

but not necessarily primality testing  
 Can <sup>hints from</sup> number theory help?

### Wilson's Thm (1771)

$N$  is prime iff  $(N-1)! \equiv -1 \pmod{N}$

Computationally terrible  $\rightarrow$  need  $O(N)$  mults  
 $\rightarrow O(N^2) = O(2^{7n})$  exponential again!

### Fermat's Little Thm (16???)

$N$  is prime  $\Leftrightarrow \forall a \in \{1, \dots, N-1\},$   
 $a^{N-1} \equiv 1 \pmod{N}$

Can be checked quickly by repeated squaring  
 $O(\log N)$  mults  $\Rightarrow O(n^3)$  time

Restated:  $N$  is composite  $\Leftrightarrow \exists a \in \{1, \dots, N\}$   
"witness"  $a^{N-1} \not\equiv 1 \pmod{N}$  (\*)

Refined

Fermat's "Pseudo-Primality": // not an algm  
 or  $a=3$  or  $a=5$  or  $a=7$   
 if (\*) holds for  $a=2$   $\wedge$  return "composite"  
 else "maybe prime"

but wrong: counterex:  $N = 341 = 11 \cdot 31$   
 for  $a=2$

counterex:  $a=2, 3, 5, 7$ :  $N = 7045248121$   
 $\sim 271 \times 2581201$

counterex:  $a=2,3,5,7$ :  $N = 7045248121 = 821 \times 8581301$   
 "Carmichael numbers"

Refined Fermat's Thm  $N$  is composite iff  $\exists a \in \{1, \dots, N-1\}$ ,

$$(*) \left\{ \begin{array}{l} a^{N-1} \not\equiv 1 \pmod{N} \text{ or} \\ \text{for some } k = (N-1)/2^i, \\ a^{2^k} \equiv 1 \text{ but } a^k \not\equiv \pm 1 \pmod{N} \end{array} \right.$$

$x^2 \equiv 1 \pmod{N}$   
 $N$  prime  
 $\Rightarrow x \equiv \pm 1$ .

Refined "Pseudo-Alg'm":

Still wrong: but for  $N < 25$  billion,  
 # counterex = 1 !

Counting Thm (Rabin 1976)

If  $N$  is prime, no  $a$  satisfies  $(*)$

If  $N$  is composite,

$$\# \text{ a's satisfying } (*) \geq \frac{3}{4}(N-1)$$

↑  
"witness"

Miller-Rabin's Rand. Alg'm (Monte Carlo)

repeat  $d$  times {

$a = \text{rand}(1, N-1)$

if  $(*)$  holds return "composite"

}  
 return "probably prime"

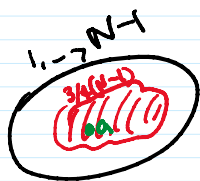
**Analysis:** runtime  $O(d n^3)$  polynomial

prob of error: "one-sided"

prob of error: "one-sided"

if  $N$  is prime, always correct

if  $N$  is composite,



let  $E_t = [a \text{ satisfies } (**) \text{ at } t^{\text{th}} \text{ iteration}]$

$$\Pr(E_t) \approx \frac{\frac{3}{4}(N-1)}{N-1} = \frac{3}{4}$$

$$\Rightarrow \Pr[\text{algm errs}] = \Pr\left(\bigcap_{t=1}^d E_t^c\right)$$

$$= \prod_{t=1}^d \Pr(E_t^c) \quad \text{by indep.}$$

$$\leq \prod_{t=1}^d \frac{1}{4} = \left(\frac{1}{4}\right)^d$$

e.g.  $d=4: \leq \frac{1}{256}$

$d=9: \leq \underline{\underline{1 \text{ in million}}}$

can error be eliminated completely?

Miller's Thm (1976) Assume "Extended Riemann Hypothesis"

$N$  is composite iff  $\exists a < \underbrace{(2 \log^2 N)}_{2n^2}$  s.t.  $(**)$  holds

$\Rightarrow$  polytime deterministically under hypothesis

Later:

Adleman-Pomerance-Rumely '83 det. time  $n^{O(\log \log n)}$

Adleman-Huang '87 expect polytime Las Vegas (no error)

AKS Thm  $N$  is composite iff

→  $N$  is a perfect power or

$\exists a < 8 \log^{3.5} N, r < 16 \log^5 N$  st.

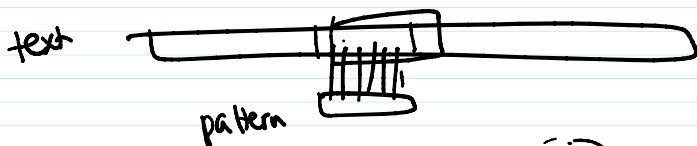
(\*\*\*)  $\left\{ \begin{array}{l} \gcd(a, N) \neq 1 \text{ or} \\ \underbrace{(x+a)^N - (x^N+a)}_{\text{polynomial in } x} \not\equiv 0 \pmod{x^r-1, N} \end{array} \right.$

⇒ polytime deterministically (no hypothesis)

Problem string matching

text: algorithmisfun       $n$        $u = a_1 \dots a_n \in \Sigma^*$   
 pattern: thmis               $m$        $v = b_1 \dots b_m \in \Sigma^*$   
 is  $v$  substring of  $u$ ?

trivial:  $O(mn)$   
 $O(m+n)$ ?



"DFA method":  $O(f(m) + n)$   
 ↑ build DFA                      ↑ run the DFA