HONORS ALGORITHMS | 2025-01-10

$N = 2^{18}$ $\qquad$ $k = 500$

X, Y : N-bit integers

initial zeros permitted

Q: $X \overset{?}{=} Y$ $\qquad$ cost: # bits communicated

p : random k-bit prime

RYS protocol

Alice : picks random k-bit prime p

Alice → Bob : $(X \bmod p)$

Bob: computes $(Y \bmod p)$

If $(X \bmod p) \neq (Y \bmod p)$

i.e., $X \not\equiv Y \bmod p$

Bob ANNOUNCES "$X \neq Y$"

else — " — "$X = Y$"

cost : $2k = 1000$ bits of communication

correctness : $(\forall X, Y)(\Pr(\text{error}) < 10^{-100})$

If $X = Y$ $\quad Pr(\text{error}) = 0$

If $X \neq Y$: case of error : $p \mid X - Y$

$$\boxed{\text{Claim} \quad Pr(\text{error}) < 10^{-100}}$$

Proof

$$Pr(\text{error}) = \frac{\# p \mid X-Y \text{ s.t. } p \leq 2^k}{\# \text{primes} \leq 2^k} = \circledast$$

HW $\quad m$: pos integer $\quad \nu(m) \leq \log_2 m$

$\nu(m)$: # distinct primes dividing m

\nu

e.g. $\nu(24) = 2$ $\quad 2, 3$

$\nu(1) = 0$

$$\circledast \leq \frac{\nu(X-Y)}{\pi(2^k)}$$

\pi

$\pi(m) = $ # primes $2 \ldots m$

PRIME NUMBER THM $\quad \pi(x) \sim \dfrac{x}{\ln x}$

i.e. $\quad \dfrac{\pi(x)}{x/\ln x} \to 1$ as $x \to \infty$

NOT EFFECTIVE

$\exists$ effective version "TRUST ME" $\quad \pi(2^k) > 0.8 \cdot \dfrac{2^k}{\ln(2^k)} > \dfrac{2^k}{k}$

$\boxed{\text{HW}}$ m pos. integer $\Longrightarrow \nu(m) \leq \log_2 m$

$$|X-Y| \leq 2^N \qquad \log_2 |X-Y| \leq N$$

$$\circledast \leq \frac{\nu(X-Y)}{\pi(2^k)} < \frac{N}{\frac{2^k}{k}} = \frac{k}{2^k} \cdot N$$

$$= \frac{500}{2^{500}} \cdot 10^{18} < \frac{500}{2^{500}} \cdot 2^{60} <$$

b/c $2^{10} > 10^3$

$$< \frac{2^9}{2^{500}} \cdot 2^{60} = \frac{1}{2^{431}} < \frac{1}{2^{400}} < \frac{1}{10^{120}} < 10^{-100} \checkmark$$

for the rest of this class

$$n \longrightarrow \infty$$

handouts
DM
ASY

DEF sequences (a_n) (b_n) are ASYMPTOTICALLY EQUAL

notation:
$$a_n \sim b_n \quad \text{if} \quad \lim_{n\to\infty} \frac{a_n}{b_n} = 1$$

DEF a predicate on set A is a function $f: A \to \{0,1\}$

R equivalence relation: binary relation s.t.

(i) reflexive
$(\forall a)(aRa)$

(ii) symmetric
$(\forall a,b)(aRb \Rightarrow bRa)$

(iii) transitive
$(\forall a,b,c)(aRb \wedge bRc \Rightarrow aRc)$

$\wedge$ AND

DEF A (binary) relation on a set A is a predicate on $A \times A$

$$R: A \times A \to \{0,1\}$$

$\boxed{\text{DO}}$ Examples of equivalence relations:

- A = set of triangles relation: similarity
- $A = \mathbb{Z}$ set of integers $m \in \mathbb{Z}$ fixed integer
  relation: congruence mod m

Is asymptotic equality of sequences of reals an <u>equiv. rel</u>?

<u>NO</u>

0, 0, 0, ... ← not reflexive
counterexample

1, 0, 0, 0, ...

1, 0, 1, 0, 1, ...

0 1 1 1 1 ...
not a counterexample

$a_n \not\sim a_n \iff$ the sequence (a_n) ...
has infinitely many zeros

<u>READ, SOLVE</u>

first few sections of ASY