Miller-Rabin primality test

review $x^2 \equiv 1 \pmod p$ only has solutions ± 1

Is n a prime?

- in the Fermat primality test:

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

  else: give up ("n likely prime")

- for Miller-Rabin we dig deeper in the latter case:

  if $a^{(n-1)/2} \not\equiv \pm 1 \pmod n$ then n is not a prime

  satisfies $x^2 \equiv 1 \pmod n$

  a^{n-1}

  if $a^{(n-1)/2} \equiv -1 \pmod n$ then give up ("n likely prime")

  if $a^{(n-1)/2} \equiv 1 \pmod n$

  then repeat with $a^{(n-1)/4}$ if possible

  satisfies $x^2 \equiv 1 \pmod n$

Miller-Rabin primality test

write $n-1 = 2^s m$ (odd)

for several random a, compute:

$$a^m, a^{2m}, \ldots, a^{2^s m} = a^{n-1}$$

if n is a prime, then these must be:

- $1, 1, \ldots, 1$ (all 1's)

or:
- $\ldots, -1, 1, \ldots, 1$

if the values are of this form
but n is not a prime
then a is a strong liar mod n

good news: if n is composite then $< 25\%$ of residues are strong liars

EG Is $n = 221$ a prime ?

$n-1 = 4 \cdot 55 = 2^s m$

$s=2 \quad m=55$

compute : $a^{55}, \ a^{110}, \ a^{220} \pmod{221}$

if 221 prime : $1, 1, 1$

or: $-1, 1, 1$

or: $\sim, -1, 1$

- $a = 47$: $47^{55} \equiv 174$ $\quad 47^{110} \equiv 174^2 \equiv -1$

  not needed: $47^{220} \equiv (-1)^2 \equiv 1$

  $\rightsquigarrow$ 221 behaving like a prime

  47 strong liar mod 221 (only 4)

- $a = 38$: $38^{55} \equiv 64$ $\quad 38^{110} \equiv 64^2 \equiv 118 \not\equiv -1$

  not needed: $38^{220} \equiv 118^2 \equiv 1$

  $\rightsquigarrow$ 221 is not a prime

  [38 is a Fermat liar mod 221 (only 14)]

- $a = 24$: $24^{55} \equiv 80$ $\quad 24^{110} \equiv 80^2 \equiv 212 \not\equiv -1$

  not needed: $24^{220} \equiv 212^2 \equiv 81 \not\equiv 1$

  $\rightsquigarrow$ 221 is not a prime