Elementary Number Theory
Math 175, Section 30
Autumn Quarter 2008
Written Exercises from Week 8

Exercise 0.0.1 Let p be prime, and suppose there exists $x \in \mathbb{Z}$ such that $x^2 \equiv -2 \pmod{p}$. Show that there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + 2b^2$.

Exercise 0.0.2 Let n be a positive integer of the form $n = 4^a \cdot (8k+7)$ for some non-negative integers a and k. Show that n cannot be written as the sum of three squares. (In fact, the converse of this statement is also true, namely, that if n is not of this form, then it can be written as the sum of three squares, but this is much harder to prove.)

Exercise 0.0.3 Prove that every positive integer can be written as the sum of four squares.

Hints:

1. Show that

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ &\quad +(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\end{aligned}$$

   and that, thus, it suffices to prove the statement for primes.

2. If p is prime, show that there exist integers a and b such that $a^2 + b^2 \equiv -1 \pmod{p}$.

3. Show that with a and b as in the previous hint, there exist $x, y, z, t \in \mathbb{Z}$ such that:

$$x \equiv az + bt \pmod{p}$$
$$y \equiv bz - at \pmod{p}$$

   with $|x|, |y|, |z|, |t| < \sqrt{p}$.

4. Show that with a, b, x, y, z, and t as in the previous hints,

$$x^2 + y^2 \equiv (a^2 + b^2)(z^2 + t^2) \equiv -(z^2 + t^2) \pmod{p},$$

   and hence

$$x^2 + y^2 + z^2 + t^2 \equiv 0 \pmod{p}.$$

5. Show that with x, y, z, and t as in the previous hints,

$$0 < x^2 + y^2 + z^2 + t^2 < 4p.$$

6. Note that if $x^2 + y^2 + z^2 + t^2 = p$, you are done.

7. Show that if $x^2 + y^2 + z^2 + t^2 = 2p$, then

$$p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2$$

   is a solution.

8. Show that if $x^2 + y^2 + z^2 + t^2 = 3p$, then

$$p = \left(\frac{y+z'+t'}{3}\right)^2 + \left(\frac{x+z'-t'}{3}\right)^2 + \left(\frac{x-y+t'}{3}\right)^2 + \left(\frac{x+y-z'}{3}\right)^2$$

   is a solution, where z' is either $\pm z$ and $z' \equiv y \pmod{3}$ and t' is either $\pm t$ and $t' \equiv y \pmod{3}$.