

## Sample Execution of Miller-Rabin Algorithm

Testing if 229 is a prime.

$$228 = 2^2 \times 57$$

---

Random Value : a = 225

$$y = a^r \pmod{229} = 1$$

Is  $y = a^r \pmod{229} = 1$ ?

Yes  $\rightarrow$  229 is a prime!

---

Random Value : a = 47

$$y = a^r \pmod{229} = 107$$

Is  $y = a^r \pmod{229} = 1$ ?

No!

for j := 0 to 1 do begin

Is  $y = a^{2^j r} \pmod{229} = -1$ ?

No!

$$y \rightarrow (y * y) \pmod{229} = 228$$

Is  $y = a^{2^j r} \pmod{229} = -1$ ?

Yes  $\rightarrow$  229 is a prime!

end

---

Random Value : a = 151

$$y = a^r \pmod{229} = 1$$

Is  $y = a^r \pmod{229} = 1$ ?

Yes  $\rightarrow$  229 is a prime!

---

Random Value : a = 101

$$y = a^r \pmod{229} = 122$$

Is  $y = a^r \pmod{229} = 1$ ?

No!

for j := 0 to 1 do begin

Is  $y = a^{2^j r} \pmod{229} = -1$ ?

No!

$$y \rightarrow (y * y) \pmod{229} = 228$$

Is  $y = a^{2^j r} \pmod{229} = -1$ ?

Yes  $\rightarrow$  229 is a prime!

end

---

*Sample Execution of Miller-Rabin Algorithm*

```

Random Value : a = 52
 $y = a^r \pmod{229} = 107$ 
Is  $y = a^r \pmod{229} = 1$ ?
No!
for j := 0 to 1 do begin
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
No!
 $y \rightarrow (y * y) \pmod{229} = 228$ 
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
Yes  $\rightarrow$  229 is a prime!
end

```

---

```

Random Value : a = 21
 $y = a^r \pmod{229} = 107$ 
Is  $y = a^r \pmod{229} = 1$ ?
No!
for j := 0 to 1 do begin
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
No!
 $y \rightarrow (y * y) \pmod{229} = 228$ 
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
Yes  $\rightarrow$  229 is a prime!
end

```

---

```

Random Value : a = 180
 $y = a^r \pmod{229} = 1$ 
Is  $y = a^r \pmod{229} = 1$ ?
Yes  $\rightarrow$  229 is a prime!

```

---

```

Random Value : a = 189
 $y = a^r \pmod{229} = 107$ 
Is  $y = a^r \pmod{229} = 1$ ?
No!
for j := 0 to 1 do begin
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
No!
 $y \rightarrow (y * y) \pmod{229} = 228$ 
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
Yes  $\rightarrow$  229 is a prime!
end

```

---

*Sample Execution of Miller-Rabin Algorithm*

```

Random Value : a = 79
 $y = a^r \pmod{229} = 107$ 
Is  $y = a^r \pmod{229} = 1$ ?
No!
for j := 0 to 1 do begin
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
No!
 $y \rightarrow (y * y) \pmod{229} = 228$ 
Is  $y = a^{2^j r} \pmod{229} = -1$ ?
Yes  $\rightarrow$  229 is a prime!
end

```

---

```

Random Value : a = 126
 $y = a^r \pmod{229} = 1$ 
Is  $y = a^r \pmod{229} = 1$ ?
Yes  $\rightarrow$  229 is a prime!

```

---

*Sample Execution of Miller-Rabin Algorithm*