Exercise 18.

(a) The Miller-Rabin Primality Test (MRPT) comprises a number of successive squarings. Suppose a 300-digit number $n$ is given. How many squarings are needed in the worst case during a single run of this primality test?

(b) Let $n \in \mathbb{N}$ be odd and composite. Repeat the MRPT with uniformly distributed random numbers $a \in \{2, \ldots, n-1\}$ until the output is "$n$ is composite". Assume that the probability of the test outcome "$n$ is prime" is $\frac{1}{4}$. Compute the probability, that the number of such tests is equal to $M$, $M \in \mathbb{N}$. What is the expected value of the number of tests?

Exercise 19. The Miller-Rabin Primality Test (MPRT) is applied $m$, $m \in \mathbb{N}$, times to check, whether $n$ is prime, where $n$ is chosen according to a uniform distribution on the odd numbers in $\{N, \ldots, 2N\}$, $N \in \mathbb{N}$.

(a) Show that

$$P(\text{"n is composite"} \mid \text{MRPT returns } m \text{ times "n is prime"}) \leq \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2^m+1}}.$$

(b) How many repetitions $m$ of the test are needed to ensure that the above probability stays below $1/1000$ for $N = 2^{512}$?

Hint: Assume $P(\text{"n is prime"}) = 2/\ln(N)$.

Exercise 20. Prove the Chinese Remainder Theorem:

Suppose $m_1, \ldots, m_r$ are pairwise relatively prime, $a_1, \ldots, a_r \in \mathbb{N}$. The system of $r$ congruences

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \ldots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \pmod{M},$$

where $M_i = M/m_i$, $y_i = M_i^{-1} \pmod{m_i}$, $i = 1, \ldots, r$. 