ALGEBRA AND NUMBER THEORY HOMEWORK

Matthew Palmer - Group 4

Due 17/11/09

43)

We want the monic $\gcd(X^4 + X^3 + 2X^2 + X + 1, X^3 + 2X^2 + X + 2)$. We use the Euclidean algorithm:

$$\begin{aligned} X^4 + X^3 + 2X^2 + X + 1 &= (X^3 + 2X^2 + X + 2)(X - 1) + (3X^2 + 3) \\ X^3 + 2X^2 + X + 2 &= (3X^2 + 3)\left(\frac{X + 2}{3}\right) = (X^2 + 1)(X + 2) \end{aligned}$$

Hence a gcd is $3X^2 + 3$, and the monic gcd is $X^2 + 1$. To re-express this in terms of $f(X)$ and $g(X)$, we have

$$X^4 + X^3 + 2X^2 + X + 1 = (X^3 + 2X^2 + X + 2)(X - 1) + 3(X^2 + 1)$$

— hence

$$\boxed{X^2 + 1 = \tfrac{1}{3}f(X) + \tfrac{1-X}{3}g(X)}$$

45i)

Let $\alpha = a_1 + a_2 i$ and $\beta = b_1 + b_2 i$ be in $\mathbb{Z}[i]$, with $\beta \neq 0$. Write

$$\frac{\alpha}{\beta} = q + \rho, \quad q \in \mathbb{Z}[i], \quad \rho = p_1 + p_2 i, \quad p_1, p_2 \in \mathbb{Q}, \quad |p_1|, |p_2| \leq \frac{1}{2}.$$

As $\beta \neq 0$, we can multiply throughout by β:

$$\alpha = q\beta + \rho\beta$$

We know that $\alpha \in \mathbb{Z}[i]$, and $q, \beta \in \mathbb{Z}[i]$ which implies $q\beta \in \mathbb{Z}[i]$, so $\alpha - q\beta \in \mathbb{Z}[i]$, and hence $\rho\beta \in \mathbb{Z}[i]$. Let $r = \rho\beta$. Then

$$r = (p_1 b_1 - p_2 b_2) + (p_1 b_2 + p_2 b_1)i,$$

and hence

$$\begin{aligned} N(r) &= (p_1 b_1 - p_2 b_2)^2 + (p_1 b_2 + p_2 b_1)^2 \\ &= p_1^2 b_1^2 - 2p_1 p_2 b_1 b_2 + p_2^2 b_2^2 + p_1^2 b_2^2 + 2p_1 p_2 b_1 b_2 + p_2^2 b_1^2 \\ &= p_1^2 b_1^2 + p_2^2 b_2^2 + p_1^2 b_2^2 + p_2^2 b_1^2 \\ &= (p_1^2 + p_2^2)(b_1^2 + b_2^2) \\ N(r) &= (p_1^2 + p_2^2)N(\beta). \end{aligned}$$

We know $|p_1|, |p_2| \leq \frac{1}{2}$ — so $p_1^2, p_2^2 \leq \frac{1}{4}$ and hence

$$p_1^2 + p_2^2 \leq \frac{1}{2}$$

$$(p_1^2 + p_2^2)N(\beta) \leq \frac{N(\beta)}{2}$$

$$N(r) \leq \frac{N(\beta)}{2} < N(\beta)$$

$$\boxed{N(r) < N(\beta)}$$

45iii)

We have $\alpha = 38 + 41i, \beta = r_0 = 8 + 31i$. Then

$$\frac{38 + 41i}{8 + 31i} = q_1 + \rho_1$$

$$\frac{63 - 34i}{41} = q_1 + \rho_1$$

$$(2 - i) + \frac{-19 + 7i}{41} = q_i + \rho_1,$$

and hence $q_1 = 2 - i,\ \rho_1 = \frac{-19+7i}{41}$. So

$$38 + 41i = (2 - i)(8 + 31i) + \frac{(-19 + 7i)(8 + 31i)}{41}$$

$$38 + 41i = (2 - i)(8 + 31i) + (-9 - 13i). \tag{1}$$

Now

$$\frac{8 + 31i}{-9 - 13i} = q_2 + \rho_2$$

$$\frac{-19 - 7i}{10} = q_2 + \rho_2$$

$$(-2 - i) + \frac{1 + 3i}{10} = q_2 + \rho_2,$$

and hence $q_2 = -2 - i, \rho_2 = \frac{1+3i}{10}$. So

$$8 + 31i = (-2 - i)(-9 - 13i) + \frac{(-9 - 13i)(1 + 3i)}{10}$$

$$8 + 31i = (-2 - i)(-9 - 13i) + (3 - 4i). \tag{2}$$

Now

$$\frac{-9 - 13i}{3 - 4i} = 1 - 3i + 0$$

and so

$$-9 - 13i = (1 - 3i)(3 - 4i).$$

So a greatest common divisor of $38 + 41i$ and $8 + 31i$ is $3 - 4i$. We express this in the form

$$\gamma(38 + 41i) + \delta(8 + 31i)$$

by back-substitution. By (2),

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

Then by (1),

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

and hence

$$3 - 4i = 8 + 31i + (2 + i)(38 + 41i + (-2 + i)(8 + 31i)) = -4(8 + 31i) + (2 + i)(38 + 41i).$$

So

$$\boxed{3 - 4i = -4(8 + 31i) + (2 + i)(38 + 41i)}$$