ &\equiv {a_m}^2-{a_m}^2 \ (\because \text{帰納法の仮定より}) \\ &=0 \end{aligned}$$

となり，$n=m+1$ のときにも (☆) は成立する。

(i)，(ii) より，$n=1,\ 2,\ \cdots$ に対して，

$$a_{n+k}\equiv a_n \pmod{a_k} \cdots (☆)$$

これより，数列 $\{a_n\}$ を a_k で割った余りは周期 k である。

n を k で割った商を q，余りを r とすれば

$$a_n\equiv a_r \pmod{a_k} \cdots (*)$$

であるため，

a_n が a_k で割り切れる $(a_n\equiv 0 \pmod{a_k})$
$\Leftrightarrow$
a_r が a_k で割り切れる $(a_r\equiv 0 \pmod{a_k})$
$\Leftrightarrow$
$\dfrac{a_r}{a_k}$ が整数となる。…(★)

ここで，$a_0=0$ と定めても，本問の構造に影響はない。

今，この数列 $\{a_n\}$ は単調増加数列であるから

$$a_0<a_1<a_2<a_3<\cdots\cdots<a_{k-1}<a_k$$

$r=0,\ 1,\ 2,\ \cdots,\ k-1$ であることも加味すると

$$(★) \Leftrightarrow a_r=0 \Leftrightarrow r=0$$

以上から，

a_n が a_k で割り切れる $\Leftrightarrow$ n が k で割り切れる

ということが言え，これが求める必要十分条件

(3) $8091=2022\cdot 4+3$ であり，(*) より

$$a_{8091}\equiv a_3 \pmod{a_{2022}}$$

$a_3=5$ なので，$a_{8091}\equiv 5 \pmod{a_{2022}}$

つまり a_{8091} を a_{2022} で割った余りが 5 である。

一般に 2 つの正の整数 α，β $(\alpha>\beta)$ の最大公約数を $G(\alpha,\ \beta)$ と表すと，ユークリッドの互除法から

$$\begin{aligned} G((a_{8091})^2,\ a_{2022}) &= G((a_{2022}q+5)^2,\ a_{2022}) \\ &= G(a_{2022},\ 25) \ (\because \text{ユークリッドの互除法}) \end{aligned}$$

したがって，求める最大公約数は a_{2022} と 25 の最大公約数に等しい。

(1) より，a_{2022} は 5 の倍数である。

また，数列 $\{a_n\}$ を 25 で割った余りについては

1，2，5 を繰り返す

ある整数 K について $\begin{cases} a_{3K-2}\equiv 1 \pmod{25} \\ a_{3K-1}\equiv 2 \pmod{25} \\ a_{3K}\equiv 5 \pmod{25} \end{cases}$ と仮定すると

$$a_{3K+1}={a_{3K}}^2+1\equiv 5^2+1\equiv 1 \pmod{25}$$
$$a_{3K+2}={a_{3K+1}}^2+1\equiv 1^2+1=2 \pmod{25}$$
$$a_{3K+3}={a_{3K+2}}^2+1\equiv 2^2+1=5 \pmod{25}$$

これより，a_{2022} は 25 では割り切れない。

つまり，a_{2022} は 25 で割り切れない 5 の倍数ということになり

a_{2022} と 25 の最大公約数は 5

以上から，a_{2022} と $(a_{8091})^2$ の最大公約数は 5 … 答

【総括】

随所随所で

問題文で問われていること以上のことを示す

という作業が出てきます。

例えば (1) では

a_3，a_6，a_9，… が 5 で割り切れる

ということよりももっと強い主張

a_1，a_2，a_3，a_4，a_5，a_6，…… を 5 で割った余りは周期 3 である

ということを証明しました。

また，(2) は結果の予想をたてるのも中々スムーズにはいかないと思います。