Problem 1. Consider the ring $R = \mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$ of Eisenstein integers, where $\omega = (-1+\sqrt{-3})/2$ (see Homeworks 17, 23 for various facts about R).

a) Let $x = a + b\omega$, $y = c + d\omega$ be elements of R such that $x \neq 0$. Prove that the complex number y/x can be written as $u + w\omega$ for some rational numbers u, w.

b) Consider the map $N : R \longrightarrow \mathbb{Z}$ defined by $N(a + b\omega) = a^2 - ab + b^2$ (so $N(x)$ is just the square of the absolute value of the complex number x). Use N to prove that R is an Euclidean domain (Hint: Mimic the argument from class for the ring of Gaussian integers).

c) Let $x = a + b\omega \in R$. Prove that there exists $c + d\omega \in R$ which is associated with x and such that $c \geq 0$, $d \geq 0$ (Hint: Use d) of Problem 1 from homework 23).

d) Let p be an odd prime such that -3 is a quadratic non-residue modulo p . Prove that p is irreducible in R. (Use h) of Problem 1 from homework 23). Prove the same for $p = 2$.

e) Suppose that p is an odd prime such that -3 is a quadratic residue modulo p. Prove that p is not irreducible in R. Conclude that there exist positive integers a, b such that $p = a^2 - ab + b^2$ (use c)).

f) Use quadrartic reciprocity to prove that -3 is a quadratic residue modulo p iff $p \equiv 1 \pmod 3$.

Solution: a) This follows from the following computation

$$\frac{y}{x} = \frac{c + d\omega}{a + b\omega} = \frac{(c + d\omega)(a + b\overline{\omega})}{(a + b\omega)(a + b\overline{\omega})} = \frac{ac + bd + ad\omega + bc\overline{\omega}}{a^2 - ab + b^2} = \frac{ac + bd - bc}{a^2 - ab + b^2} + \frac{ad - bc}{a^2 - ab + b^2}\omega$$

(we used the equality $\overline{\omega} = -1 - \omega$).

b) Let $x = a + b\omega$, $y = c + d\omega$ be elements of R, $x \neq 0$. By a) there are rational numbers u, w such that $y/x = u + w\omega$. There are integers k, m such that $|u - k| \leq 1/2$ and $|w - m| \leq 1/2$. Set $p = u - k$ and $q = w - m$. Thus $y/x = (k + l\omega) + (p + q\omega)$. In other words,

$$y = (k + l\omega)x + (p + q\omega)x.$$

Clearly, $k + l\omega \in R$ so $r = (p + q\omega)x = y - (k + l\omega)x \in R$. Thus $y = (k + l\omega)x + r$

and

$$N(r) = N((p+q\omega)x) = N(p+q\omega)N(x) = (p^2 - pq + q^2)N(x).$$

Since $|p| \leq 1/2$ and $|q| \leq 1/2$, we have $p^2 - pq + q^2 \leq |p|^2 + |p||q| + |q|^2 \leq 3/4$. Thus $N(r) \leq 3N(x)/4 < N(x)$. This shows that N is an Euclidean function on R and R is an Euclidean domain.

c) Since $1. -1, \omega, -\omega, \omega^2, -\omega^2$ are the only elements invertible in R, the elements associated with $a+b\omega$ are $a+b\omega$, $(a+b\omega)\cdot(-1) = -a-b\omega$, $(a+b\omega)\omega = -b+(a-b)\omega$, $(a+b\omega)(-\omega) = b+(b-a)\omega$, $(a+b\omega)\omega^2 = (b-a)-a\omega$, $(a+b\omega)(-\omega^2) = (a-b)+a\omega$. If both a, b are non-negative then take $c = a, d = b$. If both a, b are non-positive, take $c = -a, d = -b$. If a is non-negative and $b < 0$ take $c = a-b, d = a$. Finally, if $a < 0$ and b is nonnegative, take $c = b, d = b-a$.

d) Suppose that $p = xy$ for some $x, y \in R$. Thus $p^2 = N(p) = N(xy) = N(x)N(y)$. It follows that one of $N(x)$, $N(y)$ is divisible by p. Suppose that $p|N(x)$ (the other possibility is handled the same way). This means that if $x = a+b\omega$ then $p|N(x) = a^2 - ab + b^2$. By Problem 1 f) from homework 23, we have $p|a$ and $p|b$ so $p^2|N(x)$. From $p^2 = N(x)N(y)$ it follows now that $N(x) = p^2$ and $N(y) = 1$. Thus y is invertible by Problem 1 c) for homework 23. This proves that p is irreducible.

Alternatively, from Problem 1 h) for homework 23 the ideal pR is prime. Thus p is prime and hence irreducible.

e) In Problem 1 i) from homework 23 we showed that pR is not prime, i.e. p is not a prime element. Since R is UFD by b), we see that p is not irreducible (recall that in a UFD irreducible elements are prime). Thus $p = xy$ for some x, y non-invertible in R. It follows that $p^2 = N(p) = N(xy) = N(x)N(y)$. Since neither x nor y is invertible, both $N(x)$ and $N(y)$ are larger than 1 so we must have $N(x) = p = N(y)$. By c) there is $a+b\omega \in R$ such that $a \geq 0$, $b \geq 0$ and $a+b\omega \in R$ is associated to x. Thus $p = N(x) = N(a+b\omega) = a^2 - ab + b^2$ (we use here the simple observation that if x, y are associated then $x = yu$ for some invertible u so $N(x) = N(yu) = N(y)N(u) = N(y)$).

f) Recall that -3 is a quadratic residue modulo p iff the Legendre symbol $(\frac{-3}{p}) = 1$.

The quadratic reciprocity gives us

$$(\frac{3}{p})(\frac{p}{3}) = (-1)^{(p-1)(3-1)/4} = (-1)^{(p-1)/2}.$$

Thus

$$(\frac{3}{p}) = (\frac{p}{3})(-1)^{(p-1)/2}.$$

Recall that

$$(\frac{-1}{p}) = (-1)^{(p-1)/2}.$$

Consequently,

$$(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{(p-1)/2}(\frac{p}{3})(-1)^{(p-1)/2} = (\frac{p}{3}).$$

Clearly

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

This proves that $(\frac{-3}{p}) = 1$ iff $p \equiv 1 \pmod 4$.

Problem 2. Let R be a PID. Consider two elements $a, b \in R$. Since R is a PID, there is $d \in R$ such that $aR + bR = dR$. Prove that for any $c \in R$ we have $c|d$ iff $c|a$ and $c|b$. What would be appropriate to call d?

Solution: Note that $aR \subseteq dR$ and $bR \subseteq dR$ so $d|a$ and $d|b$. Suppose that $c|d$. Then clearly $c|a$ and $c|b$. Conversely, if $c|a$ and $c|b$ then $aR \subseteq cR$ and $bR \subseteq cR$. Since cR is an ideal, we have $aR + bR \subseteq cR$. In other words, $dR \subseteq cR$ and consequently $c|d$.

In analogy with the integers, d should be called a greatest common divisor of a and b.