2015-11-09 Introduction to number theory Problems

1. Let $m \in \mathbb{Z}$ be a square free integer (i.e., not divisible by a square other than 1). Suppose $m \neq \pm 1$. Let $K = \mathbb{Q}(\sqrt{m})$. Recall that the ring of integers $\mathcal{O}_K$ of a number field K is the set (which becomes a ring) of elements a of K such that a is a root of a monic polynomial with coefficients in $\mathbb{Z}$.
1.1. Suppose $m \equiv 2 \pmod 4$. Show that $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
1.2. Suppose $m \equiv 3 \pmod 4$. Show that $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.
1.3. Suppose $m \equiv 1 \pmod 4$. Show that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \{a + b(\frac{1+\sqrt{m}}{2}) \mid a, b \in \mathbb{Z}\}$.

2. Let $K = \mathbb{Q}(\sqrt{-26})$. From 1.1 above, it follows that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-26}]$. Let us show that $\mathcal{O}_K$ is not a unique factorization domain.
2.1.1. Show that $1 + \sqrt{-26}$ and $1 - \sqrt{-26}$ are not units.
2.1.2. Recall that a nonzero element $\alpha \in A$, which is not a unit, is a prime element if $ab \in \alpha A$ implies $a \in \alpha A$ or $b \in \alpha A$. Use $3^3 = (1 + \sqrt{-26})(1 - \sqrt{-26})$ to conclude that 3 is not a prime element.
2.2. We show that there does not exist a prime element which divides 3.
2.2.1. Suppose there exists a prime element α that divides 3. Show, using that 3 is not a prime element, that $3 = \alpha\overline{\alpha}$. (See the exercises from 2015-11-02.)
2.2.2. Set $\alpha = x + y\sqrt{-26}$. From 2.2.1, we obtain $3 = x^2 + 26y^2$. Show that there are no solutions in $\mathbb{Z}$ and conclude that $\mathcal{O}_K$ is not a unique factorization domain.
2.3. Consider ideals $\mathfrak{a} = (3, 1 + \sqrt{-26})$ and $\mathfrak{b} = (3, 1 - \sqrt{-26})$.
2.3.1. Show that $\mathfrak{a}$ is not a principal ideal.
2.3.2. Show that $\mathfrak{b}$ is not a principal ideal.
2.3.3. Show that $\mathfrak{a}$ is a prime ideal.
2.3.4. Show that $\mathfrak{b}$ is a prime ideal.
2.3.5. Recall that the product IJ of two ideals I and J is

$$IJ = \left\{ \sum_{k=1}^{n} x_k y_k \;\middle|\; n \in \mathbb{N}, x_k \in I, y_k \in J \right\}.$$

Show that $(3) = \mathfrak{a}\mathfrak{b}$.
2.3.6. Show that $(1 + \sqrt{-26}) = \mathfrak{a}^3$.
2.3.7. Show that $(1 - \sqrt{-26}) = \mathfrak{b}^3$.
Remark: Hence we can understand the equation $3^3 = (1 + \sqrt{-26})(1 - \sqrt{-26})$ using ideals in the following way: $(3^3) = \mathfrak{a}^3\mathfrak{b}^3 = ((1 + \sqrt{-26})(1 - \sqrt{-26}))$.

3.
3.1. Let A be a domain. Let $\alpha \in A$ be a nonzero element. Prove that α is a prime element if and only if αA is a prime ideal.
3.2. Show that the set of prime ideals of $\mathbb{Z}$ is $\{(p) \mid p \text{ a prime number}\} \cup \{(0)\}$.
3.3. Let K be a number field. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two fractional ideals (in the Dedekind domain $\mathcal{O}_K$). Show that their product $\mathfrak{a}\mathfrak{b}$ is also a fractional ideal. (The product of fractional ideals is defined using the same expression for the product of ideals.) (see above)
3.4. Set $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \in \mathcal{O}_K\}$. Show that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.
3.5. Show that if $\mathfrak{a}$ is a principal fractional ideal, that is, $\mathfrak{a} = a\mathcal{O}_K \subset K$ for some $a \in K^\times$, then $\mathfrak{a}^{-1} = \frac{1}{a}\mathcal{O}_K$.
3.6. Let $K = \mathbb{Q}(\sqrt{-26})$ and $\mathfrak{a} = (3, 1 + \sqrt{-26}) \subset \mathcal{O}_K$ be an ideal. Find $x, y \in K$ such that $\mathfrak{a}^{-1} = x\mathcal{O}_K + y\mathcal{O}_K$.

4.
4.1.1 Show that the unit group of $\mathbb{Q}(\sqrt{-1})$ is cyclic of order 4.
4.1.2. Show that the unit group of $\mathbb{Q}(\sqrt{-3})$ is cyclic of order 6.
4.1.3. Show that the unit group of a quadratic imaginary field $\mathbb{Q}(\sqrt{m})$, where m is a negative square free integer such that $m \neq -1, -3$, is of order 2.
4.2.1. Show that the set of roots of unity contained in a real quadratic field is $\{\pm 1\}$.
4.2.2. Let B be a subgroup of $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, whose cardinality is infinite. Suppose there is a nonzero element $b \in B$ such that $2b = 0$. Show that $B \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
4.2.3. Let $N \neq 1$ be a positive square free integer. Let $u = x + y\sqrt{N} \in \mathbb{Z}[\sqrt{N}]^\times$ be an invertible element (here, $x, y \in \mathbb{Z}$). Show that

$$\{u, -u, u^{-1}, -u^{-1}\} = \{x + y\sqrt{N}, x - y\sqrt{N}, -x + y\sqrt{N}, -x - y\sqrt{N}\}.$$

4.3. Below we may use the Dirichlet unit theorem (and its consequences).
4.3.1. Show that the unit group of $\mathbb{Q}(\sqrt{3})$ is $\{\pm(2 + \sqrt{3})^n \,|\, n \in \mathbb{Z}\}$.
4.3.2. Show that the unit group of $\mathbb{Q}(\sqrt{7})$ is $\{\pm(8 + 3\sqrt{7})^n \,|\, n \in \mathbb{Z}\}$.
4.3.3. Compute the unit group of $\mathbb{Q}(\sqrt{5})$.

5. We may use the Dirichlet unit theorem and the fact that $\mathbb{Z}[\sqrt{2}]$ is a UFD.
5.1.1. Find infinitely many pairs $(x, y) \in \mathbb{Z}^2$ such that $x^2 - 2y^2 = 7$.
5.1.2. Find all pairs $(x, y) \in \mathbb{Z}^2$ such that $x^2 - 2y^2 = 7$.
5.2.1. Find infinitely many pairs $(x, y) \in \mathbb{Z}^2$ such that $x^2 - 2y^2 = 17$.
5.2.2. Find all pairs $(x, y) \in \mathbb{Z}^2$ such that $x^2 - 2y^2 = 17$.