Anooj Pai
Intro to Algo HW2
Collaborators: Shawn Vembenil

1) Give an algorithm (pseudo code, with explanation) to compute 2^{2^n} in linear time, assuming multiplication of arbitrary size integers takes unit time. What is the bitcomplexity if multiplications do not take unit time, but are a function of the bit-length.

```
Def function(n):
        i = 0
        tot = 2

        While (i < n) {
                Tot *= tot
                i++

        return tot
```

This algorithm iterates the exponent by 1 each loop and only has 1 loop so the cost is n. When n is increased the cost becomes n*1 which still results in n so it is linear.

<u>Because the multiplications don't take unit time, we can say that the cost of each one is f(i+1). Because each iteration is just multiplying by itself, we find that the cost is f(i+1)+(Cost of iteration). This simplifies down to the summation:</u>

$N + \sum_{i=1}^{N} f(i + 1)$.

2) Consider the problem of computing N! = 1 · 2 · 3···N.

(a) If N is an n-bit number, how many bits long is N! in O() notation (give the tightest bound)?

$log_2(n!) = log_2(n * (n - 1) * ... * (n - (n - 1))) = log_2(n) + log_2(n - 1) +... log_2(1)$

Since $log_2(n!) = log_2(n * (n - 1) * ... * (n - (n - 1)))$

and $log_2(n!) < log_2(n) + log_2(n - 1) +... log_2(1)$

We find that $log_2(n!) = O(nlogn)$

<u>Number of bits of n! is O(nlogn)</u>

(b) Give an algorithm to compute N! and analyze its running time.

```
Factorial(n):
        if(n == 0): return 1
        Factorial = 1
        for(i in range(n+1)):
                Factorial *= i

        return(Factorial)
```

<u>Because the algorithm only has 1 for loop the run time is O(n)</u>

3) Find the GCD of 1492 and 1776, using

a) the prime factorization method and using Euclid's method, and

<u>Prime Factorization:</u>

1492 Primes: 2*2*373
1776 Primes: 2*2*2*2*3*37

The common factors of the numbers are 2 so we multiply them and get 4

<u>So GCD(1492,1776) = 4</u>

<u>Euclid’s Method:</u>

1776 = 1*1492+284
1492 = 5*284+72
284 = 3*72+68
72 = 1*68+4
68 = 4*17

<u>GCD(1492,1776) = 4</u>

b) express the GCD as an integer linear combination of the two inputs.

We found that the GCD(1492,1776) = 4

We use the equation from above to work backwards:

72 = 1*68+4

Then we solve 284 = 3*72+68 for 68 and substitute it into 68 for the equation above

4 = 72 - 1 * (284 - 3*72)
  = 72*4-284

Now we solve 1492 = 5*284+72 for 72 and sub it into the above equation

4 = (1492 - 5 * 284) * 4 - 284
  = 1492 * 4 - 21 * 284

For the last step we solve 1776 = 1492 + 284 for 284 and sub it into the equation above

4 = 1492 * 4 - 21(1776-1492)
  = -21 * 1776 + 25 *1492

<u>The linear combination is -21 *1776 + 25 *1492</u>