p を素数とし，m を p で割りきれない正の整数とする。

このとき，m，$2m$，$3m$，…，$(p-1)m$ を p で割った余りをそれぞれ r_1，r_2，…，r_{p-1} とする。次の問いに答えよ。

(1) r_1，r_2，…，r_{p-1} は全て異なることを証明せよ。

(2) r_1，r_2，…，r_{p-1} には，

1，2，…，$p-1$ が全て現れる

ことを証明せよ。

(3) n を正の整数とし，公差 d の等差数列 $\{a_n\}$ を考える。

$d=4$ のとき，a_n，a_{n+1}，a_{n+2}，a_{n+3} の全てが素数となる n は存在しないことを証明せよ。

(4) 公差 d の等差数列 $\{a_n\}$ について，d が $0<d<2023$ を満たす整数であるとき，a_n，a_{n+1}，…，a_{n+11} の全てが素数となる正の整数 n は存在しないことを証明せよ。

＜ 自作 ＞

【戦略】

(1) **$r_i=r_j$ となる i，j $(1\leqq i<j\leqq p-1)$ が存在すると仮定し，矛盾を導く背理法で仕留めます。**

(2) **(1) より集合 $\{r_1, r_2, \cdots, r_{p-1}\}$ の要素の中に重複がないため，要素の個数は $p-1$ 個です。**

集合 $\{1, 2, \cdots, p-1\}$ の要素の個数も $p-1$ 個であるため，これらの集合の要素同士が 1 対 1 対応することを言えばよく，集合としてこれら 2 つの集合が等しいことを目指せばよいことになります。

(3) **結局は q，$q+4$，$q+8$，$q+12$ が全て素数となることはないということを示すわけで，q，$q+4$，$q+8$，$q+12$ が全て素数と仮定して矛盾を導く背理法で仕留めることを目論みます。**

法を 3 とすると，$q+4\equiv q+1$，$q+8\equiv q+2$ ですから，どれかに 3 の倍数が紛れ込むことになり，矛盾することが見込めます。

(4) **(3) と違い d が具体的に決まっていませんが，やはり**

$$q,\ q+d,\ q+2d,\ \cdots,\ q+11d$$

が全て素数になることはないことを示すため，これらが全て素数であると仮定して矛盾を導きたいと思います。

(1)，(2) から言えていることは，

d が素数 p で割り切れないとき

d，$2d$，…，$(p-1)d$ という $p-1$ 個の数を p で割った余りは

1，2，…，$p-1$ に 1 対 1 対応する

ということです。

例えば，d が 3 の倍数でないと仮定すると，法を 3 として $d\equiv 1$，2 ということになりますが，

$$d\equiv 1 \Longrightarrow 2d\equiv 2\ ,\ \ d\equiv 2 \Longrightarrow 2d\equiv 1$$

というように，d，$2d$ を 3 で割った余りは 1，2 と 1 対 1 対応します。

$q\equiv 1$，2 でもあるため，$q+d$，$q+2d$ のどちらかは $\equiv 0$ となるため仮定に矛盾し，d は 3 の倍数ということが言えるわけです。

同様にして，d は 2 の倍数，5 の倍数，7 の倍数，11 の倍数ということが言えるため，d は $2\cdot 3\cdot 5\cdot 7\cdot 11\ (=2310)$ の倍数ということになり $0<d<2023$ といういうことに矛盾します。

【解答】

(1) im，jm を p で割った余りが等しい，すなわち

$im\equiv jm\pmod p$ なる自然数 i，j $(1\leqq i<j\leqq p-1)$ が存在すると仮定する。

このとき，$(j-i)m\equiv 0\pmod p$ であり，m は p で割り切れないため，

$$j-i\equiv 0\pmod p$$

ゆえに，$i\equiv j\pmod p$ であり，$1\leqq i<j\leqq p-1$ であることを考えると，$i=j$ となり，$i<j$ であることに矛盾する。

以上から，m，$2m$，$3m$，…，$(p-1)m$ を p で割った余りは全て異なることが示された。

(2) $$A=\{r_1, r_2, \cdots, r_{p-1}\},\ B=\{1, 2, \cdots, p-1\}$$

と定めたとき，任意の $r_k\in A$ に対して，km は p で割り切れないため，$r_k\neq 0$ であり，$r_k\in B$ であるから

$$A\subset B\ \cdots①$$

一方，$b\in B$ であるが，$b\notin A$ となる b が存在すると仮定する。

これは r_1，r_2，…，r_{p-1} のどれにも対応しない $b\in B$ が存在することを意味する。

すると，$p-1$ 個の A の要素が $p-2$ 個以下の B の要素に対応することになる。

鳩の巣原理より，同じ対応先をもつ A の要素 r_i，r_j が存在し，$r_i=r_j$ となるが，(1) の結果に矛盾する。

ゆえに任意の $b\in B$ に対して $b\in A$ であり，$B\subset A\ \cdots②$

①，② より，$A=B$ であり，A の要素と B の要素は 1 対 1 対応するため，題意は示された。

(3) $a_n=q$ として，

$$q,\ q+4,\ q+8,\ q+12$$

が全て素数であると仮定する。

[1] $q=2$，3 のとき

$q=2$ のときは $q+4$，$q+8$，$q+12$ が素数とならず，
$q=3$ のときは $q+12$ が素数とならないため，不合理。

[2] $q>3$ のとき

q は 3 で割り切れないので，q を 3 で割った余りは 1 か 2。

[2−1] q を 3 で割った余りが 1 のとき

$q+8$ が 3 より大きい 3 の倍数となり素数とならず，
仮定に反する。

[2−2] q を 3 で割った余りが 2 のとき

$q+4$ が 3 より大きい 3 の倍数となり素数とならず，
仮定に反する。

[1]，[2] いずれにせよ仮定に反し，背理法から題意は示された。

(4) $a_n = q$ として，

$$q,\ q+d,\ q+2d,\ \cdots,\ q+11d$$

が全て素数であると仮定する。

[1] q が 2，3，5，7，11 のいずれかのとき

$q+2d$，$q+3d$，$q+5d$，$q+7d$，$q+11d$ のいずれかが素数ではなくなるため，仮定に反する。

[2] q が $q>11$ なる素数であるとき

d が奇数と仮定すると，$q+d$ が 2 より大きな偶数となるため仮定に反するため，d は偶数。

d が 3 の倍数でないと仮定すると (1)，(2) より，d，$2d$ を 3 で割った余りは 1，2 と 1 対 1 対応する。

$q \equiv 1,\ 2 \pmod 3$ であるので，$q+d$，$q+2d$ のいずれかが 3 の倍数となり，仮定に反するため，d は 3 の倍数。

d が 5 の倍数でないと仮定すると (1)，(2) より，d，$2d$，$3d$，$4d$ を 5 で割った余りは 1，2，3，4 と 1 対 1 対応する。

$q \equiv 1,\ 2,\ 3,\ 4 \pmod 5$ であるため，
$q+d$，$q+2d$，$q+3d$，$q+4d$ のいずれかが 5 の倍数となり仮定に反するため，d は 5 の倍数。

d が 7 の倍数でないと仮定すると，(1)，(2) より，
d，$2d$，$\cdots$，$6d$ を 7 で割った余りは 1，2，$\cdots$，6 と 1 対 1 対応する。

$q \equiv 1,\ 2,\ 3,\ 4,\ 5,\ 6 \pmod 7$ であるため，
$q+d$，$q+2d$，$\cdots$，$q+6d$ のいずれかが 7 の倍数となり仮定に反するため，d は 7 の倍数。

d が 11 の倍数でないと仮定すると，(1)，(2) より，
d，$2d$，$\cdots$，$10d$ を 11 で割った余りは 1，2，$\cdots$，10 と 1 対 1 対応する。

$q \equiv 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10 \pmod{11}$ であるため，
$q+d$，$q+2d$，$\cdots$，$q+10d$ のいずれかが 11 の倍数となり仮定に反するため，d は 11 の倍数。

以上から，d は $2\times3\times5\times7\times11$，すなわち 2310 の倍数。

しかし，$0<d<2023$ であるため矛盾する。

以上から背理法により，題意は示された。

【総括】

(1)，(2) が後半の足がかりとなる重要な内容ですが，流れが独特であり，経験がないときちんと記述するのが難しいでしょう。

例えば，d が 5 の倍数でないとき，法を 5 として

$$d \equiv 1 \Longrightarrow \begin{cases} 2d \equiv 2 \\ 3d \equiv 3 \\ 4d \equiv 4 \end{cases}$$

$$d \equiv 2 \Longrightarrow \begin{cases} 2d \equiv 4 \\ 3d \equiv 1 \\ 4d \equiv 3 \end{cases}$$

$$d \equiv 3 \Longrightarrow \begin{cases} 2d \equiv 1 \\ 3d \equiv 4 \\ 4d \equiv 2 \end{cases}$$

$$d \equiv 4 \Longrightarrow \begin{cases} 2d \equiv 3 \\ 3d \equiv 2 \\ 4d \equiv 1 \end{cases}$$

というように，いずれにせよ，d，$2d$，$3d$，$4d$ を 5 で割った余りは 1，2，3，4 と 1 対 1 に対応するということになるわけです。

これを一般的に保証したのが (1)，(2) です。

(3) は公差が 4 の等差数列の中に素数が 4 連続というのはありえないことを示すことになります。
数式的に言うと，q，$q+4$，$q+8$，$q+12$ の全てが素数となることがありえないことを示すわけです。

ただ，$q=2$，3，5，$\cdots$ と逐一全ての素数について調べることは無理がありますから，整数問題の基本的な考え方の 1 つである「余りに注目」という考え方をします。

4，8，12 を 3 で割った余りがそれぞれ 1，2，0 と異なることに注目します。

(4) はより一般論となりますから，(3) の考え方がそのまま使えるわけではありませんが，(3) の面影を感じ取りながら議論を進めていくことになります。

公差 d のまま議論を進めていくわけですが，結局は
$q+d$，$q+2d$，$\cdots$，$q+11d$ の中に合成数が紛れ込むから矛盾するということを睨み続けるという点は (3) と変わりません。

もちろん背理法という大方針はこのレベルの受験生であれば手なりにとれるでしょうから，条件である $0<d<2023$ に反することを目指していくことになると分かれば，d に関する制約条件を考えていくという道にいくことは不自然ではないでしょう。

ただ，それでも (1)，(2) の助けを借りないとツラいものがあると思います。