PROBLEM SESSION 2024-01-12

1.68 3^x has $\sim x \log_2 3 > 2^{n-1} \cdot \log_2 3 \sim c \cdot 2^n$

x has <u>n bits</u> $2^{n-1} \le x < 2^n$

NTS $(\forall c)(n^c = o(2^n))$

NTS $\lim_{n\to\infty} \frac{n^c}{2^n} = 0$ $c > 0$

$\lim_{x\to\infty} \frac{x^c}{2^x} = 0$

$\left(\frac{x}{2^{x/c}}\right)^c \to 0$

NTS $\frac{x}{2^{x/c}} \to 0$

$a = 2^{1/c} > 1$

$\lim \frac{x}{a^x} = \lim \frac{1}{\;}$

L'Hôpital

$a^x = e^{x \ln a}$

$(a^x)' = a^x \cdot \ln a$

$a_n = o(b_n)$ if

little-oh $\frac{a_n}{b_n} \to 0$

p large prime

Thm GRH $\Rightarrow$ smallest non-residue is $O((\log p)^2)$

$\longrightarrow$ "is x a quadr. residue mod p" in poly time

DET. try $1, 2, \ldots$

\# trials: $O((\log p)^2)$

$\times$ $(\log p)^c$ work testing

$O((\log p)^{c+2})$ ✓

RANDOMIZED target: $\Pr(\text{success}) \geq 1 - 10^{-6}$

$999 = 3^3 \cdot 37$

$1001 = 7 \cdot 11 \cdot 13$

Lemma $\Pr(x \in [p-1] \text{ is q. nonres.}) = \frac{1}{2}$

Do this 20 times indep. choices $\Bigg\} \Rightarrow \Pr(\text{failure}) = \frac{1}{2^{20}} < \frac{1}{10^6}$

$2^{20} = 1{,}048{,}576$

$2^{10} = 1024 > 10^3$

Fermat's little Theorem $\quad$ p prime

If $\gcd(a,p)=1$ then $a^{p-1} \equiv 1 \mod p$

find smallest composite p that satisfies FlT

$\mu(n)$: # prime factors with multiplicity $\quad \mu(24) = 4$
$\qquad 2\cdot2\cdot2\cdot3$

$k = \mu(m) \leq \log_2 m$

Proof: $\quad m = p_1 \cdots p_k \geq 2 \cdot \cdot 2 = 2^k$

$\log_2 m \geq k$ ✓

$\mu^*(m) = \max\limits_{t \leq m} \mu(t)$

Claim $\mu^*(2^n) = n$

① $\mu^*(2^n) \overset{?}{\geq} n$ b/c $\mu(2^n) = n$

② $\mu^*(2^n) \leq n$ i.e. $(\forall t \leq 2^n)(\mu(t) \leq n)$

2.30 $a_n, b_n > 1$

$a_n \sim b_n$ i.e. $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$

$\overset{?}{\Rightarrow} \ln a_n \sim \ln b_n$ ANS : <u>NO</u>

if $a_n, b_n \geq 1+c$ then ANS: YES

$\exists c>0$ s.t.

they are bounded away from 1

$a_n = e^{1/n}$ $b_n = e^{1/n^2} \longrightarrow 1$

$\frac{1}{n} \not\sim \frac{1}{n^2}$

$a_n = 1+\frac{1}{n}$ $b_n = 1+\frac{1}{n^2} \longrightarrow 1$

$\ln a_n \sim \frac{1}{n}$ $\ln b_n \sim \frac{1}{n^2}$

Lemma:
$\ln(1+x) \sim x$
as $x \to 0$

$c > 0$

$$\frac{a_n, b_n \geq 1+c \qquad a_n \sim b_n}{\text{NTS} \quad \ln a_n \sim \ln b_n}$$

$$\frac{\text{ASSN:} \quad \frac{a_n}{b_n} \to 1 \qquad a_n, b_n \geq 1+c}{\text{DC} \quad \frac{\ln a_n}{\ln b_n} \to 1}$$

desired conclusion

$$\ln\left(\frac{a_n}{b_n}\right) \to \ln 1 = 0$$

$$\ln a_n - \ln b_n \to 0$$

$$\left|\frac{\ln a_n}{\ln b_n} - 1\right| = \left|\frac{\ln a_n - \ln b_n}{\ln b_n}\right| \leq \frac{|\ln a_n - \ln b_n|}{|\ln(1+c)|} \to 0$$

positive const.

$$\therefore \frac{\ln a_n}{\ln b_n} \to 1 \quad \checkmark$$

2.33 $\quad \ln(n!) \sim\ ?$

$\leftarrow$ important for analysis of sorting by comparisons

$$\left(\frac{n}{e}\right)^n < n! < n^n$$

$$n \ln\left(\frac{n}{e}\right) < \ln(n!) < n \ln n$$

$$\underline{n(\ln n - 1)} < \ln(n!) < \underline{n \ln n}$$

but $\quad n(\ln n - 1) \sim n \ln n$

b/c $\quad$ quotient $= \dfrac{\ln n - 1}{\ln n} = 1 - \underbrace{\dfrac{1}{\ln n}}_{\downarrow\, 0} \longrightarrow 1$

by squeeze principle

$$\underline{\ln(n!) \sim n \cdot \ln n}$$

$a_n, b_n > 0$

$$a_n = O\left(2^{b_n}\right) \overset{?}{\not\Rightarrow} a_n = 2^{O(b_n)}$$

big - Oh

meaning: $a_n = 2^{c_n}$ where $c_n = O(b_n)$

meaning: $\boxed{|\log_2 a_n| = O(b_n)}$

ANS: <u>NO</u>

Example 1: $a_n = 2^{-n}$ $\quad b_n = 1$ $\quad |-n| \neq O(1)$

Example 2: $a_n = 2$ $\quad b_n = 1/n$ $\quad 1 \neq O(1/n)$

DMmini
ASY

} asymp. notation

$e_n = O(f_n)$ means $\exists C \, \exists n_0$
$(\forall n \geq n_0)\ (\ |e_n| \leq C|f_n|\ )$

$\cancel{a_n, b_n > 0}$ $a_n, b_n \geq c > 0$ (8)

$$a_n = \underset{\uparrow \text{ big-Oh}}{O\left(2^{b_n}\right)} \overset{?}{\not\Rightarrow} a_n = 2^{O(b_n)}$$

$a_n = 2^{c_n}$ $c_n = O(b_n)$

$c_n = \log_2 a_n$

ASSN $0 \underset{\text{YES}}{<} c \leq a_n \leq C \cdot 2^{b_n}$ DC $\boxed{|\log_2 a_n| = O(b_n)}$

① $a_n \geq 1$ $\log a_n \leq \underline{\log C} + \underbrace{b_n}_{\geq c} \leq (1+\varepsilon) \cdot b_n$

$\log C \leq \frac{\log C}{c} \cdot b_n$ where $\underbrace{c}_{\varepsilon}$

② $a_n < 1$ $|\log a_n| \leq |\log c| = O(b_n)$

b/c $c < a_n$

b/c $b_n \geq c$ ✓

BON 2.25

Alice : input X p $(X, Y \bmod p)$

Bob : Y p – " –

$X \not\equiv Y \bmod p$ i.e. $(X \bmod p) \not\equiv (Y \bmod p)$

Need to find i s.t. $X_i \neq Y_i$ ith bit

$2 < p < 2^k$ k bits

target complexity poly$(k, \log n)$

$A \to B$ $(X_0 \bmod p)$

$k+1$ bits of comm.

repeat $\log n$ times :

$(k+1)\log_2 n$ bits of comm.

$X = X_0 + 2^{\frac{n}{2}} X_1$ $Y = Y_0 + 2^{\frac{n}{2}} Y_1$

n bits $\underbrace{X_0}_{n/2}$, $\underbrace{X_1}_{n/2}$

If $\left.\begin{array}{l} X_0 \equiv Y_0 \bmod p \\ X_1 \equiv Y_1 \bmod p \end{array}\right\} \Rightarrow X \equiv Y \bmod p$

$\longrightarrow \longleftarrow$

binary search

$\frac{10}{1}$

$$f(n) \le 3 \cdot f\left(\frac{n}{2}\right)$$

(a) $f(n) = O(n^{\alpha})$ $\boxed{\alpha = \log_2 3}$ ≈ 1.58

(b) $f(n) = o(n^{\alpha})$ does not follow :

find $f(n)$ s.t. $f(n) \le 3 \cdot f\left(\frac{n}{2}\right)$

but $f(n) \ne o(n^{\alpha})$

$\frac{f(n)}{n^{\alpha}} \to 0$

Soln: $f(n) = n^{\alpha}$

$f(n) = 3f\left(\frac{n}{2}\right)$

$f(n) = 1$ wrong b/c $\frac{1}{n^{\alpha}} \to 0$

$$f(n) \le 3 f\left(\frac{n}{2}\right) \qquad f(1) = 1$$

$$\therefore \quad f(n) \le n^{\alpha}$$

and $f(n) = n^{\alpha}$ satisfies the conditions