# Math 113 Homework 10. Due 11/24

**Reading corresponding to lectures:**
Tuesday 11/ 17 DF 8.3
Thursday 11/ 19 DF 9.2, beginning of 9.4
Tuesday 11/ 24 DF 9.3, 9.4

**Problems to hand in:**

1. Do the following problems from DF section 8.3: 5a, for 2 and $\sqrt{-n}$ only. (hint: use the "norm" $N$)

2. Show that $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.
   (hint: you can use problem 1, or find an example similar to the example for $\mathbb{Z}[\sqrt{-5}]$)

3. (a) Let $F$ be a field. Show that $x^2 = 1$ has only two solutions in $F$.
   (hint: $F[x]$ is a Euclidean domain, so a UFD. Factor the polynomial $x^2 - 1$ into irreducibles to understand solutions of $x^2 - 1 = 0$)

   (b) Let $p$ be prime. For which integers $n$ is $n$ equal to its own multiplicative inverse mod $p$? (use part a and that $\mathbb{Z}/p\mathbb{Z}$ is a field)

   (c) We will use the result of part b) above to prove the following lemma used in class:
   *Fermat's lemma: If $p$ is a prime integer, and $p = 4a + 1$, then $p$ divides $(2a)!^2 + 1$*

   Outline: First show that
   $$(2a)!^2 \equiv 1 \cdot 2 \cdot ... \cdot 2a \cdot (-(2a+1)) \cdot (-(2a+2))...(-(p-1)) \pmod p$$
   Now cancel things with their multiplicative inverses (justify this using part b) to conclude that
   $$(2a)!^2 \equiv -1 \pmod p$$
   and say why this proves the lemma.

4. Do the following problems from DF section 9.2: 1, 2 (these should feel familiar!), 8.

5. In this question you'll prove that irreducible polynomials in $\mathbb{R}[x]$ must be degree 1 or 2. This is probably a familiar fact to you (every polynomial of degree at least 3 can be factored), but now you will prove it.

   (a) Define a function $\phi : \mathbb{C} \to \mathbb{C}$ by $\phi(a + bi) = a - bi$. (this is just the usual complex conjugation). Show that $\phi$ is a ring homomorphism.

   (b) Suppose $f \in \mathbb{R}[x]$ (i.e. $f$ is a polynomial with real coefficients) and suppose $\alpha$ is a complex number with $f(\alpha) = 0$ Show that $f(\phi(\alpha)) = 0$, using the fat that $\phi$ is a ring homomorphism.

   (c) It is known that any $f \in \mathbb{C}[x]$ with degree $> 0$ can be factored as a product of degree 1 polynomials in $\mathbb{C}[x]$. Use this fact and your work above to show that if $f \in \mathbb{R}[x]$ is irreducible then f has degree 1 or 2.
   (hint: suppose degree$(f) > 1$ and look at a root $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. Apply part b) above to conclude $\phi(\alpha)$ is also a root. Let $g(x) = (x - \alpha)(x - \phi(\alpha))$ and show that $g$ divides $f$ in $\mathbb{R}[x]$, by using the Euclidean algorithm in $\mathbb{R}[x]$ – if there is a remainder term $r(x)$, what is $r(\alpha)$? – Conclude either $f$ is reducible or $f$ is a constant multiple of $g$)