CS 124 Lecture 14 (1)

Primes & Crypto

Primality testing

prime numbers are frequent

$\pi(x) =$ # of primes from 1 to x

$\pi(x) \approx \frac{x}{\ln x}$ $\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} \to 1$

→ need prime testing to find random primes

→ fraction of primes [redacted] in 1 to 10^{250}

$$\frac{10^{250}}{250 \ln 10} \approx \frac{10^{250}}{440} \quad \frac{1}{640}$$

[redacted], also throw out multiples of 5, 3 easily

Find a (random) prime approach

Pick a random # from 1 to $\underbrace{10^{250}}_{e.g.}$

TEST if prime

yes → return prime (big, most #s > 10^{240})

else repeat.

Baseline

test if prime upto $\sqrt{n}$

not prime $\iff \exists$ a prime factor $\leq \sqrt{n}$

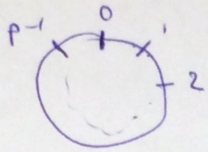
(prime factorization)

! exponential in # of digits, bits (representation size)

$$\sqrt{10^{250}} = 10^{125}$$

we want $O(\underset{\uparrow \text{ \# bits}}{\log n})$ alg, based of # of digits/bits mod p : remainder when divided by p

$x = y \mod p$: remainder of x is equal to remainder of y after dividing by z.



multiplicative inverse: $a \neq 0 \mod p$, then $\exists a^{-1}$, s.t. $a a^{-1} = 1 \mod p$

ex: $5^{-1} \mod 7 = 3$, $4^{-1} \mod 7 = 2$, $6^{-1} \mod 7 = 6$

Fermat's little theorem

$a^{p-1} = 1 \mod p$

for p prime, $1 \leq a < p$

Proof (part 1)

let $S = \{1, 2, \_\_\_\_, p-1\}$
$aS = \{a1, a2 \_\_\_\_, a(p-1)\}$

Prove $aS = S \mod p$,

by contradiction, pick two elts in aS,
suppose $ai = aj \mod p$

[redacted]

ex: $p = 7$, $a = 3$
$\{1, 2, 3, 4, 5, 6\}$
$\downarrow a$
$\{3, 6, 9, 12, 15, 18\}$
$\downarrow \mod p$
$\{3, 6, 2, 5, 1, 4\}$ ✓

multiply by a multiplicative inverse a^{-1}
since $ai = aj \mod p$ and $a^{-1} = a^{-1} \mod p$
$\Rightarrow a a^{-1} i = a a^{-1} j \mod p$ (modular arithmetic)
$\Rightarrow i = j \mod p$
[redacted] $\Rightarrow$ contradiction

the only way to have two elements in aS s.t.
$ai = aj \mod p$
is to to multiply i and j by a [redacted], where
$i = j \mod p$,
BUT, there are no such two elements in S

$\Rightarrow$ [redacted] for all elts in aS [redacted]
$ai \neq aj \mod p$
and there $p-1$ such elts
and none is $0 \mod p$ (p is not in any operators) is not a factor in prime factorization of any elts)

$\Rightarrow aS = S \mod p$

Proof (part 2)

$$\prod_{x \in S} x = \prod_{y \in aS} y \mod p$$ since S and aS are the same products of their elts are the same mod p by modular arithmetic

$$(p-1)! = a^{p-1} (p-1)! \mod p$$

$$\underbrace{(p-1)!}_{} = a^{p-1} \underbrace{(p-1)!}_{} \mod p$$

no factor p

$\Rightarrow \not\equiv 0 \mod p$

$\Rightarrow$ has a multiplicative inverse

multiply by inverse (by modular ariph.)

$$\boxed{1 = a^{p-1} \mod p}$$

Fermat test

Fermat little theorem

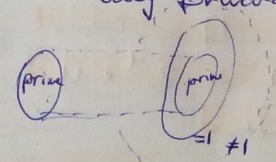
p prime, $1 \le a < p \Longrightarrow a^{p-1} = 1 \mod p$

only forward direction

- given $p > 2$
- compute $2^{p-1} \mod p$

~~$= 1 \rightarrow$ prime~~ ✗ NO

$\neq 1 \rightarrow$ composite ✓ YES



Potential fix? → NO

try different a's

3^{p-1}

5^{p-1}

⋮

e.g. $2^{340} = 1 \mod p$

341 not prime

2-pseudoprime for Fermat's test

Carmichael #'s (n)

$a^{n-1} = 1 \mod n$

$\forall a$ where a, n do not share a factor

→ infinitely many Carmichael #'s

Rabin – Miller Primality test

mod prime (p)
1 — no non-trivial root of 1

mod composite (n)
2 — there are

e.g. $n = 15$
$4^2 = 16 = 1 \bmod 15$
[redacted] multiply with itself to get 1 mod n

1 $x^2 = 1 \bmod p$
$\Downarrow$ by mod. arithmetic
$(x+1)(x-1) = 0 \bmod p$
for 0 mod p,
$x + 1 = 0 \bmod p$
or
$x - 1 = 0 \bmod p$
by mod. arithmetic.
$\Rightarrow \underbrace{x = 1 \bmod p \text{ or } x = -1 \bmod p}_{\text{trivial roots}}$

2 $x^2 = 1 \bmod n$
$\underbrace{(x+1)}_{\text{factor of } 3}\underbrace{(x-1)}_{\text{factor } 5} = 0 \bmod$ [redacted] n for $n = 15$
or vice versa
[redacted]
$\Rightarrow$ non-trivial roots

FLT Fermat little theorem, and exploit [redacted] the root property

Test n (odd)
$n - 1 = 2^t \cdot u$ ← odd part
compute

rep. squaring $O(\log n)$

a^u
$\Downarrow$
a^{2u}
$\Downarrow$
a^{4u}
⋮

$a^{2^{t-1}u} =$
- $\neq -1$ or $1 \bmod n$ → composite, non trivial root of 1 found
- $1 \bmod n$, keep going
- $-1 \bmod n$ DONE, cannot continue taking roots

$\Downarrow$
$a^{2^t u} = a^{n-1}$

if $a^{n-1} \neq 1 \bmod n$
→ composite by FLT

if $a^{n-1} = 1 \bmod n$, look at previous term, square root

Alg.

candidate witness that n is composite

choose a randomly, $1 < a < n$

run Rabin-Miller

if n is composite

$\Rightarrow$ return with prob. $\geq 3/4$ (LT Number theory)

(a is witness)

else

$\Rightarrow$ with $< 1/4$ prob, pass, repeat.

if pass 50 times

return prime with False positive rate $< 2^{-100}$

$O(\log n)$

no problem with Carmichael #s

there is a de-randomized alg. now, but randomized is efficient

Gen. Crypto Framework.

Alice $\longrightarrow$ Bob

$\uparrow$ $e(X)$

Eve

Alice $x \to e(x)$ (encoding fxn)

Bob $e(x) \to d(e(x)) = x$

Eve cannot recover x from $e(x)$

(1) information theoretic

$Pr(x$ was the message $| e(x)$ crossed wire$)$

$= Pr(x$ was the message$)$

$\Rightarrow e(x)$ does not change inf

e.g. one-time pad

Alice, Bob share a random string r

Alice : $x \to e(x) = x \oplus r$

Bob : $e(x) \to d(e(x)) =$

$= e(x) \oplus r$

$= (x \oplus r) \oplus r = x$

$$\begin{array}{r} 0\,1\,1\,0 \oplus \\ 0\,1\,0\,1 \\ \hline 0\,0\,1\,1 \oplus \\ 0\,1\,0\,1 \\ \hline 0\,1\,1\,0 \end{array}$$

in $e(x)$ each bit is equally likely to be 0 or 1 $\Rightarrow$ no info

(2) RSA, computational.

from $e(x)$, x cannot be computed in $\leq 2^{50}$ ops

with prob. $1 - 2^{-100}$

problems with one-pad

$$e(x) = x \oplus r$$

reuse

$$e(y) = y \oplus r$$

$$e(x) \oplus e(y) = x \oplus r \oplus y \oplus r = x \oplus y$$

reuse the random string leaks info

↳ can only use once