D: Identity Function

原案：大槻

問題文：矢藤

解答：澤・矢藤・中須賀

解説：中須賀

問題概要

- 以下の定義で与えられる関数$F_k(a)$が存在する
  - $f(a) = a^N \ mod \ N$
  - $F_1(a) = f(a)$
  - $F_{k+1}(a) = F_k(f(a))$

- 整数Nが与えられるので、1以上N未満の全ての整数aに対して$F_k(a) = a$を満たす最小のkを出力せよ(無ければ-1を出力せよ)
  - 2<=N<=10^9

考察

- まず、$F_k(a) = a^{N^k} mod\ N$である
  - 帰納法で$F_{k+1}(a) = F_k\big(f(a)\big) = (a^N)^{N^k} = a^{N^k \cdot N} = a^{N^{(k+1)}}$より示せる

- Nが1より大きな平方数を約数に持つ場合はkは存在しない
  - $N = m^2 N'$とした時、$m^{N^k} \equiv m(mod\ N)$を満たすことができないため

考察

- $N = p_1 p_2 \cdots p_m (p_i$は素数$)$とすると
  - $a^{N^k} \equiv a (mod\ N)$
  - $\leftrightarrow$ 任意の$i(1 \leq i \leq m), a(1 \leq a < N)$に対して$a^{N^k} \equiv a (mod\ p_i)$
  - $\leftrightarrow$ 任意の$i(1 \leq i \leq m)$に対して$N^k - 1 \equiv 0 (mod\ p_i - 1)$
    (オイラーの定理より)

- よって、$\mathrm{lcm}(p_1 - 1, p_2 - 1, \cdots, p_m - 1) = L$とした時、$N^k - 1$がLで割り切れればよい

解法

- つまり、$N^k \equiv 1 (mod\ L)$を満たす最小のkを求めればよい
  - NとLが互いに素でない場合は、そのようなkは存在しない
  - 互いに素な場合は、kはφ(L)の約数となる（φはオイラー関数）
  - φ(L)の中から$N^k \equiv 1 (mod\ L)$を満たす最小のkが答えとなる

- 計算量は$O(\sqrt{N} + logN)$
  - $O(N)$かかっても書き方によっては間に合いそう

結果

- 正解 / 提出
  - 8 / 66 (12%)
- オンサイトFA
  - sleep 18000 (83:08)