Math 7770 Spring 2011
Homework 6
Due: March 14, 2011

You are welcome to work together but everyone needs to write up **distinct** solutions. If you use any books outside of our textbook or other people, please make sure to give them credit. Make sure your solutions are complete. If your handwriting is atrocious, I am happy to give you a basic introduction to LaTeX.

Warmup

- §3.1 # 4. Find the values of $\left(\frac{a}{p}\right)$ in each of the 12 cases $a = -1, 2, -2, 3$ and $p = 11, 13, 17$.
- §3.1 # 7. Which of the following congruences have solutions? How many?
  $$x^2 \equiv \pm 2 \bmod 61 \quad x^2 \equiv \pm 2 \bmod 59 \quad x^2 \equiv \pm 2 \bmod 122 \quad x^2 \equiv \pm 2 \bmod 118.$$
- §3.2 # 4. Which of the following congruences are solvable? (Note that 227, 229, and 1009 are prime).
  $$x^2 \equiv \pm 5 \bmod 227 \quad x^2 \equiv \pm 5 \bmod 229 \quad x^2 \equiv \pm 7 \bmod 1009$$
- §3.2 # 5. Find the values of $\left(\frac{p}{q}\right)$ for the nine cases obtained from all combinations of $p = 7, 11, 13$ and $q = 227, 229$, and 1009.
- §3.2 # 10. Of which primes is -2 a quadratic residue?
- §5.1 # 2. Find all solutions of $10x - 7y = 17$.
- §5.3 # 6. Describe those relatively prime positive integers u and v such that $6uv$ is a perfect square.
- §5.4 # 1. Show that the equation $x^2 + y^2 = 9z + 3$ has no integral solution.

Problems

1. §3.1 # 9. Let p be a prime and let $(a, p) = (b, p) = 1$. Prove that if $x^2 \equiv a \bmod p$ and $x^2 \equiv b \bmod p$ are not solvable, then $x^2 \equiv ab \bmod p$ is solvable.
2. §3.2 # 2. Prove that if p and q are distinct primes of the form $4k + 3$ and if $x^2 \equiv p \bmod q$ has no solution, then $x^2 \equiv q \bmod p$ has two solutions.
3. §5.1 # 7. Let a, b, c be positive integers. Prove that there is no solution of $ax + by = c$ in positive integers if $a + b > c$.
4. §5.3 # 11. Using Theorem 5.5, determine all solutions of the equation $x^2 + y^2 = 2z^2$. (Hint: Write the equation in the form $(x + y)^2 + (x - y)^2 = (2z)^2$.)

Challenge

I. §3.2 # 22. Suppose that $(ab, p) = 1$ and that $p > 2$. Show that the number of solutions (x, y) of the congruence $ax^2 + by^2 \equiv 1 \bmod p$ is $p - \left(\frac{-ab}{p}\right)$.