Primality Testing

Input: A positive integer N.
(n bits long)

Output: 1 if N is prime;
0 otherwise.

- If N is 1 or even: output 0; if $N=2$: output 1.
- If $N = a^b$, for some $a, b \geq 2$: output 0.
- Set Flag = False.

Can be checked deterministically in polynomial time.

REPEAT 5 TIMES {
- Pick $a \in \{1, 2, \ldots, N-1\}$ at random.
- If $\gcd(a, N) \geq 2$: output 0.
- If $a^{N-1} \not\equiv 1 \pmod N$: output 0.
- If $a^{(N-1)/2} \not\equiv \pm 1 \pmod N$: output 0.
- If $a^{(N-1)/2} \equiv -1 \pmod N$: Flag = True.
}

- If Flag = True: output 1
  Else output 0.

Efficiency:

From our earlier discussion, all steps can be performed in $O(n^3)$ steps.

CLAIM: N prime $\Rightarrow \Pr[\text{error}] \leq 1/2^5$.

N not prime $\Rightarrow \Pr[\text{error}] \leq 1/2^5$.

Why?

In the following assume $a \in \{1, 2, \ldots, N-1\}$

FACT 1:
- N prime $\Rightarrow a^{N-1} = 1 \pmod N$
- N prime $\Rightarrow a^{(N-1)/2} = 1$, $a^{(N-1)/2} = -1$ each for half the elements in $\{1, 2, \ldots, N-1\}$

Exercise: Fact 1 $\Rightarrow$ { N prime $\Downarrow$ $\Pr[\text{error}] \leq 1/2^5$

FACT 2: Suppose N is not a prime power.

Suppose there is an a such that

$$a^{(N-1)/2} = -1 \pmod{N}.$$

Then, for at least half the elements a such that $a^{N-1} = 1 \pmod{N}$, we have $a^{(N-1)/2} \neq \pm 1$

EXERCISE: FACT 2 $\Longrightarrow$

N composite

$\Downarrow$

$\Pr[\text{error}] \leq 1/2^s$