February 21, 2023 1:39 PM

Problem Given (large) n-bit number N,
is N prime or composite?

Trivial Alg'm:
for $a = 2$ to ~~$N-1$~~ $\sqrt{N}$
if N is divisible by a then return "composite"
return "prime"

$N = ab \quad a \le b$
$a^2 \le N, \quad a \le \sqrt{N}$

$$\Rightarrow O(\sqrt{N}\, n^2) = O(2^{n/2} n^2) \le O(1.415^n)$$
exponential!

Rmk - factoring is probably hard
but not necessarily primality testing

Wilson's Thm (17??)
N is prime iff $(N-1)! \equiv -1 \pmod N$

$\#$ mults $= O(N) = O(2^n)$

computationally useless

Fermat's Little Thm ((16??)
N is prime $\Longleftrightarrow$ $\forall a \in \{1, .., N-1\}$, $a^{N-1} \equiv 1 \pmod N$

can be computed quickly
repeated square
$\#$ mult $= O(\log N) = O(n)$

checkable in $O(n^3)$ time

Restated:
N is composite $\Longleftrightarrow$ $\exists a \in \{1, .., N-1\}$, $a^{N-1} \not\equiv 1 \pmod N$ $\quad (*)$

called "witness"

Fermat's "Pseudo-Alg'm": // not an alg'm
if $(*)$ holds for $a = 2$ or $a=3$ or $a=5$ or $a=7$ then return "composite"
else return "maybe prime?"

... counterex: $N = 341 = 11 \cdot 31$

else return "maybe ..."

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

still wrong! counterex: $N = 7045248121$
$= 821 \times 8581301$

"Carmichael numbers"

Refined Fermat's Thm N is composite

$\iff \exists\, a \in \{1, \dots, N-1\}$,

$a^{N-1} \not\equiv 1 \pmod{N}$ or

for some $k = (N-1)/2^i$,

$a^{2k} \equiv 1$ but $a^k \not\equiv \pm 1 \pmod{N}$ $\Big\}$ (**)

"witness"

$x^2 \equiv 1$
$x \not\equiv \pm 1$

Rmk: Can test (**) just as quickly as (*)

Refined "Pseudo-Alg'm":

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

still wrong

Counting Thm (Rabin 1976)

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

If N is composite,
\# a's satisfying (**) $\geq \frac{3}{4}(N-1)$

a's

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

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

repeat d times {

  a = rand(1, N−1)

  if (**) holds return "composite"

}

return "probably prime"

Analysis: runtime $O(\underline{dn^3})$ polynomial

Prob. of error: ("one-sided")

if N is prime, always correct

if N is composite, rand var

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

$$\Pr(E_t) \geq \frac{\#\, a\text{'s satisfying } (**)}{N-1}$$

$$\geq 3/4$$

$$\Rightarrow \Pr(\text{alg'm errs}) = \Pr\left(\bigcap_{t=1}^{d} E_t^c\right)$$

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

$$\leq \left(\frac{1}{4}\right)^d.$$

e.g. $d=9 \Rightarrow \leq 1$ in million chance of error

can error be eliminated completely?

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

N is composite $\iff \exists\, a < 2\log^2 N$ s.t. (**) holds

$\Rightarrow$ polytime deterministically

$\Rightarrow$ polytime deterministically under hypothesis

Later: Adleman et al. '83 $n^{O(\log\log n)}$ time

Adleman-Huang '87 Las Vegas expected polytime

⋮

Agrawal-Kayal-Saxena's Thm (2002)

N is composite $\Leftrightarrow$

N is a perfect power or

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

$\gcd(a, N) \neq 1$ or

$(x+a)^N - (x^N + a) \not\equiv 0 \pmod{x^r - 1, N}$

(~~***~~) testable in polytime

$\Rightarrow$ polytime deterministically (no hypothesis)

Problem Given strings $u = a_1 a_2 \cdots a_n \in \{0,1\}^*$ ← text

$v = b_1 b_2 \cdots b_m \in \{0,1\}^*$ ← pattern

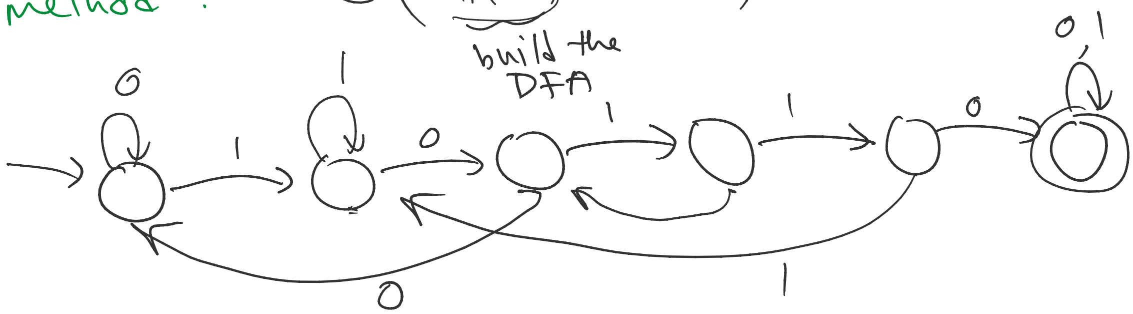
is v a substring of u? $(m \ll n)$

e.g. $u = 0110\boxed{1011010}$

$v = 10110$

brute force: $O(mn)$ time

"DFA method": $O(\underbrace{f(m)}_{\text{build the DFA}} + n)$ time



Knuth-Morris-Pratt '77: $O(n)$ time

(by compressed version of DFA)

(regardless of $|\Sigma|$)

... a rand. $O(n)$-time alg'm

that is simpler ...