

# RANDOMIZED ALGIMS

alg'm that can make random choices

↗ access to rand number generator

rand\_bit() → 0 or 1

rand(a, b) → a or a+1 or ... or b

It's Las Vegas if it's always correct & runtime depends on rand choices



↗ analyze expected time

e.g. randomized quicksort

It's Monte Carlo if correctness depends on rand choices



↗ analyze probability of error

Probability space is over the sequence of rand bits/numbers

↗ assume uniform & independent

Still worst-case input

## Quick Probability Review:

events  $E, E'$

$$\Pr(E \cup E') \leq \Pr(E) + \Pr(E') \quad \begin{matrix} \text{always} \\ \text{union bd} \end{matrix} \quad (\text{equal if disjoint})$$

$$\Pr(E^c) = 1 - \Pr(E)$$

$$\Pr(E \cap E') = \Pr(E) \cdot \Pr(E') \quad \text{if } \underline{\text{independent}}$$

$$\Pr(E | E') = \frac{\Pr(E \cap E')}{\Pr(E')}$$

↗ conditional prob.



rand vars  $X, Y$

$$E[X] = \sum_x x \Pr[X=x]$$

$$E[X+Y] = E[X] + E[Y] \quad \text{always}$$

linearity of expectation

$$E[cX] = cE[X]$$

$$E[XY] = E[X]E[Y] \quad \text{if independent}$$

e.g. Markov's ineq.: if  $X \geq 0$  and  $E[X] = \mu$ ,

$$\Pr[X \geq c\mu] \leq \frac{1}{c}.$$

(can convert Las Vegas  $\rightarrow$  Monte Carlo with good worst-case runtime)

Pf:

$$\mu = E[X] \geq \sum_{x \geq c\mu} x \Pr[X=x] \geq \sum_{x \geq c\mu} c\mu \Pr[X=x] = c\mu \Pr[X \geq c\mu]$$

□

---

Problem Given a <sup>large</sup> <sub>n-bit</sub> number  $N$ ,  
is  $N$  prime or composite?

Trivial Alg'm:  $\forall N$   $N = ab \geq a^2$   $a \leq b$   
for  $a = 2$  to  $\sqrt{N}$   
if  $N$  is divisible by  $a$  return "composite"  
return "prime"

$$\Rightarrow O\left(\frac{N}{\sqrt{N}} \cdot n^2\right) = O\left(2^{n/2} n^2\right) \quad \text{Exponential!}$$

Rmk - factoring is probably hard

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  
 $\rightarrow O(N^2) = O(2^{12})$   
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  
 $\approx O(n)$

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