2015-11-02 Introduction to number theory Problems

Some goals: 2.7, 2.9, 3.10, 4.8, 5, 6.2.

1. Set $A = \mathbb{Z}$. Note that A is a UFD (as proved in the first lecture).
1.1. Show that the set of units of A is $\{\pm 1\}$.
1.2. Show that a prime number $p \in \mathbb{Z}$ is a prime element.
1.3. Show that if $\alpha \in \mathbb{Z}$ is a prime element, then $\alpha = \pm p$ for some prime number p.

2. Set $A = \mathbb{Z}[\sqrt{-2}]$. We may use below that A is a UFD. For $\alpha = x + y\sqrt{-2}$, write $\overline{\alpha} = x - y\sqrt{-2}$.
2.1. Determine the units in A.
2.2. Show that

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod 8, \\ -1 & \text{if } p \equiv 5, 7 \pmod 8. \end{cases}$$

2.3. Let $p \in \mathbb{Z}$ be prime such that $p \equiv 5$ or $7 \pmod 8$. Show that $p \in A$ is prime.
2.4.1. Let $p \in \mathbb{Z}$ be prime such that $p \equiv 1$ or $3 \pmod 8$. Show that $p = \alpha\overline{\alpha}$ for some prime $\alpha \in A$.
2.4.2. Show that $\alpha A \neq \overline{\alpha} A$.
2.5. Note that $2 = -(\sqrt{-2})^2$. Show that $\sqrt{-2} \in A$ is prime.
2.6. Let $\alpha \in A$ be prime. Show that α is equal to βu where β is one of the primes above and u is a unit.
2.7. Show that the set of solutions in $\mathbb{N}$ of the equation $y^2 = x^3 - 2$ is $\{(3, 5)\}$.
2.8. Let p be a prime number in $\mathbb{Z}$ such that $p \equiv 5$ or $7 \pmod 8$. Show that the equation $p = x^2 + 2y^2$ has no solution in $\mathbb{Q}$. (Suggestion: Consider the equation $pz^2 - 2w^2 = 1$, compute the Hilbert symbols $a_v = (p, -2)_v$, then use the theorem that if $a_v \neq 1$ for some v then there exists no solution in $\mathbb{Q}_v$ (hence in $\mathbb{Z}$).)
2.9. Let p be an odd prime number. Show that a prime number $p \in \mathbb{Z}$ can be expressed in the form $x^2 + 2y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1$ or $3 \pmod 8$. (Suggestion: use 2.4.1 and 2.7)

3. Set $A = \mathbb{Z}[\zeta_3]$ where $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$. We may use below that A is a UFD. For $\alpha = x + y\zeta_3$ with $x, y \in \mathbb{Z}$, write $\overline{\alpha} = x + y\overline{\zeta_3}$ where $\overline{\zeta_3} = \frac{-1-\sqrt{-3}}{2}$.
3.1. Show that the set of units in A is $\{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$.
3.2. Show that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

3.3. Let $p \in \mathbb{Z}$ be prime such that $p \equiv 2 \pmod 3$. Show that $p \in A$ is prime.
3.4. Let $p \in \mathbb{Z}$ be prime such that $p \equiv 1 \pmod 3$. Show that $p = \alpha\overline{\alpha}$ for some prime $\alpha \in A$.
3.5. Note that $3 = -(\sqrt{-3})^2$. Show that $\sqrt{-3}$ is prime.
3.6. Let $\alpha \in A$ be prime. Show that α is equal to βu where β is one of the primes above and u is a unit.
3.7. Let $\beta \in A$. Show that there exists $i = 0, 1, 2$ such that $\zeta_3^i \beta \in \mathbb{Z}[\sqrt{-3}]$.
3.8. Let $p \in \mathbb{Z}$ be a prime number. Show that if $p \equiv 2 \pmod 3$, then the equation $p = x^2 + 3y^2$ has no solution in $\mathbb{Q}$.
3.9. (deleted)
3.10. Let $p \in \mathbb{Z}$ be a prime number. Show that $p \in \mathbb{Z}$ can be expressed in the form $x^2 + 3y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 3$. (Suggestion: use 3.4,3.7,3.9)

4. Set $A = \mathbb{Z}[\sqrt{2}]$. For $\alpha = x + y\sqrt{2} \in A$ with $x, y \in \mathbb{Z}$, write $\overline{\alpha} = x - y\sqrt{2}$. We may use below that A is a UFD.

4.1. Find 10 units in $\mathbb{Z}[\sqrt{2}]$.
4.2. Show that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

4.3. Let $p \in \mathbb{Z}$ be prime such that $p \equiv 3$ or $5 \pmod 8$. Show that $p \in A$ is prime.
4.4.1. Let $\alpha \in A$ be an element such that $\alpha\overline{\alpha} = -p$. Let $\gamma = (1-\sqrt{2})\alpha$. Show that $\gamma\overline{\gamma} = p$.
4.4.2. Let $p \in \mathbb{Z}$ be prime such that $p \equiv 1$ or $7 \pmod 8$. Show that $p = \alpha\overline{\alpha}$ for some prime $\alpha \in A$.
4.4.3. Show that $\alpha A \neq \overline{\alpha} A$.
4.5. Note that $2 = (\sqrt{2})^2$. Show that $\sqrt{2} \in A$ is prime.
4.6. Let $\alpha \in A$ be prime. Show that α is equal to βu where β is one of the primes above and u is a unit.
4.7. Let $p \in \mathbb{Z}$ be prime such that $p \equiv 3$ or $5 \pmod 8$. Show that the equation $p = x^2 - 2y^2$ has no solution in $\mathbb{Q}$.
4.8. Let p be a prime number. Show that there exist $x, y \in \mathbb{Z}$ such that $p = x^2 - 2y^2$ if and only if $p \equiv 1$ or $7 \pmod 8$.

5. You may use below that $A = \mathbb{Z}[i]$ is a UFD. Show that the set of solutions in $\mathbb{N}$ of the equation $y^2 = x^3 - 4$ is $\{(2,2),(5,11)\}$.

6. You may use below the fact that $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ is a unique factorization domain.
6.1. Determine the units in $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$.
6.2. Show that the set of solutions in $\mathbb{Z}$ of the equation $y^2 = x^3 - 11$ is $\{(3, \pm 4), (15, \pm 58)\}$.

7. Let A be a UFD. Let $\alpha_1, \ldots, \alpha_r, \beta \in A$ be nonzero elements. Suppose $\alpha_1 \cdots \alpha_r = \beta^k$ for some $k \in NN$. Suppose α_i and α_j are not divisible by the same prime element for $i \neq j$. (This means that there does not exist a prime element $\gamma \in A$ such that $\alpha_i A \supset \gamma A$ and $\alpha_j A \supset \gamma A$.) Prove that, for each $1 \leq i \leq r$, there exists a unit u_i and an element δ_i such that $\alpha_i = u_i \delta_i^k$.