2/13/2023

test prime - ss - different prime test from assignment
- random keys - solivay strassman
- generates # bt random - we're doing miller-Rabin ★
- we'll use gmp multiprecision to generate random
- write utility functs
  - isevan, isodd
  - power mod
  - Jacobi symbol - don't have to do
  - is prime
    - probabilistic primality test
    - run multiple times to increase accuracy

"when you look @ number theory, you see gods shadow."
- pick random # & check if prime very is prime
  - density of primes is approx logorithmic
- carmical pseudo prime
  - rare
- greatest common divisor
  - O(n) = log n
  - euclidean algorithm
- least common multiple
- inverse (multiplicative) $a \times b = -1$
  - uses gcd
  - mod n #s

- write sense of utility
  - write test w/ 64 bits, then replace w/ gmp multiprecision
  - in python too

Compilers:

IMSAI 8080 - uses switches for addresses, then data

-old compiler

clang -S, shows .s file w/ assembly, clang -E, shows preprocessor

C → preprocessor → compiler → assembler → linker → EXE

- Macros & Macroprocessor

assembly

object code

patches object code together

libraries

Compiler steps:

1) lexical - lex/flex language

2) Syntax - checks int, {, (, w/ other symbols
- uses parse trees, to analyze syntax
- abstract syntax tree
- recursively traverse tree

3) Translator
- translation to machine code from assembly
- creates tokens

4) Optimization
5) Storage assignment
6) Code generation
7) Assembly phase

Loader lives in operating system
- allocates memory
- links - resolves symbolic references
- relocation - changes necessary dependencies
- Loading place machine code & data into process

man exec

python, java script - interpreted language
- translates line by line

interpreter - walks through syntax tree & just does it

interpreted languages are slower

bash is interpreted language