Álgebra I Segundo parcial 21 de Diciembre de 2017

Nombre del alumno: _____

Este examen tiene 4 ejercicios, para un total de 10 puntos y una duración de dos horas.

Ejercicio	1	2	3	4	Total
Puntos	3	3	2	2	10
Puntuación					

1. En $\mathbb{Z}[\sqrt{-14}]$.
   (a) [1 puntos] Demostrar que $3, 5, 1+\sqrt{-14}, 1-\sqrt{-14}$ son irreducibles.
   (b) [1 puntos] Demostrar que $3, 5, 1+\sqrt{-14}, 1-\sqrt{-14}$ no son primos.
   (c) [1 puntos] Demostrar que 15 tiene dos factorizaciones en irreducibles esencialmente distintas.

Solución:

(a) En $\mathbb{Z}[\sqrt{-14}]$, $N(3) = 9$ no es primo en $\mathbb{Z}$, pero 3 es irreducible en $\mathbb{Z}[\sqrt{-14}]$. En efecto, si $3 = uv$ en $\mathbb{Z}[\sqrt{-14}]$, entonces tomando normas, $9 = N(u)N(v)$ en $\mathbb{Z}$. Las normas de u y v deben ser 3, ya que son de la forma $a^2 + 14b^2$ y no son 1, puesto que u y v no son unidades, pero la ecuación $3 = a^2 + 14b^2$ no tiene solución en $\mathbb{Z}$, por tanto no existen elementos de norma 3.

Análogamente, ya que $N(5) = 25$ and 5 no es la norma de ningún elemento de $\mathbb{Z}[\sqrt{-14}]$, 5 es irreducible en $\mathbb{Z}[\sqrt{-14}]$.

La norma de $1+\sqrt{-14}$ es 15, que factoriza en $\mathbb{Z}$, pero $1+\sqrt{-14}$ es irreducible en $\mathbb{Z}[\sqrt{-14}]$. En efecto, si $1+\sqrt{-14} = uv$, entonces tomando normas $15 = N(u)N(v)$. Ya que no existen elementos de norma 3 ni elementos de norma 5, $N(u) = 1$ o $N(v) = 1$, por tanto u ó v es una unidad.

La norma de $1-\sqrt{-14}$ es 15, que factoriza en $\mathbb{Z}$, pero $1-\sqrt{-14}$ es irreducible en $\mathbb{Z}[\sqrt{-14}]$. En efecto, si $1+\sqrt{-14} = uv$, entonces tomando normas $15 = N(u)N(v)$. Ya que no existen elementos de norma 3 ni elementos de norma 5, $N(u) = 1$ o $N(v) = 1$, por tanto u ó v es una unidad.

(b) El elemento irreducible 3 divide a $(1+\sqrt{-14})(1-\sqrt{-14})$, pero no divide a ninguno de los factores.

El elemento irreducible 5 divide a $(1+\sqrt{-14})(1-\sqrt{-14})$, pero no divide a ninguno de los factores.

El elemento irreducible $(1+\sqrt{-14})$ divide a $3 \cdot 5$, pero no divide a ninguno de los factores.

El elemento irreducible $(1-\sqrt{-14})$ divide a $3\cdot 5$, pero no divide a ninguno de los factores.

(c) $15 = 3\cdot 5 = (1+\sqrt{-14})(1-\sqrt{-14})$ y los irreducibles de una factorización no están asociados a los irreducibles de la otra factorización.

2. (a) [1 puntos] ¿Es $\mathbb{Q}[X]/(X^4+4X^3+5X^2-2X+3)$ un cuerpo?

   (b) [1 puntos] Factorizar en irreducibles, el polinomio $f(X) = 15X^5 - 5X^4 - 10X^3 - 5X^2 + 6X - 1 \in \mathbb{Z}[X]$.

   (c) [1 puntos] Un polinomio $f(X)$ dividido por $X+1$ da resto 3 y dividido por $X-3$ da resto 15. Calcular el resto de la división de $f(X)$ por X^2-2X-3.

Solución:

(a) Sea $f(X) = X^4+4X^3+5X^2-2X+3$. Reduciendo módulo 2, tenemos que $\overline{f}(X) = X^4+X^2+\overline{1} = (X^2+X+\overline{1})^2$. Reduciendo módulo 3, tenemos que $\overline{f}(X) = X^4+X^3+\overline{2}X^2+X = X(X^3+X^2+\overline{2}X+\overline{1})$. Ya que se trata de reducciones incompatibles, $f(X)$ es irreducible sobre $\mathbb{Z}$, y como es primitivo, irreducible sobre $\mathbb{Q}$. Así $\mathbb{Q}[X]/(X^4+4X^3+5X^2-2X+3)$ es un cuerpo.

(b) Sea $f(X) = 15X^5-5X^4-10X^3-5X^2+6X-1$. Ya que $f(1) = 15-5-10-5+6-1 = 0$, tenemos que $f(X) = (X-1)(15X^4+10X^3-5X+1)$. Sea $g(X) = 15X^4+10X^3-5X+1$. Ya que $g_{rec}(X) = X^4-5X^3+10X+15$ es irreducible sobre $\mathbb{Z}$, por el criterio de Eisenstein para $p=5$, $g(X)$ es irreducible sobre $\mathbb{Z}$ y $f(X) = (X-1)(15X^4+10X^3-5X+1)$ es una factorización en irreducibles.

(c) Ya que $X^2-2X-3 = (X+1)(X-3)$, el resto de dividir $f(X)$ por X^2-2X-3 es distinto de cero, luego $f(X) = (X^2-2X-3)q(X)+r(X)$ donde $r(X) = aX+b$. Entonces $3 = f(-1) = r(-1) = -a+b$ y $15 = f(3) = r(3) = 3a+b$. Así $a=3$ y $b=6$, de donde $r(X) = 3X+6$.

3. (a) [1 puntos] Factorizar en irreducibles los enteros de Gauss: $4-2i$ y $7-6i$

   (b) [1 puntos] Utilizando el apartado anterior, calcular el máximo cómún divisor y el mínimo común múltiplo de dichos elementos. La respuesta debe darse en el primer cuadrante.

Solución:

(a) $4-2i = 2(2-i) = (1+i)(1-i)(2-i)$. Ya que $N(1+i) = 2$, $N(1-i) = 2$ y $N(2-i) = 5$, se trata de una factorización en irreducibles.

$(7-6i) = (2-i)(4-i)$. Ya que $N(2-i) = 5$ y $N(4-i) = 17$, se trata de una factorización en irreducibles.

(b) $\mathrm{m.\,c.\,d}(4-2i, 7-6i) = (2-i)$. En el primer cuadrante sería $\mathrm{m.\,c.\,d}(4-2i, 7-6i) = (2-i)i = 1+2i$.

$\mathrm{m.\,c.\,m}(4-2i, 7-6i) = (1+i)(1-i)(2-i)(4-i) = 14-12i$. En el primer cuadrante sería $\mathrm{m.\,c.\,m}(4-2i, 7-6i) = (14-12i)i = 12+14i$.

4. [2 puntos] Resolver, si es posible, el siguiente sistema de congruencias en $\mathbb{Z}[i]$ dando la solución general:

$$\begin{aligned} x &\equiv i \pmod{(1+2i)} \\ x &\equiv (2+i) \pmod{(1+i)} \end{aligned}$$

Solución:

i	a	m	c	d	b
1	i	1 + 2i	1 + i	2	-2 + 2i
2	2 + i	1 + i	1 + 2i	-i	5

La solución es $(3+2i) \pmod{(-1+3i)}$.

Otra forma:

$x = i+(1+2i)k$, de donde $i+(1+2i)k \equiv (2+i) \pmod{(1+i)}$, esto es, $(1+2i)k \equiv (2) \pmod{(1+i)}$. Calculemos el inverso de $1+2i$ módulo $(1+i)$.

i	q	r	s
0	-	1 + 2i	1
1	1	1 + i	0
2	1-i	i	1
		1	-i

Ya que dicho inverso es $-i$, tenemos que $k \equiv (-2i) \pmod{(1+i)}$ y así $k = -2i + (1+i)k'$, de donde $x = i + (1+2i)[-2i + (1+i)k'] = (4-i) + (-1+3i)k'$.