MATH 124, PROBLEM SET 1

Due: 12:00PM, September 12, 2014.
Note: Collaboration is permitted and encouraged. We only ask that you write up your solutions independently, and list your collaborators on your problem sets. Hard copies typed in TEX are preferred. Please separate your submissions as indicated below.

For Hirsh Jain

The Euclidean algorithm is possible in the integers $\mathbb{Z}$ because they form a *Euclidean domain*. Other examples include the Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ and the (ring of) polynomials with rational coefficients $\mathbb{Q}[X]$.

1.) Use the Euclidean algorithm to find $\gcd(3058011, 979578)$.

2.) Use the Euclidean algorithm to find $\gcd(7469, 2464)$. Then, substitute backwards to find integers x, y such that $7469x + 2464y = \gcd(7469, 2464)$.

3.) Show that $\frac{55n+7}{22n+3}$ is in lowest terms for all $n \in \mathbb{Z}$.

What makes the Euclidean algorithm possible is the existence of 'division' in Euclidean domains like $\mathbb{Z}$, which is encapsulated by the following result:

4.) Let $a, b \in \mathbb{Z}$, with $b \neq 0$. Prove that there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.

(**Hint:** Consider the set $\{a - kb \mid k \in \mathbb{Z}\}$. Show that its smallest non-negative element is r.)

A useful concept is the *p-adic order* of a number (where p is prime), which we denote $\nu_p(n)$. It is the largest exponent a such that $p^a \mid n$. Intuitively, it is p's exponent in n's prime factorization.

5.) Recall that the GCD is the largest number that divides both a and b, and that the LCM is the smallest number that both a and b divide.

(a) Prove that $\nu_p(\gcd(a, b)) = \min(\nu_p(a), \nu_p(b))$ for any prime p.

(b) Prove that $\nu_p(\mathrm{lcm}(a, b)) = \max(\nu_p(a), \nu_p(b))$ for any prime p.

(c) Conclude that $ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$.

For Julian Salazar

We learned about the largest known prime in class. It is of the form $2^p - 1$, with p prime. Primes of this form are called *Mersenne primes*. We distinguish this form because of the following result:

6.) Prove that if $a^n - 1$ is prime with $n > 1$, then $a = 2$ and n is prime.

Now, a quick exercise in divisibility:

7.) Describe all $n > 1$ such that $n \mid (n - 1)!$.

Finally, use congruences to solve these last few problems:

8.) Let n be odd. What are the possible remainders when n^2 is divided by 8?

9.) What is the last digit of 3^{4^5}?