Example 2: Greatest Common Divisor

- Best case:
  1. When does the best case happen?
     when $\gcd(a,b) = \min(a,b)$
  2. What is $C_{best}(n)$? $C_{best}(n) = 1$

- Average case:
  1. Assumptions:
     - Assume that a and b are two randomly chosen integers
     - Assume that all integers have the same probability of being chosen
     - **hint**: The probability that an integer d is a and b's greatest common divisor is $P_{a,b}(d) = \frac{6}{\pi^2 d^2}$
  2. When does the average case happen?
     when K and A satisfy our assumptions
  3. What is $C_{avg}(n)$?
     Let us denote $n = \min(a,b)$
     $C_{avg}(n) = 1 \cdot P_{a,b}(n) + 2 \cdot P_{a,b}(n-1) + \cdots + (n) \cdot P_{a,b}(1)) =$
     $\frac{6}{\pi^2}(\frac{1}{n^2} + \frac{2}{(n-1)^2} + \cdots + \frac{n}{1^2})$
     (when $n = 10$,
     $(\frac{1}{100} + \frac{2}{81} + \frac{3}{64} + \frac{4}{49} + \frac{5}{36} + \frac{6}{25} + \frac{7}{16} + \frac{8}{9} + \frac{9}{4} + 10) \cdot (6/\pi^2) = 8.58300468)$

Question: what is the tightest upper bound of C_avg(n)? is it O(n), O(n^2) or O(nlogn) and why?

Useful Property

1. $f(n) \in O(f(n))$

   Proof. □

2. $f(n) \in O(g(n))$ if and only if $g(n) \in \Omega(f(n))$

   Proof. □

3. $f(n) \in O(g(n))$ and $g(n) \in O(h(n))$, then $f(n) \in O(h(n))$

   Proof. □

4. $f_1(n) \in O(g_1(n))$ and $f_2(n) \in O(g_2(n))$, then $f_1(n) + f_2(n) \in O(\max\{g_1(n), g_2(n)\})$

   Proof. □

Orders of growth of some important functions

1. All logarithmic functions $\log_a n$ belong to the same class $\Theta(\log n)$ no matter what the logarithm's base $a > 1$ is

   Proof. □

2. All polynomials of the same degree k belong to the same class: $a_k n^k + a_{k-1} n^{k-1} + \cdots + a_0 \in \Theta(n^k)$

   Proof. □

3. Exponential functions a^n have different orders of growth for different a's, i.e., $2^n \notin \Theta(3^n)$

   Proof. □

4. order $\log n <$ order $n^{a>0} <$ order $a^n <$ order $n! <$ order n^n