Exámen final – soluciones

1. Sean $a, n \in \mathbb{Z}$, donde $n > 1$.

   a) (1 pt) Define: a y n son primos relativos.

   ▷ Dos enteros son primos relativos si su máximo común divisor es 1. (Un divisor de un número entero n es un número entero $d \neq 0$ tal que $n = dm$ para algun entero m.) Notación: $(a, n) = 1$. □

   b) (1 pt) Define: $b \in \mathbb{Z}$ es un recíproco de a mod n.

   ▷ b es un recíproco de a mod n si $ab \equiv 1 \bmod n$ (n divide a $ab - 1$). □

   c) (10 pts) Demuestra: a tiene un recíproco mod n ssi a y n son primos relativos.

   ▷ Suponemos que $(a, n) = 1$ y demostramos que a tiene un recíproco mod n. $a \neq 0$ ya que $(0, n) = n$. Primero tratamos el caso de $a > 0$ por inducción sobre a. Si $a = 1$ podemos tomar $b = 1$. Si $a > 1$ dividimos a n entre a con resíduo r, i.e. $n = am + r$ para algun entero m y $0 \leq r < a$. Si $r = 0 \implies a|n \implies (a, n) = a > 1$, así que $r > 0$. Luego, todo divisor de a, n es tambien divisor de $r = n - ma$ así que $(a, n) = (a, r) = 1$ y podemos aplicar la hipótesis de la inducción para concluir que r tiene un recíproco mod a, o sea un b_1 y m_1 tal que $rb_1 = 1 + m_1 a$. Multiplicando la ecuación $n = am + r$ por b_1 se obtiene $nb_1 = amb_1 + rb_1 = amb_1 + 1 + m_1 a = a(mb_1 + m_1) + 1 \implies b := -(mb_1 + m_1)$ es un recíproco de a mod n.

   Para $a < 0$, sea b_1 un recíproco de $-a$ mod n, entonces $b = -b_1$ es un recíproco de a.

   Suponemos ahora que a tiene un recíproco mod n y demostramos que $(a, n) = 1$. Si b es un tal recíproco entonces $ab = 1 + mn$ para algun m. Si d es un divisor común de a, n entonces es divisor de $ab - mn = 1$ así que $d \leq 1$, por lo que $(a, n) = 1$. □

   d) (4 pts) Encuentra un recíproco de 7 mod 2008.

   ▷ Dividimos a 2008 entre 7 y obtenemos $2008 = 7 \cdot 286 + 6$, luego $2008 = 7 \cdot 287 - 1 \implies 7 \cdot 287 = 1 + 2008 \implies 287$ es un recíproco de 7 mod 2008. □

   e) (4 pts) Encuentra el número de enteros a en el rango $0 \leq a < 2008$ que son primos relativos a 2008.

   ▷ Esto es $\phi(2008)$ (ϕ es la función de Euler). Luego $2008 = 2^3 \cdot 251$ (factorización en primos), por lo que $\phi(2008) = \phi(2^3)\phi(251) = 4 \cdot 250 = 1000$. □

2. *a*) (1 pt) Define: el producto escalar de dos vectores en $\mathbb{R}^2$.

   ▷ Si $\mathbf{v}_i = (x_i, y_i) \in \mathbb{R}^2$, $i = 1, 2$, $\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = x_1 x_2 + y_1 y_2$. ▷

   b) (1 pt) Define: la norma de un vector en $\mathbb{R}^2$.

   ▷ Si $\mathbf{v} = (x, y) \in \mathbb{R}^2$, $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle} = \sqrt{x^2 + y^2}$. □

   c) (18 pts) Demuestra: para todo $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{R}^2$, $\|\mathbf{v}_1 + \mathbf{v}_2\| \leq \|\mathbf{v}_1\| + \|\mathbf{v}_2\|$.

   ▷ Ambos lados de la desigualdad son no-negativos así que basta demostrar la desigualdad de sus cuadrados. La diferencia de los cuadrados de ambos lados es $(\|\mathbf{v}_1\|^2 + \|\mathbf{v}_2\|)^2 - (\|\mathbf{v}_1 + \mathbf{v}_2\|)^2 = 2(\|\mathbf{v}_1\|\mathbf{v}_2\| - \langle \mathbf{v}_1, \mathbf{v}_2 \rangle)$, así que basta demostrar que $\|\mathbf{v}_1\|\|\mathbf{v}_2\| - \langle \mathbf{v}_1, \mathbf{v}_2 \rangle \geq 0$. Para esto, definimos a $p(t) = \|\mathbf{v}_1 + t\mathbf{v}_2\|^2$. Entonces $p(t) \geq 0$ para todo $t \in \mathbb{R}$, y $p(t) = t^2\|\mathbf{v}_2\|^2 + 2\langle \mathbf{v}_1, \mathbf{v}_2 \rangle t + \|\mathbf{v}_1\|^2$, así que es un polinomio cuadrático en t con descriminante $\Delta \leq 0$. Ahora $\Delta = 4\langle \mathbf{v}_1, \mathbf{v}_2 \rangle^2 - 4\|\mathbf{v}_1\|^2\|\mathbf{v}_2\|^2 \leq 0 \implies |\langle \mathbf{v}_1, \mathbf{v}_2 \rangle| \leq \|\mathbf{v}_1\|\|\mathbf{v}_2\| \implies \langle \mathbf{v}_1, \mathbf{v}_2 \rangle \leq \|\mathbf{v}_1\|\|\mathbf{v}_2\| \implies \|\mathbf{v}_1\|\mathbf{v}_2\| - \langle \mathbf{v}_1, \mathbf{v}_2 \rangle \geq 0$. □

3. *a*) (10 pts) Encuentra una transformación lineal $L : \mathbb{R}^2 \to \mathbb{R}^2$ que manda la elipse $x^2 + 2y^2 = 3$ a un círculo.

   ▷ Si $L(x, y) = (x, y\sqrt{2}) = (x', y')$ entonces $x = x'$, $y = y'/\sqrt{2}$ así que L manda la elipse a la curva con ecuación $x'^2 + y'^2 = 3$, lo cual es un círculo. □

   b) (10 pts) Encuentra una rotación $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ que manda la elipse $x^2 + 2xy + 3y^2 = 4$ a una elipse que tiene su eje mayor a lo largo del eje de x.

   ▷ La ecuación característica es $(1 - \lambda)(3 - \lambda) - 1 = 0 \implies \lambda = 2 \pm \sqrt{2}$. El eje mayor corresponde al valor propio menor, $\lambda = 2 - \sqrt{2}$. Los vectores propios asociados son las soluciones de la ecuacion $(\sqrt{2} - 1)x + y = 0$. Ahora si $\rho(x, y) = (ax + by, -bx + ay) = (x', y')$, con $a^2 + b^2 = 1$, tenemos que $(x, y) = \rho^{-1}(x', y') = (ax' - by', bx' + ay')$. La imagen bajo ρ del eje mayor de la elipse está dado entonces por $(\sqrt{2} - 1)(ax' - by') + (bx' + ay') = 0 \implies [(\sqrt{2} - 1)a + b]x' + [a - (\sqrt{2} - 1)b]y' = 0$. Esto es el eje de x ssi $(\sqrt{2} - 1)a + b = 0$, o sea $b = (1 - \sqrt{2})a$. Substituyimos en $a^2 + b^2 = 1$ y obtenemos $[(1 - \sqrt{2})^2 + 1]a^2 = 1 \implies a = 1/\sqrt{(1 - \sqrt{2})^2 + 1} = \left(\sqrt{2 + \sqrt{2}}\right)/2$, $b = \sqrt{1 - a^2} = \left(\sqrt{2 - \sqrt{2}}\right)/2$. □

4. (20 pts) Factoriza el polinomio $x + x^2 + x^3 + x^4 + x^5 + x^6$ en factores irreducibles en $\mathbb{R}[x]$. (Es decir, expresalo como producto de polinomios con coeficientes reales de grado más bajo posible).

   ▷ $x + x^2 + x^3 + x^4 + x^5 + x^6 = xq(x)$, con $q(x) = 1 + x + x^2 + x^3 + x^4 + x^5 = (x^6 - 1)/(x - 1)$. Para factorizar $q(x)$ factorizamos a $z^6 - 1$ en $\mathbb{C}[z]$. Los factores son $z - z_i$ con z_i las 6 sextas raices de 1. Son ± 1 y $(\pm 1 \pm i\sqrt{3})/2$. Los productos de pares de factores que corresponden a raices conjugadas dan los factores cuadráticos reales irreducibles: $(z - z_i)(z - \bar{z}_i) = z^2 - 2Re(z_i)z + |z_i|^2$. Para $z_i = (\pm 1 + \sqrt{3}i)/2$ obtenemos los factores $z^2 \pm z + 1$.

   Así que: $x + x^2 + x^3 + x^4 + x^5 + x^6 = x(x + 1)(x^2 + x + 1)(x^2 - x + 1)$ es la factorización buscada. □

5. (20 pts) Encuentra una transformación de Möbius que manda la recta $y = 1$ al círculo $x^2 + y^2 = 1$.

   ▷ La transformación $z \mapsto 1/z$ manda la recta $y = 1$ al círculo con centro en $-i/2$ y radio $1/2$. Luego la traslación $z \mapsto z + i/2$ manda este círculo al círculo con centro en el origen y el mismo radio. Luego la dilatación $z \mapsto 2z$ manda este círculo al círculo $x^2 + y^2 = 1$. Así que la transformación $f(z) = 2((1/z) + i/2) = (iz + 2)/z$ manda la recta $y = 1$ al círculo $x^2 + y^2 = 1$. □