# HONORS ALGORITHMS | 2025-01-08

COMP. TASK $f: D \longrightarrow K$

if $K = \{0,1\}$ Boolean
N/Y
F/T

often $D = \{0,1\}^N$ : (0,1)-strings of length $N$

COST $C(A, x)$

$x \in D$ input

$A$: algorithm

$|x|$ : size of input

Worst-case analysis of $A$: ① correctness ② complexity

$$C_A(n) = \max_{\substack{x \in D \\ |x| = n}} C(A, x)$$

sup

Complexity of $\underline{\underline{f}}$

$$C_f(n) = \min_A C_A(n)$$

Randomized algorithms

$A(x, \underline{r})$ — random string

Correctness:

$(\forall x \in D)\left(\Pr_{\underline{r}}(A(x, \underline{r}) = f(x)) \geq \frac{2}{3}\right)$

for all inputs

amplifying success:

repeat w indep. random strings

$\underline{m}$ times,

take majority vote

$\Rightarrow \Pr(\text{success}) > 1 - c^m$

$0 < c < 1$

# Communication complexity

Alice, Bob — processors w unlimited computational power

$X$ $\quad$ $Y$ strings $(0,1)$

$f(X,Y)$

$$A \longleftrightarrow B$$

cost : # bits communicated

---

Example from Monday:

$X, Y \in \{0,1\}^N$ $\quad$ $N = 10^{18}$

$$f(X,Y) = \begin{cases} 1 & \text{if } X = Y \\ 0 & \text{o/w} \end{cases}$$ identity fctn

M.S $\Longrightarrow$ $C_f = N$

lower bd

Divisibility: $a \mid b$   a divides b

if $(\exists x)(ax=b)$

4

$(a \bmod q) = t$

$q \neq 0$

if $0 \leq t \leq |q|-1$

and $q \mid a-t$

$0 \mid 0$ ? y

$x := 17$

$0 \cdot 17 = 0$

$(26 \bmod 7) = 5$

b/c
- $0 \leq 5 \leq 7-1$
- $7 \mid 26-5=21$

$26 = 3 \cdot 7 + \underline{\underline{5}}$

Notation: $a \equiv b \pmod{m}$

a is congruent to b modulo m

if $m \mid a-b$

Ex: $26 \equiv 5 \pmod{7}$

$26 \equiv 40 \pmod{7}$

$(a \bmod q) \equiv a \pmod{q}$

$26 \equiv -2 \pmod{7}$

Made with Goodnotes

# Rabin-Yao-Simon protocol

INPUT: N-bit numbers $X, Y$
QUESTION: $X \stackrel{?}{=} Y$

$k = 500$

Alice generates random k-bit prime $p$

$A \to B$ : $p$, $(X \bmod p)$

communication 1000 bits

Bob computes $(Y \bmod p)$

Bob returns NO if $(X \bmod p) \neq (Y \bmod p)$
YES o/w

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

**Case 1** $X = Y$ $\quad \Pr(\text{error}) = 0$

**Case 2** $X \neq Y$

error occurs if $X \equiv Y \bmod p$

i.e. $(X \bmod p) = (Y \bmod p)$

$\equiv$ $=$ $=$

**Q.** $\Pr(p \mid X-Y)$

$$= \frac{\#\text{ prime divisors of } X-Y \text{ that are } < 2^k \text{ (distinct)}}{\#\text{ all primes } < 2^k}$$

---

$\#$ primes $\leq x$ denoted $\pi(x)$

prime counting function

---

$\nu(x)$ : $\#$ distinct primes $\mid x$

---

**Obs** $\nu(x) \leq \log_2 x$ $\boxed{\text{DO}}$

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

PRIME NUMBER THM

asymptotic equality

$a_n \sim b_n$ if $\lim\limits_{n\to\infty} \frac{a_n}{b_n} = 1$