Math 300 Assignment 6

PROBLEMS: 6.37b, 7.1, 7.2, 7.6, 7.8, 7.9, 7.11, 7.17(b), 7.20, 7.30(b)

1. Let p be a prime.
   Prove that if $p = 3m + 1$ for some integer m, then m is must be even.
   (This fact implies that such a prime p must also be of the form $p = 6n + 1$.)
2. Complete TWO of the exploratory problems on the following pages.

The problems above are DUE WEDNESDAY, March 9th at lecture or during office hours.

HOMEWORK NOTES/HINTS

- **Problem 6.37b**: Use induction on n and during the inductive step you will need to make use of the binomial theorem (and part (a)).
- **Problem 7.6**: "The ones digit of a number in the base 8" = "the smallest positive remainder when the number is divided by 8". So you need to figure out what $9^{100} \equiv ??? \pmod 8$, $10^{100} \equiv ??? \pmod 8$, and $11^{100} \equiv ??? \pmod 8$ (each answer should be either 0, 1, 2, ..., or 7).
- **PROBLEM 7.17(b)**: Any number, n, must be in one of six congruence classes modulo 6. Show that the theorem is true for all six cases.
- **1**: Try an indirect proof.
- The challenge problems are not due, but I will award at least 1 point of extra credit per challenge problem correctly completed.
  CHALLENGE PROBLEMS: 6.51, (and each additional exploratory problem completed)

Math 300 Exploratory Problems

Complete TWO of the following four "exploratory" problems.
(1 extra credit point for each additional exploratory problem completed)

I Define the function $\pi(x) : \mathbb{R} \Rightarrow \mathbb{N} \cup \{0\}$ by $\pi(x)$='the number of primes less than or equal to x'. So for example $\pi(2) = 1$, $\pi(4) = 2$, $\pi(7) = 4$, and $\pi(10) = 4$ (because 2, 3, 5, and 7 are all the primes less than 10).

It has been proven (called the prime number theorem), that $\pi(x)$ is 'approximately the same' as the formula $\frac{x}{\ln(x)}$ as x gets larger. To prove this requires tools well beyond the scope of this course. However, we can get some information in this direction. In the following parts of this problem, I guide you through a proof that

$$\text{For } n \in \mathbb{N}, \pi(2n) - \pi(n) < 1.3863\frac{n}{\ln(n)}.$$

1. Compute the values of $\pi(20)$, $\pi(40)$, and $\pi(80)$ (by listing out the primes).
2. Let $n \in \mathbb{N}$. If p is a prime with $n < p \leq 2n$, then explain why p must divide $\binom{2n}{n}$.

   (Look at the numerator and denominator of the formula for $\binom{2n}{n}$.)
3. From the previous part, we know that $\prod_{n<p\leq 2n} p \mid \binom{2n}{n}$ (where the p's are primes). Give the justification for each steps below (each step follows from definitions, previous parts, or from facts earlier in the term):

$$\begin{aligned} &(1) \quad n^{\pi(2n)-\pi(n)} && = \prod_{n<p\leq 2n} n \\ &(2) && \leq \prod_{n<p\leq 2n} p \\ &(3) && \leq \binom{2n}{n} \\ &(4) && < 2^{2n}. \end{aligned}$$

   Thus, $n^{\pi(2n)-\pi(n)} < 2^{2n}$ which implies (by algebraic manipulations) that $\pi(2n) - \pi(n) < (2n)\ln(2)/\ln(n) < \frac{1.3863n}{\ln(n)}$. This tells us that the number of primes between n and $2n$ must be less than $1.3863n/\ln(n)$.
4. Verify this fact for $n = 40$, that is compute $\pi(80) - \pi(40)$ and $1.3863\frac{n}{\ln(n)}$ at $n = 40$ (is the correct one bigger).
5. What does the formula tell you about the number of primes between 1,000,000 and 2,000,000?

II (Introduction to Number-Theoretic Functions) This problem will introduce three of the most fundamental functions in number theory. Define the functions τ, σ and ϕ from $\mathbb{N}$ to $\mathbb{N}$ by:

$$\begin{aligned} \tau(n) &= \text{ the number of divisors of } n = \textstyle\sum_{d|n} 1 \\ \sigma(n) &= \text{ the sum of the divisors of } n = \textstyle\sum_{d|n} d \\ \phi(n) &= \text{ the number of positive integers less than, and relatively prime to, } n \end{aligned}$$

As an example for the number 12, these functions evaluate to

$\tau(12) = 6$ (there are 6 divisors of 12 namely 1, 2, 3, 4, 6, 12)
$\sigma(12) = 28$ (the sum of the divisors of 12 is 1+2+3+4+6+12)
$\phi(12) = 4$ (the numbers a=1, 5, 7, 11 are the only numbers less than 12 such that $\gcd(a, 12) = 1$.)

All three of these functions are multiplicative meaning that $f(ab) = f(a)f(b)$ when $\gcd(a, b) = 1$ (we will not prove this). Thus, if we can factor n, then we can compute $f(n)$ by first computing the value for each prime factor.

1. The formula for prime powers, p^e, for each function is (these formulas only work when p is a prime and e is a positive integer):

$$\tau(p^e) = e + 1, \quad \sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}, \quad \phi(p^e) = p^e - p^{e-1}.$$

   Verify these formula by computing $\tau(n)$, $\sigma(n)$ and $\phi(n)$ for $n = 3$, $n = 3^2$ and $n = 3^3$. (That is, compute the values using the definition (*i.e.* listing out the divisors and the numbers relatively prime to n) and then compute the values with the formula and to see that you get the same thing).

2. Since the functions are multiplicative, if $n = \prod_{i=1}^{k} p_i^{e_i}$ is the prime factorization of n, then $\tau(n) = \prod_{i=1}^{k} \tau(p_i^{e_i})$, $\sigma(n) = \prod_{i=1}^{k} \sigma(p_i^{e_i})$, and $\phi(n) = \prod_{i=1}^{k} \phi(p_i^{e_i})$.
   Use this to compute $\tau(n)$, $\sigma(n)$ and $\phi(n)$ for $n = 500 = 2^2 5^3$ (that is compute the values for 2^2 and then for 5^3 and multiply to get the answers).

3. How many divisors does $n = 34650$ have?
   What are the sum of the divisors of $n = 8128$ (this is a perfect number, you can read about them in the next problem part (d))?
   How many positive integers are less than 980 and relatively prime to 980?

III (Discussion of Three Unsolved Problems) This problem will introduce three unsolved problems from number theory.

1. (Twin primes) If p and $p + 2$ are primes, then they are called twin primes. An unsolved problem is the following: Are there infinitely many twin primes? Here are a couple tamer questions:
   (a) Find the first 5 twin primes.
   (b) Prove that if p and $p+2$ are twin primes and $p > 3$, then 12 divides their sum, $p+(p+2)$. (Hint: Think about the possible remainders when a prime, $q > 3$, is divided by 6.).
2. (Goldbach's Conjecture) An unsolved problem is the following:
   Is every even number, $m = 2n > 2$, the sum of two primes? Here are a few that have been solved.
   (a) Find all the ways to write 40 as the sum of two primes.
   (b) Explain why Goldbach's Conjecture is equivalent to the conjecture:
   Every positive integer, $n > 1$, is the average of two primes?
3. (Fermat's Last Theorem) If n is an integer bigger than 2, then there are no positive integers a, b and c that satisfy the equation $a^n + b^n = c^n$. Fermat wrote that he had a short proof for this in 1637, but never gave his proof. It went on to be a great unsolved problem until Andrew Wiles gave a proof, to quite a bit of fanfare, in 1993 (with final corrected paper in 1995).
   (a) For $n = 2$, solutions to this equation are called Pythagorean Triples. Give two triples of positive numbers a, b and c such that $a^2 + b^2 = c^2$. (Fermat's Theorem says this is impossible for $n > 2$.)
   (b) A solution (a, b, c) to $a^n + b^n = c^n$ is called *primitive* if $\gcd(a, b) = 1$, $\gcd(a, c) = 1$, and $\gcd(b, c) = 1$ (in other words, a, b and c are all relatively prime to each other). Prove that if $x, y, z \in \mathbb{N}$ with $x^n + y^n = z^n$ and $\gcd(x, y) = d$, then $a = x/d$, $b = y/d$ and $c = z/d$ are all integers and (a, b, c) is a primitive solution to $a^n + b^n = c^n$.

IV (Discussion of Two More Unsolved Problems) Here are two more unsolved problems

1. (One more than a Square) An unsolved problem is the following: Are there infinitely many primes of the form $n^2 + 1$ for some integer n? Try solving these instead.
   (a) Find the first 5 such primes.
   (b) Prove that if $n^2 + 1$ is an odd prime, then n must be even. (Try the contrapositive)

2. (Perfect numbers) A perfect number is a positive integer such that the sum of its proper divisors (divisors not including n) equals itself (that is, $\sigma(n) - n = n$ or simply $\sigma(n) = 2n$). For example, the divisors of 6 are 1, 2, 3, and 6 and the sum of the proper divisors is 1+2+3=6. These numbers held mystical/religious importance to the ancient Greeks. An unsolved problem is the following: Are there any odd perfect numbers? Here is a couple related problems:
   (a) The number 6 is the smallest perfect number. Find the next smallest perfect number. (You won't have to go past 30. To find the third smallest would take longer unless you used part (b)).
   (b) By listing and summing the divisors, prove if $2^n - 1$ is a prime number for some $n \in \mathbb{N}$, then $m = 2^{n-1}(2^n - 1)$ is a perfect number.

   Hint 1: If it helps try listing, organizing and summing the divisors for $6 = 2^1(2^2 - 1)$, then do the same for the example you found in part (a). Then see if you can find a general reason that all the proper divisors of $2^{n-1}(2^n - 1)$ sum to $2^{n-1}(2^n - 1)$.

   Hint 2: You will likely want to use the geometric series at some point. If you are unfamiliar with this series or if you have forgotten it, the geometric series is given by

$$\sum_{k=0}^{m} q^k = \frac{1 - q^{m+1}}{1 - q},$$

   so in particular, $1 + 2 + 4 + \cdots + 2^m = \frac{1-2^{m+1}}{1-2} = -(1 - 2^{m+1}) = 2^{m+1} - 1$.

   Aside: It was conjectured by Euclid that all perfect numbers are of this form and it is still unknown if he is right. It is known that all even perfect numbers are of this form, but it is not known if there are any odd perfect numbers. If you could just find one example of an odd perfect number you would answer this questions and become famous, in the mathematical community.