Problem 4
Integer Factorization

Let M' be the product of "enough small" prime numbers. Then by the hint we know that

$$a^{M'} \equiv 1 \bmod p, \qquad a^{M'} \not\equiv 1 \bmod q,$$

for any a coprime to p and q, since we can write $M' = k_p \cdot (p-1)$ for some k_p, but not $M' = k_q \cdot (q-1)$ for some k_q since $p-1$ is smooth and $q-1$ is not. From this it follows that $p \mid a^{M'} - 1$ and $q \nmid a^{M'} - 1$. We see that $\gcd(a^{M'} - 1, N) = p$, as the only divisors of N are p and q.

Now to calculate the factorization of N, we will calculate for $\gcd(a^{M'!} - 1, N)$ for some random a coprime to N. We take here an $M'!$ to make sure we get all the small primes. We saw before that if M' is big enough, then $\gcd(a^{M'!} - 1, N) = p$.

Note that computing $a^{M!}$ should be avoided since it is a huge number. One should reduce modulo N at every iteration to keep the memory usage low.

Thus we get the following pseudo-code:
N = Console.Read();
$a := 2$;
$M := 1$;
$d := 1$;
While $(d = 1$ or $d = N)$
    $M \cdot = M + 1$;
    $a := a^M \bmod N$;
    $d := \mathrm{GCD}(N, a - 1)$;

output(d);
output(N div d);