

Fermat primality test

EG $N = 135066 \dots$ 300 digits $\dots 563$

1991: \$100,000 for factoring N

Is N maybe a prime?

Definitely not! $2^{N-1} \equiv 12 \dots 851 \pmod{N}$

$$a \not\equiv 0 \pmod{n} \neq 1$$

THM
restatement
of little Fermat

If $a^{n-1} \not\equiv 1 \pmod{n}$ then n is not a prime.

a Fermat witness mod n

a is a Fermat liar mod n

if $a^{n-1} \equiv 1 \pmod{n}$ although n is not a prime

Fermat primality test

input: n

output: "not a prime" or "likely prime"

repeat k times: parameter

pick random a from $\{2, 3, \dots, n-2\}$

if $a^{n-1} \not\equiv 1 \pmod{n}$ then

stop: "not a prime"

else "likely prime" (after repeating k times)

EG Is $n = 221$ a prime?

• first "random" pick: $a = 38$

$$38^{220} \equiv 1 \pmod{221}$$

221 is behaving like a prime

• second pick: $a = 24$

$$24^{220} \equiv 81 \not\equiv 1 \pmod{221}$$

STOP!

221 is not a prime

38 Fermat liar mod 221

24 Fermat witness mod 221

rare!

only 14/218
6.4%

BAD NEWS There exist composite numbers n such that every residue a is a Fermat liar or $\gcd(a, n) > 1$.

absolute pseudo-prime