(A) Keep it up

Algebra and Number Theory

43) Using the Euclidean algorithm on:

$$f(x) = X^4 + X^3 + 2X^2 + X + 1$$
$$g(x) = X^3 + 2X^2 + X + 2$$

in the field $\mathbb{Q}[X]$ gives:

$$X^4 + X^3 + 2X^2 + X + 1 = (X-1)(X^3 + 2X^2 + X + 2) + (3X^2 + 3)$$
$$X^3 + 2X^2 + X + 2 = (\tfrac{1}{3}X + \tfrac{2}{3})(3X^2 + 3) + 0$$

The last non-zero remainder is $3X^2 + 3$, so this is then a greatest common divisor of $f(x)$ and $g(x)$.

This gcd can be normalised to the monic gcd $X^2 + 1$ by multiplying $3X^2 + 3$ by $3^{-1} = \tfrac{1}{3} \in \mathbb{Q}$

Back-tracking through the steps of the Euclidean algorithm shows:

$$3X^2 + 3 = (X^4 + X^3 + 2X^2 + X + 1) - (X-1)(X^3 + 2X^2 + X + 2)$$
$$= f(x) - (X-1)g(x).$$

Then we get:

$$\begin{aligned} X^2 + 1 &= \tfrac{1}{3}(3X^2 + 3) \\ &= \tfrac{1}{3}(f(x) - (X-1)g(x)) \\ &= \tfrac{1}{3}f(x) - \tfrac{1}{3}(X-1)g(x) \\ &= \tfrac{1}{3}f(x) + (-\tfrac{1}{3}X + \tfrac{1}{3})g(x) \end{aligned}$$

So the monic gcd of $f(x)$ and $g(x)$ is $X^2 + 1$, and it can be written as:

$$\begin{aligned} X^2 + 1 &= \tfrac{1}{3}f(x) + (-\tfrac{1}{3}X + \tfrac{1}{3})g(x) \\ &= a(x)f(x) + b(x)g(x) \end{aligned}$$

with $a(x) = \tfrac{1}{3}$ and $b(x) = -\tfrac{1}{3}X + \tfrac{1}{3}$.

✓ Good

45) Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$.

Consider α and β as elements in $\mathbb{Q}[i]$ since $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$. Since $\mathbb{Q}[i]$ is a field, multiplicative inverses exist for all non-zero elements, so division is possible.

Since $\beta \neq 0$, $\alpha/\beta \in \mathbb{Q}[i]$, so $\alpha/\beta = x + iy$ for some $x, y \in \mathbb{Q}$.

Since x and y are rational, they are at most $\frac{1}{2}$ from an integer.

So we can write $x = x' + a$, $y = y' + b$ with x', y' integers and $|a| \leq \frac{1}{2}$, $|b| \leq \frac{1}{2}$. Note that since $a = x - x'$, $b = y - y'$, and $x, y \in \mathbb{Q}$, $x', y' \in \mathbb{Z} \subseteq \mathbb{Q}$. Then $a, b \in \mathbb{Q}$ since $\mathbb{Q}$ is a ring.

And we have:

$$\begin{aligned} \alpha/\beta &= (x' + a) + (y' + b)i \\ &= (x' + iy') + (a + ib) \end{aligned}$$

Now take $q = x' + iy'$, and $\rho = a + ib$, so that $\alpha/\beta = q + \rho$.

Clearly $q = x' + iy' \in \mathbb{Z}[i]$ since x' and y' are integers, and $\rho = a + ib \in \mathbb{Q}[i]$ with $|a| \leq \frac{1}{2}$, $|b| \leq \frac{1}{2}$, since a, b are rational.

Now we get: $\alpha = (q + \rho)\beta = q\beta + \rho\beta$.

Take $r = \rho\beta$. Since $\alpha = q\beta + r$, then $r = \alpha - q\beta$, and as $\alpha, \beta, q \in \mathbb{Z}[i]$, so $r \in \mathbb{Z}[i]$ as $\mathbb{Z}[i]$ is a ring.

Extend N to be defined from $\mathbb{Q}[i]$ to $\mathbb{Q}_{\geq 0}$, by $N(a+ib) = a^2 + b^2$ for any $a+ib \in \mathbb{Q}[i]$. This new definition agrees with the old definition on $\mathbb{Z}[i]$ since for any $a+ib \in \mathbb{Q}[i]$ with a, b integers so that $a+ib \in \mathbb{Z}[i] \subseteq \mathbb{Q}[i]$, $N_{\mathbb{Z}[i]}(a+bi) = a^2 + b^2 = N_{\mathbb{Q}[i]}(a+bi)$.

Note that $N(a+bi) \geq 0$ since for any $x \in \mathbb{Q}$, $x^2 \geq 0$, and that $N(a+bi) = 0$ if and only if $a = b = 0$ so that $a + bi = 0$ since for any $x \in \mathbb{Q}$, $x^2 = 0$ if and only if $x = 0$.

Algebra and Number Theory.

Question 12ii) shows that this N preserves multiplication, so:

$$\begin{aligned} N(r) &= N(\rho\beta) \\ &= N(\rho)N(\beta) \\ &= N(a+bi)N(\beta) \\ &= (a^2+b^2)N(\beta) \\ &\leqslant ((1/2)^2 + (1/2)^2)N(\beta) \quad \text{since } |a|\leqslant 1/2,\ |b|\leqslant 1/2 \text{ from above, giving } a^2\leqslant (1/2)^2,\ b^2\leqslant (1/2)^2 \\ &= ((1/4)+(1/4))N(\beta) \\ &= 1/2\, N(\beta) \\ &< N(\beta) \quad \text{since } N(\beta)\geqslant 0, \text{ and } N(\beta)\neq 0 \text{ since } \beta\neq 0 \text{ by assumption.} \end{aligned}$$

So as required, for any $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$, we can write $\alpha = q\beta + r$ for some $q, r \in \mathbb{Z}[i]$ with $N(r) < N(\beta)$.

✓ great

iii) Applying the procedure to $38+41i$, $8+31i$ to find a gcd of them in $\mathbb{Z}[i]$ gives:

— Take $\alpha = 38+41i$, $\beta = 8+31i \neq 0$

$$\frac{\alpha}{\beta} = \frac{38+41i}{8+31i}$$

$$= \frac{(38+41i)(8-31i)}{(8+31i)(8-31i)}$$

$$= \frac{(38\times 8 + 41\times 31) + (38\times -31 + 41\times 8)i}{8^2+31^2}$$

$$= \frac{1575 + -850i}{1025}$$

$$= \frac{63}{41} - \frac{34}{41}i$$

But $\frac{63}{41} = 2 - \frac{19}{41}$, where $\frac{19}{41} \leqslant \frac{1}{2}$, and

$-\frac{34}{41} = -1 + \frac{7}{41}$, where $\frac{7}{41} \leqslant \frac{1}{2}$

So $q = 2-i$

And $r = \alpha - q\beta$

$= (38+41i) - (2-i)(8+31i)$

$$= (38+41i) - (47+54i)$$
$$= -9 - 13i$$

$$\Rightarrow (38+41i) = (2-i)(8+31i) + (-9-13i)$$

— Take $\alpha = 8+31i$, $\beta = -9-13i \neq 0$.

$$\frac{\alpha}{\beta} = \frac{8+31i}{-9-13i}$$

$$= -\frac{19}{10} - \frac{7}{10}i$$

$$= \left(-2+\frac{1}{10}\right) + \left(-1+\frac{3}{10}\right)i$$

where $\frac{1}{10} < \frac{1}{2}$, $\frac{3}{10} < \frac{1}{2}$

So $q = -2-i$

$$r = (8+31i) - (-2-i)(-9-13i)$$
$$= (8+31i) - (5+35i)$$
$$= 3-4i$$

$$\Rightarrow (8+31i) = (-2-i)(-9-13i) + (3-4i)$$

— Take $\alpha = -9-13i$, $\beta = 3-4i \neq 0$

$$\frac{\alpha}{\beta} = \frac{-9-13i}{3-4i}$$

$$= 1-3i.$$

So $q = 1-3i$, $r = 0$

$$\Rightarrow (-9-13i) = (1-3i)(3-4i) + 0.$$

So the steps of this Euclidean algorithm are:

$$38+41i = (2-i)(8+31i) + (-9-13i)$$
$$8+31i = (-2-i)(-9-13i) + (3-4i)$$
$$-9-13i = (1-3i)(3-4i) + 0$$

And the last non-zero remainder is $3-4i$, so $3-4i$ is a gcd of $38+41i$ and $8+31i$ in $\mathbb{Z}[i]$.

Algebra and Number Theory

Back-tracking through the steps of this algorithm shows:

$$\begin{aligned}
3-4i &= (8+31i) - (-2-i)(-9-13i) \\
&= (8+31i) - (-2-i)[(38+41i) - (2-i)(8+31i)] \\
&= (1 + (-2-i)(2-i))(8+31i) \\
&\qquad - (-2-i)(38+41i) \\
&= (1+(-4-1))(8+31i) + (2+i)(38+41i) \\
&= (-4)(8+31i) + (2+i)(38+41i)
\end{aligned}$$

So a gcd of $38+41i$, and $8+31i$ in $\mathbb{Z}[i]$ is $3-4i$, and this can be written as:

$$\begin{aligned}
3-4i &= (2+i)(38+41i) + (-4)(8+31i) \\
&= \gamma(38+41i) + \delta(8+31i)
\end{aligned}$$

with $\gamma = 2+i$ and $\delta = -4$

✓ Brilliant

Nice thorough explanation