

HONORS ALGORITHMS | 2025-01-10

(P1)

$$\underline{N = 2^{18}}$$

$$\underline{k = 500}$$

$X, Y : \underline{N\text{-bit integers}}$

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

p: random k-bit prime

initial
zeros
permitted

RYS protocol

Alice: picks random k-bit prime p

Alice \rightarrow Bob: $(X \bmod p)$

Bob: computes $(Y \bmod p)$

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

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

Bob ANNOUNCES " $X \neq Y$ "

else

- " -

" $X = Y$ "

cost: $2k = 1000$ bits of communication

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

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

P2

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

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

Proof

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

HW

$$m: \text{pos integer} \rightarrow \gamma(m) \leq \log_2 m$$

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

num

$$\text{e.g. } \gamma(24) = 2$$

$$\textcircled{*} \leq \frac{\gamma(X-Y)}{\pi(2^k)}$$

$$\pi(m) = \#\text{primes}_{2 \dots m}$$

$$\pi(x) \sim \frac{x}{\ln x}$$

PRIME NUMBER THM

$$\text{i.e. } \frac{\pi(x)}{x/\ln x} \rightarrow 1 \text{ as } x \rightarrow \infty$$

↑
NOT EFFECTIVE

Effective version "TRUST ME"

$$\pi(2^k) > 0.8 \cdot \frac{2^k}{\ln(2^k)} > \frac{2^k}{k}$$

HW

m pos. integers $\Rightarrow \nu(m) \leq \log_2 m$

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

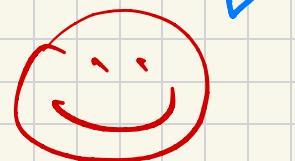
$$\log_2 |X - Y| \leq N$$

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

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

$$< \frac{2^4}{2^{500}} \cdot 2^{60} = \frac{1}{2^{431}} < \frac{1}{2^{400}} < \frac{1}{10^{120}} < 10^{-100}$$

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



for the rest of this class

$$n \longrightarrow \infty$$

handouts

DM

ASY

DEF Sequences (a_n) (b_n) are ASYMPTOTICALLY EQUAL

notation:

$$a_n \sim b_n \text{ if } \lim_{n \rightarrow \infty} \frac{a_n}{b_n} = 1$$

R equivalence relation:

binary relation s.t.

DEF a predicate

on set A is a

function $f: A \rightarrow \{0,1\}$

(i) reflexive

$$(\forall a)(aRa)$$

(ii) symmetric

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

(iii) transitive

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

AND

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

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

DO Examples of equivalence relations:

- $A = \text{set of triangles}$ relation: similarity

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

(PS)

Is asymptotic equality of sequences of reals an equiv. rel?

NO

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

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

0 1 1 1 ...
not a counterexample

$a_n \neq a_n \Leftrightarrow$ the sequence $(a_n) \dots$

has infinitely many zeros

READ, SOLVE

first few sections of ASY