Math 5230 - Algebraic Number Theory (Fall 2012) Due in MSB 318
Problem Set 2 9/21/12 at 4 PM

A generalization made not for the vain pleasure of generalizing, but rather for the solution of problems previously posed, is always a fruitful generalization. Lebesgue

1. Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field, with d a squarefree integer. Write $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\omega$ for some ω. (For instance, we could take $\omega = \sqrt{d}$ or $(1+\sqrt{d})/2$, depending on d mod 4. But the particular choice of ω for which $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\omega$ does not matter.) In this exercise, you will find *all* subrings of $\mathcal{O}_K$.

   a) For $c \geq 1$, show $\mathbf{Z} + \mathbf{Z}c\omega = \mathbf{Z}[c\omega]$ is the unique subring of $\mathcal{O}_K$ with index c. (Hint: Start by showing any subring of index c must contain $c\omega$.)

   b) Show any subring of $\mathcal{O}_K$ other than $\mathbf{Z}$ has finite index in $\mathcal{O}_K$, and therefore by part a it is $\mathbf{Z}[c\omega]$ for some c. (Hint: Use the structure of subgroups of finitely generated abelian groups.)

2. a) If d is a positive nonsquare integer such that $d \equiv 1 \bmod 4$, show any unit $u = a + b\frac{1+\sqrt{d}}{2}$ in $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ that is greater than 1 has $a \geq 0$ and $b \geq 1$. (The example of the unit $\frac{1+\sqrt{5}}{2}$ in $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$ shows the case $a = 0$ can happen.)

   b) Verify that the following is the least unit greater than 1 in $\mathbf{Z}[\sqrt{d}]$ subject to the indicated constraint. (The values of d in the table may not be squarefree, but they are never perfect squares.)

d	Least Unit > 1	Constraint
n^2+1	$n+\sqrt{n^2+1}$	$n \geq 1$
n^2-1	$n+\sqrt{n^2-1}$	$n \geq 2$
n^2+2	$n^2+1+n\sqrt{n^2+2}$	$n \geq 1$
n^2-2	$n^2-1+n\sqrt{n^2-2}$	$n \geq 3$

   c) Verify the following is the least unit > 1 in $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ subject to the indicated constraint.

d	Least Unit > 1	Constraint
n^2+4	$\frac{n+\sqrt{n^2+4}}{2}$	odd $n \geq 1$
n^2-4	$\frac{n+\sqrt{n^2-4}}{2}$	odd $n \geq 5$

3. Let $K = \mathbf{Q}(\sqrt{-3})$. Inside K is $\zeta_3 = (-1+\sqrt{-3})/2$, a nontrivial cube root of unity. (Note ζ_3 is *not* $(1+\sqrt{-3})/2 = 1+\zeta_3 = -\zeta_3^2$.) The ring $\mathbf{Z}[\zeta_3]$ is the full ring of integers in K. It contains $\mathbf{Z}[\sqrt{-3}] = \mathbf{Z}[2\zeta_3]$ with index 2.

   The norm formulas from K to $\mathbf{Q}$ with respect to the two $\mathbf{Q}$-bases $\{1, \sqrt{-3}\}$ and $\{1, \zeta_3\}$ are

$$\mathrm{N}(x+y\sqrt{-3}) = x^2+3y^2, \quad \mathrm{N}(a+b\zeta_3) = a^2-ab+b^2$$

   for rational x, y, a, and b.

a) Prove the units of $\mathbf{Z}[\zeta_3]$ are $\{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$.

b) Show $\mathbf{Z}[\zeta_3]$ is Euclidean with respect to the norm, so $\mathbf{Z}[\zeta_3]$ is a UFD (unlike $\mathbf{Z}[\sqrt{-3}]$).

c) Explain why the equation $21 = 3 \cdot 7 = (3 + 2\sqrt{-3})(3 - 2\sqrt{-3})$ is not an example of non unique factorization in $\mathbf{Z}[\zeta_3]$.

d) Although $\mathbf{Z}[\sqrt{-3}]$ is a proper subset of $\mathbf{Z}[\zeta_3]$, show the norm values are the same: for any $\alpha \in \mathbf{Z}[\zeta_3]$ there is a $\beta \in \mathbf{Z}[\sqrt{-3}]$ such that $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$. (The other way is automatic: for every $\beta \in \mathbf{Z}[\sqrt{-3}]$ there is an $\alpha \in \mathbf{Z}[\zeta_3]$ such that $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$ because we can use $\alpha = \beta$.) In simpler terms, you're being asked to show for any a and b in $\mathbf{Z}$ that $a^2 - ab + b^2 = x^2 + 3y^2$ for some x and y in $\mathbf{Z}$. (Hint: Consider the norm of $(a + b\zeta_3)u$ for $u = 1, \zeta_3$, or ζ_3^2.)

e) Use previous parts of this exercise to show for any prime $p \neq 2$ or 3 that

$$-3 \equiv \Box \bmod p \Longleftrightarrow p = x^2 + 3y^2 \text{ for some } x, y \in \mathbf{Z}.$$

This would follow from $\mathbf{Z}[\sqrt{-3}]$ being a UFD, but it is *not* a UFD. The result is nevertheless correct! (Warning: It is false that if $p|(c + \sqrt{-3})$ in $\mathbf{Z}[\zeta_3]$ for some $c \in \mathbf{Z}$ then $p|1$: $\{1, \sqrt{-3}\}$ is not a $\mathbf{Z}$-basis of $\mathbf{Z}[\zeta_3]$.)

4. Let F be a field not of characteristic 2. For a nonconstant squarefree[1] polynomial $f(X) \in F[X]$, the polynomial $T^2 - f(X)$ is irreducible in $F(X)[T]$. Prove the integral closure of $F[X]$ in $F(X)(\sqrt{f})$ is $F[X][\sqrt{f}] = F[X, \sqrt{f}]$. (For example, the ring $\mathbf{C}[X, \sqrt{X^3 - X}]$ is integrally closed.)

   Comment. Although $F[X]$ is a UFD, its integral closure in the field $F(X, \sqrt{f})$ need not be a UFD. This is similar to the situation in quadratic fields, where $\mathbf{Z}$ is a UFD but $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.

5. Let A be a ring. A sequence $a_1, a_2, a_3, \ldots$ in A satisfies an r-term linear recursion when there are constants $c_1, c_2, \ldots, c_r$ in A such that

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_r a_{n-r}$$

   for all $n > r$. Without mentioning r, the sequence is called linearly recursive.

   The set of all sequences in A obviously is a ring under termwise addition and multiplication. Remarkably, the linearly recursive sequences in A are a subring. This will be proved using ideas similar to the proof that integral elements over a ring are closed under addition and multiplication.

   a) Show the squares of the Fibonacci numbers, F_n^2, satisfy the linear recursion $F_n^2 = 2F_{n-1}^2 + 2F_{n-2}^2 - F_{n-3}^2$. More generally, if a sequence $a_1, a_2, a_3, \ldots$ satisfies the 2-term linear recursion $a_n = a_{n-1} + a_{n-2}$, show the sequence $b_n := a_n^2$ satisfies the 3-term linear recursion $b_n = 2b_{n-1} + 2b_{n-2} - b_{n-3}$. (Admittedly the recursion for F_n^2 is coming out of nowhere.)

[1] Squarefree for polynomials means no irreducible factor appears more than once. It has nothing to do with *constant* factors that may be squares: $4X(X + 1)$ is considered squarefree.

b) Let Seq(A) denote the set of all sequences in A. We think of them as infinite-length vectors: $\mathbf{a} = (a_1, a_2, a_3, \ldots)$. Define the shift operator $S\colon \mathrm{Seq}(A) \to \mathrm{Seq}(A)$ by $S(a_1, a_2, a_3, \ldots) = (a_2, a_3, a_4, \ldots)$. It drops the first term and moves all other terms back by one position. Show S is a ring homomorphism.

c) Show $(S^2 - S - I)(\mathcal{F}) = \mathbf{0}$, where $\mathcal{F} = (1, 1, 2, 3, 5, \ldots)$ is the Fibonacci sequence, and more generally a sequence $\mathbf{a}$ in A satisfies a linear recursion if and only if $f(S)(\mathbf{a}) = \mathbf{0}$ for some *monic* polynomial $f(T) \in A[T]$. This is the link between linear recursions and integrality.

d) Use part c to show the sum of two linearly recursive sequences is linearly recursive.

e) A subset M of Seq(A) is called shift-stable if $S(M) \subset M$. Show the following conditions on a sequence $\mathbf{a}$ in Seq(A) are equivalent:

1) $\mathbf{a}$ is linearly recursive,
2) the A-module $\sum_{n\geq 0} AS^n(\mathbf{a}) = A\mathbf{a} + AS(\mathbf{a}) + AS^2(\mathbf{a}) + \cdots$ is finitely generated and shift-stable,
3) $\mathbf{a}$ is contained in a finitely generated shift-stable A-submodule of Seq(A).

This is similar to a theorem from class that linearizes the property of algebraic integers, and as in that proof the hardest part is going from the last condition to the first one.

f) Deduce that the product of two linearly recursive sequences is linearly recursive and use your work to derive the recursion in part a for F_n^2 in a systematic way.