189-346/377B: Number Theory

Assignment 6

Due: Monday, April 4

1. Let p be an odd prime. Show that -2 is a quadratic residue modulo a prime p if and only if p is a prime of the form $m^2 + 2n^2$.

2. Use question 1 and quadratic reciprocity to get a complete characterisation of all the integers that are of the form $m^2 + 2n^2$.

3. Repeat questions 1 and 2 with $m^2 + 2n^2$ replaced by $m^2 + 3n^2$.

4. Show that there are primes p for which -5 is a quadratic residue modulo p, yet which are not of the form $m^2 + 5n^2$.

5. Make a list of the integers ≤ 100 that can be written in the form m^2+5n^2, and $2m^2+2mn+3n^2$. Can you formulate some conjectures about how these sets of integers behave? (You may find it useful to write each integer in factored form.)

6. By elementary arguments (working in $\mathbf{Z}$) show that the diophantine equation $x^2 + 1 = y^n$ has no solution when

   1. x is odd and $n > 1$.
   2. n is even.

Use this to show that if $n > 1$, then there exists a Gaussian integer $a + bi$ for which $x + i = (a + bi)^n$. Conclude that $b = \pm 1$ and that the equation in question has no solution for $n = 3$, 5 and 7.

7. Solve the Pell equation $x^2 - 133y^2 = 1$ by using the continued fraction method (clearly indicate all the steps that you follow).

Math 377 students only:

8. Section 8.4, Problem 4 in Leveque.

9. Section 8.4, Problem 5 in Leveque.