Problema 34. Considerem l'anell $\mathbb{Z}[i] := \{a + b\,i \;:\; a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ i la seva norma $N(a + b\,i) = a^2 + b^2$, $a, b \in \mathbb{Z}$.

(a) Demostreu que per a tota parella d'elements $x, y \in \mathbb{Z}[i]$, $y \neq 0$, existeixen q, $r \in \mathbb{Z}[i]$ tals que $x = qy + r$, amb $r = 0$ o bé $N(r) < N(y)$.

(b) Deduïu que $\mathbb{Z}[i]$ és un domini d'ideals principals.

Solució.

(a) Com que $\mathbb{C}$ és un cos, la fracció existeix. A més, $\mathbb{Z}[i] \subseteq \mathbb{C}$ és un anell. Tot això ens permet dir que $x, y \neq 0 \in \mathbb{Z}[i]$ són de la forma $x = a+bi$, $y = c+di$ amb $a, b, c, d \in \mathbb{Z}$.

Fem: $\frac{x}{y} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{\alpha+\beta i}{c^2+d^2}$, amb $\alpha, \beta \in \mathbb{Z}$. Per tant, tenim que $\frac{x}{y} = \frac{\alpha}{c^2+d^2} + \frac{\beta i}{c^2+d^2}$, on $\frac{\alpha}{c^2+d^2}, \frac{\beta}{c^2+d^2} \in \mathbb{Q}$.

Anomenem $q_1 = \frac{\alpha}{c^2+d^2}$ i $q_2 = \frac{\beta}{c^2+d^2}$, i ens queda $\frac{x}{y} = q_1 + q_2 i \in \mathbb{Q}[i]$. Per tant, $x = y(q_1 + q_2 i)$.

Aproximem q_1, q_2 als enters més propers, és a dir, agafem $q_1', q_2' \in \mathbb{Z}$ tals que $|q_1' - q_1| \leq 1/2$ i $|q_2' - q_2| \leq 1/2$.

Per tant, tenim que $x = [(q_1 + q_2 i) - (q_1' + q_2' i) + (q_1' + q_2' i)]y = [q_1 + q_2 i - (q_1' + q_2' i)]y + (q_1' + q_2' i)y$.

Anomenem $Q = q_1' + q_2' i$ i $R = [q_1 + q_2 i - (q_1' + q_2' i)]y$. Per tant, ens queda
$x = yQ + R \Longrightarrow x - yQ = R$. Com que $Q, x, y \in \mathbb{Z}[i] \Longrightarrow R \in \mathbb{Z}[i]$.

Hem demostrat l'existència de $Q, R \in \mathbb{Z}[i]$. Aem a veure que o bé $R = 0$ o bé $N(R) < N(y)$.

Cas 1: $\frac{\alpha}{c^2+d^2} \in \mathbb{Z}$ i $\frac{\beta}{c^2+d^2} \in \mathbb{Z} \Longrightarrow R = 0$ ja que la divisió és entera.

Cas 2: $\frac{\alpha}{c^2+d^2} \notin \mathbb{Z}$ i $\frac{\beta}{c^2+d^2} \notin \mathbb{Z}$, veiem que $N(R) < N(y)$.

$N(R) = N([q_1 + q_2 i - (q_1' + q_2' i)]y) = N([q_1 + q_2 i - (q_1' + q_2' i)])N(y) = N([(q_1 - q_1') + (q_2 - q_2')i])N(y) = [(q_1 - q_1')^2 + (q_2 - q_2')^2]N(y) \leq [(1/2)^2 + (1/2)^2]N(y) = 1/2N(y) < N(y)$.

(b) L'anell $\mathbb{Z}[i]$ és domini d'ideals principals (DIP) si tot ideal $I \subseteq \mathbb{Z}[i]$ és principal. Sabem que si $\mathbb{Z}[i]$ és un domini euclidià (DE) $\Rightarrow \mathbb{Z}[i]$ és un DIP. Per tant, n'hi ha prou amb demostrar que $\mathbb{Z}[i]$ és un DE, és a dir, que compleix:

(a) $\mathbb{Z}[i]$ és un domini d'integritat. Veiem-ho:
$\mathbb{C}$ és un cos $\Longrightarrow \mathbb{C}$ és un domini $\Longrightarrow \mathbb{Z}[i] \subseteq \mathbb{C}$ és un domini i, en particular, és un domini d'integritat perquè $\mathbb{C}$ és un cos commutatiu i, per tant, no té divisors de zero. Així doncs, $\mathbb{C}$ és un domini d'integritat i $\mathbb{Z}[i] \subseteq \mathbb{C}$ també.

(b) Existeix una funció $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ tal que:

(i) Si $a|b, a, b \in \mathbb{Z}[i] \Longrightarrow N(a) \leq N(b)$. Veiem-ho:
Si $a|b \Longrightarrow \exists c \in \mathbb{Z}[i]$, $c \neq 0$, tal que $b = a \cdot c$.
I tenim $N(b) = N(a \cdot c) = N(a)N(c)$.

- Si $b = 0 \Longrightarrow b = a \cdot c = 0 \Longrightarrow a = 0$, ja que $\mathbb{Z}[i]$ és un domini d'integritat i $c \neq 0$. Així doncs, $N(a) = 0$ i $N(b) = 0$, per tant, es compleix $N(a) \leq N(b)$.
- Si $b \neq 0 \Longrightarrow a \neq 0$ i $b \neq 0$ per ser $\mathbb{Z}[i]$ un domini d'integritat. Definim $c := x + yi \in \mathbb{Z}[i]$ i veiem que $N(c) = 0 \Longleftrightarrow x^2 + y^2 = 0 \Longleftrightarrow x = y = 0$. Aquesta última igualtat ens diu que $c = 0$ però $c \neq 0$ per definició. Per tant, si $c \neq 0 \Longrightarrow N(c) \neq 0$ i, concretament, $N(c) \geq 1$. Es compleix $N(a) \geq N(a)N(c) = N(a \cdot c) = N(b)$.

(ii) $\forall x, y \in \mathbb{Z}[i]$, $y \neq 0$, existeixen q, $r \in \mathbb{Z}[i]$ tals que $x = qy + r$, amb $r = 0$ o bé $N(r) < N(y)$.
Que és l'enunciat de l'apartat (a) del problema i ja hem demostrat que es compleix.