Miller–Rabin Primality Test: Step-by-Step Workbook

1 1. Understanding Congruence (Modular Arithmetic)

1.1 1.1 What Does "$a \equiv b \pmod{m}$" Mean?

We say "a is congruent to b modulo m" when a and b leave the same remainder upon division by m.

- Divide a by m: remainder r_a.
- Divide b by m: remainder r_b.
- If $r_a = r_b$, then $a \equiv b \pmod{m}$.

Equivalently, m divides the difference: $m \mid (a - b)$.

Example: $14 \equiv 2 \pmod{4}$ since both leave remainder 2 when divided by 4.

1.2 1.2 Why Addition and Multiplication Work

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

- $a - b = mk$ and $c - d = m\ell$ for some integers k, ℓ.
- Summing: $(a + c) - (b + d) = m(k + \ell)$, so $a + c \equiv b + d \pmod{m}$.
- Multiplying: $ac - bd = (a - b)c + b(c - d) = mck + mb\ell = m(ck + b\ell)$, so $ac \equiv bd \pmod{m}$.

1.3 1.3 Exercises

Exercise 1.1 Find the remainder when 123 is divided by 7, and when 200 is divided by 7. Show that $123 \equiv 200 \pmod{7}$.____________________

Exercise 1.2 Show that if $a \equiv b \pmod{m}$, then for any positive integer k, $a^k \equiv b^k \pmod{m}$.____________________

2 2. Computing Large Powers by Hand

2.1 2.1 Breaking Exponents into Powers of Two

Any exponent k can be written in binary, e.g.

$$45 = 32 + 8 + 4 + 1 \quad (45_{10} = 101101_2).$$

Then

$$a^{45} = a^{32} \times a^8 \times a^4 \times a^1.$$

We compute each a^{2^i} by successive squaring:

$$a^2 = (a^1)^2, \quad a^4 = (a^2)^2, \quad a^8 = (a^4)^2, \ldots$$

2.2 2.2 Worked Example

Compute $3^{17} \bmod 23$:

1. Write $17 = 16 + 1$ (binary 10001_2).
2. Compute:

$$3^1 = 3, \quad 3^2 = 9, \quad 3^4 = 9^2 = 81 \equiv 12, \quad 3^8 = 12^2 = 144 \equiv 6, \quad 3^{16} = 6^2 = 36 \equiv 13.$$

3. Multiply: $3^{17} = 3^{16} \times 3^1 \equiv 13 \times 3 = 39 \equiv 16 \pmod{23}$.

2.3 2.3 Exercises

Exercise 2.1 Compute $7^{45} \bmod 1001$ by breaking 45 into powers of two and doing successive squaring and multiplication.______________________________

Exercise 2.2 Show all steps for $13^{37} \bmod 101$.______________________________

3 3. Fast (Binary) Exponentiation Algorithm

3.1 3.1 Why It Is Faster

Multiplying a by itself $k-1$ times takes $k-1$ multiplications. Binary exponentiation uses about $2\log_2 k$ multiplications instead of k.

3.2 3.2 Algorithm (Pseudocode)

```
function binExp(a, k, m):
    result = 1
    base   = a mod m
    while k > 0:
```

```
        if (k mod 2 == 1):
            result = (result * base) mod m
        base = (base * base) mod m
        k = floor(k / 2)
    return result
```

3.3 3.3 Example Table

Compute $5^{27} \bmod 97$ by tracking (k, base, result):

k	base	result
27	5	1
13	25	5
6	$25^2 \bmod 97 = \dots$	$\dots$

3.4 3.4 Exercises

Exercise 3.1 Finish the table to compute $5^{27} \bmod 97$.____________________________

Exercise 3.2 Compute $7^{2025} \bmod 2027$ by binary exponentiation.____________________________

4 4. The Miller–Rabin Primality Test

4.1 4.1 Setup

Let $n > 2$ be odd. Write $n - 1 = 2^s d$ where d is odd (pull out factors of two).

4.2 4.2 One Test Round

Pick base a with $1 < a < n - 1$ and do:

1. Compute $x = a^d \bmod n$ via binExp.
2. If $x = 1$ or $x = n - 1$, return **PASS**.
3. Repeat $s - 1$ times:
   - $x = x^2 \bmod n$.
   - If $x = n - 1$, return **PASS**.
4. Otherwise return **COMPOSITE**.

4.3 4.3 Guided Example

Test $n = 561$, $a = 2$:

1. $561 - 1 = 560 = 2^4 \times 35$, so $s = 4$, $d = 35$.
2. Compute $2^{35} \bmod 561$ (use binExp).

3. Check if $x = 1$ or 560; otherwise square up to 3 times checking for 560.
4. Conclude **COMPOSITE**.

4.4 4.4 Exercises

Exercise 4.1 Carry out one round of Miller–Rabin on $n = 561$, $a = 2$. Fill in each x value.________________________

Exercise 4.2 Test $n = 1105$, $a = 2$.______________________________

5 5. Why Miller–Rabin Works (Theory)

5.1 5.1 Square Roots of 1 Modulo n

A number y with $y^2 \equiv 1 \pmod{n}$ is a square root of unity. For prime p, only $y = \pm 1$. For composite n, there can be more.

5.2 5.2 Witnesses and Non-Witnesses

A base a is a *witness* if the test returns **COMPOSITE**. Otherwise a *non-witness*.

5.3 5.3 Witness Property Theorem

Theorem. If n is odd composite, at least $3/4$ of $a \in \{2, \ldots, n-2\}$ are witnesses.

5.4 5.4 Proof Sketch

Non-witnesses force all intermediate x values to be ± 1. Counting roots of unity shows there are at most 2^{s+1} possibilities, which is $\leq (n-3)/4$ for composite n.

5.5 5.5 Exercises

Exercise 5.1 Explain why for prime p, there are exactly two square roots of unity mod p.________________________

Exercise 5.2 Argue why composite n has at most four such roots if n is not a prime power.________________________