Primality Testing Assignment Solution

Ankan Ghosh (CrS2402)

August 2025

Solution 1

(a) Concept and Intuition

The Miller–Rabin primality test (MR) is a *one-sided Monte Carlo test*:

- If n is prime, the test always accepts.
- If n is composite, it may be falsely accepted as "probably prime."

Each round of the MR test chooses an independent random base a. For any fixed odd composite n, at least $\frac{3}{4}$ of all possible bases (coprime to n) are *witnesses* that expose its compositeness. At most $\frac{1}{4}$ are *strong liars* that incorrectly suggest primality.

Therefore, the probability of error decreases exponentially with the number of rounds k:

$$\Pr[\text{MR outputs "prime" on composite } n] \ \le\ \left(\tfrac{1}{4}\right)^k.$$

Thus, increasing k drastically reduces the risk of error, which is essential in cryptographic applications.

(b) Proof of the Error Bound

Let $n-1 = 2^s d$ with d odd. The MR test accepts n with base a if

$$a^d \equiv 1 \pmod n \quad \text{or} \quad a^{2^r d} \equiv -1 \pmod n \quad \text{for some } 0 \le r < s.$$

Group-theoretic arguments show that for any odd composite n, at most one quarter of the bases a satisfy this condition. Hence

$$\Pr[\text{accept in one round}] \le \tfrac{1}{4}.$$

With k independent random bases,

$$\Pr[\text{all } k \text{ rounds accept}] \le \left(\tfrac{1}{4}\right)^k = 2^{-2k}.$$

(c) Required k for a 512-bit Candidate

We require the error probability to be less than 2^{-80}:

$$\left(\tfrac{1}{4}\right)^k \;\le\; 2^{-80}.$$

Since $(1/4)^k = 2^{-2k}$, this inequality reduces to

$$2k \;\ge\; 80 \quad\Rightarrow\quad k \;\ge\; 40.$$

Hence, for a 512-bit candidate prime, choosing $k = 40$ rounds ensures an error probability below 2^{-80}.

Solution 2

Let us generate two random 256-bit prime numbers, say p and q, and form their product

$$n = p \times q,$$

which is a composite number of approximately 512 bits.

(a) Prime Generation and composite production

Using standard prime generation procedure (Miller–Rabin with $k = 20$ iterations for each candidate), I obtained two primes p and q.

The composite number is then computed as:

$$n = p \cdot q.$$

The generated numbers are provided in the 'miller_rabin_output' txt file. This n is guaranteed to be composite, since it has at least the factors p and q.

(b) Miller–Rabin Trials on n

We now perform several *single-round* Miller–Rabin tests on n with randomly chosen bases $a \in [2, n-2]$.

Each trial outputs either:

- "composite" (correct answer), or
- "probably prime" (a *liar*, i.e., a false positive).

Suppose we repeat the test T times (e.g., $T = 1000000$). Let L denote the number of times n is wrongly reported as prime. Then the empirical liar rate is

$$\text{Liar Rate} = \frac{L}{T}.$$

In my case, the experiment gave:

$$L = 0 \quad \text{out of } T = 1000000 \quad\Rightarrow\quad \text{Liar Rate} = 0.$$

(c) Interpretation

This experiment confirms the theoretical analysis:

- For any odd composite n, at most $\frac{1}{4}$ of the possible bases a can be liars.
- With multiple independent rounds, the error probability decreases exponentially, namely $\leq (1/4)^k$ after k rounds.

Hence, my experiment supports the theoretical guarantee, since I got 0 liars.