DATE: ___/___/___

PAGE: ______

Rabin-Miller Primality test

Theorem: Let 'N' be an odd integer such that $N-1 = 2^n \cdot r$ where 'r' is odd.

If there is an integer $a \neq 0$ such that

(i) $a^r \not\equiv 1 \pmod N$

(ii) $a^{2^j \cdot r} \not\equiv N-1 \pmod N$ for all $j \in \{0, 1, \dots, n-1\}$

then 'N' is composite. Otherwise, 'N' is probably a prime.

Lemma: If x and n are integers such that $x^2 \equiv 1 \pmod n$ and $x \not\equiv \pm 1 \pmod n$ then 'n' is composite.

Pseudocode Miller-Rabin Primality Test

Input: ① Prime candidate N with $N-1 = 2^u \cdot r$

② Security parameter s

Output: "N is composite" or "N is likely prime"

```
For i = 1 to s
    Choose a ∈ {2, ..., N-2} uniformly at random
    If a^(N-1) ≢ 1 (mod N)
        Return "composite";
        Stop;
    end

    For j = 1 to u
        If a^(2^j · r) ≡ 1 (mod N) and a^(2^(j-1) · r) ≢ ±1 (mod N)
            Return "composite".
            Stop
    end
end
```

PAGE:

Note:- The Miller-Rabin Test could still give a false prime (saying N is 'prime') when it is actually composite). The probability of this happening depends on S.

Ex: ① Apply the Miller-Rabin test to $N = 229$, ~~with the security parameter S=4.~~

Solu:- Given $N = 229$

$$N-1 = 228 = 2^2 \cdot 57$$

$$\Rightarrow u = 2, \; r = 57$$

We choose ~~S=4~~ random number a is $\{2, 3, \ldots, 227\}$

computations for $a = 2$

~~$a^{N-1} \equiv x \pmod{N}$~~

~~$2^{228} \equiv \pmod{229}$~~, ~~$2^8 \equiv 256 \equiv 27 \pmod{229}$~~

Consider $a^{2^j \cdot r} \equiv x \pmod{229}$

$j = 0$,

$$a^{57} = 2^{57}$$

$2^8 \equiv 27 \pmod{229}$

$2^{16} \equiv 27^2 \equiv 42 \pmod{229}$

$2^{32} \equiv 42^2 \equiv 161 \pmod{229}$

$2^{48} \equiv 42 \times 161 \pmod{229}$

$2^{48} \equiv 121 \pmod{229}$

$2^{56} \equiv 121 \times 27 \pmod{229}$

$2^{56} \equiv 61 \pmod{229}$

$2^{57} \equiv 61 \times 2 \pmod{229}$

$2^{57} \equiv 122 \pmod{229}$

$$\Rightarrow 2^{57} \equiv 122 \pmod{229}$$

$$\therefore 2^{57} \not\equiv \pm 1 \pmod{229}$$

$j = 1$. $a^{2 \times r} \equiv a^{2 \times 57}$

$$\therefore 2^{2 \times 57} \equiv (2^{57})^2 \equiv 122^2 \equiv 228 \pmod{229}$$

$$2^{2 \times 57} \equiv 228 \equiv -1 \pmod{229}$$

$\Rightarrow \therefore 229$ is a prime number.

DATE: /
PAGE:

Apply Rabin-Miller test to $N = 29$

Soln:- $N = 29$

$N - 1 = 29 - 1 = 28 = 2^2 \times 7$

$u = 2, \; r = 7$

Choose a random number 'a' between 2 to 27 $(2 \le a \le 27)$

$a = 3$,

find $3^7 = 2187 \equiv 12 \pmod{29}$

$a^r \not\equiv 1 \pmod{29}$

$\therefore$ Consider $a^{2^j \cdot r} \equiv x \pmod{29}$

$j = 1$, $3^{2 \times 7} \equiv 3^{14} \equiv (12)^2 \equiv 144 \equiv 28 \equiv -1 \pmod{29}$

$\Rightarrow$ 29 is a prime number.

③ Apply the Miller-Rabin test to $N = 561$ to determine whether it is composite, and if composite, find its factors.

Soln:- $N = 561$

$N - 1 = 561 - 1 = 560 = 2^4 \times 35$

$u = 4, \; r = 35$

Choose a random number 'a' in $\{2, 3, \ldots, 559\}$

take $a = 2$

$j = 0$ $2^{35} \equiv 263 \pmod{561}$

$j = 1$ $(2^{35})^2 \equiv (263)^2 \equiv 166 \pmod{561}$

$j = 2$ $(2^{70})^2 \equiv 166^2 \equiv 67 \pmod{561}$

$j = 3$ $(2^{140})^2 \equiv (67)^2 \equiv 1 \pmod{561}$

$\therefore$ $2^{280} \equiv 1 \pmod{561}$

$\Rightarrow$ 561 is a composite number.

DATE: __/__/__

PAGE: ____

Note that, we have

$$67^2 \equiv 1 \pmod{561}$$

$$67^2 - 1 \equiv 0 \pmod{561}$$

$$(67-1)(67+1) \equiv 0 \pmod{561}$$

$$66 \times 68 \equiv 0 \pmod{561}$$

This means that 561 divides 66×68

But since $66, 68 < 561$ then some factors of 561 must be common with factors of 66 while others must be common with factor of 68