CS170 cribsheet midterm1

Order of Growth

Formal

UpperBound O : LowerBound Ω : Constant Θ
$\frac{a(n)}{b(n)} > 0, a(n) \in \Omega(b(n))$ $\frac{a(n)}{b(n)} < c, a(n) \in O(b(n))$
$\frac{a(n)}{b(n)} = c, a(n) \in \Theta(b(n))$

Tricks

$7^{\log(n)^2} = (2^{\log(7)})^{(\log(n))^2} = (2^{\log(n)})^{\log(7)\log(n)} \approx n^{\log(n)}$
$n! = 2^{n\log(n)}$
Solve the comparison by integration.

Prove

Geom sum series: $g(n) = \frac{1-c^{n+1}}{1-c} = \frac{c^{n+1}-1}{c-1}$
Induction: $\gcd(F_{k+1}, F_{k+1}) = \gcd(F_{k+1}, F_{k+2} - F_{K+1}) = \gcd(F_{k+1}, F_k) = 1$
Numbers before prime $1/n$: in $O(n)$ time. Geom dist.$E[X] = \sum_{i=1}^{\infty} i * P[X = i] = \sum_{i=1}^{\infty} i * (1-p)^{(i-1)}p$
$p = probheads, i - 1 = tailsthrows$
$= p * dp/dt(\sum_{i=1}^{\infty} -(1-p)^i) \rightarrow_{sums} = -1/p$ Integrate:
$E[X] = p * (1/p^2) = 1/p$
Binary Search: if N is a square. Why only $\log n$ for power max? $N = q^k \rightarrow \log N = k \log \rightarrow k = \log N / \log q \leq \log N$

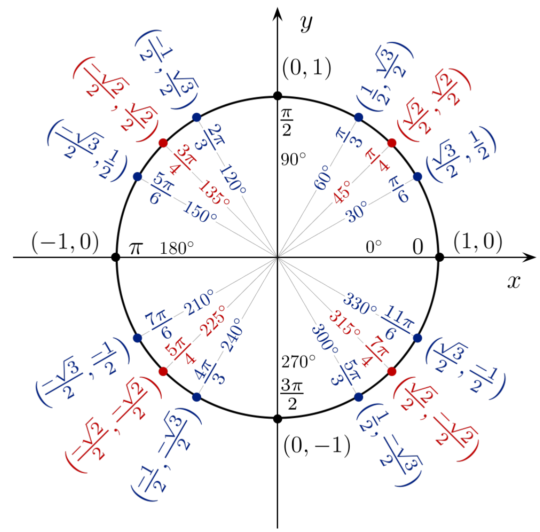
For any power: poweringoperation$\{\sum_{i=1}^{k} in * n = O(k^2 n^2)\}$
Repeat $\log n$ times to get $O(n^6)$

Modular Arithmetic

Quadratic residue busniess. Fermat's theorem
$\forall 1 \leq a < p : a^{p-1} \equiv 1 mod p$ if p is prime.
Multitudes:
$2013^{2014} = 3^{2012+2} = (3^{503})^4 * 3^2 = 1 * 3^2 = 4 all mod 5$
$2012^{2013} = 2^{2012+1} = (2^{503})^2 * 2^1 = 1 * 2 = 2 all mod 5$
$5^{170^{70}} mod 5$: take $170^{70} = 4s + t$ form
$170^{70} = (2 * 85)^{(2*35)} = (4 * 85^2)^{35} = 0 mod 4$
Worst RSA: We know N,e,d: $k = (ed-1)/(p-1)(q-1)$, limit k$\in 1, 2$ by $e = 3, d < (p-1)(q-1)$ Solve two eq system for p and q modulating k, use $N = pq$.
Randomize recoverable RSA w/ $(M^e * k^e)^d mod N = Mk mod N$ then multiply by k^{-1}

Divide and Conquer

Master's Theorem:
$T(n) = aT(n/b) + O(n^d), a > 0, b > 1, d \geq 0$
$O(n^d) \rightarrow d > \log_b a$ :: $O(n^d \log n) \rightarrow d = \log_b a$ ::
$O(n^{\log_b a}) \rightarrow d < \log_b a$
Majority Element: If there is a majority element then it will be a majority element of A_1 or A_2, , $O(n \log n)$. Or you could use the pairing-discard approach $T(n) = T(n/2) + O(n) = O(n)$
Closest pair of points: ugh...



Complex number practice: $\omega = e^{2\pi i/8} = \sqrt{2}/2 + i\sqrt{2}/2$
$\omega^7 = e^{2\pi i(7/8)} = \sqrt{2}/2 - i\sqrt{2}/2 = \omega^{-1}, \omega^7 + \omega = \sqrt{2}$
$p(x) = x^2 + 1, p(\omega) = 1 + i, p(\omega^2) = 0, p(\omega^3) = 1 - i$

2013 Zack Field