Primality Testing: Assignment Solutions

Sujoy Maity
Roll No: CrS2409

August 2025

Solution 1

(a) Idea and intuition

The Miller–Rabin test is a randomized primality check that never wrongly rejects a prime, but may occasionally label a composite number as "probably prime". Each iteration of the algorithm selects a random base a and examines certain modular exponentiation conditions derived from the factorization $n-1 = 2^s d$ (with d odd). If one of these conditions fails for the chosen base a, the test certifies n as composite immediately; otherwise that base provides no witness and the round reports "probably prime".

Because each round uses an independently chosen base, repeating the test reduces the chance that a composite escapes detection. In cryptographic contexts we pick the number of rounds k so that the chance of mistakenly accepting a composite becomes astronomically small.

(b) Sketch of the error bound

Write $n-1 = 2^s d$ with d odd. For a base a coprime to n, the Miller–Rabin test accepts n for that base if either

$$a^d \equiv 1 \pmod{n} \qquad \text{or} \qquad a^{2^r d} \equiv -1 \pmod{n}$$

for some $0 \le r < s$. Number-theoretic results show that, for any fixed odd composite n, the set of bases a satisfying these accept conditions has size at most one quarter of all units modulo n. Consequently, the probability that a uniformly random base causes the test to accept a composite in a single round is bounded by $1/4$.

With k independent rounds (independent bases), the probability that all rounds accept a composite does not exceed

$$\left(\tfrac{1}{4}\right)^k = 2^{-2k},$$

which is the classic MR error bound.

(c) Choosing k for a 512-bit candidate

We want the error probability to be less than 2^{-80}. Using the bound

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

we obtain $2k \geq 80$, hence $k \geq 40$. Thus running at least 40 independent Miller–Rabin rounds suffices to guarantee an error probability below 2^{-80} for a 512-bit candidate.

Solution 2

We now describe the practical experiment: generate two random 256-bit probable primes p and q, form $n = p \cdot q$ (a composite of 512 bits), and then perform many single-round Miller–Rabin trials on n to measure how often the single-round test erroneously reports "probably prime".

(a) How primes were generated and the composite formed

- Use a reliable big-integer library (for example GMP) and a cryptographically strong RNG.
- Repeatedly create 256-bit odd candidates (set the MSB and LSB), and test each candidate with Miller–Rabin using $k = 20$ rounds. When a candidate passes the $k = 20$ generation test, accept it as a probable prime.
- Repeat to obtain two independent primes p and q. Compute the composite $n = p \cdot q$. Save p, q, n (hex) for reproducibility.

Because n is produced as the product of two generated primes, it is guaranteed composite and has bit-length around 512.

(b) Single-round Miller–Rabin trials on n

1. Fix $n = p \cdot q$.
2. For T independent trials (for example $T = 10^6$), perform:
   - Choose a uniform random base $a \in \{2, 3, \ldots, n-2\}$ (or sample uniformly mod n and reject gcds).
   - Run a *single* Miller–Rabin iteration using this base (equivalently, set $k = 1$ with that base).
   - If the test returns "probably prime", record this trial as a liar; otherwise it returns "composite".
3. Let L denote the number of liar trials observed. The empirical liar-rate is

$$\widehat{r} = \frac{L}{T}.$$

In our experiment (for the parameters used in the submitted code), we sampled $T = 1{,}000{,}000$ bases and observed $L = 0$, hence $\widehat{r} = 0$.

(c) Discussion and interpretation

- The theoretical result states that for any odd composite n the proportion of bases that are strong liars is at most $1/4$. That is an upper bound — it does not say that a typical composite attains that bound.
- Random composites obtained from two random primes (as in $n = pq$) generally have substantially fewer liars than the worst-case bound; hence it is common to observe very small liar-rates in practice, often zero for moderately large T.
- The experiment therefore reinforces the theory: the observed liar-rate is at most the bound and typically much smaller. Combining independent MR rounds quickly reduces the acceptance probability of a composite to negligible levels.

Notes on reproducibility

For reproducible results include:

- The exact code used for prime generation and for the trial loop (e.g., C with GMP).
- The value of the RNG seed (if reproducibility is desired).
- The value of T and the generation parameter k used when producing p, q.
- The output file containing p, q, n, and the list of liar bases (if any).

Concluding remarks

Miller–Rabin is both practical and trustworthy for cryptographic prime generation: by selecting an appropriate k during generation and verification (e.g. $k \geq 40$ for 512-bit candidates) the error probability is made negligible for all practical purposes. Experimental checks, such as the single-round liar-rate measurement described above, provide useful empirical confirmation that the composite $n = pq$ is not unusually deceptive with respect to MR.