Homework 2

Remember that it is OK to work with your peers on the homework problems, but you should write up the solutions yourself. Also, if you do work with someone else on the homework, you should acknowledge that you worked with them on your write-up.

Problem numbers below refer to the course textbook, “An introduction to the theory of numbers”, by Niven, Zuckerman, and Montgomery.

1. Prove that the equation $x^2 + 5y^2 - 4z^4 = 3$ has no solutions $(x, y, z)$ with $x, y$ and $z$ all integers. **Hint:** Consider solutions modulo $p$ for a prime number $p < 10$.

2. Section 2.1, number 6: Prove that if $p$ is a prime and $a^2 \equiv b^2 \pmod{p}$, then $p|(a + b)$ or $p|(a - b)$.

3. This problem is different from a usual homework problem. Many times in number theory, before one tries to prove something, one does “numerical experiments” to try to figure out what is likely to be true. For example, we did this the first day of class, when we tried to figure out which prime numbers could be expressed as the sum of two squares. The purpose of this problem is to force you to do a numerical experiment that suggests a specific fact that we will prove later.

   Suppose $p \geq 5$ is a prime, and $a$ a residue class modulo $p$. Then $a$ is said to be a cube modulo $p$ if there exists $r$ so that $r^3 \equiv a \pmod{p}$. For example 3 is a cube modulo 5 because $2^3 \equiv 3 \pmod{5}$, and in fact all five classes 0, 1, 2, 3, 4 are cubes modulo 5. However, only the residue classes 0, 1 and 6 are cubes modulo 7. Thus there are 4 nonzero cubes modulo 5 but only 2 nonzero cubes modulo 7. Do a numerical experiment to try to find a simple rule to determine the number of nonzero cubes modulo $p$.

   In terms of what you should turn in, please:

   (a) State a simple formula in terms of $p$ for what you think is the number of nonzero cubes modulo $p$.

   (b) A little bit of data (e.g., a few tables) that show you really did this experiment.

You are encouraged to use a computer or calculator to help you with this problem. **Note:** If you read ahead in your text, you will likely find the answer to this. However, even if you already know how to prove the answer, I ask that you do the above experiment regardless.