

Alice and Bob are practicing in developing toy cryptographic applications for smartphones. This year they have invented **Calculator** that allows one to perform the following operations modulo 2019:

- to insert at most 4-digit positive integers (digits from 0 to 9);
- to perform addition, subtraction and multiplication of two numbers;
- to store temporary results and read them from the memory.

Suppose that Alice wants to send Bob a ciphertext y (given by a 4-digit integer). She sends y from her smartphone to Bob's Calculator memory. To decrypt y, Bob needs to get the plaintext x (using his Calculator) by the rule $x = f(y) \mod 2019$, where f is a secret polynomial known to Alice and Bob only.

At the most inopportune moment, Bob dropped his smartphone and broke its screen. Now, the button + as well as all digits except 2 are not working.

Help Bob to invent an efficient algorithm how to decrypt any ciphertext y using Calculator in his situation if the current secret polynomial is $f(y) = y^5 + 1909y^3 + 401y$. More precisely, suggest a short list of commands, where each command has one of the following types $(1 \leq j, k < i)$:

$$\begin{array}{lll} S_i = y, & S_i = 2, & S_i = 222, & S_i = S_j - S_k, \\ S_i = 22, & S_i = 2222, & S_i = S_j * S_k. \end{array}$$

The first command has to be $S_1 = y$. In the last command, the resulted plaintext x has to be calculated. We remind that all calculations are modulo 2019. In particular, the integer 2222 becomes 203 immediately after entering. The shorter the list of commands you suggest, the more scores you get for this problem.

Example. The following list of commands calculates $x = y^2 - 4$:

Command	Result
$S_1 = y$	y
$S_2 = S_1 * S_1$	y^2
$S_3 = 2$	2
$S_4 = S_3 * S_3$	4
$S_5 = S_2 - S_4$	$y^2 - 4$

o 🗩 v 🕖 w 1 o



r 1 m d y w C p R b Y i o P a T d O i d d y e o 2019

nsucrypto.nsu.ru Page

e r y

Page 10 from 13

nsucrypto@nsu.ru