Homework 9

Due: 11/19 11:00am

1. Let p be an odd prime with $p \equiv 5 \pmod 8$. Find an explicit solution to the congruence $x^2 \equiv -1 \pmod p$. (Hint: You know $(2/p) = -1$. Apply Euler's criterion.)

2. (a) Use the previous problem to find a solution x to the congruence $x^2 \equiv -1 \pmod{541}$. (Reduce modulo p so that $0 < x < 541$)

   (b) Use part (a) to express a multiple of 541 as a sum of squares.

   (c) Use Fermat's method of descent to express 541 as a sum of squares.

3. Let $\alpha = a + bi$ be a Gaussian integer. Show that if $N(\alpha) = a^2 + b^2$ is divisible by an odd prime p with $p \equiv 3 \pmod 4$, then both a and b are divisible by p.

   (Hint: By contradiction, assume a and b are not divisible by p. Then the Legendre symbols $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ are well-defined. Now derive a contradiction.)

4. Show how to factor 27007 if you know both 885 and 7816 are square roots of 22 modulo 27007.

5. Find the four incongruent solutions of the quadratic congruence $x^2 \equiv 30 \pmod{133}$.

6. We have seen that any prime of the form $p = 4k + 1$ can be expressed as a sum of two squares. Prove that this representation is unique (except for swapping the order of the two summands).

   (Hint: Suppose that $p = a^2 + b^2 = c^2 + d^2$, where a, b, c, d are all positive integers. First argue that $a^2d^2 \equiv b^2c^2 \pmod p$, so then $ad \equiv bc \pmod p$ or $ad \equiv -bc \pmod p$. Next, argue that these two cases imply, respectively, that $ad - bc = 0$ or $ad + bc = p$. If $ad + bc = p$, use the product formula to write p^2 as a sum of squares and then use the resulting equation to conclude $ac - bd = 0$. Thus, it follows that either $ad = bc$ or $ac = bd$. Now draw the rest of the owl.)