18.786 Problem Set 1 (due Thursday Feb 11)

1. Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square. (Hint: use "descent" in the sense of Fermat).

2. Give an alternative proof of the structure theorem for modules over a PID A, as follows:

   (a) Show that A is Noetherian as an A-module, and that any finitely generated module M over A is Noetherian. (Hint: Show that if N is a submodule of a module M, then M is Noetherian iff both N and M/N are).

   (b) Now let M be a finitely generated free module over A and N a non-zero submodule. Write a (finite) set of generators of N over A as linear combinations of some fixed basis of M, and so as row vectors of a $q \times n$ matrix G. Argue that invertible row and column operations are permitted (i.e. left or right multiplying G by invertible matrices). (Hint: these should correspond to permissible change of bases/generators for M or N).

   (c) Show that using these operations, you can ensure that the top left entry of the matrix is the gcd of all the entries of the matrix. Use it to clear the first row and column, and induct.

3. Let p be a prime. How many irreducible polynomials of degree n are there in the polynomial ring $\mathbb{F}_p[t]$? (Hint: group the elements of $\mathbb{F}_{p^n}$ by their minimal polynomials, count and use Möbius inversion.)

4. If M and N are submodules of some free modules P over a PID A, does there necessarily exist a basis $e_1, \ldots, e_n$ of P such that $a_1e_1, \ldots, a_ne_n$ is a basis of M and $b_1e_1, \ldots, b_ne_n$ is a basis of N, for some sets of integers a_i and b_i? Prove or give a counterexample (with proof).

5. Let $q = p^e$ be a prime power such that $q \equiv 1 \pmod 4$ and consider the graph on q vertices labeled by the elements of $\mathbb{F}_q$, where x is joined to y iff $x-y$ is a square in $\mathbb{F}_q$. Show that this is an undirected graph, and that it is strongly regular. That is, not only is it regular (every vertex has the same degree), but also for any vertices x and y, the number of vertices connected to both x and y only depends on whether x and y are joined or not, and independent of the specific choice of x and y. This is called a Paley graph. Show that it has at least $eq(q-1)/2$ automorphisms.

6. Use gp/PARI to express the Mersenne prime $p = 2^{127}-1$ in the form a^2+ab+b^2. Attach a printout of the gp session. (Hint: work in $\mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/3}$ is a cube root of unity. It is a PID. Find $\alpha \not\equiv 1 \pmod p$ such that $\alpha^3 \equiv 1 \pmod p$ and then take the gcd of $\alpha - \omega$ and p.)

18.786 Topics in Algebraic Number Theory
Spring 2010