Homework 6 : Due Wednesday, March 10

Problem 1: Classify all primes for which -5 is a quadratic residue. Your answer should be along the lines of the one in Proposition 4.14 in the notes (so you should use one common modulus in your description).

Problem 2: Show that $(2y^2+3) \nmid (x^2-2)$ whenever $x, y \in \mathbb{Z}$.
Hint: Begin by thinking about the possible prime divisors of x^2-2.

Problem 3: Suppose that p is a prime with $p \equiv_3 1$.
a. Show using the tools from class that -3 is a quadratic residue modulo p.
b. Here we give a more constructive proof of a without using Quadratic Reciprocity. Since $p \equiv_3 1$, the group $U(\mathbb{Z}/p\mathbb{Z})$, having $p-1$ elements, has order divisible by 3. Since $U(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group of order some multiple of 3, there exists an element $b \in U(\mathbb{Z}/p\mathbb{Z})$ with order equal to 3 (for example, if g is a primitive root modulo p, then $g^{(p-1)/3}$ has order 3). Show that $(2b+1)^2 = -3$ in $\mathbb{Z}/p\mathbb{Z}$.

Problem 4: Suppose that R is a PID. Let $a, b \in R$. Show that there exists a least common multiple of a and b. That is, show that there exists $c \in R$ with the following properties.

- $a \mid c$ and $b \mid c$
- Whenever $d \in R$ satisfies both $a \mid d$ and $b \mid d$, it follows that $c \mid d$.

Hint: Think about the set of common multiples of a and b and how you can describe it as an ideal.

Problem 5: Let R be a commutative ring, and let I and J be ideals of R. The product of I and J, denoted IJ, is the set

$$IJ = \{c_1d_1 + c_2d_2 + \cdots + c_kd_k : k \in \mathbb{N}^+, c_i \in I, d_i \in J\}$$

a. Prove that IJ is an ideal of R and that $IJ \subseteq I \cap J$.
b. Show that if $I = \langle a \rangle$ and $J = \langle b \rangle$, then $IJ = \langle ab \rangle$.
c. Find an example of ideals I and J of some commutative ring R for which $IJ \subsetneq I \cap J$
d. Show that an ideal P is prime if and only if whenever I and J are ideals of R with $IJ \subseteq P$, either $I \subseteq P$ or $J \subseteq P$.

Problem 6: Let R be the ring of all continuous functions on $[-1, 1]$ with addition and multiplication defined as pointwise addition and multiplication of functions. Let

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

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 $f = gu$.