The cautious seldom err. – Confucius

In the UFD problems below it will be helpful to set $\alpha = \prod p_i^{a_i}$, $\beta = \prod p_i^{b_i}$, $\gamma = \prod p_i^{c_i}$, $\kappa = \prod p_i^{d_i}$.

1. Let $D$ be a Unique Factorization Domain. Let $0 \neq \alpha, \beta, \gamma \in D$. Define the least common multiple $lcm(\alpha, \beta)$ by

$$\kappa = lcm(\alpha, \beta) = \frac{\alpha \beta}{gcd(\alpha, \beta)}$$

(a) Express the exponents $d_i$ of $\kappa$ as a simple expression of the exponents $a_i, b_i$ of $\alpha, \beta$.

(b) Show that $\alpha | \kappa$ and $\beta | \kappa$.

(c) Show that if $\alpha | \lambda$ and $\beta | \lambda$ then $\kappa | \lambda$.

2. Continuing, in a UFD $D$.

(a) Let $\kappa = gcd(gcd(\alpha, \beta), \gamma))$. Show that $\kappa$ doesn’t depend on the order of $\alpha, \beta, \gamma$. We call this $\kappa = gcd(\alpha, \beta, \gamma)$.

(b) Let $\kappa = lcm(lcm(\alpha, \beta), \gamma))$. Show that $\kappa$ doesn’t depend on the order of $\alpha, \beta, \gamma$. We call this $\kappa = lcm(\alpha, \beta, \gamma)$. (This extends to any number of variables.)

(c) Show

$$gcd(lcm(\alpha, \beta), lcm(\alpha, \gamma), lcm(\beta, \gamma)) = lcm(gcd(\alpha, \beta), gcd(\alpha, \gamma), gcd(\beta, \gamma))$$

3. In $\mathbb{Z}[i]$ let $\overline{\pi}$ denote the complex conjugate and $\sim$ denote associate.

(a) Set $\pi = 1 + i$. Show that $\pi \sim \overline{\pi}$.

(b) Show that $\pi = 1 + i$ is the only nonreal prime in $\mathbb{Z}[i]$ with $\pi \sim \overline{\pi}$.

(We don’t count, say, $3i$ as nonreal as it has a real associate $3$.)

(c) Let $m, n \in \mathbb{Z}$, nonzero. Show that $gcd(m, n)$, as defined in $\mathbb{Z}$, is the same as $gcd(m, n)$, defined in $\mathbb{Z}[i]$.

4. By $C^*$ we mean $C - \{0\}$, the nonzero complex numbers. Here we examine $(C^*, \cdot)$, the group under multiplication. Let $S$ be the set of solutions to the equation $z^{12} = 1$. 
(a) Draw a nice picture of $S$ on the complex plane $C$.
(b) For each $z \in S$ marked above, give the minimal positive integer $s$ with $z^s = 1$.
(c) Prove that $S$ is a subgroup of $C^*$
(d) Prove that $S$ is the only subgroup of $C^*$ with (precisely) twelve elements.
(e) Just for Fun – check out: https://www.youtube.com/watch?v=O21xFX7QBpE

5. Set $\mathbb{Z}[\sqrt{-2}] = \{a+b\sqrt{-2}\}$. This is a Euclidean Domain (a nice exercise but not requested) with $d(\alpha) = |\alpha|^2 = a^2 + 2b^2$. Assuming that show:

(a) If $d(\alpha)$ is an integer prime then $\alpha$ is a prime.
(b) If $p$ is an integer prime and there $p = x^2 + 2y^2$ has an integer solution then $p$ is not a prime in $\mathbb{Z}[\sqrt{-2}]$.
(c) If $p$ is an integer prime and there $p = x^2 + 2y^2$ has no integer solution then $p$ is a prime in $\mathbb{Z}[\sqrt{-2}]$.

Mathematics, rightly viewed, possesses not only truth, but supreme beauty - a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of painting or music, yet sublimely pure, and capable of a stern perfection such as only the greatest art can show. The true spirit of delight, the exaltation, the sense of being more than Man, which is the touchstone of the highest excellence, is to be found in mathematics as surely as in poetry
– Bertrand Russell, The Study of Mathematics, 1902