**Homework 8 for 504, Fall 2015**
due Wednesday, December 3

All rings are commutative with identity.

**Definition.** (1). Let $\{\mathfrak{a}_i\}_{i\in I}$ be ideals in $A$. The ideal $\sum_I \mathfrak{a}_i$ is defined as

$$\sum_I \mathfrak{a}_i = \{a_1 + \ldots + a_n \,|\, a_k \in \mathfrak{a}_{i_k}\}$$

(2) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in $A$. Then $\prod_1^n \mathfrak{a}_i$ is the ideal *generated* by all products $(a_1 \ldots a_n)$, $a_i \in \mathfrak{a}_i$.

One has to check that this actually defines ideals but it is immediate. Note that we could have defined the sum as the ideal *generated* by all possible sums of elements from the corresponding ideals. In (2), though, we did not have options: if we simply take the set of all products, this is not necessarily an ideal. So we have to consider the ideal *generated* by all products.

**Problem 1.** Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in $A$ such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for any $i \neq j$.

(1) Show that there exists $x \in A$ such that
$x \equiv 1 (\mathrm{mod}\, \mathfrak{a}_1)$
$x \equiv 0 (\mathrm{mod}\, \mathfrak{a}_2)$
...
$x \equiv 0 (\mathrm{mod}\, \mathfrak{a}_n)$

(2) Prove **"Chinese remainder theorem"**: For any $m_1, \ldots, m_n$ there exists an element $x \in A$ such that
$x \equiv m_1 (\mathrm{mod}\, \mathfrak{a}_1)$
$x \equiv m_2 (\mathrm{mod}\, \mathfrak{a}_2)$
...
$x \equiv m_n (\mathrm{mod}\, \mathfrak{a}_n)$

Moreover, the residue of $x$ in $A/\prod_1^n \mathfrak{a}_i$ is uniquely defined.

(3) (This is merely a reformulation in a more ring-theoretic language.) Show that the following are isomorphic:

$$A/(\cap \mathfrak{a}_i) \simeq A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$$

**Definition.** Let $A$ be an integral domain. A Euclidean function on $A$ is a function $\lambda : A\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that any $a, b \in A, b \neq 0$ there exist $q, r \in A$ such that $a = bq + r$ and either $r = 0$ or $\lambda(r) < \lambda(b)$. $A$ is a **Euclidean domain** if it has a Euclidean function associated with it.

(Heuristically, $A$ is a **Euclidean domain** if $A$ satisfies the Euclidean algorithm.)

**Problem 2.** Prove that a Euclidean domain is a PID.

**Corollary.** Euclidean domains are UFD.

**Problem 3.** Let $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in Z\}$ be the ring of Gaussian integers. Here, $i$ is the square root of $-1$. Let

$$\lambda(a + bi) = N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

(the *Norm* of $a + bi$).

(1) Prove that $\mathbb{Z}[i]$ is a UFD.
(2) Find the units of $\mathbb{Z}[i]$.
(3) Describe all irreducible elements of $\mathbb{Z}[i]$.
**Hint.** You can use *Fermat's theorem on the sum of two squares*: An odd prime number is a sum of two squares if and only if it is 1 mod 4. If you haven't seen this in a number theory course, I encourage you to look up a proof (there are many, the first one attributed to Euler) of this beautiful fact.

**Problem 4.** Give an example of an integral domain $A$ and an irreducible element $a \in A$ such that the ideal $(a)$ is not prime.

**Problem 5.** Let $F$ be a field, $F[X]$ be the polynomial ring over $F$, and define $\deg f : F[X] \to \mathbb{Z}_{\geq 0}$ as the degree of the polynomial $f(X)$. Show that $F[X]$ is Euclidean (with respect to the function deg).

**Remark.** For more than one variable we have that $F[X_1, \ldots, X_n]$ is a UFD but not a PID.

For the next problem, note that by definition a polynomial $f(X) = a_0 + a_1X + \ldots + a_nX^n \in F[X]$ is zero if and only if all coefficients are zero: $a_0 = a_1 = \ldots = a_n = 0$.

**Problem 6.** (a). Let $F$ be a field, and $f(X)$ be a polynomial of degree $n$. Show that $f(X)$ has no more then $n$ roots.
(b). Let $f(X) \in F[X]$. Then $f$ determines a function $f : F \to F$ by evaluation. Assume $F$ is an infinite field. Show that if the function determined by $f$ is zero then $f(X) \equiv 0$ in $F[X]$.
(c). Give a counterexample to the previous statement for a finite field.