1. 373 で割った余りが 109 でありかつ 511 で割った余りが 367 である正整数 n であって $n \leq 1000000 = 10^6$ を満たすものを 1 つ挙げよ。

. . . .

373 で割り切れて 511 でも割り切れる数を m とする。

$$m \equiv 0 \mod 373, \quad m \equiv 0 \mod 511 \tag{1}$$

$m = 373 \times 511$ とおく。
ユークリッドの互除法より

$$373 \times 137 + 511 \times (-100) = 1 \tag{2}$$

である。これを移項し次の式が得られる。

$$373 \times 137 = 1 + 511 \times 100 \tag{3}$$

これは 373 で割り切れるが、511 で割ると 1 余る。

$$373 \times 137 \equiv 0 \mod 373, \quad 373 \times 137 \equiv 1 \mod 511 \tag{4}$$

373 で割った余りが 109 である数 n は次のように表される。

$$n = 373k + 109 \ (k \in \mathbb{Z}) \tag{5}$$

これが次を満たすように k の値を求める。

$$n = 373k + 109 \equiv 367 \mod 511 \tag{6}$$

$373 \times 137 \equiv 1 \mod 511$ であるので、

$$(373 \times 137) \times (367 - 109) + 109 \equiv 367 \mod 511 \tag{7}$$

となる。つまり、$k = 137 \times (367 - 109) = 35346$ となる。
式 (5) に k を当てはめて計算すると

$$n = 373 \times 35346 + 109 = 13184167 \tag{8}$$

となるが、$n > 10^6$ であるので $m = 373 \times 511$ を繰り返し引き、この範囲に収まるようにする。

$$n = (373 \times 35346 + 109) - (69m) = 373 \times 87 + 109 = 32560 \tag{9}$$

よって、$n = 32560$ である。

$$32560 = 511 \times 63 + 367 \tag{10}$$

---

2. G を群とする。任意の $x \in G$ に対して、写像 $C(x) : G \to G$ を $y \mapsto xyx^{-1}$ と定義する。

   (a) 任意の $x \in G$ に対して、$C(x)$ は G の自己同型写像であることを示せ。

   ....

   $y, z \in G$ に対して $C(x)(yz) = xyzx^{-1} = xyx^{-1}xzx^{-1} = C(x)(y)C(x)(z)$ であるので $C(x)$ は準同型写像である。
   $\mathrm{Ker}C(x) = \{e\}$ であるので単射である。
   ${}^{\forall}z \in G$ に対して $C(x)(x^{-1}zx) = xx^{-1}zxx^{-1} = z$ であるので全射である。
   よって、$C(x)$ は自己同型写像である。

   (b) 写像 $C : G \to \mathrm{Aut}G$ を $x \mapsto C(x)$ と定義する。このとき、C は準同型写像であることを示せ。

   ....

   $x_1, x_2 \in G$ に対して

   $$C(x_1x_2)(y) = x_1x_2y(x_1x_2)^{-1} = x_1x_2yx_2^{-1}x_1^{-1} = C(x_1)\left(C(x_2)(y)\right) \tag{11}$$

   であるので $C(x_1x_2) = C(x_1) \circ C(x_2)$ となり C は準同型写像である。

   (c) C の核は $\{x \in G \mid {}^{\forall}y \in G,\ xy = yx\}$ であることを示せ。

   ....

   $\mathrm{Aut}G$ の単位元は恒等写像 id_G である。
   $C(x)(y) = xyx^{-1} = y$ であるためには $xy = yx$ であればよい。右から x^{-1} をかけることで $xyx^{-1} = y$ となる。よって、$xy = yx$ を満たせば $C(x) = id_G$ となるので $\mathrm{Ker}C = \{x \in G \mid {}^{\forall}y \in G,\ xy = yx\}$ である。
