Homework 2 : Due Wednesday, February 8

Problem 1: Show that there are infinitely many primes $p \equiv 5 \pmod 6$.

Problem 2: Let R be a ring. An element $r \in R$ is *nilpotent* if there exists $k \in \mathbb{N}$ with $r^k = 0$. Given $n \in \mathbb{N}^+$, determine the nilpotent elements in the ring $\mathbb{Z}/n\mathbb{Z}$.

Problem 3: Suppose that $a, b \in \mathbb{Z}$ and that $n \in \mathbb{N}^+$. Let $d = \gcd(a, n)$.
a. Show that there exists a solution to $\overline{a} \cdot x = \overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$ if and only if $d \mid b$.
b. Show that if if $d \mid b$, then there are exactly d solutions to $\overline{a} \cdot x = \overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$.

Problem 4:
a. Show that if p is an odd prime and $k \in \mathbb{N}^+$, then $x^2 = 1$ has exactly 2 solutions in $\mathbb{Z}/p^k\mathbb{Z}$.
b. Show that $x^2 = 1$ has 1 solution in $\mathbb{Z}/2\mathbb{Z}$, 2 solutions in $\mathbb{Z}/4\mathbb{Z}$, and 4 solutions in $\mathbb{Z}/2^k\mathbb{Z}$ for all $k \geq 3$.
Hint: The properties of ord_p you established in Homework 1 are useful.

Problem 5: Let R be the commutative ring of all continuous functions on $[-1, 1]$ with addition and multiplication defined as pointwise addition and multiplication of functions. Hence, an element of R is a continuous function $f\colon [-1, 1] \to \mathbb{R}$, addition $f + g$ is defined to be the function $(f + g)(x) = f(x) + g(x)$, and multiplication $f \cdot g$ is defined to be the function $(f \cdot g)(x) = f(x) \cdot g(x)$.
a. Characterize the units of R.
b. Let

$$f(x) = \begin{cases} 2x + 1 & \text{if } -1 \leq x \leq -\frac{1}{2} \\ 0 & \text{if } -\frac{1}{2} \leq x \leq \frac{1}{2} \\ 2x - 1 & \text{if } \frac{1}{2} \leq x \leq 1 \end{cases}$$

Let $g(x) = |f(x)|$. Show that in the ring R we have both $f \mid g$ and $g \mid f$, but there is no unit $u \in R$ with $f = gu$.

Problem 6: Notice that if (a, b, c) is a Pythagorean triple, then $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$, so $(\frac{a}{c}, \frac{b}{c})$ is a point on the unit circle $x^2 + y^2 = 1$ with rational coordinates. Conversely, if $(\frac{a}{c}, \frac{b}{c})$ is a rational point on the unit circle, then (a, b, c) is a Pythagorean triple. Thus, we can understand Pythagorean triples by understanding these rational points.

A geometric idea to approach this problem is as follows. Given two rational points on $x^2 + y^2 = 1$, the unique line through them has rational slope. Thus, we take one known rational point, consider all possible rational slopes, and find where the corresponding lines intersect the circle. We will see that the other intersection point of these lines is always a rational point. Although there are several natural choices for this one special point, we will take $(0, -1)$ because it makes the calculations a bit cleaner.
a. Using the above ideas, show that every rational point on the unit circle has the form

$$\left(\frac{2\lambda}{\lambda^2 + 1}, \frac{\lambda^2 - 1}{\lambda^2 + 1} \right)$$

for some $\lambda \in \mathbb{Q}$.
b. Using part a, show that if (a, b, c) is a primitive Pythagorean triple, then there exist relatively prime positive integers $m < n$ having distinct parities such that $a = 2mn$, $b = n^2 - m^2$, and $c = n^2 + m^2$.