Homework 2

due on Monday, September 22

Problem 1. Prove that R_d is Euclidean for $d = 2, 3, 5, 6, 7, 13, 17, 21, 29$. Hint: Show that the absolute value of the norm can be used as Euclidean norm.

Remark. It can be proved that in addition to the above values of d the absolute value of the norm is an Euclidean norm on R_d iff $d = 11, 33, 37, 41, 57, 73, 76$. On the other hand, asuming the Extended Riemann Hypothesis, it was proved that for $d > 0$ the ring R_d is a UFD iff it is Euclidean under some norm. It is an open problem whether there is infinitely many $d > 0$ for which R_d is a UFD.

Problem 2. Consider the ring $R_{-3} = R = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ of Eisenstein integers, where $\omega = (-1 + \sqrt{-3})/2$ (note that the ω here is slightly different than the one used in class, but the ring is the same). Observe that that $\omega^2 + \omega + 1 = 0$ (so $\omega^3 = 1$).

a) Let p be an odd prime such that -3 is not a square modulo p. Prove that if a, b are integers such that $p|a^2-ab+b^2$ then $p|a$ and $p|b$. **Hint.** $(2a-b)^2+3b^2 = 4(a^2-ab+b^2)$.

b) Prove that if a, b are integers such that $2|a^2 - ab + b^2$ then $2|a$ and $2|b$.

c) Use a), b) to conclude that if $p = 2$ or p is an odd prime such that -3 is not a square modulo p then pR is a prime ideal. Conclude that pR is maximal.

d) Suppose now p is an odd prime such that -3 is a square modulo p. Prove that pR is not a prime ideal. Conclude that p is not irreducible and $p = a^2 - ab + b^2$ for some integers a, b. Show that the ideal pR is a product of two maximal ideals which are different iff $p \neq 3$.

e) Prove that every element of R is associated to an element of the form $a + b\omega$ with both a, b non-negative and at least one of a, b even.

f) Use quadrartic reciprocity to prove that -3 is a square modulo p iff $p \equiv 1 \pmod 3$.
Challenge. Can you prove this without using quadratic reciprocity.

g) Prove that a natural number n is of the form $a^2 + 3b^2$ iff evrery prime divisor of n which is $\equiv 2 \pmod 3$ appears in n to an even power.

Problem 3. Let I be an ideal of the ring R. Define $I[x]$ as the subset of $R[x]$ which consists of all the polynomials in $R[x]$ whose all coefficients belong to I. Prove that $I[x]$ is an ideal of $R[x]$ and that $R[x]/I[x]$ is naturally isomorphic to the polynomial ring $(R/I)[x]$.

Problem 4. Let R be a commutative ring and let $R[x]$ be the ring of polynomials in x with coefficients in R. Let $f = f_0 + f_1x + ... + f_nx^n \in R[x]$. Prove that

a) f is invertible iff $f_0 \in R^\times$ and $f_1, ..., f_n$ are nilpotent.

b) f is nilpotent iff $f_0, ..., f_n$ are nilpotent.

c) f is a zero divisor iff $af = 0$ for some $0 \neq a \in R$.

d) Let P be a prime ideal of R and $f, g \in R[x]$. Prove that all coefficients of fg belong to P iff either all coefficients of f or all coefficients of g belong to P.

e) If f belongs to every maxiaml ideal of $R[x]$ then f is nilpotent.

Problem 5. Ler R be an integral domain.

a) Let $f, g \in R[x]$ be such that $fg = cx^n$ for some n and some $c \in R$, $c \neq 0$. Prove that there exist elements $a, b \in R$ and $m \leq n$ such that $f = ax^m$ and $g = bx^{n-m}$ and $ab = c$.

b) Suppose that $f = f_0 + f_1x + ... + f_nx^n \in R[x]$. Suppose that there is a prime ideal P of R such that $f_n \notin P$, $f_0, ..., f_{n-1} \in P$ and $f_0 \notin P^2$. Prove that if $f = gh$ for some $g, h \in R[x]$ then one of g, h is constant. Conclude that if in addition f is monic then it is irreducible in $R[x]$. This result is known as **Eisenstein criterion**. Hint: Assume that $f = gh$ and both g, h have positive degree. Pass to the ring $(R/P)[x]$ and apply a) to show that constant terms of g and h belong to P. Derive contradiction.

c) Prove that the polynomial $2x^{10} + 21x^8 - 35x^2 + 14$ is irreducible in $\mathbb{Z}[x]$. Hint: Apply Eisenstein criterion with appropriate prime ideal P.

Problem 6. Find a greatest common divisor $d(x)$ of the polynomials $p(x) = x^3 + 4x^2 + x - 6$ and $q(x) = x^5 - 6x + 5$ in the ring $\mathbb{Q}[x]$ and find $a(x), b(x) \in \mathbb{Q}[x]$ such that $d(x) = a(x)p(x) + b(x)q(x)$.

Problem 7. Let $K \subseteq L$ be fields. Suppose that $f, g \in K[x]$ and $f|g$ in the ring $L[x]$. Prove that $f|g$ in the ring $K[x]$.