MATH 7230 Homework 1 - Fall 2018

Due Wednesday, Aug. 29 at 1:30

https://www.math.lsu.edu/%7Emahlburg/teaching/2018F-MATH7230.html

You are required to turn in at least **one** of the following problems, and must complete a total of **20** by semester's end. Group work is allowed, but your solutions must be written up individually.

The notation "Ash A.B.C" means Problem C from Section A.B in the textbook.

In lecture we determined which integer primes are representable as the sum of two integers by using the norm in the Gaussian integers ($N(a+bi) = a^2+b^2$), as well as the fact that $\mathbb{Z}[i]$ is a Euclidean Domain (and hence a Unique Factorization Domain). In Problems 1 – 3 you will explore some similar features of the Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega := e^{\frac{2\pi i}{3}}$ is a third root of unity.

1. The norm map in $\mathbb{Z}[\omega]$ is defined by $N(a+b\omega) := (a+b\omega)(a-b-b\omega)$.
   (a) Prove that $N(a+b\omega) = a^2 - ab + b^2$.
   (b) Prove that the norm is *multiplicative*; this means that if $x, y \in \mathbb{Z}[\omega]$, then $N(xy) = N(x)N(y)$.
   Hint: How does the norm relate to complex conjugation?
   (c) Prove that $N(a+b\omega) = 0$ if and only if $a+b\omega = 0$.
   (d) Show that an integer prime p such that $p \equiv 2 \pmod 3$ is irreducible in $\mathbb{Z}[\omega]$.

   Remark: As mentioned in lecture, it is also true that **every** $p \equiv 1 \pmod 3$ *factorizes in* $\mathbb{Z}[\omega]$*! However, it is fairly involved to prove this.*

2. (a) Prove that the Eisenstein integers form a Euclidean Domain. This means that for any $x, y \in \mathbb{Z}[\omega]$ there are $q, r \in \mathbb{Z}[\omega]$ such that
   $$y = qx + r, \qquad \text{with} \quad 0 \le N(r) < N(x).$$
   (b) Show that for integers $x, y \in \mathbb{Z}$, the remainder bound in the classical Euclidean algorithm can be strengthened to
   $$y = qx + r, \qquad \text{with} \quad 0 \le |r| \le \frac{|x|}{2}.$$
   In lecture, we also showed that for the Gaussian integers the norm bound is
   $$0 \le N(r) \le \frac{1}{2}N(x).$$
   What is the best possible bound for the Eisenstein integers?

3. Factor the following Eisenstein integers into irreducibles/primes (this is possible due to Problem 2). It will be very helpful to calculate norms!

(a) 52,

(b) $10 + 8\omega$.

4. In lecture we used Wilson's Theorem (that $(n-1)! \equiv -1 \pmod{n} \iff n$ prime) to find that $x := \left(\frac{p-1}{4}\right)!$ is a solution to $x^2 \equiv -1 \pmod{p}$ for primes $p \equiv 1 \pmod{4}$. However, there is another way to find such a solution if you understand the structure of the field $\mathbb{Z}/p\mathbb{Z}$.

   (a) Review at least one proof of the fact that the multiplicative subgroup $\left((\mathbb{Z}/p\mathbb{Z})^\times, \cdot\right)$ is a cyclic group with $p-1$ elements. For example, K. Conrad provides **seven** proofs at:

   `http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/cyclicmodp.pdf`.

   Remark: I recommend Proofs 3 and 7, which both essentially use Galois Theory.

   (b) Now suppose that a is a *primitive root* modulo p, which means that a is a generator of the group. Equivalently, $a, a^2, \cdots, a^{p-1} \equiv 1 \pmod{p}$ are all distinct. If $p \equiv 1 \pmod{4}$, find an element x such that $x^2 \equiv -1 \pmod{p}$.

   (c) Similarly, if $p \equiv 3 \pmod{4}$, show that there is no such x.

5. For each of the following algebraic elements α, show that α is integral over $\mathbb{Z}$ by finding a monic $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. In each case, do you believe that you have found an $f(x)$ of minimal degree? Can you prove it?

   (a) $\alpha = \sqrt{3} + \sqrt{5}$,

   (b) $\alpha = i\sqrt[3]{3}$,

   (c) $\alpha = \zeta_5 + \zeta_5^{-1}$, where $\zeta_n := e^{\frac{2\pi i}{n}}$.

6. (a) Ash 1.1.1.

   (b) Ash 1.1.2.

7. Ash 1.1.3.