Math 154. Homework 2

1. (i) By using arithmetic in $\mathbf{Z}[i]$ (i.e., unique factorization and knowledge of units), show $n \in \mathbf{Z}^+$ has the form x^2+y^2 if and only if each prime factor $p \equiv 3 \bmod 4$ of n occurs with even multiplicity. Use arithmetic in $\mathbf{Z}[\sqrt{-2}]$ to show for p a positive prime in $\mathbf{Z}$ that if $p = x^2+2y^2$ then (x,y) is unique up to signs.

(ii) Using unique factorization in $\mathbf{Z}[\sqrt{2}]$ and $\mathbf{Z}[\sqrt{3}]$, prove for *any* prime $p \in \mathbf{Z}^+$ that

$$\pm p = x^2 - 2y^2 \text{ with } x, y \in \mathbf{Z} \Leftrightarrow 2 = \square \bmod p, \;\; \pm p = x^2 - 3y^2 \text{ with } x, y \in \mathbf{Z} \Leftrightarrow 3 = \square \bmod p$$

where we mean that at least one of p or $-p$ has the desired form. For $p \neq 2, 3$, convert the right side of each equivalence into congruence conditions on p by using quadratic reciprocity.

(iii) For the unit $1+\sqrt{2} \in \mathbf{Z}[\sqrt{2}]$, note that $\mathrm{N}(1+\sqrt{2}) = -1$. Using this, show the sign on p can be dropped in the first equivalence in (ii). But show -1 is not a norm from $\mathbf{Z}[\sqrt{3}]$, and correspondingly show by example that the sign cannot be dropped in the second equivalence. (Beware that in general -1 can fail to be a norm from $\mathbf{Z}[\sqrt{d}]$ yet be a norm from $\mathbf{Q}(\sqrt{d})$: ± 33 are norms from $\mathbf{Z}[\sqrt{34}]$, so their ratio -1 is a norm from $\mathbf{Q}(\sqrt{34})$, but it can be shown that -1 is *not* a norm from $\mathbf{Z}[\sqrt{34}]$.)

2. Let $\zeta = (-1+\sqrt{-3})/2 \in K = \mathbf{Q}(\sqrt{-3})$, so ζ is a primitive cube root of unity: $\zeta^3 = 1$ but $\zeta \neq 1$ (i.e., $\zeta^2+\zeta+1 = 0$). Note this is *not* $(1+\sqrt{-3})/2 = 1+\zeta = -\zeta^2$, which is a primitive 6th root of unity! The ring $\mathbf{Z}[\zeta]$ is the ring of integers of K, called the *Eisenstein integers*. It contains $\mathbf{Z}[\sqrt{-3}] = \mathbf{Z} + \mathbf{Z} \cdot 2\zeta$ as an additive subgroup of index 2. Formulas for the norm $\mathrm{N} : K \to \mathbf{Q}$ relative to the respective $\mathbf{Q}$-bases $\{1, \sqrt{-3}\}$ and $\{1, \zeta\}$ are $\mathrm{N}(x+y\sqrt{-3}) = x^2+3y^2$ and $\mathrm{N}(a+b\zeta) = a^2-ab+b^2$ with $x, y, a, b \in \mathbf{Q}$.

(i) Using the second norm formula, prove that the group of units in $\mathbf{Z}[\zeta]$ is $\{\pm 1, \pm\zeta, \pm\zeta^2\}$.

(ii) Show that $\mathbf{Z}[\zeta]$ is Euclidean using this norm, so it is a UFD (unlike $\mathbf{Z}[\sqrt{-3}]$).

(iii) Although $\mathbf{Z}[\sqrt{-3}]$ is a proper subring of $\mathbf{Z}[\zeta]$, show the norms $\mathrm{N} : \mathbf{Z}[\sqrt{-3}] \to \mathbf{Z}$ and $\mathrm{N} : \mathbf{Z}[\zeta] \to \mathbf{Z}$ have the same image, so for any $a, b \in \mathbf{Z}$ we can write a^2-ab+b^2 in the form x^2+3y^2 for some $x, y \in \mathbf{Z}$. (Hint: Look at the norm of $(a+b\zeta)u$ for $u = 1, \zeta, \zeta^2$.)

(iv) Show a prime $p > 3$ has the form x^2+3y^2 with $x, y \in \mathbf{Z}$ if and only if $-3 \equiv \square \bmod p$; convert this into a congruence on p by quadratic reciprocity. (This is what we'd expect if $\mathbf{Z}[\sqrt{-3}]$ is a UFD, but it isn't!)

3. Let K be a number field and choose $\alpha \in \mathscr{O}_K$.

(i) By working in a Galois closure of K over $\mathbf{Q}$, show that the minimal polynomial $f \in \mathbf{Q}[X]$ for α has coefficients that are algebraic integers, and so deduce that $f \in \mathbf{Z}[X]$.

(ii) Rigorously prove that the natural map of rings $\mathbf{Z}[X]/(f) \to \mathbf{Z}[\alpha]$ defined by $X \mapsto \alpha$ is an isomorphism. (Hint: For a nonzero commutative ring R and $f \in R[X]$ a *monic* polynomial of degree $n > 0$, prove $R[X]/(f)$ is a free R-module with basis given by the residue classes of $1, X, \dots, X^{n-1}$.)

4. Let $d \in \mathbf{Z}_{>1}$ be squarefree. *Pell's equation* concerns solutions to $x^2 - dy^2 = 1$ in $\mathbf{Z}$ with $x, y > 0$; i.e., up to signs one seeks elements of $\mathbf{Z}[\sqrt{d}] - \{\pm 1\}$ with norm 1. Let $K = \mathbf{Q}(\sqrt{d})$ and let $\mathscr{O}$ be its ring of integers. *Dirichlet's unit theorem*, proved later, implies $\mathscr{O}^\times$ is infinite cyclic up to a sign. A *fundamental unit* of K is $\varepsilon \in \mathscr{O}^\times$ such that $\mathscr{O}^\times = \langle -1 \rangle \times \varepsilon^{\mathbf{Z}}$ (so the fundamental units are $\pm\varepsilon$ and $\pm 1/\varepsilon$). If an embedding $j : K \hookrightarrow \mathbf{R}$ is *chosen*, the unique fundamental unit > 1 is often called "the" fundamental unit (relative to j).

(i) Show $x^2 - dy^2 \neq -1$ for all $x, y \in \mathbf{Z}$ if $d \equiv 3 \bmod 4$. For $d \equiv 1, 2 \bmod 4$ such that $-1 \equiv \square \bmod d$, the *only known way* to show $x^2 - dy^2 = -1$ has no $\mathbf{Z}$-solution is to check if a fundamental unit has norm 1.

The link between Pell's equation and fundamental units is explained in §4.6 of the text beneath Proposition 1, where it is explained how to find a fundamental unit. Read that discussion (which implicitly uses one of the two embeddings of K into $\mathbf{R}$ to make sense of inequalities in K). Note that (i) a fundamental unit may have norm -1 (e.g., $1+\sqrt{2}$), and (ii) $\mathscr{O}$ may be larger than $\mathbf{Z}[\sqrt{d}]$ (if $d \equiv 1 \bmod 4$), so the fundamental units may not lie in $\mathbf{Z}[\sqrt{d}]$; e.g., $\varepsilon = (1+\sqrt{5})/2$ for $d = 5$ and $\varepsilon = (3+\sqrt{13})/2$ for $d = 13$.

(ii) Prove by parity considerations that if $\alpha \in \mathscr{O} - \mathbf{Z}[\sqrt{d}]$ then $\alpha^2 \notin \mathbf{Z}[\sqrt{d}]$! This is as bad as it gets: using $\mathbf{Z}[X]/(X^2 - X + (1-d)/4) \simeq \mathscr{O}_K$ defined by $X \mapsto (1+\sqrt{d})/2$ (Exercise 3), reduce mod 2 to infer $\mathscr{O}/2\mathscr{O} \simeq \mathbf{F}_4$ (resp. $\mathscr{O}/2\mathscr{O} \simeq \mathbf{F}_2 \times \mathbf{F}_2$) as rings when $d \equiv 5 \bmod 8$ (resp. $d \equiv 1 \bmod 8$). Since $\mathbf{Z}[\sqrt{d}] = \mathbf{Z} + 2\mathscr{O}$, conclude via the structure of $(\mathscr{O}/2\mathscr{O})^\times$ that $d \equiv 1 \bmod 8 \Rightarrow \mathscr{O}^\times \subset \mathbf{Z}[\sqrt{d}]$ and $d \equiv 5 \bmod 8 \Rightarrow (\mathscr{O}^\times)^3 \subset \mathbf{Z}[\sqrt{d}]$. This is a more conceptual explanation for the end of §4.6 where Samuel uses some messy calculations.