Homework 5 : Due Wednesday, February 29

Problem 1: Suppose that $p, m \in \mathbb{N}^+$ where p is prime. Let $d = \gcd(m, p-1)$. As in Problem 6b on Homework 4, define $\psi\colon U(\mathbb{Z}/p\mathbb{Z}) \to U(\mathbb{Z}/p\mathbb{Z})$ by letting $\psi(x) = x^m$. Given $\overline{a} \in U(\mathbb{Z}/p\mathbb{Z})$, show that $\overline{a} \in \text{range}(\psi)$ if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$.

Problem 2: 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: Find a generator of a certain ideal.

Problem 3: Let R be an integral domain. Some books require a Euclidean function N on R to have the additional requirement that $N(a) \leq N(ab)$ whenever $a, b \in R\backslash\{0\}$ (in other words, nonzero multiples of an element always have larger "size"). Notice that the standard Euclidean functions on $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$ do indeed satisfy this. We show in this problem that every Euclidean domain has a Euclidean function (possibly different from the original one) with this additional property.

Suppose then that R is a Euclidean domain with Euclidean function N. Define $d\colon R\backslash\{0\} \to \mathbb{N}$ by letting

$$d(a) = \min\{N(ac) : c \in R\backslash\{0\}\}$$

Notice that $d(a) \leq N(a)$ for all $a \in R\backslash\{0\}$ by taking $c = 1$.
a. Show that $d(a) \leq d(ab)$ whenever $a, b \in R\backslash\{0\}$.
b. Show that d is a Euclidean function on R.

Problem 4: Suppose that you have a Euclidean function N on R with the property that $N(a) \leq N(ab)$ whenever $a, b \in R\backslash\{0\}$.
a. Show that $N(1) \leq N(a)$ for all $a \in R\backslash\{0\}$.
b. Show that if $a, u \in R\backslash\{0\}$ with u a unit, then $N(a) = N(au)$.
c. Show that if $a, b \in R\backslash\{0\}$ with b not a unit, then $N(a) < N(ab)$.

Problem 5:
a. Let R be a Euclidean domain with Euclidean function N. Suppose that that for each $n \in \mathbb{N}$, the set $\{a \in R : N(a) = n\}$ is finite. Show that R/I is finite for every nonzero ideal I of R.
b. Show that $\mathbb{Z}[i]/I$ is finite for every nonzero ideal I of $\mathbb{Z}[i]$.

Problem 6: A commutative ring R is called *Artinian* if for every descending chain of ideals

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

there exists an N such that $I_n = I_N$ for all $n \geq N$. Show that if R is an Artinian integral domain, then R is a field.
Note: It is a nontrivial theorem that every Artinian commutative ring is Noetherian.