Math 4400 Homework 6
Due: Wednesday, July 5th, 2017

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. (5 points) Let R be a ring and let $r \in R$. Show that $(-1_R) \cdot r = -r$. In other words, show that $(-1_R) \cdot r + r = r + (-1_R) \cdot r = 0_R$.

2. (10 points) Let ω be a quadratic rational. Prove that $\mathbb{Q}[\omega]$ is a field. (Hint: First prove that $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{D}]$ for some $D \in \mathbb{Q}$, and then prove $\mathbb{Q}[\sqrt{D}]$ is a field by "rationalizing the denominator" like we did in class)

3. (a) (10 points) Prove that there are infinitely many prime numbers congruent to 2 modulo 3. Hint: proceed by contradiction. Suppose that $S = \{p_1, p_2, \cdots, p_s\}$ is the set of all primes congruent to 2 modulo 3, aside from 2. Consider the number $m = 3p_1p_2 \cdots p_s + 2$. Show that m is divisible by a prime congruent to 2 modulo 3, but that at the same time m is not divisible by 2 nor by any element of S.
   (b) (2 points) What happens if we try to use the same method to prove there are infinitely many primes congruent to 1 modulo 3? What goes wrong?

4. (a) (5 points) Find the inverse of $5 + 4i$ in $\mathbb{Z}[i]/7\mathbb{Z}[i]$
   (b) (5 points) Find the inverse of $1 + 2\sqrt{6}$ in $\mathbb{Z}[\sqrt{6}]/7\mathbb{Z}[\sqrt{6}]$.
   (c) (2 points) Is $2 + 6\sqrt{5}$ invertible in $\mathbb{Z}[\sqrt{5}]/11\mathbb{Z}[\sqrt{5}]$? Why or why not?

5. (a) (5 points) Let k be a field of characteristic 0. For all $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ in $k[X]$, define the derivative of $f(X)$, denoted $f'(X)$, as $(n \cdot a_n)X^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + (2a_2)X + a_1$. Prove that, if $f'(X) = 0$, then $f(X) = c$, for some $c \in k$.
   (b) (5 points) Show, by example, that this is not necessarily true if char $k \neq 0$.

6. (a) (5 points) What are all the elements of $(\mathbb{Z}[i])^\times$?
   (b) (5 points) Prove that the groups $(\mathbb{Z}[i])^\times$ and $\mathbb{Z}/4\mathbb{Z}$ are isomorphic

7. (5 points) Use the Lucas-Lehmer test to show that M_{11} is not prime.

Extra credit

8. (10 points (bonus)) Prove that $\mathbb{Z}[\sqrt{2}]/5\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]/5\mathbb{Z}[\sqrt{3}]$ are isomorphic as rings.

9. (10 points (bonus)) Let F be a field of characteristic 0. Show that F contains a subring isomorphic to $\mathbb{Q}$

10. (10 points (bonus)) Use the Lucas-Lehmer test to determine which of the following Mersenne numbers are prime: M_{19}, M_{23}, and M_{31}