CIS 3362 10/26/22

(1) Finish Miller Rabin
(2) Factoring

→ Idea (Testing if n is prime
1. Pick random a → if gcd(a,n) != 1 return composite
2. Calculate $a^{n-1} \bmod n$
3. If ans != 1 ⟹ COMPOSITE
   else IS PROBABLY PRIME

→ redo 100 times
only ans "is prob prime" if we never returned comp.

→ for very few composites this ALWAYS equals 1 as long as gcd(a,n)=1.
→ Carmichael Numbers
↑ how to screen out.

We know for prime p, $a^{p-1} \equiv 1 \pmod p$
$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$

On mod exp chart for all primes

base exp	$\frac{p-1}{2^k}$	...	$\frac{p-1}{8}$	$\frac{p-1}{4}$	$\frac{p-1}{2}$	$p-1$
b_1				-1	1	1
b_2	1	1	1	1	1	1

If p prime one of these 2 patterns hold

$\int$ Order$(b_1) = \frac{p-1}{2^m}$ for some m and $b_1^{\frac{p-1}{2^{m+1}}} \equiv -1 \bmod p$

Order $(b_1) = \frac{p-1}{2^m}$ for some m and $b_1^{\frac{p-1}{2^{m+1}}} \equiv -1 \bmod p$

OR $b_1^{\frac{p-1}{2^k}} \equiv 1 \bmod p$ where

$\frac{p-1}{2^k} \in$ Odd Int

Miller-Rabin (n, rep) ⟹ Calculate k such that $\frac{p-1}{2^k} \in$ Odd Int

Rewrite $p-1 = 2^k m$, $m \in$ Odd, $k \geq 1$

Repeat rep # times:

1. Pick random a, $1 < a < n-1$
2. Let $X = a^m \bmod n$
   a. if $X == 1$, continue
   b. ~~for~~ Repeat $k-1$ times:
      b1. if $X == -1$, break
      b2. $X = (X * X) \bmod n$
   c. If we never get break
      Return Composite

Return Is Probably Prime

Factoring

1) Fermat Factoring
- Always succeeds
- Could really slow

2) Pollard-Rho *
- Sometimes fails
- When it doesn't is faster Fermat

Assume factoring ODD product of 2 primes

17 (20) 23 $\quad 17 \times 23 = (20-3)\times(20+3)$

diff even $\quad (x-y)\times(x+y)$

$n = 391 = (x-y)(x+y) = x^2 - y^2 \Rightarrow x^2 = 391 + y^2$

$x > \sqrt{391} = 19.\sim$

x	$x^2 - 391$	Is Perfect Sq
20	9	yes // Stop

$(20-\sqrt{9})(20+\sqrt{9})$

17×23

$23 \times 67 = 1541$ $\sqrt{1541} \sim 39...$

x	$x^2 - 1541$	Is perfect sq
40	59	no
41	140	no
42	223	no
43	308	no
44	395	no
45	484	yes

$1541 = (45-22)(45+22)$

23×67 ✓

Better if 2 odd primes are "close"
worst case is no better than trial division but it'll always give an ans.

Pollard - Rho

Create a sequence with a rule:

$a_1 = 2$, $a_n = (a_{n-1} * a_{n-1} + 1) \bmod X$

where X is value to be factored

Start: 2, 5, 26, 678, ...

$X = p \times q$, p, q ∈ Primes

investigate mod p

mod q

Calculate $Y = a_{2i} - a_i \bmod X$, $i = 1, 2, 3, \ldots$

test $\gcd(X, Y) \neq 1$, then that's a factor of X.

if $Y == 0 \bmod X$ test fails