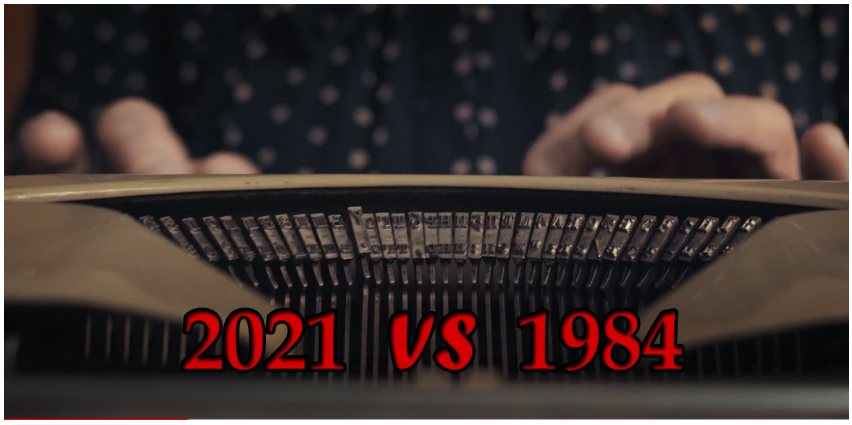
Problem 1. «2020»

A cipher machine WINSTON can transform a binary sequence in the following way. A sequence S is given, a cipher machine can add to S or remove from S any subsequence of the form 11, 101, 1001, $10\ldots01$. Also, it can add to S or remove from S any number of zeros.

When special agent Smith entered the room there were two identical WINSTON machines. He was curious to encrypt number 2020 and he tried to encrypt the number in it's binary form. The first cipher machine returned the binary form of number 1984, the second one returned the binary form of number 2021. Smith understood that one of the machines is broken. How did he know that?



Problem 2. «POLY»

During a job interview, Bob was proposed to think up a small cryptosystem that operates with integers. Bob invented and implemented a complex algorithm POLY that can be represented mathematically as a polynomial. Namely, if x is a plaintext, then ciphertext y is equal to $p(x)$, where p is a polynomial with integer coefficients.

Bob's employer decided to test it. At first, he encrypted the number 20 and obtained the number 7. Secondly, he encrypted the number 15 and obtained the number 5. After that he said to Bob that there was a mistake in the implementation of the algorithm and did not hire him. What was wrong?

Problem 3. «A secret house»

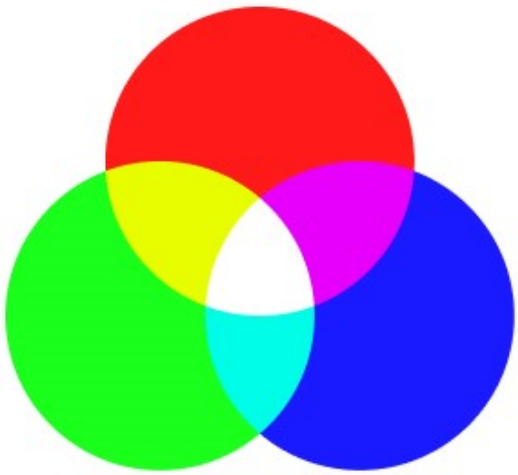
Here you can see a secret house.

Looking on it, could you understand what should be shown inside the frame left blank?

Problem 4. «RGB»

Victor is studying the Moctod search server. Inside its software, he found two integer variables a and b that change their values when special search queries "`RED`", "`GREEN`" and "`BLUE`" are processed. More precisely, the pair (a, b) is changed to $(a+18b, 18a-b)$ when processing the query "`RED`", to $(17a+6b, -6a+17b)$ when processing "`GREEN`", and to $(-10a-15b, 15a-10b)$ when processing "`BLUE`". When any of a or b reaches a multiple of 324, it resets to 0. Whenever $(a, b) = (0, 0)$, the server crashes.

On the server startup, the variables (a, b) are set to $(20, 20)$. Prove that the server will never crash with these initial values, regardless of the search queries processed.



Problem 5. «Miller — Rabin revisited»

Bob decided to improve the famous Miller — Rabin primality test. The odd number n being tested is represented in the form $n-1 = 2^k 3^\ell m$, where m is not divisible by 2 or 3.

The modified primality test is the following:

1. Take a random $a \in \{2, \ldots, n-2\}$.
2. Put $a \leftarrow a^m \bmod n$. If $a = 1$, return "`PROBABLY PRIME`".
3. For $i = 0, 1, \ldots, \ell - 1$ do the following steps:
   (a) $b \leftarrow a^2 \bmod n$;
   (b) if $a + b + 1$ is divisible by n, return "`PROBABLY PRIME`";
   (c) $a \leftarrow ab \bmod n$.
4. For $i = 0, 1, \ldots, k - 1$ repeat:
   (a) if $a + 1$ is divisible by n, return "`PROBABLY PRIME`";
   (b) $a \leftarrow a^2 \bmod n$.
5. Return "`COMPOSITE`".

Prove that the algorithm does not fail, that is, not return "`COMPOSITE`", for a prime n.

Remark. The expression $a \leftarrow a^m \bmod n$ means that a takes a new value that is equal to the remainder of dividing a^m by n.

Problem 6. «Mysterious event»

Mr. Bob is the editor in-chief of a well known magazine. He has many interests and activities in addition to work: meetings with bright people of politics and art, dancing, fishing, and even stenography and linguistics.

Every week, the magazine publishes a hard Sudoku on the last page. Mr. Bob likes this game too! So, it is a pleasure for him to personally analyze all solutions from the readers. He sits down in his office with a cup of coffee and looks through all the PNG-files with photos of solutions.

But suddenly Mr. Bob disappeared. The last solution he could see on his monitor was the following (here is a **link** to it, if you are interested in).

But what happened? Where is Mr. Bob?