18.784, Extra Problems
Due: WHENEVER

This set of problems discusses the representations of integers by quadratic forms, described in Chapter 3 of Berndt.

- Theorems 3.7.3 and 3.7.5 in Berndt's book give formulae for the number of representations of a positive integer n as $x^2 + 2y^2$ and $x^2 + 3y^2$, respectively. Of course, we know these quantities are non-negative. Show (by elementary means, not the theorem) that the right-hand sides of the equalities in these theorems are indeed non-negative.

We talked in class about whether we could extend the methods in the book to other quadratic forms (or more generally other Diophantine equations). While we didn't immediately see an obstacle to doing this, for say $x^2 + ny^2$, there are reasons to believe that it should be quite hard.

In particular, any answer to this question also determines (in principal) the primes p which can be represented in the form $x^2 + ny^2$. This problem has a long and storied history, and is nearly the sole subject of the entire book "Primes of the Form $x^2 + ny^2$" by David Cox.

- Fermat stated and Euler proved the following results (Euler used the method of infinite descent to give a proof by contradiction, which you can read about in Cox's book):

$$p = x^2 + 2y^2 \quad \text{for some } x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod 8$$

$$p = x^2 + 3y^2 \quad \text{for some } x, y \in \mathbb{Z} \iff p = 3 \text{ or } p \equiv 1 \pmod 3$$

  Use the theorems quoted above in Berndt to give an alternate proof of these results.

- Can you formulate (and prove) a similar statement for primes of the form $x^2 + xy + y^2$?

These results are rather simple, but here's an example of the results for primes of the form $x^2 + 14y^2$:

$$p = x^2+14y^2 \quad \text{for some } x, y \in \mathbb{Z} \iff \begin{cases} \text{-14 is a quadratic res. mod } p \text{ and} \\ (z^2+1)^2 \equiv 8\,(p) \text{ has soln } z \text{ mod } p \end{cases}$$

The story of the solutions to this equation use deep theorems of class field theory, and so it would be surprising if these results followed from manipulations of q-series as in the earlier theorems of Berndt. But this is all the more reason to ask HOW or WHY these methods fail for larger n. Try it!