MATH7421 Coursework 5 Solutions

1. We have that:
$$14 = 2 \cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13}).$$
Since $\mathbb{Z}[\sqrt{-13}]^\times = \{\pm 1\}$ we see that these factorisations are not simply a reordering and/or unit multiple of each other. It follows that these factorisations will be inequivalent if we can show that each factor is irreducible.

   Suppose that $2 = \alpha\beta$ for two non-zero non-units $\alpha, \beta \in \mathbb{Z}[\sqrt{-13}]$. Taking norms gives $4 = N(\alpha)N(\beta)$ and since $N(\alpha), N(\beta) \in \mathbb{Z}$ we have that $N(\alpha), N(\beta)|4$. Since we cannot have that $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$ (since otherwise α or β would be a unit) we must have that $N(\alpha) = N(\beta) = \pm 2$. However, there are no such elements since the equation $x^2 + 13y^2 = \pm 2$ has no integer solutions. Hence 2 is irreducible in $\mathbb{Z}[\sqrt{13}]$.

   Suppose that $7 = \alpha\beta$ for two non-zero non-units $\alpha, \beta \in \mathbb{Z}[\sqrt{-13}]$. Taking norms gives $49 = N(\alpha)N(\beta)$ and since $N(\alpha), N(\beta) \in \mathbb{Z}$ we have that $N(\alpha), N(\beta)|49$. Since we cannot have that $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$ (since otherwise α or β would be a unit) we must have that $N(\alpha) = N(\beta) = \pm 7$. However, there are no such elements since the equation $x^2 + 13y^2 = \pm 7$ has no integer solutions. Hence 7 is irreducible in $\mathbb{Z}[\sqrt{13}]$.

   Suppose that $1 \pm \sqrt{-13} = \alpha\beta$ for two non-zero non-units $\alpha, \beta \in \mathbb{Z}[\sqrt{-13}]$. Taking norms gives $14 = N(\alpha)N(\beta)$ and since $N(\alpha), N(\beta) \in \mathbb{Z}$ we have that $N(\alpha), N(\beta)|14$. Since we cannot have that $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$ (since otherwise α or β would be a unit) we must have that $N(\alpha) = 2$ and $N(\beta) = \pm 7$ or vice verse. However, we just proved that no such elements exist. Hence $(1 \pm \sqrt{-13})$ are both irreducible.

2. (a) We have that $v = 5 + 2\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$ is a unit, since $N(v) = 5^2 - 6 \cdot 2^2 = 1$.

   (b) Suppose that $1 < w < v$ is a smaller such unit and write $w = a + b\sqrt{6}$. Then by the strategy in the notes (or Exercise 1) we have that $0 < a < \frac{1+v}{2} = 3 + \sqrt{6} < 6$. Since $a \in \mathbb{Z}$ we must have that $1 \leq a \leq 5$.

   If $a = 1$ then $N(w) = a^2 - 6b^2 = 1 - 6b^2 = \pm 1$, which only has solution $b = 0$, so that $w = 1$. This is an invalid solution.

   If $a = 2$ then $N(w) = a^2 - 6b^2 = 4 - 6b^2 = \pm 1$, which has no solution.

   If $a = 3$ then $N(w) = a^2 - 6b^2 = 9 - 6b^2 = \pm 1$, which has no solution.

   If $a = 4$ then $N(w) = a^2 - 6b^2 = 16 - 6b^2 = \pm 1$, which has no solution.

   If $a = 5$ then $N(w) = a^2 - 6b^2 = 25 - 6b^2 = \pm 1$, which only has solution $b = \pm 2$, so that $w = 5 \pm 2\sqrt{6}$. This is an invalid solution.

   We've shown that there is no unit $1 < w < v$, so that v is the smallest such unit.

(c) In the notes we have proved that if $K = \mathbb{Q}(\sqrt{d})$ with $d > 1$ square-free and $v > 1$ is the smallest element of $\mathcal{O}_K^\times$ then $\mathcal{O}_K^\times = \{\pm v^m \,|\, m \in \mathbb{Z}\}$.

By the work done in (a) and (b) we then have that:

$$\mathbb{Z}[\sqrt{6}]^\times = \{\pm(5 + 2\sqrt{6})^m \,|\, m \in \mathbb{Z}\}.$$

(d) We saw in the notes that the integer solutions to $x^2 - dy^2 = \pm 1$ are in bijection with units $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

We can generate three positive integer solutions to $x^2 - 6y^2 = \pm 1$ by using our fundamental unit $v \in \mathbb{Z}[\sqrt{3}]$.

Since $v = 5 + 2\sqrt{6}$ we find that $(x, y) = (5, 2)$ is a solution (indeed $5^2 - 6 \cdot 2^2 = 1$).

Since $v^2 = (5 + 2\sqrt{6})^2 = 49 + 20\sqrt{6}$ we find that $(x, y) = (49, 20)$ is a solution (indeed $49^2 - 6 \cdot 20^2 = 1$).

Since $v^3 = (5 + 2\sqrt{6})(49 + 20\sqrt{6}) = 485 + 198\sqrt{3}$ we find that $(x, y) = (485, 198)$ is a solution (indeed $485^2 - 6 \cdot 198^2 = 1$).