MATH 152: PROBLEM SET 1

DUE OCTOBER 2

1. Recall the set $\mathcal{S} = \{a + b\sqrt{-5} : \quad a, b \in \mathbb{Z}\}$ used in class to show that unique factorization can fail sometimes. This exercise justifies the steps left unproved in class.

(i) Show that $\mathcal{S}$ is a group under addition. (This is easy and the main point is to remind you of the definition of a group. If you don't know what a group is, just google it!)

(ii) Show that $\mathcal{S}$ is closed under multiplication: that is, the product of any two elements from $\mathcal{S}$ is also in $\mathcal{S}$.

(iii) For an element $a + b\sqrt{-5}$ of $\mathcal{S}$ define the "norm" $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Show that for any two elements α, $\beta \in \mathcal{S}$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$. Show that the norm of any non-zero element is at least one. What are the elements in $\mathcal{S}$ of norm 1? What are the elements of norm 2 and norm 3?

(iv) Say that an element $\alpha \in \mathcal{S}$ is prime if $N(\alpha) > 1$ and α cannot be written as $\beta\gamma$ with $N(\beta)$ and $N(\gamma)$ both > 1. Prove that 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all primes.

(v) Explain why our proof of unique factorization for integers fails for the set $\mathcal{S}$. What goes wrong with the division algorithm, Euclidean algorithm ...?

2. Irrational numbers. The following are in ascending order of difficulty: although the last part contains all others you may want to do the parts in order to get an idea of how to prove that.

(i) Show that $\sqrt{p}$ is irrational for any prime p.

(ii) Show that $\sqrt{n}$ is irrational unless n is the square of an integer.

(iii) Suppose α is a solution to the polynomial equation $x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0$ where $a_1, \ldots, a_n$ are integers. Show that either α is an integer or α is irrational.

3. Show that $n|(n-1)!$ for all composite integers $n > 4$. (A natural number is called composite if it is not a prime.)

4. Prove that $a|bc$ if and only if $\frac{a}{(a,b)}|c$.

5. The n-th Fermat number is $F_n := 2^{2^n} + 1$. If $m > n$ show that F_n divides $F_m - 2$. Conclude that any two different Fermat numbers are coprime. Use this observation to give another proof that there are infinitely many primes.

6. If 100! were written out in the ordinary decimal notation, how many zeros in a row would there be at the right end?