CS 212 **DUE: Thursday, March 7 at 11:59 PM**
Spring 2019
Assignment 2
2/26/2019 **10 points**

Introduction: This assignment will give you practice doing proofs (direct and indirect).

This is an individual effort homework assignment. You must write up your solutions in LaTeX. Use the `a2.tex` template that I provide and be sure to replace each "Put your answer here." with your answers but leave everything else alone. Your solutions must be written up in a clear, concise and rigorous manner.

When you are done, zip up your .TEX file and corresponding .PDF file. Upload your .ZIP file to the **a2** dropbox on d2l. After you have uploaded the file, double-check to ensure your file was uploaded correctly. It is your responsibility to ensure your submission was done correctly. Assignments that are not uploaded correctly are worth 0 points.

YOU MUST USE THESE DEFINITIONS FOR THIS ASSIGNMENT: We say that a *prime* number is a positive integer greater than 1 that is divisible only by 1 and itself. A number greater than 1 that is not prime is called *composite*. Moreover, a positive integer d is said to *divide* another non-negative integer q, if and only if there exists an integer e, such that, $1 \leq e \leq q$ and $d \cdot e = q$.

1. (4 points) Consider the following statements:

   1. For all positive integers p, if p is prime and $p+2$ is prime, then $p+1$ is divisible by 6.
   2. For all positive integers q, if q is not prime, then $q = 1$, or there exist positive integers d and e, such that $1 < d, e < q$ and $d \cdot e = q$.

   Exactly one of the previous statements is true and the other is false.

   (a) (2 points) Prove the one that is true, using a direct proof.

   Starting with statement 2: Let q be an arbitrary positive integer. Now let's consider all possible values of q. First of all, we must assume from the first part of the implication that q is not prime. If q is 1, then the statement is true, as it makes the conclusion of the implication true. Now let's assume q is not prime or 1, making it composite. If it is composite, then there would exist positive integers d and e, both of which are greater than 1 (which follows from above), less than q (which follows from the previous statement), and multiply together to equal q. Therefore, statement 2 is true because no matter the value of q, the truth value of the overall statement is never false. □

   (b) (2 points) Disprove the one that is false, by giving the smallest possible counter example.

   Statement 1 states that between every pair of twin primes, there exists a number which is divisible by 6. This is true for *nearly* every twin prime. There is, however, one exception: 3 and 5. Here is a pair of twin primes (3 is prime and 3+2 is prime), but the number between them is 4. Since 4 is not divisible by 6, statement 1 is false. □

2. (6 points) The following is a method that may or may not correctly compute whether a given `int` is composite, depending on whether the `for` loop was coded correctly:

```
public static boolean isComposite(int q) {
  if (q == 1 || q == 2)
     return false;
  if (q % 2 == 0)
     return true;
  int stop = (int)Math.sqrt(q);
  for (int i = 3; i <= stop; i += 2)
    if (q % i == 0)
      return true;
  return false;
}
```

Note that the above method only searches for possible divisors of `q`, starting with 2 and going up to – and including – the square root of `q`. If it finds such a divisor, then `true` is returned, because, in such a case, `q` must be composite. Otherwise, if no divisors of `q` were found, or `q` is 1, then `false` is returned.

Is the `isComposite` method correct? After all, what if the loop terminates too soon? What if `q` has a divisor that is greater than `Math.sqrt(q)` and the loop terminates before finding it, erroneously reporting that the the given `q` is not composite?

(a) (3 points) Prove that this situation can never happen, i.e., prove the following statement:

For all positive integers q, if q is composite, then there exists a positive integer d, such that, d divides q, and $1 < d \leq \sqrt{q}$.

You must use an **indirect proof** to prove the previous statement. You must give a detailed proof, where every step follows directly from the previous step.

Start by assuming that q is composite. From the definition of composite, we know that q can be broken down into two factors a and b such that $a * b = q$. Now we assume, for the sake of contradiction, that there are no positive integer divisors of q both greater than 1 and less than or equal to $\sqrt{q}$. Since we are restricted to the set of all positive integers, neither factor can be less than 1, and neither factor can be equal to one, as that would not prove q to be composite. Because of this, both of these factors must be greater than the square root of q such that $a > \sqrt{q}$ and $b > \sqrt{q}$. This way, we must check for values higher than $\sqrt{q}$ when proving a number to be composite. However, if this were the case, then $a * b$ would be greater than q (since $a * b$ would be greater than $\sqrt{q}^2$). Since this contradicts our original assumption that $q = a * b$, one of q's factors must be smaller than its square root, or $a = b$ and they are both equal to the square root. Therefore, a number can be proved to be composite if it has at least one factor less than or equal to its square root other than 1. □

(b) (2 points) If you change the `<=` to `<` in `isComposite`, then will the method still be correct? Either way, justify your answer.

If the <= were changed to a < in the program, it would not be accurate. The above theorem states that all numbers up to the square root must be checked. If the square root itself is not accounted for, the theorem above does not apply. An example of this would be 4, because the only factor of 4 other than 1 and itself is 2, which *is* the square root of 4.

(c) (1 point) Disprove the following statement:

For all positive integers q, if q is composite, then for every positive integer d, if $1 < d \leq \sqrt{q}$, then d divides q.

Justify your answer.

To disprove this statement, since it utilizes a universal quantifier, then a simple counterexample can be presented. Let $q = 16$ (a composite number). The square root of q would then be 4. According to the above statement, d may equal 3. 3 does not evenly divide the composite number q, but is greater than 1 and less than or equal to 4 (the square root of q). Therefore, the above statement is false. □