

RANDOMIZED ALG'S

an algm that can make random choices

↗ i.e. access to rand. number generator

rand_bit() $\rightarrow$ 0 or 1

rand(a,b) $\rightarrow$ 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. choice

↗ analyze probability of error

probability space is over sequence of rand bits/numbers

↗ assume uniform & independent

note - still worst-case input (do not assume rand. input)

Quick Probability Review:

events E, E'
rand vars X, Y

union bound $\rightarrow$ $\Pr(E \cup E') \leq \Pr(E) + \Pr(E')$
equal if disjoint
($\Pr(E \cup E') = \Pr(E) + \Pr(E') - \Pr(E \cap E')$)

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

$\rightarrow$ $\Pr(E \cap E') = \Pr(E) \cdot \Pr(E')$
if E, E' are independent

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

↑
conditional prob.

$$E[X] = \sum_x x \cdot \Pr(X=x) \quad (\text{integral if continuous})$$

linearity of expectation $\rightarrow$ $E[X+Y] = E[X] + E[Y]$ always
 $E[cX] = cE[X]$

"of expectation" $E(cX) = cE(X)$

→ $E(XY) = E[X] \cdot E[Y]$ if independent

e.g. Markov's inequality: if $X \geq 0$ and $E(X) = \mu$,
 $\Pr[X \geq c\mu] \leq \frac{1}{c}$.

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

□

Problem Given ^{large} n -bit number N ,
is N prime or composite?

Trivial Alg'm: (?? B.C.)

for $a = 2$ to $\sqrt{N}$
if (N is divisible by a) return "composite"
return "prime"

$a^2 \leq ab = N \quad a \leq b$
 $\Rightarrow a \leq \sqrt{N}$

↑ can be done in $O(\sqrt{N})$ time

$O(\sqrt{N} n^2) = O(\underbrace{2^{n/2}}_{\uparrow} n^2)$ still exponential

Rmk: factoring is probably hard
but not necessarily primality testing

Wilson's Thm (1???)

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

Rmk- completely useless!
computationally speaking

← requires
 $O(N)$ mults.:
exponential time

Fermat's Little Thm (16??)

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

$\uparrow$
can be computed by repeated squaring
 $O(n^3)$ time $\left(\begin{array}{l} \# \text{ mults} = O(\log N) = O(n) \\ \text{each mult } O(n^2) \end{array} \right.$

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

Fermat's "Pseudo-Alg'm":

or $a=3$ or $a=5$ or $a=7$
If $(*)$ holds for $a=2$ return "composite"
else "maybe prime?"

but wrong! counterex: $N=341 = 11 \cdot 31$

still strong! counterex: $N=7045248121$
"Carmichael numbers" $= 821 \cdot 8581301$