HERKANSING ALGEBRA 2, 10–13 UUR

1 a) We bepalen α met het algoritme van Euclides
Merk op: $N(3+5i) = 3^2+5^2 = 34$, $N(8) = 64$
Er geldt

$$\frac{8}{3+5i} = \frac{8(3-5i)}{34} = \frac{12}{17} - \frac{20}{17}i = 1-i + \left(-\frac{5}{17} - \frac{3}{17}i\right)$$

Dus

$$8 = (1-i)(3+5i) + \left(-\frac{5}{17} - \frac{3}{17}i\right)(3+5i)$$
$$= (1-i)(3+5i) - 2i$$

Dus $(3+5i, 8) = (3+5i, -2i)$

$$\frac{3+5i}{-2i} = \frac{-5+3i}{2} = -3+i + \left(-\frac{1}{2} + \frac{1}{2}i\right)$$

$3+5i = (-2i)(-3+i) + 1-i$, $(3+5i, -2i) = (-2i, 1-i) = (1-i)$,

want $-2i = (1-i)^2$. Dus $\boxed{(8, 3+5i) = (1-i)}$

$1-i$ is een irreducibel element dus een priemelement van $\mathbb{Z}[i]$. Dus $(1-i)$ is een priemideaal

b) $X^2 - X(Y^2-2Y+1) + Y^2 - Y = X^2 - X(Y-1)^2 + Y(Y-1)$
Volgens het criterium van Eisenstein, toegepast op $\mathbb{C}[Y]$ en het irreducibele element $Y-1$, is $X^2 - X(Y-1)^2 + Y(Y-1)$ irreducibel in $\mathbb{C}[Y][X] = \mathbb{C}[X,Y]$. Dus $(X^2 - X(Y^2-2Y+1) + Y^2 - Y)$ is een priemideaal

c) Volgens het criterium van Eisenstein toegepast met het priemgetal 7, is $X^4 - 14X + 28 = X^4 - 2 \cdot 7X + 2^2 \cdot 7$ irreducibel in $\mathbb{Z}[X]$. Dus $(X^4 - 14X + 28)$ is een priemideaal

$(X^4 - 14X + 28, 3) = (X^4 + X + 1, 3)$

$\mathbb{Z}[X]/(X^4+X+1, 3) \cong \mathbb{F}_3[X]/(X^4+X+1)$

X^4+X+1 is ~~irreducibel~~ in $\mathbb{F}_3[X]$ want 1 is een nulpunt

Dus $\mathbb{Z}[X]/(X^4+X+1, 3)$ is geen priemideaal

2 a) $D(f_c) = -R(f_c, f_c') = -R(X^3+3X^2+6X+c,\ 3X^2+6X+6)$
$= -R(3X^2+6X+6,\ X^3+3X^2+6X+c) = -3^3 R(X^2+2X+2,\ X^3+3X^2+6X+c)$

$$\begin{array}{l|l}
X^2+2X+2 \,/\, X^3+3X^2+6X+c & X+1 \\
\quad\ \underline{X^3+2X^2+2X} & \\
\qquad\quad X^2+4X+c & \\
\qquad\quad \underline{X^2+2X+2} & \\
\qquad\qquad 2X+c-2 &
\end{array}$$

$= -3^3 R(X^2+2X+2,\ 2X+c-2)$
$= -3^3 R(2X+c-2,\ X^2+2X+2) = -3^3 2^2 R(X+\frac{c-2}{2},\ X^2+2X+2)$
$= -108\left\{\left(\frac{c-2}{2}\right)^2 - 2\,\frac{c-2}{2} + 2\right\} = \boxed{-27\{c^2-8c+20\}}$

f_c heeft dubbele nulpunten $\Leftrightarrow D(f_c)=0 \Leftrightarrow \boxed{c = 4 \pm 2i}$

b) Stel f_p is reducibel in $\mathbb{Z}[X]$. Dan heeft f_p een lineaire factor $X-a$ met $a \mid p$, en $f(a)=0$. Dus $a = \pm 1$ of $\pm p$.
$f_p(1)>0$, $f_p(p)>0$, $f_p(-1) = -1+3-6+p = p-4 \neq 0$, en
$f_p(-p) = -p^3+3p^2-6p+p = -p^3+3p^2-5p = -p(p^2-3p+5) \neq 0$.

Dus f_p is $\boxed{\text{irreducibel}}$

3 a) Er geldt: $\mathbb{Z}[[X]]^* = \{\pm 1 + a_1X + a_2X^2 + \dots \ : a_n \in \mathbb{Z}\}$
M Stel $f = \sum_{n\geq 0}^{\infty} a_n X^n$ met $a_n \in \mathbb{Z}$ en er is ~~g...~~
$g = \sum_{n\geq 0}^{\infty} b_n X^n$, ~~met~~ met $b_n \in \mathbb{Z}$ zodat $f \cdot g = 1$

Dan is $a_0 b_0 = 1$, dus $a_0 = \pm 1$.
Stel omgekeerd dat $f = \sum_{n\geq 0}^{\infty} a_n X^n \in \mathbb{Z}[[X]]$ met $a_0 = \pm 1$.
We vinden $g = \sum_{n\geq 0}^{\infty} b_n X^n \in \mathbb{Z}[[X]]$ ~~recursie~~ met $fg = 1$
recursief.

M. Stel we hebben $b_0, b_1, b_2, \ldots, b_{n-1} \in \mathbb{Z}$ gevonden.
Dan vinden we b_n uit $a_n b_0 + a_{n-1} b_1 + \ldots + a_0 b_n = 0$,

$$b_n = -a_0^{-1}(a_n b_0 + a_{n-1} b_1 + \ldots + a_1 b_{n-1}) \in \mathbb{Z}.$$

b) Definieer het ringhomomorfisme

$$g: \mathbb{Z}[[X]] \to \mathbb{Z}/p\mathbb{Z}$$
$$\sum_{n\geq 0} a_n X^n \mapsto a_0 \bmod p$$

Er geldt: g is surjectief, en
$\ker g = \{\sum_{n\geq 0} a_n X^n : a_0 \equiv 0 \pmod p\} = \{up + a_1 X + a_2 X^2 + \ldots : a_n \in \mathbb{Z}\}$
$= (X, p)$
Dus $\mathbb{Z}[[X]]/(X,p) \cong \mathbb{F}_p$ is een lichaam en (X,p) is een maximaal ideaal.

c) Er geldt: $M \subsetneq \mathbb{Z}[[X]]$ en er is geen ideaal J van $\mathbb{Z}[[X]]$ met $M \subsetneq J \subsetneq \mathbb{Z}[[X]]$
~~Stel $f(M)$~~ Er geldt: $1 \notin f(M)$ omdat anders
$1 + a_1 X + a_2 X^2 + \ldots \in M$ voor zekere $a_n \in \mathbb{Z}$, dus M bevat een eenheid, en $M = \mathbb{Z}[[X]]$, in strijd met de aanname.

Stel er is een ideaal $J \subseteq \mathbb{Z}$ zodat $f(M) \subsetneq J \subsetneq \mathbb{Z}$.
Dan is $M \subsetneq f^{-1}(J) \subsetneq \mathbb{Z}[[X]]$. $f^{-1}(J)$ is een ideaal, dus dit is in strijd met de aanname.
Dientengevolge is $f(M)$ een maximaal ideaal van $\mathbb{Z}$.

d) Er geldt: $f(M) = (p)$ voor zeker priemgetal p.
Dus alle elementen van M zijn van de vorm
$a_0 + a_1 X + a_2 X^2 + \ldots$ met $a_0 \equiv 0 \pmod p$, dus $M \subseteq (X, p)$.
Omdat (X,p) maximaal is, is $M = (X,p)$

4) a) het is rechttoe-rechtaan om te controleren dat f een R-moduul homomorfisme is. We gaan de surjectiviteit na.
Stel $(y_n)_{n\geq 1}^{\infty} \in M$.
Kies $(x_n)_{n\geq 1}^{\infty}$ als volgt:
x_1, x_2 willekeurig, en ~~ik~~ dan achtereenvolgens
$x_3 = y_1 + 2x_2 - x_1$, $x_4 = y_2 + 2x_3 - x_2$, $x_5 = y_3 + 2x_4 - x_3$, ——

Dan is $f((x_n)_{n\geq 1}^{\infty}) = (y_n)_{n\geq 1}^{\infty}$

b) Er geldt: $N = \{(x_n)_{n\geq 1}^{\infty} : x_n = 2x_{n-1} - x_{n-2} \text{ voor } n \geq 3\}$

x_1 en x_2 zijn vrij te kiezen, en $x_3, x_4, —$ worden door x_1 en x_2 bepaald.
Preciser: definieer ~~ik~~ de afbeelding

$g : R^2 \to N$, $(x_1, x_2) \mapsto (x_n)_{n\geq 1}^{\infty} : x_n = 2x_{n-1} - x_{n-2}$ voor $n \geq 3$

g is een R-moduul homomorfisme.
~~Als~~ Als $(x_n)_{n\geq 1}^{\infty} = (0)$ dan is $x_1 = x_2 = 0$. Dus g is injectief
~~Als~~ g is duidelijk surjectief
Dus g is een isomorfisme

Er volgt: $R^2 \cong N$. Dus N is een vrij R-moduul van rang $\underline{\underline{2}}$.