Problem 1. «A 1024-bit key»

Alice has a 1024-bit key for a symmetric cipher (the key consists of 0s and 1s). Alice is afraid of malefactors, so she changes her key everyday in the following way:

1. Alice chooses a subsequence of key bits such that the first bit and the last bit are equal to 0. She also can choose a subsequence of length 1 that contains only 0.
2. Alice inverts all the bits in this subsequence (0 turns into 1 and vice versa); bits outside of this subsequence remain as they are.

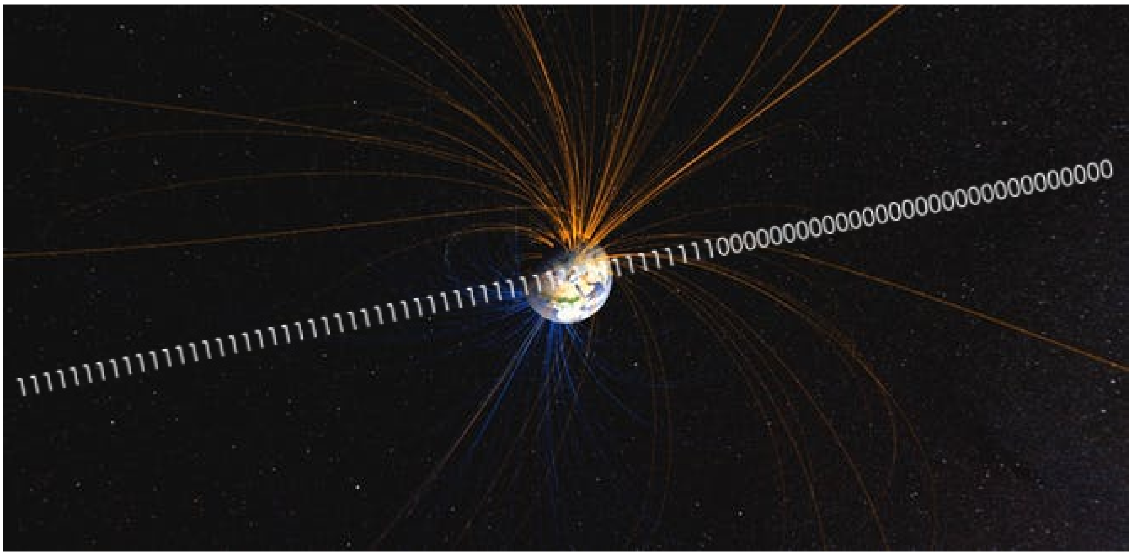
Prove that the process will stop. Find the key that will be obtained by Alice in the end of the process.

Example of an operation. 11001$\underbrace{01101110}$011... turns to 11001$\underbrace{10010001}$011...

Problem 2. «The magnetic storm»

A hardware random number generator is a device that generates random sequences consisting of 0s and 1s. Unfortunately, a disturbance caused by a magnetic storm affected this random number generator. As a result, the device had generated a sequence of 0s of length k (where k is a positive integer), and then started to generate an infinite sequence of 1s.

Prove that at some point the generator will produce a number $1\ldots10\ldots0$ that is divisible by 2019.



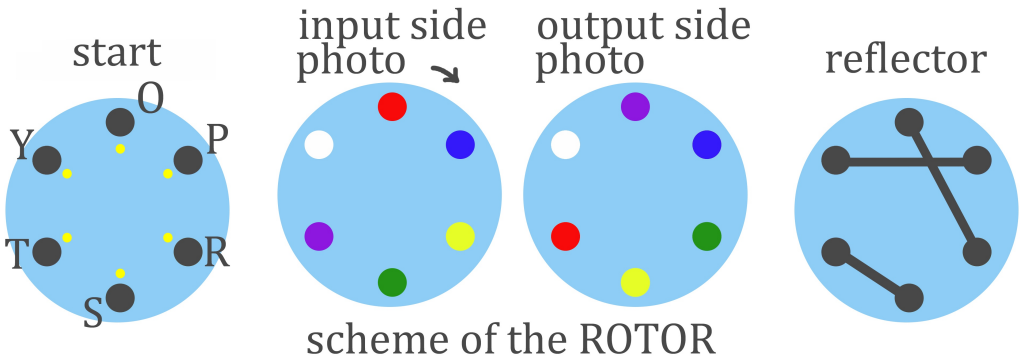
Problem 3. «Autumn leaves»

Read a hidden message!..

Problem 4. «A rotor machine»

In one country rotor machines were very useful for encryption of information.

Eve knows that for some secret communication a simple rotor machine was used. It works with letters `O`, `P`, `R`, `S`, `T`, `Y` only and has an input circle with lamps (start), one rotor and a reflector. See the scheme below.



The input circle and the reflector are fixed in their positions while the rotor can be in one of 6 possible positions. After pressing a button on a keyboard, an electrical signal corresponding to the letter goes through the machine, comes back to the input circle, and the appropriate lamp shows the result of encryption. After each letter is encrypted, the rotor turns right (i. e. clockwise) on 60 degrees. Points of different colors on the rotor sides indicate different noncrossing signal lines within the rotor.

For instance, if the rotor is fixed as shown on the picture above, then if you press the button `O`, it will be encrypted as `T` (the signal enters the rotor via red point, is reflected and then comes back via purple line). If you press `O` again, it will be encrypted as `R`. If you press `T` then, you will get `S` and so on.

Eve intercepted a secret message: `TRRYSSPRYRYROYTOPTOPTSPSPRS`. Help her to decrypt it keeping in mind that Eve does not know the initial position of the rotor.

Problem 5. «Broken Calculator»

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 (that is to get the result as the reminder of division by 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 is equal to the remainder of dividing $f(y) = y^5 + 1909y^3 + 401y$ by 2019.

At the most inopportune moment, Bob dropped his smartphone and broke its screen. Now, the button [+] as well as all digits except [1] and [5] are not working.

Help Bob to invent an efficient algorithm how to decrypt any ciphertext y using `Calculator` in his situation. More precisely, suggest a short list of commands, where each command has one of the following types ($1 \leqslant j, k < i$):

$$S_i = y, \qquad S_i = a, \qquad S_i = S_j - S_k, \qquad S_i = S_j * S_k,$$

where a is an at most 4-digit integer consisting of digits 1 and 5 only; for example, $a = 1$, $a = 15$, $a = 551$, $a = 5115$, etc.

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 2500 becomes 481 and -1000 becomes 1019 immediately after entering or calculations. The shorter the list of commands you suggest, the more scores you get for this problem.

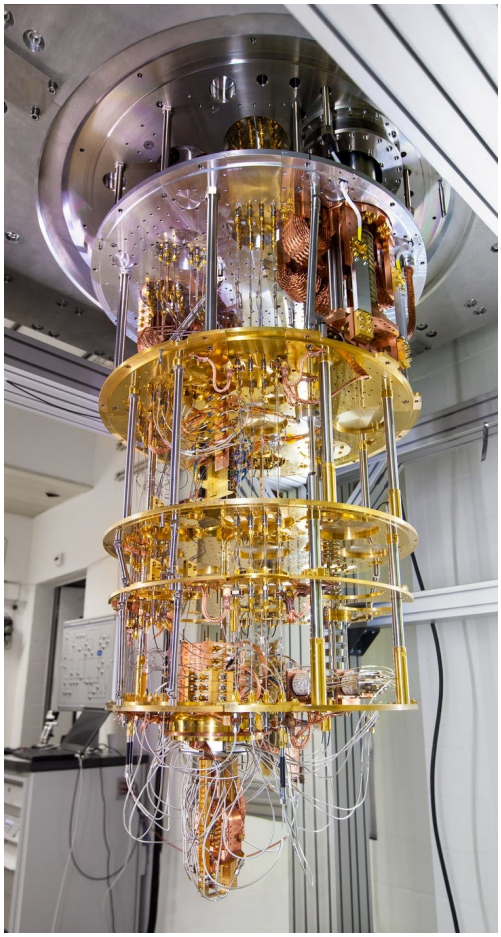
Example. The following list of commands calculates $x = y^2 - 55$:

Command	Result
$S_1 = y$	y
$S_2 = S_1 * S_1$	y^2
$S_3 = 11$	11
$S_4 = 5$	5
$S_5 = S_3 * S_4$	55
$S_6 = S_2 - S_5$	$y^2 - 55$

Problem 6. «A promise»

Young cryptographers, Alice, Bob and Carol, are interested in quantum computings and really want to buy a quantum computer. A millionaire gave them a certain amount of money (say, X_A for Alice, X_B for Bob, and X_C for Carol). He also made them promise that they would not tell anyone, including each other, how much money everyone of them had received.

- Could you help the cryptographers to invent an algorithm how to find out (without breaking the promise) whether the total amount of money they have, $X_A + X_B + X_C$, is enough to buy a quantum computer?
- What weaknesses does your algorithm have (if someone breaks the promise)? Does it always protect the secret of the honest participants from the dishonest ones?



IBM's 50 qubit quantum computing system