1. (i) Roughly, how many numbers less than or equal to 1000 are prime?

   (ii) Roughly, what is the probability that an integer in `[1 ... 1000]` is prime?

   (iii) Exactly, how many numbers less than or equal to 1000 are prime?

   (iv) Exactly, what is the probability that an integer in `[1 ... 1000]` is prime?

   (v) Using the Miller-Rabin algorithm from class, you randomly pick 1000 bit numbers until you find one that is probably prime. On average, how many picks do you make before you find a probable prime?

2. Show the recursive calls, in order made, from `Karatsuba(1752,3946)`. Assume the decimal version of the algorithm, and that a recursive call is made only when the first parameter is at least 11.

3. Sort the following functions by increasing Θ order of complexity.

   $n^{2.5}$

   $n^{1.01}$

   $n + 200$

   3^n

   $n^{.5}$

   $n^{2/3}$

   $9n + (\lg n)^3$

   2^{n+1}

   $\lg(3n)$

   $\ln(n^5)$

   $100n + \lg n$

   $n \lg^3 n$

   $5^{\lg n}$

   $n2^n$

   2^n

   $n + 100$

solutions

1. (i) about $1000/(\ln 1000 - 1) \approx 169$

   (ii) about .169

   (iii) run a prime checker and count: 168

   (iv) $168/1000 = .168$

   (v) The probability that a 1000 bit number is prime is roughly $p = 1/(\ln(2^{1000}) - 1) \approx .0014\ldots$. So the average number of picks is $1/\mathrm{p} \approx 692$ if all possible numbers are considered. But the algorithm only considers odd numbers, so the average number of picks is 1/2 this, so ≈ 346.

2.
```
K(1752,3946)
    K(17,39)
        K(1,3)
        K(7,9)
        K(8,12)
    K(52,46)
        K(5,4)
        K(2,6)
        K(7,10)
    K(69,85)
        K(6,8)
        K(9,5)
        K(15,13)
            K(1,1)
            K(5,3)
            K(6,4)
```

3.

$\ln(n^5)\ \lg(3n)$	$\in \Theta(\log n)$
$n^{.5}$	$\in \Theta(n^{.5})$
$n^{2/3}$	$\in \Theta(n^{2/3})$
$n{+}100\ n{+}200\ 9n{+}(\lg n)^3\ 100n{+}\lg n$	$\in \Theta(n)$
$n \lg^3 n$	$\in \Theta(n \log^3 n)$
$n^{1.01}$	$\in \Theta(n^{1.01})$
$5^{\lg n}$	$\in \Theta(n^{\lg 5}) = \Theta(n^{2.32\ldots})$
$n^{2.5}$	$\in \Theta(n^{2.5})$
$2^n\ 2^{n+1}$	$\in \Theta(2^n)$
$n2^n$	$\in \Theta(n2^n)$
3^n	$\in \Theta(3^n)$