Problem 6. «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 $a \in \{2, \dots, n-2\}$.
2. Put $a \leftarrow a^m \bmod n$. If $a = 1$, return "PROBABLY PRIME".
3. For $i = 0, 1, \dots, \ell - 1$ 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 $i = 0, 1, \dots, k-1$ repeat:
   (a) if $a + 1$ is divisible by n, return "PROBABLY PRIME";
   (b) $a \leftarrow a^2 \bmod n$.
5. Return "COMPOSITE".

Q1 Prove that this algorithm does not fail, that is, not return "COMPOSITE", for a prime n.

Q2 Bonus problem (extra scores, a special prize!)

A composite integer n may be classified as "PROBABLY PRIME" by a mistake. It is known that for the usual Miller — Rabin test the error probability is less than $1/4$. Can this estimation be improved when we are switching to the described algorithm?

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.