PMATH 340 Number Theory, Exercises for Chapter 6 (Quadratic Rings)

1: (a) For $x, y \in \mathbf{Q}$, let $E(x + y\sqrt{2}) = \left|x^2 - 2y^2\right|$ and recall that E is a Euclidean norm in $\mathbf{Z}[\sqrt{2}\,]$. Let $a = 17 + 26\sqrt{2} \in \mathbf{Z}[\sqrt{2}\,]$ and $b = 5 + 3\sqrt{2} \in \mathbf{Z}[\sqrt{2}\,]$. Find $q, r \in \mathbf{Z}[\sqrt{2}\,]$ with $a = qb + r$ and $E(r) < E(b)$.

(b) Let $a = -20 + 30\,i \in \mathbf{Z}[i]$ and $b = -5 + 14\,i$ in $\mathbf{Z}[i]$. Use the Euclidean Algorithm to find $d = \gcd(a, b) \in \mathbf{Z}[i]$ then use Back-Substitution to find $s, t \in \mathbf{Z}[i]$ such that $as + bt = d$.

2: (a) Find the smallest unit $u > 1$ in $\mathbf{Z}[\sqrt{18}\,]$.

(b) Show that $\mathbf{Z}[\sqrt{10}\,]$ is not a unique factorization domain.

3: Let $w = e^{i\,\pi/3} = \frac{1+\sqrt{3}\,i}{2}$ and let $\mathbf{Z}[w] = \left\{a + bw \,\middle|\, a, b \in \mathbf{Z}\right\}$ and $\mathbf{Q}[w] = \left\{a + bw \,\middle|\, a, b \in \mathbf{Q}\right\}$.

(a) Show that $\mathbf{Z}[\sqrt{3}\,i] \subsetneq \mathbf{Z}[w]$ and $\mathbf{Q}[\sqrt{3}\,i] = \mathbf{Q}[w]$.

(b) Find all the units in $\mathbf{Z}[w]$.

(c) Show that $\mathbf{Z}[w]$ is a unique factorization domain (indeed a Euclidean domain) but $\mathbf{Z}[\sqrt{3}\,i]$ is not.

4: (a) Find the association classes in $\mathbf{Z}_{18}$.

(b) Find all the units and all the zero divisors in $\mathbf{Z}_{18}$.

(c) Find all the irreducible elements and all the prime elements in $\mathbf{Z}_{18}$.

5: (a) Use the method of the Sieve of Eratosthenes to find all irreducible elements $u \in \mathbf{Z}[\sqrt{2}\,i]$ with $\|u\| \le 10$ (where $\|u\|$ denotes the complex norm of u). Begin by drawing a grid which shows all the elements $u \in \mathbf{Z}[\sqrt{2}\,i]$ with $\|u\| \le 10$ and crossing off 0 and ± 1. At each step, circle the remaining elements of smallest complex norm and cross off their multiples: if you have circled u then cross off the elements uv with $v \in \mathbf{Z}[\sqrt{2}\,i] \setminus \{\pm 1\}$. To locate the multiples uv on your grid, it helps to make use of the fact that to multiply u and v you must multiply their lengths and add their angles.

(b) Let p be an odd prime in $\mathbf{Z}^+$. Show that p is reducible in $\mathbf{Z}\left[\sqrt{2}\,i\right]$ if and only if $p = x^2 + 2y^2$ for some $x, y \in \mathbf{Z}$.