MTH 350 Problem Set 2 Due: 11:59pm Eastern, Sunday February 21

Reminders:

- Remember to review the instructions for Problem Sets before turning in work.
- **Individual** problems (second section below) that are marked with a star (⋆) may be included in your Proof Portfolio.

1 Team Problems

1. This problem is a piece of unfinished business from the proofs about integer equivalence from Module 2.

   (a) Prove that for all natural numbers n and all integers a, b,

   $$a^n - b^n = (a-b)\left(a^{n-1}b^0 + a^{n-2}b^1 + a^{n-3}b^2 + \cdots + a^2b^{n-3} + a^1b^{n-2} + a^0b^{n-1}\right) = (a-b)\sum_{i=1}^{n} a^{n-i}b^{i-1}$$

   (b) Show that for all integers a, b and any natural numbers m, n, if $a \equiv b \pmod{n}$ then $a^m \equiv b^m \pmod{n}$.

2. Consider the claim: For all $x, n \in \mathbb{N}$ with $x^2 \equiv 1 \pmod{n}$, then $x \equiv 1 \pmod{n}$ or $x \equiv -1 \pmod{n}$.

   (a) Is this statement true? If so, provide a proof; if not, give a specific counterexample and explain why your example is a counterexample.

   (b) Prove that the statement is true if n is a prime number.

2 Individual Problems

1. Prove that for any integers a, b, if p is prime and $a^2 \equiv b^2 \pmod{p}$ then $p|(a+b)$ or $p|(a-b)$. (Where do you use the assumption that p is prime?)

2. **Both** of the following are starred problems; **pick exactly one** and do it for this Problem Set. You may have the opportunity to do the other one for your Portfolio later.

   (a) (⋆) Let $a, b \in \mathbb{Z}$. Prove or disprove: If 3 divides $a^2 + b^2$, then 3 divides a or 3 divides b.

   (b) (⋆) Recall that an *irrational number* is one that cannot be written as a ratio $\frac{a}{b}$ where a, b are integers and $b \neq 0$. Prove that for all positive integers n and q, if $\sqrt[q]{n}$ is not an integer, then $\sqrt[q]{n}$ is irrational. (*Suggestions: Euclid's Lemma might be useful; also in MTH 210 you probably proved a special case of this result, namely that $\sqrt{2}$ is irrational, so maybe that proof would be helpful.*)