

Problem Tutorial: “Fancy Formulas”

Firstly, note that the sum of the numbers stays the same modulo p . If this condition doesn't hold, just output -1 .

Now, let $s = (a + b) \bmod p$. Multiply all numbers a, b, c, d by s^{-1} , and the smallest number of operations clearly won't change. Note that from pair $(a, 1 - a)$ we can go to one of $(2a \bmod p, (1 - 2a) \bmod p)$, and $((2a - 1) \bmod p, 2(1 - a) \bmod p)$. Now, we can reformulate our problem in the following way:

- You are given integer a . In one operation, you can change a to $2a \bmod p$ or $2a - 1 \bmod p$. Find the smallest number of operations needed to make a equal b .

This problem is easier to handle. Note that after the set of reachable numbers after k operations is the set of remainders modulo p of numbers from segment $[2^k a - (2^k - 1), 2^k a]$. For $k \geq 30$, the length of this segment will exceed p , so all remainders will be available. So, we just need to check k one by one, until we find the first one for which the segment $[2^k a - (2^k - 1), 2^k a]$ contains a number which equals to b modulo b . Asymptotics $O(\log p)$ per query.