

Fermat's Little Thm (16??)

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

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

Restated: $N \text{ is composite} \Leftrightarrow \exists a \in \{1, \dots, N-1\}, \quad \left. \begin{array}{l} a^{N-1} \not\equiv 1 \pmod{N} \end{array} \right\} (*)$

Fermat's "Pseudo-Alg'm":

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

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

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

Refined Fermat's Thm

N is composite iff

$$\exists a \in \{1, \dots, N-1\}, \quad a^{N-1} \not\equiv 1 \pmod{N} \quad \leftarrow (*)$$

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

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

can test $(**)$ just as quickly
as $(*)$

Refined "Pseudo-Alg'm":

if $(**)$ holds for $a=2$ or $a=3$ or 5 or 7
return "composite"

else "maybe prime?"

(still wrong: but for $N < 25$ billion, $\# \text{ counterex} = 1$)

Counting Thm (Rabin 1976)

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

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

$\uparrow$
witness

$\{1, \dots, N-1\}$

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

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

 if (**) holds return "composite"

}
return "probably prime" $\leftarrow$

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

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

if N is prime, always correct

if N is composite,

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

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

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

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

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

e.g. $d=9 \Rightarrow \leq 1$ in million chances of error!
(no counterex)

$\neg \exists$ (no counterex)
 or bad input

can error be eliminated completely?

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

N is composite iff $\exists a < 2 \log^2 N$ st.
 (**) holds $\leftarrow O(n^2)$

$\Rightarrow$ polytime deterministically under hypothesis.

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

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

Agrawal-Kayal-Saxena's Thm (2002)

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

$$a^N \not\equiv a$$

N is composite iff

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

(***)
testable
in polynomial

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

$\Rightarrow$ polytime deterministically (no hypothesis) but not as practical.