MATH 332: HOMEWORK 8

Exercise 1. For each of the following pairs of integers a and b, use the Euclidean algorithm to determine their greatest common divisor d and write d as a linear combination $ax + by$ of a and b.

(a) $a = 20$, $b = 13$.
(b) $a = 69$, $b = 372$.
(c) $a = 91442056588823$, $b = 779086434385541$.

Problem 2. Find a generator for the ideal $(85, 1 + 13i)$ in $\mathbb{Z}[i]$, *i.e.*, a greatest common divisor for 85 and $1 + 13i$, by the Euclidean algorithm. Do the same for the ideal $(47 - 13i, 53 + 56i)$.

Problem 3. Read pp.229-230 of the book on quadratic integer rings. Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field and let $\mathcal{O}$ be its associated quadratic integer ring. Let N be its field norm.

(a) Suppose $D = -3$. Prove that $\mathcal{O}$ is a Euclidean domain with respect to N. (You will likely need to show that every element of F differs from an element of $\mathcal{O}$ by an element show norm is at most $1/3 < 1$.)
(b) Suppose that $D = -163$. Prove that $\mathcal{O}$ is not a Euclidean domain with respect to any norm. (Apply a proof similar to the one in the book for the case $D = -19$.)

Exercise 4. Prove that the quotient of a PID by a prime ideal is again a PID.

Problem 5. Let R be an integral domain and suppose that every *prime* ideal in R is principal. Use the following outline to prove that *every* ideal in R is principal, *i.e.*, R is a PID.

(a) Assume that the set of ideals of R that are not principal is nonempty and prove that this set has a maximal element under inclusion. By hypothesis, this ideal is not prime. [Use Zorn's lemma!]
(b) Let I be an ideal which is maximal with respect to being non principal, and let $a, b \in R$ with $ab \in I$ but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ and let $I_b = (I, b)$. Define $J = \{r \in R \mid rI_a \subseteq I\}$. Prove that $I_a = (\alpha$ and $J = (\beta)$ are principal ideals in R with $I \subsetneq I_b \subsetneq J$ and $I_a J = (\alpha\beta) \subseteq I$.
(c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_a J$ is principal, a contradiction, and conclude that R is a PID.

Problem 6. Let R be a commutative ring with 1 and let a, b be nonzero elements of R. A *least common multiple* of a and b is an element e of R such that

(i) $a \mid e$ and $b \mid e$, and

Date: 6.IV.15.

(ii) if $a \mid e'$ and $b \mid e'$, then $e \mid e'$.

(a) Prove that a least common multiple of a and b (if such exists) is a generator for the unique largest PID contained in $(a) \cap (b)$.
(b) Deduce that any two nonzero elements in a Euclidean domain have a least common multiple which is unique up to multiplication by a unit.
(c) Prove that in a Euclidean domain the least common multiple of a and b is $\frac{ab}{(a,b)}$, where (a, b) is the greatest common divisor of a and b.

Problem 7. Let a and b be nonzero elements of a PID R. Prove that a and b has a least common multiple. Now assume hat R is additionally a UFD. Describe the least common multiple of a and b in terms of the prime factorizations of a and b.

Problem 8. (a) Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.
(b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \pmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.
(c) Let $p \in \mathbb{Z}$ be a prime with $p \equiv 1 \pmod 4$ and write $p = \pi\bar{\pi}$ for some $\pi \in \mathbb{Z}[i]$. Prove that the hypotheses of the Chinese Remainder Theorem are satisfied, and thus

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi})$$

as rings. Show that the ring $\mathbb{Z}[i]/(p)$ has order p^2 and that each of $\mathbb{Z}[i]/(\pi)$, $\mathbb{Z}[i]/(\bar{\pi})$ is a field of order p.

Challenge 9. An integral domain R in which every ideal generated by two elements is principal is called a *Bezout domain*.

(a) Prove that the integral domain R is a Bezout domain if and only if every pair of elements $a, b \in R$ has a greatest common divisor d in R that can be written as an R-linear combination of a and b.
(b) Prove that every finitely generated ideal of a Bezout domain is principal.
(c) Prove that R is a PID if and only if R is a UFD that is also a Bezout domain. (We have proven in class that every PID is a UFD, and PIDs are obviously Bezout domains. Thus it only remains for you to prove that UFD's which are Bezout domains are in fact PIDs. Let $0 \neq a \in I \trianglelefteq R$ where a has the minimal number of irreducible factors amongst elements of I. Prove that $I = (a)$ by showing that if there is an element $b \in I$ that is not in (a), then $(a, b) = (d)$ leads to a contradiction.