Math 255 - Spring 2022
Quadratic congruences proofs
10 points

This homework invites you to write some proofs about quadratic congruences.

1. For $n > 1$, let $f(n)$ be the number of solutions to the equation $x^2 \equiv 1 \pmod{n}$, and let $\omega(n)$ be the number of distinct primes dividing n.

   (a) Give a closed formula for $f(n)$. Your formula should use $\omega(n)$.

   (b) Is $f(n)$ ever odd? When?

   (c) Assume that $f(n)$ is even. Show that

   $$\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} a \equiv (-1)^{f(n)/2} \pmod{n}.$$

   Hint: This can be shown using a technique similar to the proof of Wilson's theorem.

   (d) Assuming still that $f(n)$ is even, when is

   $$\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} a \equiv -1 \pmod{n}?$$

2. Prove that the quadratic congruence $6x^2 + 5x + 1 \equiv 0 \pmod{p}$ has a solution for each prime p, but the equation $6x^2 + 5x + 1 = 0$ does not have an integer solution.