Álgebra y Algoritmos

Ángel Ríos San Nicolás

14 de marzo de 2021

Ejercicio 1. *Realice una implementación efectiva de un algoritmo de factorización en $\mathbb{F}_p$ con p primo basada en el teorema de Berlekamp. Tenga especial cuidado con el coste de escribir la matriz de la función $\alpha^p - \alpha$.*

Solución. Implementamos el algoritmo de Berlekamp para encontrar un factor irreducible de un polinomio mónico y libre de cuadrados con coeficientes en un cuerpo finito $\mathbb{F}_q$ con $q = p^m$, $p, m \in \mathbb{N}$ y p primo. En particular funciona para cuerpos finitos con $m = 1$.

```
from random import sample

def factorBerlekamp(f): # Calcula un factor de f mónico libre de cuadrados
    # sobre un cuerpo finito mediante el algoritmo de Berlekamp.
    if gcd(f,f.derivative()) != 1 or f[f.degree()] != 1:
        print("El polinomio no es libre de cuadrados o no es mónico.")
        return
    BR = f.base_ring() # Cuerpo finito de los coeficientes de f.
    p = BR.characteristic()
    m = BR.degree()
    q = p ** m
    n = f.degree()
    Rx.<x> = PolynomialRing(BR)
    Phi = [] # Guardará la matriz de a |--> a^q-a.
    for _ in range(n):
        pol = power_mod(x, _ * q, f) # Cálculo eficiente de x^(iq) mod f
        coef = [] # Guardará los coeficientes.
        if type(pol) == int:
            coef = [pol] + [0] * (n - 1) # Añadimos ceros hasta n.
        else:
            coef = list(pol)
            lenc = len(coef)
            coef = coef + [0] * (n - lenc) # Añadimos ceros hasta n.
        Phi.append(coef)
    Phi = matrix(BR, Phi) - matrix.identity(BR, n)
    Ker = Phi.transpose().right_kernel() # Ker(Phi): Álgebra de Berlekamp.
    BaseKer = Ker.basis_matrix() # Base de Ker(Phi).
    r = BaseKer.dimensions()[0] # Número de factores de f.
    BKer = [Rx(list(_)) for _ in BaseKer]
    if r == 1: # Si r = 1, es irreducible.
        return f, 1, 1
    while True: # Repetimos hasta obtener un factor de f.
        a = sample(list(Ker), 1)[0] # Tomamos a del núcleo pseudoaleatorio.
        a = Rx(list(a)) # Interpretamos a como polinomio.
        b = power_mod(a, (q - 1) // 2, f) # a ^ ((q - 1) / 2)
        d = gcd(f, b)
        if d != 1 and d != f:
            return d, f // d, r # Obtenemos un factor de f.
        d = gcd(f, b - 1)
        if d != 1 and d != f:
            return d, f // d, r # Obtenemos un factor de f.
```

Implementamos ahora un método que encuentra todos los factores de un polinomio libre de cuadrados sobre $\mathbb{F}_q$ y, en particular, también sobre $\mathbb{F}_p$. La idea es calcular $f = gh$ con el algoritmo anterior y comprobar con el mismo algoritmo si g es irreducible o h es irreducible. Se aplica el mismo proceso al factor reducible hasta que llegar a un producto de dos irreducibles.

```
def Berlekamp(f):  # Factorización de f libre de cuadrados sobre
    # un cuerpo finito con el algoritmo de Berlekamp.
    fact = []  # Guardará los factores de f.
    c = f[f.degree()]
    if c != 1:  # Si f no es mónico, el coeficiente principal es un factor.
        fact = [c]
    g = f // c
    while g.degree() != 0:  # Mientras g no sea constante.
        [d, g, r] = factorBerlekamp(g)  # Aplicamos el algoritmo anterior.
        if r == 1:
            return f
        [d1, g1, r1] = factorBerlekamp(d)  # Buscamos un factor de d.
        [d2, g2, r2] = factorBerlekamp(g)  # Buscamos un factor de g.
        if r1 == 1 and r2 != 1:  # d es irreducible.
            fact.append(d)
        elif r1 != 1 and r2 == 1:  # g es irreducible.
            fact.append(g)
            g = d
        else:  # d y g son irreducibles.
            fact.append(g)
            fact.append(d)
            return fact
```

Para el caso general de $f \in \mathbb{F}_q$. Calculamos $h = \gcd(f, f')$ y consideramos tres casos.

1. Si $h = 1$, entonces f es libre de cuadrados y aplicamos el método anterior.
2. Si $h = f$, entonces $f' = 0$ y $f = g^{p^r}$ para $g \in \mathbb{F}_q[x]$ que podemos hallar calculando raíces en $\mathbb{F}_q[x]$. El problema se reduce a factorizar g.
3. En otro caso, h es un factor irreducible y el problema se reduce a factorizar f/h con el mismo procedimiento.

Ejercicio 2. *Usando solamente el algoritmo de factorización de sage para polinomios racionales, calcule la factorización de $f(x) = x^6 - 2x^3 + 5 \in \mathbb{Q}(\alpha)[x]$ donde α es raíz de f. A partir de esta factorización, justifique que el grupo de Galois del cuerpo de escisión de f sobre $\mathbb{Q}$ no es el grupo de permutaciones S_6.*

Solución. Como $\gcd(f, f') = 1$, el polinomio f es libre de cuadrados. Vamos a factorizar f en $\mathbb{Q}(\alpha)$ con α una raíz de f. Consideramos el polinomio mínimo de α sobre $\mathbb{Q}[y]$ que es $g(y) = y^6 - 2y^3 + 5$. Calculamos la norma $N(f)$ con la resultante

$$N(f) = \mathrm{Res}_y(f, g) = \mathrm{Res}_y\left(x^6 - 2x^3 + 5, y^6 - 2y^3 + 5\right) = x^{36} - 12x^{33} + 90x^{30} - 460x^{27} +$$
$$+1815x^{24} - 5592x^{21} + 13964x^{18} - 27960x^{15} + 45375x^{12} - 57500x^9 + 56250x^6 - 37500x^3 + 15625.$$

No es libre de cuadrados porque

$$\gcd(N(f), N(f)') = x^{30} - 10x^{27} + 65x^{24} - 280x^{21} + 930x^{18} - 2332x^{15} +$$
$$+ 4650x^{12} - 7000x^9 + 8125x^6 - 6250x^3 + 3125 \neq 1.$$

Probamos con $N(f(x - 2\alpha))$ que calculamos de nuevo con la resultante

$$N(f(x - 2\alpha)) = \mathrm{Res}_y(f(x - 2\alpha), y^6 - 2y^3 + 5) = x^{36} - 108x^{33} + 6042x^{30} - 137484x^{27} -$$
$$- 1095945x^{24} - 38781720x^{21} + 9696177676x^{18} - 44969134392x^{15} - 1474118148609x^{12} +$$
$$+ 7323966993924x^9 + 161779763521530x^6 - 950902005872700x^3 + 1411901425931625.$$

En este caso sí es libre de cuadrados porque $\gcd(N(f(x-2\alpha)), N(f(x-2\alpha))') = 1$. Factorizamos la norma $N(f(x-2\alpha)$ en irreducibles de $\mathbb{Q}[x]$ y obtenemos $N(f(x-2\alpha)) = g_1 g_2 g_3$ donde

$$\begin{aligned} g_1 &= x^6 - 54x^3 + 3645 \\ g_2 &= x^{12} - 162x^6 + 18225 \\ g_3 &= x^{18} - 54x^{15} - 357x^{12} + 22572x^9 + 2411031x^6 - 13999446x^3 + 21253933 \end{aligned}$$

Los factores irreducibles de $f(x-2\alpha)$ en $\mathbb{Q}(\alpha)[x]$ son

$$\begin{aligned} h_1 &= \gcd(h_1, f(x-2\alpha)) = x - 3\alpha \\ h_2 &= \gcd(h_2, f(x-2\alpha)) = x^2 - 3\alpha x + 3\alpha^2 \\ h_3 &= \gcd(h_3, f(x-2\alpha)) = x^3 - 6\alpha x^2 + 12\alpha^2 x - 7\alpha^3 - 2 \end{aligned}$$

Obtenemos los factores irreducibles de f en $\mathbb{Q}(\alpha)[x]$ deshaciendo el cambio

$$\begin{aligned} h_1(x+2\alpha) &= x - \alpha \\ h_2(x+2\alpha) &= x^2 + \alpha x + \alpha^2 \\ h_3(x+2\alpha) &= x^3 + \alpha^3 - 2 \end{aligned}$$

con lo que la factorización de f en irreducibles de $\mathbb{Q}(\alpha)[x]$ es

$$f = (x-\alpha)\left(x^2 + \alpha x + \alpha^2\right)\left(x^3 + \alpha^3 - 2\right).$$

Observamos que f factoriza en $Q(\alpha)[x]$ en el producto de un polinomio lineal y dos irreducibles de grados 2 y 3 respectivamente. Consideramos $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)[x]/(x^2 + \alpha x + \alpha^2)$ que es una extensión de grado $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = 6 \cdot 2 = 12$ donde $x^2 + \alpha x + \alpha^2$ se escinde. Distinguimos tres casos para el factor $(x^3 + \alpha^3 - 2)$.

- Si se escinde en $\mathbb{Q}(\alpha,\beta)[x]$, entonces f se escinde y $\mathbb{Q}(\alpha,\beta)$ es el cuerpo de escisión de f.
- Si factoriza en $\mathbb{Q}(\alpha,\beta)[x]$ en el producto de un polinomio de grado 1 y un polinomio p de grado 2 irreducible, consideramos la extensión $\mathbb{Q}(\alpha,\beta,\gamma) = \mathbb{Q}(\alpha,\beta)[x]/(p)$ que es una extensión de grado $[\mathbb{Q}(\alpha,\beta,\gamma) : \mathbb{Q}] = 6 \cdot 2 \cdot 2 = 24$ donde f se escinde y, por lo tanto, es el cuerpo de escisión.
- Si es irreducible en $\mathbb{Q}(\alpha,\beta)[x]$, consideramos $\mathbb{Q}(\alpha,\beta,\gamma) = \mathbb{Q}(\alpha,\beta)[x]/(x^3 + \alpha^3 - 2)$ que es una extensión de grado $[\mathbb{Q}(\alpha,\beta,\gamma) : \mathbb{Q}] = 6 \cdot 2 \cdot 3 = 36$ donde tenemos que

  $$x^3 + \alpha^2 - 2 = (x-\gamma)q$$

  con q de grado 2. Distinguimos dos casos para q.

  - Si q se escinde en $\mathbb{Q}(\alpha,\beta,\gamma)[x]$, entonces f se escinde y $\mathbb{Q}(\alpha,\beta,\gamma)$ es el cuerpo de escisión de f.
  - Si q es irreducible en $\mathbb{Q}(\alpha,\beta,\gamma)[x]$, entonces consideramos

    $$\mathbb{Q}(\alpha,\beta,\gamma,\delta) = \mathbb{Q}(\alpha,\beta,\gamma)[x]/(q)$$

    que es una extensión de grado $[\mathbb{Q}(\alpha,\beta,\gamma,\delta) : \mathbb{Q}] = 6 \cdot 2 \cdot 3 \cdot 2 = 72$ donde q se escinde y f también con lo que $\mathbb{Q}(\alpha,\beta,\gamma,\delta)$ es el cuerpo de escisión de f.

  Por el teorema fundamental de la teoría de Galois, existe una biyección entre el conjunto de subgrupos del grupo de Galois de $K/\mathbb{Q}$ y el conjunto de cuerpos intermedios tal que si $S \subseteq \mathrm{Gal}(K/\mathbb{Q})$ es un subgrupo, su orden es $|S| = [K : K^S]$ donde K^S es el subcuerpo de K de los elementos fijados por todo S. En particular, el orden del grupo de Galois es $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}]$. Por la discusión de casos anterior, sabemos que el grado de la extensión es $[K : \mathbb{Q}] \in \{12, 24, 36, 72\}$. Por lo tanto, como el orden del grupo de Galois no es 6!, no es el grupo de permutaciones S_6.

Ejercicio 3. *Describa brevemente un algoritmo que tome como entrada una polinomio $f \in \mathbb{Q}[x]$ y devuelva como output un polinomio g tal que el cuerpo de escisión de f sea $\mathbb{Q}[x]/(g)$. ¿Es capaz de calcular dicho polinomio para $f(x) = x^6 - 2x^3 + 5$?*

Solución. Sea $f \in \mathbb{Q}[x]$. Podemos factorizar f en irreducibles y obtenemos

$$f = f_1^{m_1} \cdots f_n^{m_s}.$$

Consideramos la extensión $\mathbb{Q}(\alpha_1) = \mathbb{Q}[x]/(f_1)$. Factorizamos f en $\mathbb{Q}(\alpha_1)[x]$ donde al menos f_1 se escinde y tenemos

$$f = g_1^{r_1} \cdots g_{s'}^{r_{s'}}.$$

Si f se escinde, es decir, si $r_1 = \cdots = r_{s'} = 1$, entonces $g = f_1$ y hemos terminado. Si no, tomamos un factor irreducible g_1 y construimos $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1)[x]/(g_1)$. Podemos factorizar el polinomio f en $\mathbb{Q}(\alpha_1, \alpha_2)[x]$. Como el número de factores irreducibles es finito, repetimos el proceso hasta obtener $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, el cuerpo de escisión de f sobre $\mathbb{Q}$ que es una extensión separable y finita. Por el teorema del elemento primitvo es simple y existe un $\gamma \in \mathbb{Q}(\alpha_1, \ldots, \alpha_s)$ que la genera como $\mathbb{Q}$-espacio vectorial de dimensión finita.

En el proceso anterior de construcción del cuerpo de escisión obtenemos en cada paso el polinomio mínimo $f_i \in \mathbb{Q}[x_1, \ldots, x_i]$ de α_i sobre $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ que denotamos f_i. Como el cuerpo de escisión $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es numerable, podemos enumerar sus elementos como combinaciones lineales de la forma $f(\alpha_1, \ldots, \alpha_n)$ con $f \in \mathbb{Q}[x_1, \ldots, x_n]$ hasta que encontramos un polinomio g con $\gamma = g(\alpha_1, \ldots, \alpha_n)$ primitivo. Consideramos el siguiente ideal de $\mathbb{Q}[x_1, \ldots, x_n, y]$.

$$\mathfrak{a} = (f_1, \ldots, f_n, y - f(x_1, \ldots, x_n))$$

El polinomio mínimo de γ sobre $\mathbb{Q}$ se puede calcular como el único generador mónico en la base de Gröbner reducida del ideal de eliminación $\mathfrak{a} \cap \mathbb{Q}[x_1, \ldots, x_n]$. Si tomamos un elemento del cuerpo de escisión de manera aleatoria será primitivo, pero su polinomio mínimo tendrá coeficientes enormes. En la práctica probamos con combinaciones sencillas hasta que obtenemos γ primitivo y su polinomio mínimo g con los que concluimos que $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\gamma) = \mathbb{Q}[x]/(g)$ como queríamos.

Vamos a aplicar el algoritmo descrito a $f = x^6 - 2x^3 + 5$. Del apartado anterior, tenemos la factorización de f en su cuerpo raíz $\mathbb{Q}(\alpha)$.

$$f = (x - \alpha)(x^2 + \alpha x + \alpha^2)(x^3 + \alpha^3 - 2)$$

Consideramos $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)/(x^2 + \alpha x + \alpha^2)$ y podemos factorizar f en $\mathbb{Q}(\alpha, \beta)[x]$ donde vemos que $x^3 + \alpha^3 - 2$ es irreducible. Tomamos $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\alpha, \beta)[x]/(x^3 + \alpha^3 - 2)$, factorizamos el polinomio $x^3 + \alpha^3 - 2$ en $\mathbb{Q}(\alpha, \beta, \gamma)[x]$ y se escinde

$$x^3 + \alpha^2 - 2 = (x - \gamma)\left(x + \left(\left(\frac{-1}{5}\alpha^5 + \frac{2}{5}\alpha^2\right)\beta + 1\right)\gamma\right)\left(x + \left(\left(\frac{1}{5}\alpha^5 - \frac{2}{5}\alpha^2\right)\beta\right)\gamma\right).$$

Por lo tanto, $\mathbb{Q}(\alpha, \beta, \gamma)$ es el cuerpo de escisión de f que es una extensión de grado 36. Los polinomios mínimos de α, β y γ respectivamente sobre $\mathbb{Q}$, $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\alpha, \beta)$ son

$$\begin{aligned} x^6 - 2x^3 + 5 &\in \mathbb{Q}[x] \\ y^2 + \alpha y + \alpha^2 &\in \mathbb{Q}(\alpha)[y] \\ z^3 + \alpha^3 - 2 &\in \mathbb{Q}(\alpha, \beta)[z] \end{aligned}$$

Ahora probamos con diferentes elementos de $\mathbb{Q}(\alpha, \beta, \gamma)$ hasta encontrar un elemento primitivo. Probamos, por ejemplo, con $\alpha + \beta + \gamma$. Consideramos el siguiente ideal en $\mathbb{Q}[x, y, z, t]$.

$$\mathfrak{a} = \left(x^6 - 2x^3 + 5, y^2 + \alpha y + \alpha^2, z^3 + \alpha^3 - 2, t - (x + y + z)\right)$$

Calculando la base de Gröbner reducida del ideal de eliminación $\mathfrak{a} \cap \mathbb{Q}[x, y, z]$, tenemos que el único generador, que es el polinomio mínimo de $\alpha + \beta + \gamma$ sobre $\mathbb{Q}$, es

$$t^{18} + 318t^{12} + 6033t^6 + 4096$$

con lo que $\alpha+\beta+\gamma$ no es primitivo.

Probamos con $\alpha-\beta+\gamma$. Definimos el ideal

$$\mathfrak{b}=\left(x^6-2x^3+5, y^2+\alpha y+\alpha^2, z^3+\alpha^3-2, t-(x-y+z)\right).$$

Calculando la base de Gröbner reducida del ideal de eliminación $\mathfrak{b}\cap\mathbb{Q}[x,y,z]$, hallamos el polinomio mínimo de $\alpha-\beta+\gamma$ que es

$$g=t^{36}-12t^{33}-396t^{30}+50732t^{27}+1418262t^{24}+10093164t^{21}+1852742516t^{18}+5520435348t^{15}+$$
$$+196631283201t^{12}+1504151875936t^{9}+7378647677568t^{6}+11198537803776t^{3}+5708466638848.$$

Por lo tanto, $\alpha-\beta+\gamma$ es primitivo y $\mathbb{Q}(\alpha,\beta,\gamma)=\mathbb{Q}(\alpha-\beta+\gamma)=\mathbb{Q}[x]/(g(x))$.

Ejercicio 4. *Sea $L=[R_0,\ldots,R_k]$ una lista de polinomios en $\mathbb{R}[x]$. Sea $S\in\mathbb{R}[x]$ un polinomio y $c\in\mathbb{R}$ con $S(c)\neq 0$. Sea $L'=[SR_0,\ldots,SR_k]$. Denotemos por $v_T(c)$ el número de cambios de signo de la lista T en c. Demuestre que:*

$$v_L(c)=v_{L'}(c)$$

Solución. Es claro que los ceros se conservan. Si $i\in\{0,1,\ldots,k\}$ tal que $R_i(c)=0$, entonces $S(c)R_i(c)=0$. Podemos suponer sin pérdida de generalidad que las listas evaluadas en c no tienen ceros. Ahora, como $S(c)\neq 0$, es $S(c)<0$ o $S(c)>0$ y para todo $i\in\{0,1\ldots,k\}$,

$$\begin{array}{ll}\operatorname{sig}(S(c)R_i(c))=-\operatorname{sig}(R_i(c)) & \text{si } S(c)<0\\ \operatorname{sig}(S(c)R_i(c))=\operatorname{sig}(R_i(c)) & \text{si } S(c)>0\end{array}$$

Para cada $i\in\{0,1,\ldots,k\}$ tal que se conserva el signo $\operatorname{sig}(R_i(c))=\operatorname{sig}(R_{i+1}(c))$, se cumplen:

- Si $S(c)<0$,

$$\operatorname{sig}(S(c)R_i(c))=-\operatorname{sig}(R_i(c))=-\operatorname{sig}(R_{i+1}(c))=\operatorname{sig}(S(c)R_{i+1}(c))$$

- Si $S(c)>0$,

$$\operatorname{sig}(S(c)R_i(c))=\operatorname{sig}(R_i(c))=\operatorname{sig}(R_{i+1}(c))=\operatorname{sig}(S(c)R_{i+1}(c))$$

y cambia el signo también en L'.

Para cada $i\in\{0,1,\ldots,k\}$ tal que tenemos un cambio de signo $\operatorname{sig}(R_i(c))=-\operatorname{sig}(R_{i+1}(c))$, se cumplen:

- Si $S(c)<0$,

$$\operatorname{sig}(S(c)R_i(c))=-\operatorname{sig}(R_i(c))=\operatorname{sig}(R_{i+1}(c))=-\operatorname{sig}(S(c)R_{i+1}(c)).$$

- Si $S(c)>0$,

$$\operatorname{sig}(S(c)R_i(c))=\operatorname{sig}(R_i(c))=-\operatorname{sig}(R_{i+1}(c))=-\operatorname{sig}(S(c)R_{i+1}(c)).$$

y se conserva el signo también en L'.

Por lo tanto, $v_L(c)=v_{L'}(c)$.

Ejercicio 5. *Sea $P,Q\in\mathbb{R}[x]$. Sean $a<b$ con $P(a)\neq 0\neq P(b)$*

$$\begin{aligned}n_+&=|\{c\in(a,b)|P(c)=0,Q(c)>0\}|\\ n_-&=|\{c\in(a,b)|P(c)=0,Q(c)<0\}|\end{aligned}$$

Tomemos la sucesión:

$$L=[R_0,R_1,\ldots,R_k]$$

donde

$$R_0 = P, R_1 = P'Q, R_{i+1} = -(R_{i-1}\%R_i), R_k = \gcd(P, P'Q)$$

Denotemos por $v_L(c)$ el número de cambios de signo de la sucesión anterior en c. Demuestre que:

$$v_L(a) - v_L(b) = n_+ - n_-$$

Pista: En el Teorema 2.3 se demuestra la igualdad para la lista $L' = [R_0/R_k, \ldots, R_k/R_k]$. Use el ejercicio anterior.

Solución. Probamos primero que $R_k(a) \neq 0 \neq R_k(b)$. Sabemos que $R_k = \gcd(P, P'Q)$, en particular divide a P, existe $H \in \mathbb{R}[x]$ tal que $P = R_k H$. Como $P(a) \neq 0$, se cumple

$$P(a) = R_k(a)H(a) \neq 0.$$

Por ser $\mathbb{R}[x]$ un dominio de integridad, $R_k(a) \neq 0$ y análogamente deducimos que $R_k(b) \neq 0$.

Por el Teorema 2.3, si $L = [R_0/R_k, R_1/R_k, \ldots, R_k/R_k]$, entonces

$$v_{L'}(a) - v_{L'}(b) = n_+ - n_-.$$

Aplicando el resultado del problema anterior, como $R_k(a) \neq 0 \neq R_k(b)$,

$$\left.\begin{array}{l} v_{L'}(a) = v_L(b) \\ v_{L'}(b) = v_L(b) \end{array}\right\} \Longrightarrow v_L(a) - v_L(b) = v_{L'}(a) - v_{L'}(b) = n_+ - n_-.$$

Ejercicio 6. *Sea P, Q polinomios y $c \in \mathbb{R}$ una constante no nula. Demuestre que:*

- $(cQ)\%P = c(Q\%P)$
- $Q\%(cP) = Q\%P$
- *Si* $\deg(P) = \deg(Q)$*, existe una constante no nula d con* $(Q\%P) = d(P\%Q)$.

Solución.

- $(cQ)\%P = c(Q\%P)$

  Aplicamos la división con resto en $\mathbb{R}[x]$ por la que existen unos únicos cocientes $F, F' \in \mathbb{R}[x]$ y restos $(cQ)\%P, Q\%P \in \mathbb{R}[x]$ tales que

  $$\begin{array}{l} cQ = PF + (cQ)\%P \\ Q = PF' + Q\%P \end{array}$$

  con $\deg((cQ)\%P), \deg(Q\%P) < \deg(P)$. Como c es no nulo por hipótesis, también se cumple

  $$Q = P\left(\frac{1}{c}F\right) + \frac{1}{c}\left((cQ)\%P\right).$$

  Por unicidad, debe ser $F' = \left(\frac{1}{c}F\right)$ y, como queríamos, $(cQ)\%P = c(Q\%P)$ porque multiplicar por una constante no nula no cambia el grado.

- $Q\%(cP) = Q\%P$

  Aplicamos la división con resto en $\mathbb{R}[x]$ por la que existen unos únicos cocientes $F, F' \in \mathbb{R}[x]$ y restos $Q\%(cP), Q\%P \in \mathbb{R}[x]$ tales que

  $$\begin{array}{l} Q = (cP)F + (Q\%(cP)) \\ Q = PF' + (Q\%P) \end{array}$$

  con $\deg(Q\%(cP)), \deg(Q\%P) < \deg(cP) = \deg(P)$. Como

  $$(cP)F + (Q\%(cP)) = P(cF) + (Q\%(cP)),$$

  recuperamos la división por P. Por unicidad, $F' = cF$ y, como queríamos,

  $$Q\%(cP) = Q\%P.$$

- Si $\deg(P) = \deg(Q)$, existe una constante no nula d con $(Q\%P) = d(P\%Q)$.

  Denotamos $n = \deg(P)$. Si $P = a_n x^n + \cdots + a_1 x + a_0$ y $Q = b_n x^n + \cdots + b_1 x + b_0$. Las divisiones con resto de P y Q entre sí son

  $$\begin{aligned} P &= \tfrac{a}{b}Q + (P\%Q) \\ Q &= \tfrac{b}{a}P + (Q\%P) \end{aligned}$$

  que se obtienen en un paso del algoritmo de la escuela. Despejando tenemos

  $$\begin{aligned} P\%Q &= P - \tfrac{a}{b}Q \\ Q\%P &= Q - \tfrac{b}{a}P = \tfrac{b}{a}\left(\tfrac{a}{b}Q - P\right) = -\tfrac{b}{a}\left(P - \tfrac{a}{b}Q\right) = -\tfrac{b}{a}(P\%Q) \end{aligned}$$

  con lo que existe un único $d = -\frac{b}{a} \in \mathbb{R}$ no nulo que lo cumple. Es no nulo porque por hipótesis $\deg(P) = n$.

Ejercicio 7. *Sea $P, Q \in \mathbb{R}[x]$. Tomemos las sucesiones:*

$$L : R_0 = P, R_1 = Q, R_{i+1} = -(R_{i-1}\%R_i), R_k = \gcd(P, Q)$$

y

$$L' : S_0 = -P, S_1 = -Q, S_{i+1} = -(S_{i-1}\%S_i), S_{k'} = \gcd(-P, -Q)$$

Demuestre que:

- *$k = k'$ y $S_i = -R_i, 0 \leq i \leq k$.*
- *Si $c \in \mathbb{R}, v_L(c) = v_{L'}(c)$.*

Solución.

- $k = k'$ y $S_i = -R_i, 0 \leq i \leq k$.

  Por defínción, $S_0 = P = -(-P) = -R_0$. Suponemos que $S_j = -R_j$ para $0 \leq j \leq i \leq k$. Aplicando los resultados del ejercicio anterior,

  $$S_{i+1} = -(S_{i-1}\%S_i) = (-S_{i-1}\%(-S_i)) = (R_{i-1}\%R_i) = -R_{i+1}.$$

  En particular, $S_{k+1} = -(S_{k-1}\%S_k) = R_{k+1} = 0$ con lo que el anterior es el máximo común divisor $S_k = \gcd(-P, -Q)$ y esto prueba que $k = k'$.

- Si $c \in \mathbb{R}, v_L(c) = v_{L'}(c)$.

  Como $-1 \in \mathbb{R}[x]$ tal que $(-1)(c) = -1 \neq 0$, aplicando el resultado del Ejercicio 4,

  $$v_L(c) = v_{L'}(c).$$

Los siguientes dos ejercicios no es la forma usual de resolver estos apartados. Se introducen para practicar con los conceptos vistos.

Ejercicio 8. *Sea P, Q como en el Teorma 2.3. Supongamos que* $\deg(P'Q) > \deg(P)$. *Sea $T = (P'Q)\%P$ el resto sin cambiar de signo. Definimos la lista de polinomios:*

$$L : R_0 = P, R_1 = P'Q, R_{i+1} = -(R_{i-1}\%R_i), R_k = \gcd(P, P'Q)$$

$$L' : S_0 = P, S_1 = T, S_{i+1} = -(S_{i-1}\%S_i), S_{k'} = \gcd(P, T) = \gcd(P, P'Q)$$

Demuestre que:

- *$R_2 = -P$, $R_3 = -T$, $R_{i+2} = -S_i$*
- *Si $P(c) \neq 0$, $v_L(c) = v_{L'}(c) + 1$. En particular,*

  $$v_L(a) - v_L(b) = v_{L'}(a) - v_{L'}(b) = n_+ - n_-$$

Solución.

- $R_2 = -P$, $R_3 = -T$, $R_{i+2} = -S_i$

  Por definición, $R_2 = -(R_0 \% R_1) = -(P\%(P'Q))$. Pero $P = P'Q \cdot 0 + P$ donde $\deg(P) < \deg(P'Q)$ por hipótesis, con lo que el resto es $(P\%(P'Q)) = P$ y entonces $R_2 = -P$.

  Por definición, $R_3 = -(R_1 \% R_2) = -((P'Q)\%(-P)) = -((P'Q)\%P) = -T$.

  Suponemos que se cumple $R_{j+2} = -S_j$ para $0 \leq j \leq i \leq k$. Desarrollando, tenemos

$$R_{(i+1)+2} = R_{i+3} = -(R_{i+1} \% R_{i+2}) = -(-S_{i-1}\%(-S_i)) = (S_{i-1}\%S_i) = -S_{i+1}$$

- Si $P(c) \neq 0$, $v_L(c) = v_{L'}(c) + 1$. En particular,

$$v_L(a) - v_L(b) = v_{L'}(a) - v_{L'}(b) = n_+ - n_-.$$

  La lista L se puede escribir de la siguiente manera.

$$L = [R_0, R_1, R_2, R_3, \ldots, R_k] = [P, P'Q, -S_0, -S_1, \ldots, -S_{k-2}]$$

  donde, por el Ejercicio 4, $[-S_0, -S_1, \ldots, -S_{k-2}]$ tiene el mismo número de cambios de signos que L' porque el polinomio $-1 \in \mathbb{R}[x]$ no se anula en c. Además, $-S_0 = -P$ con lo que independientemente del signo de PQ en c, la lista L siempre tiene un cambio de signo más que L', es decir, $v_L(c) = v_{L'}(c) + 1$.

  Para las igualdades que quedan suponemos, como en el Teorema 2.3, que $a, b \in \mathbb{R}$ con $a < b$ no son raíces de P. Sabemos que $v_L(a) = v_{L'}(a) + 1$ y $v_L(b) = v_{L'}(b) + 1$. Restando y aplicando el Ejercicio 5 a L',

$$v_L(a) - v_L(b) = v_{L'}(a) - v_{L'}(b) = n_+ - n_-.$$

Ejercicio 9. *Sean P, Q como en el Teorema 2.3. Supongamos que* $\deg(P'Q) = \deg(P)$. *Sea $T = (P'Q)\%P$ el resto sin cambiar de signo. Definimos la lista de polinomios:*

$$R : R_0 = P, R_1 = P'Q, R_{i+1} = -(R_{i-1}\%R_i), R_k = \gcd(P, P'Q)$$

$$S : S_0 = P, S_1 = T, S_{i+1} = -(S_{i-1}\%S_i), S_{k'} = \gcd(P, T) = \gcd(P, P'Q)$$

sea $P = ax^n + \cdots, Q = bx + \cdots$, $P'Q = anbx^n + \cdots$ y sea $d = nb$. Denotemos por

$$R' = [R_2, \ldots, R_k]$$

$$S' = [S_1, \ldots, S_{k'}]$$

Demuestre que:

- $S_1 = dR_2$
- $S_2 = d^{-1}R_3$
- $S_{2i+1} = dR_{2i+2}, i \leq 0$
- $S_{2i} = d^{-1}R_{2i+1}, i \leq 1$
- $v_{R'}(c) = v_{S'}(c)$

Rellene la siguiente tabla con los signos que faltan.

d	P	$P'Q - dP$	$P'Q$	$d^{-1}(P'Q - dP)$	$v([R_0, R_1, R_2])$	$v([S_0, S_1])$
$+$	$+$	$+$				
$+$	$+$	$-$				
$+$	$+$	0				
$+$	$-$	$+$				
$+$	$-$	$-$				
$+$	$-$	0				
$-$	$+$	$+$				
$-$	$+$	$-$				
$-$	$+$	0				
$-$	$-$	$+$				
$-$	$-$	$-$				
$-$	$-$	0				

Concluya que:

- *Si $d > 0$, entonces para todo c con $P(c) \neq 0$, $v_R(c) = v_S(c)$*
- *Si $d < 0$, entonces para todo c con $P(c) \neq 0$, $v_R(c) = v_S(c) + 1$*
- *En cualquier caso si $a < b$ y $P(a)P(b) \neq 0$,*

$$v_S(a) - v_S(b) = v_R(a) - v_R(b) = n_+ - n_-.$$

Solución. Como $P = ax^n + \cdots$ y $P'Q = anbx^n + \cdots$, la división con resto es

$$P'Q = dP + ((P'Q)\%P).$$

Por lo tanto, aplicando lo visto en el Ejercicio 6, $((P'Q)\%P) = -d(P\%(P'Q))$.

- $S_1 = dR_2$
  Por definición, $dR_2 = -d(R_0\%R_1) = -d(P\%(P'Q)) = ((P'Q)\%P) = T = S_1$.
- $S_2 = d^{-1}R_3$

$$d^{-1}R_3 = d^{-1}(R_1\%R_2) = d^{-1}((P'Q)\%(d^{-1}S_1)) = d^{-1}((P'Q)\%S_1)$$
$$= d^{-1}((P'Q)\%((P'Q)\%P)) = d^{-1}((P'Q)\%P) = -(P\%(P'Q)) =$$
$$= -(P\%((P'Q)\%P)) = -(S_0\%S_1) = S_2.$$

- $S_{2i+1} = dR_{2i+2}, i \leq 0$
  Suponemos que se cumple $S_{2j+1} = dR_{2j+2}$ para $0 \leq j \leq i$.

$$S_{2i+2} = -(S_{2i}\%S_{2i+1}) = -(d^{-1}R_{2i+1}\%S_{2i+1}) = -(d^{-1}R_{2i+1}\%dR_{2i+2}) =$$
$$= -d^{-1}(R_{2i+1}\%R_{2i+2}) = -d^{-1}R_{2i+3}.$$

- $S_{2i} = d^{-1}R_{2i+1}, i \leq 1$
  Suponemos que se cumple $S_{2j} = d^{-1}R_{2j+1}$ para $0 \leq j \leq i$.

$$S_{2i+3} = -(S_{2i+1}\%S_{2i+2}) = -(dS_{2i+2}\%d^{-1}S_{2i+3}) = -d(R_{2i+2}\%R_{2i+3}) = -dR_{2i+4}.$$

- $v_{R'}(c) = v_{S'}(c)$
  La lista R' se puede escribir de la siguiente manera.

$$R' = [R_2, R_3, \ldots, R_k] = [d^{-1}S_1, dS_2, \ldots, d^{(-1)^{k'}}S_{k'}].$$

  Tiene el mismo número de cambios de signo en c que $S' = [S_1, S_2, \ldots, S'_k]$ porque d y d^{-1} son constantes no nulas con el mismo signo y no varían el número de cambios de signo. Por lo tanto, $v_{R'}(c) = v_{L'}(c)$.

Rellenamos la tabla con los signos que faltan. Los signos de la cuarta columa no son más que el producto de los de la primera y la tercera. Para completar la cuarta columna usamos la igualdad $P'Q = dP + (P'Q - dP)$. Hay ciertos signos que no podemos deducir, pero podemos rellenar las columnas $v([R_0, R_1, R_2]) = v([P, P'Q, d^{-1}(P'Q - dP)])$ y $v([S_0, S_1]) = v([P, P'Q - dP])$ porque en esos casos sabemos que hay un cambio de signo determinado por P y $d^{-1}(P'Q - dP)$ con lo que independientemente del signo del $P'Q$, hay un único cambio de signo.

d	P	$P'Q - dP$	$P'Q$	$d^{-1}(P'Q - dP)$	$v([R_0, R_1, R_2])$	$v([S_0, S_1])$
$+$	$+$	$+$	$+$	$+$	0	0
$+$	$+$	$-$	?	$-$	1	1
$+$	$+$	0	$+$	0	0	0
$+$	$-$	$+$	?	$+$	1	1
$+$	$-$	$-$	$-$	$-$	0	0
$+$	$-$	0	$-$	0	0	0
$-$	$+$	$+$	?	$-$	1	0
$-$	$+$	$-$	$-$	$+$	2	1
$-$	$+$	0	$-$	0	1	0
$-$	$-$	$+$	$+$	$-$	2	1
$-$	$-$	$-$	?	$+$	1	0
$-$	$-$	0	$+$	0	1	0

- Si $d > 0$, entonces para todo c con $P(c) \neq 0$, $v_R(c) = v_S(c)$.

  Sabemos que $v_{R'}(c) = v_{L'}(c)$ con lo que nos fijamos en si hay cambios de signo en $[R_0, R_1, R_2]$ y $[S_0, S_1]$ que son los primeros términos de R' y S'. Mirando en la tabla, tenemos que si $d > 0$, entonces $v([R_0, R_1, R_2]) = v([S_0, S_1])$ y $v_R(c) = v_L(c)$.

- Si $d < 0$, entonces para todo c con $P(c) \neq 0$, $v_R(c) = v_S(c) + 1$

  Como antes, $v_{R'}(c) = v_{L'}(c)$ y solo nos tenemos que fijar en $[R_0, R_1, R_2]$ y $[S_0, S_1]$. De la tabla tenemos que si $d < 0$, entonces $v([R_0, R_1, R_2]) = v([S_0, S_1]) + 1$ y $v_R(c) = v_L(c) + 1$.

- En cualquier caso si $a < b$ y $P(a)P(b) \neq 0$,

  $$v_S(a) - v_S(b) = v_R(a) - v_R(b) = n_+ - n_-.$$

  Independientemente de si d es positivo o negativo, restando y aplicando lo anterior y el Ejercicio 4 a R,

  $$v_S(a) - v_S(b) = v_R(a) - v_R(b) = n_+ - n_-.$$

Codificación *à la Thom* de un número real.

Ejercicio 10. *Sea $F \in \mathbb{R}[x]$ un polinomio real en una variable no nulo de grado $n \geq 0$. Consideremos la lista de derivadas:*

$$DF = [F, F', \ldots, F^{(n)}]$$

Para cada distribución de signos $\sigma \in \{-1, 0, 1\}^{n+1}$ sea:

$$R(\sigma) = \{c \in \mathbb{R} | \text{sig}(F^{(i)}(c)) = \sigma_i, 0 \leq i \leq n\}$$

Demuestre las siguientes afirmaciones (Pista: use inducción en n y el hecho de que si F' es de signo constante en un intervalo (a, b) entonces F es monótona en ese intervalo.):

- *Para cada σ, $R(\sigma)$ es, o bien vacío, o bien un punto o bien un intervalo real abierto (a, b) (tal vez no acotado).*
- *Una condición necesaria para que $R(\sigma)$ sea un punto es que σ tenga algún signo cero.*
- *Demuestre que si c es una raíz de F, c queda completamente determinado por los signos de las derivadas de F en c,*

  $$\text{sig}(F'(c)), \ldots, \text{sig}(F^{(n)}(c))$$

Solución.

- Para cada σ, $R(\sigma)$ es, o bien vacío, o bien un punto o bien un intervalo real abierto (a, b) (tal vez no acotado).

  Si $n = 0$, entonces $F \in \mathbb{R}$. Tenemos que $R(\sigma) = \emptyset$ si $\sigma \neq \text{sig}(F)$ y $R(\sigma) = \mathbb{R}$ si $\sigma = \text{sig}(F)$. Suponemos que se cumple para grado $n-1$. Sea $F \in \mathbb{R}[x]$ con $\deg(F) = n$ y una tupla de signos $\sigma \in \{-1, 0, 1\}^{n+1}$. Tenemos que

  $$R(\sigma) = R_{F'}(\tilde{\sigma}) \cap \{c \in \mathbb{R} : \text{sig}(F(c)) = \sigma_{n+1}\}$$

  donde $R_{F'}(\tilde{\sigma}) = \{c \in \mathbb{R} : \text{sig}(F^{(i+1)}(c)) = \sigma_i : 0 \leq i \leq n-1\}$ y $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$. Como $\deg(F') = n-1$, aplicando la hipótesis de inducción, se da una de las siguientes igualdades.

  $$R_{F'}(\tilde{\sigma}) = \emptyset \qquad R_{F'}(\tilde{\sigma}) = \{x_0\} \qquad R_{F'}(\tilde{\sigma}) = (a, b)$$

  Si $R_{F'}(\tilde{\sigma}) = \emptyset$, entonces claramente $R(\sigma) = \emptyset$. Si $R_{F'}(\tilde{\sigma}) = \{x_0\}$, entonces

  $$R(\sigma) = \begin{cases} \{x_0\} & \text{si } x_0 \in \{c \in \mathbb{R} : \text{sig}(F(c)) = \sigma_{n+1}\} \\ \emptyset & \text{en otro caso} \end{cases}$$

  Si por el contrario $R_{F'}(\tilde{\sigma}) = (a, b)$, el polinomio F define una función polinomial monótona en el intervalo (a, b). Distinguimos si es monótona creciente o decreciente, si se anula en un único $x_0 \in (a, b)$ o no se anula y el signo σ_{n+1}. Por continuidad, tenemos las siguientes situaciones.

$R(\sigma)$	F es monótona creciente			F es monótona decreciente		
$\sigma_{n+1} = 1$	$\emptyset$	(x_0, b)	(a, b)	(a, b)	(a, x_0)	$\emptyset$
$\sigma_{n+1} = 0$	$\emptyset$	$\{x_0\}$	$\emptyset$	$\emptyset$	$\{x_0\}$	$\emptyset$
$\sigma_{n+1} = -1$	(a, b)	(a, x_0)	$\emptyset$	$\emptyset$	(x_0, b)	(a, b)

  Por lo tanto, $R(\sigma)$ es vacío, unipuntual o un intervalo abierto no necesariamente acotado.

- Una condición necesaria para que $R(\sigma)$ sea un punto es que σ tenga algún signo cero.

  Si $n = 0$, entonces $F \in \mathbb{R}$. Si $\sigma \in \{-1, 1\}$, entonces $R(\sigma) = \emptyset$ o $R(\sigma) = \mathbb{R}$ porque es constante con lo que $\text{sig}(F(c)) = \text{sig}(F) = \sigma$ o $\text{sig}(F(c)) = \text{sig}(F) = -\sigma$. Suponemos que se cumple para grado $n-1$, es decir, que si $F \in \mathbb{R}[x]$ con $\deg(F) = n-1$ y $\sigma \in \{-1, 1\}^n$, entonces $R(\sigma)$ no es conjunto unipuntual. Sea $F \in \mathbb{R}[x]$ con $\deg(F) = n$ y $\sigma \in \{-1, 1\}^{n+1}$. Como antes, tenemos que

  $$R(\sigma) = R_{F'}(\tilde{\sigma}) \cap \{c \in \mathbb{R} : \text{sig}(F(c)) = \sigma_{n+1}\}$$

  donde $R_{F'}(\tilde{\sigma}) = \{c \in \mathbb{R} : \text{sig}(F^{(i+1)}(c)) = \sigma_i : 0 \leq i \leq n-1\}$ y $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$. Como $\deg(F') = n-1$, aplicando la hipótesis de inducción $R_{F'}(\tilde{\sigma})$ no es unipuntual. Se cumple una de las siguientes igualdades.

  $$R_{F'}(\tilde{\sigma}) = \emptyset \qquad R_{F'}(\tilde{\sigma}) = (a, b)$$

  Pero, si $\sigma_{n+1} \in \{-1, 1\}$, entonces, por el apartado anterior $R(\sigma)$ no es unipuntual como queríamos probar. Si $R_{F'}(\tilde{\sigma} = \emptyset)$, entonces $R(\sigma) = \emptyset$ y si $R(\tilde{\sigma}) = (a, b)$, entonces se da una de las siguientes igualdades con $x_0 \in \mathbb{R}$.

  $$R(\sigma) = (a, x_0) \qquad R(\sigma) = (a, b) \qquad R(\sigma) = (x_0, b).$$

- Demuestre que si c es una raíz de F, c queda completamente determinado por los signos de las derivadas de F en c,

  $$\text{sig}(F'(c)), \ldots, \text{sig}(F^{(n)}(c)).$$

Si $n = 0$, entonces $F \in \mathbb{R}$ y $F^{(0)} = F$. Si $F = 0$, entonces $F(0) = 0 = F(1)$, pero $0 \neq 1$. Lo probamos para $n = 1$. Es trivial porque un polinomio de grado 1 tiene una única raíz. Suponemos que se cumple para grado $n-1$, es decir, que si existen $c_1, c_2 \in \mathbb{R}$ raíces de F con $\deg(F) = n-1$ y $\operatorname{sig}(F^{(i)}(c_1)) = \operatorname{sig}(F^{(i)}(c_2))$ para todo $1 \leq i \leq n-1$, entonces $c_1 = c_2$. Lo probamos para grado n. Sea $F \in \mathbb{R}[x]$ con $\deg(F) = n$ y $c_1, c_2 \in \mathbb{R}$ raíces de F tales que $\operatorname{sig}(F^{(i)}(c_1)) = \operatorname{sig}(F^{(i)}(c_2))$ para todo $1 \leq i \leq n$. Tomamos $\sigma_i = \operatorname{sig}(F^i(c_1))$. Como antes, tenemos que

$$R(\sigma) = R_{F'}(\tilde{\sigma}) \cap \{c \in \mathbb{R} : \operatorname{sig}(F(c)) = 0\}$$

donde $R_{F'}(\tilde{\sigma}) = \{c \in \mathbb{R} : \operatorname{sig}(F^{(i+1)}(c)) = \sigma_i : 0 \leq i \leq n-1\}$ y $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$. Claramente por hipótesis, $c_1, c_2 \in R(\sigma)$ porque las derivadas en c_1 y en c_2 tienen los mismos signos y además son raíces de F. En particular $R(\sigma) \neq \emptyset$. Pero como $F \in \mathbb{R}[x]$ es de grado n, no puede tener más de n raíces y, en particular, $R(\sigma)$ no es un intervalo. Por lo tanto, $R(\sigma)$ es un conjunto unipuntual y necesariamente $c_1 = c_2$ como queríamos probar.

Ejercicio 11. *Con la misma notación que el ejercicio anterior. Sean $x, y \in \mathbb{R}$. Sea σ la sucesión de signos que toman F y sus derivadas en x y τ la correspondiente sucesión de signos en y. Supongamos que $\sigma \neq \tau$. Sea k el mayor índice $0 \leq k < n$ tal que $F^{(k)}(x) \neq F^{(k)}(y)$. Entonces*

- $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) \neq 0$
- *Si* $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) = 1$,
$$x > y \leftrightarrow F^{(k)}(x) > F^{(k)}(y)$$
- *Si* $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) = -1$,
$$x > y \leftrightarrow F^{(k)}(x) < F^{(k)}(y)$$

Solución.

- $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) \neq 0$

  Como k es el mayor tal que $F^{(k)}(x) \neq F^{(k)}(y)$, tenemos que $F^{(i)}(x) = F^{(i)}(y)$, y en particular que $\operatorname{sig}(F^{(i)}(x)) = \operatorname{sig}(F^{(i)}(y))$, para todo $k+1 \leq i \leq n$. Razonamos por reducción al absurdo, si $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) = 0$, entonces aplicando el ejercicio anterior, como x e y son raíces de $F^{(k+1)}$ y coinciden los signos de las derivadas en x e y, deben ser iguales $x = y$, lo que contradice el hecho de que $F^{(k)}(x) \neq F^{(k)}(y)$.

- Si $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) = 1$,
$$x > y \leftrightarrow F^{(k)}(x) > F^{(k)}(y)$$

  Tomamos $\sigma_i = \operatorname{sig}(F^{(i)}(x))$ para cada $k+1 \leq i \leq n$. Tenemos que $x, y \in R_{F^{(k+1)}}(\sigma)$. Como $x \neq y$, el conjunto $R_{F^{(k+1)}}(\sigma)$ es no vacío con dos elementos distintos y, por lo tanto, es un intervalo abierto no necesariamente acotado que contiene al intervalo abierto I determinado por x e y. Como $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) = 1$, la función polinomial dada por $F^{(k)}$ es monótona creciente en I y, por definición, usando que $F^{(k)}(x) \neq F^{(k)}(y)$,
$$x > y \leftrightarrow F^{(k)}(x) > F^{(k)}(y).$$

- Si $\operatorname{sig}(F^{(k+1)}(x)) = \operatorname{sig}(F^{(k+1)}(y)) = -1$,
$$x > y \leftrightarrow F^{(k)}(x) < F^{(k)}(y)$$

  Tomamos $\sigma_i = \operatorname{sig}(F^{(i)}(x))$ para cada $k+1 \leq i \leq n$. Tenemos que $x, y \in R_{F^{(k+1)}}(\sigma)$. Como $x \neq y$, el conjunto $R_{F^{(k+1)}}(\sigma)$ es no vacío con dos elementos distintos y, por lo tanto, es un

intervalo abierto no necesariamente acotado que contiene al intervalo abierto I determinado por x e y. Como $\text{sig}(F^{(k+1)}(x)) = \text{sig}(F^{(k+1)}(y)) = -1$, la función polinomial dada por $F^{(k)}$ es monótona decreciente en I y, por definición, usando que $F^{(k)}(x) \neq F^{(k)}(y)$,

$$x > y \leftrightarrow F^{(k)}(x) > F^{(k)}(y).$$

El siguiente algoritmo calcula $V(L, -\infty, \infty)$, para L la sucesión de restos con signo cambiado a partir de P y Q.

```
def sturmcount(P, Q):
    if P == 0 or Q == 0:
        raise(ValueError)
    L = [P, Q]
    while L[-1] != 0:
        L.append(-L[-2] % L[-1])
    L = L[:-1]
    count = 0
    for i in range(len(L) - 1):
        n = L[i].degree()
        m = L[i+1].degree()
        if (n-m) % 2 == 1:
            an = L[i][n]
            bm = L[i+1][m]
            count = count + sign(an * bm)
    return count
```

Ejercicio 12. *Sean $F = x^3 - 3x^2 + 3$, $G = 10x^2 - 15x + 1$. Calcule la codificación à la Thom de la única raíz α de F que cumple $Q(\alpha) < 0$. Solo puede usar el algoritmo sturmcount anterior en dos polinomios para extraer información.*

Solución. Con la notación del Corolario 2.5, podemos calcular el número $V(P, Q)$ variaciones de signo la sucesión L de restos con signo cambiado a partir de P y $P'Q$ aplicando el algoritmo anterior como $\text{sturmcount}(P, P'Q) = V(P, Q)$. Por lo tanto, podemos calcular,

$$\begin{aligned} n_+ &= |\{c \in \mathbb{R} : P(c) = 0, Q(c) > 0\}| = \frac{V(P, Q^2) + V(P, Q)}{2} \\ n_- &= |\{c \in \mathbb{R} : P(c) = 0, Q(c) < 0\}| = \frac{V(P, Q^2) - V(P, Q)}{2} \\ n_0 &= |\{c \in \mathbb{R} : P(c) = 0, Q(c) = 0\}| = V(P, 1) - V(P, Q^2) \end{aligned}$$

y el número de raíces disintas de P que es $n_0 + n_+ + n_- = |\{c \in \mathbb{R} : P(c) = 0\}| = V(P, 1)$.

Queremos calcular los signos $\text{sig}(F'(\alpha)), \text{sig}(F''(\alpha)), \text{sig}(F'''(\alpha))$ donde α es la única raíz de F tal que $G(\alpha) < 0$. El número de raíces distintas de F es $|\{c \in \mathbb{R} : F(c) = 0\}| = V(F, 1) = 3$. Como $|\{c \in \mathbb{R} : F(c) = 0, G(c) < 0\}| = 1$, efectivamente F tiene una única raíz α tal que $G(\alpha) < 1$.

Tenemos que $|\{c \in \mathbb{R} : F(c) = 0, F'(c)G(c) < 0\}| = 0$. Lo podemos expresar como

$$|\{c \in \mathbb{R} : F(c) = 0, F'(c) < 0, G(c) > 0\}| + |\{c \in \mathbb{R} : F(c) = 0, F'(c) > 0, G(c) < 0\}|.$$

Ambos sumandos deben ser 0 para que la suma lo sea.

Además, $|\{c \in \mathbb{R} : F(c) = 0, F'(c)G(c) > 0\}| = 2$, que coincide con la suma

$$|\{c \in \mathbb{R} : F(c) = 0, F'(c) > 0, G(c) > 0\}| + |\{c \in \mathbb{R} : F(c) = 0, F(c) < 0, G(c) < 0\}|.$$

La suma podría ser $1 + 1$, $2 + 0$ o $0 + 2$, pero los dos últimos casos no se pueden dar porque teniendo en cuenta que F tiene una única raíz α tal que $G(\alpha) < 0$,

$$\begin{aligned} |c \in \mathbb{R} : F(c) = 0, G(c) < 0| = |\{c \in \mathbb{R} : F(c) = 0, F'(c) < 0, G(c) < 0\}| + \\ + |\{c \in \mathbb{R} : F(c) = 0, F'(c) > 0, G(c) < 0\}| = 1 \end{aligned}$$

donde tenemos de antes que el primer sumando es nulo, con lo que el segundo debe ser 1. Por lo tanto, el primer signo de la codificación es $\text{sig}(F'(c)) = -1$.

Tenemos que $|\{c \in \mathbb{R} : F(c) = 0, F''(c)G(c) < 0\}| = 2$. Lo podemos expresar como

$$|\{c \in \mathbb{R} : F(c) = 0, F''(c) < 0, G(c) > 0\}| + |\{c \in \mathbb{R} : F''(c) > 0, G(c) < 0\}|.$$

Además, $|\{c \in \mathbb{R} : F(c) = 0, F''(c)G(c) > 0\}| = 1$, que coincide con la suma

$$|\{c \in \mathbb{R} : F(c) = 0, F''(c) > 0, G(c) < 0\}| + |\{c \in \mathbb{R} : F(c) = 0, F''(c) < 0, G(c) < 0\}|.$$

La primera suma podría ser $1+1$, $2+0$ o $0+2$ y la segunda podría ser $1+0$ o $0+1$. Teniendo en cuenta la únicidad de α, tenemos en conjunto dos casos posibles $1+1$ y $1+0$ o $2+0$ y $0+1$. No es suficiente con estas descomposiciones para averiguar el valor de los sumandos. Calculamos también $|\{c \in \mathbb{R} : F(c) = 0, F''(c) < 0\}| = 1$ que es

$$|\{c \in \mathbb{R} : F(c) = 0, F''(c) < 0, G(c) > 0\}| + |\{c \in \mathbb{R} : F(c) = 0, F''(c) < 0, G(c) < 0\}|,$$

con lo que la suma del primer sumando de la primera descomposición y el segundo de las segunda es 1 y la única posibilidad es que sean $1+1$ y $1+0$. En particular, el segundo signo de la codificación es $\text{sig}(F''(\alpha)) = 1$.

Tenemos que $|\{c \in \mathbb{R} : F(c) = 0, F'''(c)G(c) < 0\}| = 1$. Lo podemos expresar como

$$|\{c \in \mathbb{R} : F(c) = 0, F'''(c) < 0, G(c) > 0\}| + |\{c \in \mathbb{R} : F(c) = 0, F'''(c) > 0, G(c) < 0\}|.$$

Además, $|\{c \in \mathbb{R} : F(c) = 0, F'''(c)G(c) > 0\}| = 2$, que coincide con la suma

$$|\{c \in \mathbb{R} : F(c) = 0, F'''(c) > 0, G(c) > 0\}| + |\{c \in \mathbb{R} : F(c) = 0, F'''(c) < 0, G(c) < 0\}|.$$

La primera suma podría ser $1+0$ o $0+1$ y la segunda podría ser $1+1$, $2+0$ y $0+2$. Teniendo en cuenta la únicidad de α, tenemos en conjunto dos casos posibles $0+1$ y $2+0$ o $1+0$ y $1+1$. No es suficiente con estas descomposiciones para averiguar el valor de los sumandos. Calculamos también $|\{c \in \mathbb{R} : F(c) = 0, F'''(c) < 0\}| = 0$ que es

$$|\{c \in \mathbb{R} : F(c) = 0, F'''(c) < 0, G(c) > 0\}| + |\{c \in \mathbb{R} : F(c) = 0, F'''(c) < 0, G(c) < 0\}|,$$

con lo que la suma del primer sumando de la primera descomposición y el segundo de las segunda es 0 y la única posibilidad es que sean $2+0$ y $0+1$. En particular, el segundo signo de la codificación es $\text{sig}(F''(\alpha)) = 1$.

La codificación *à la Thom* de α es $(-,+,+)$.

Ejercicio 13. *Sea $f = x^5 - 2x^4 - 3x^3 + 6x^2 - 4x + 8$. Sin calcular explícitamente las raíces y sin calcular factorizaciones:*

- *Calcule cuántas raíces reales distintas tiene f.*
- *Calcule la multiplicidad de cada raíz.*
- *Dadas x, y raíces de f determinadas por su multiplicidad, determine cuál es mayor.*

Solución.

- Calcule cuántas raíces reales distintas tiene f.

  Directamente aplicando el algoritmo anterior

  $$n_0 + n_+ + n_- = |\{c \in \mathbb{R} : f(c) = 0\}| = V(f, 1) = \text{sturmcount}(f, f') = 2,$$

  con lo que f tiene dos raíces reales distintas.

- Calcule la multiplicidad de cada raíz.

  Para calcular la multiplicidad, aplicamos el Corolario 2.3 a f con sus derivadas. Como

  $$|\{c \in \mathbb{R} : f(c) = 0, f'(c) = 0\}| = V(f, 1) - V(f, f'^2) = \\ = \text{sturmcount}(f, f') - \text{sturmcount}(f, f'f'^2) = 1,$$

  tiene una raíz simple y la otra al menos con multiplicdad 2. Probamos con la segunda derivada y tenemos

  $$|\{c \in \mathbb{R} : f(c) = 0, f''(c) = 0\}| = V(f, 1) - V(f, f''^2) = \\ = \text{sturmcount}(f, f') - \text{sturmcount}(f, f'f''^2) = 0,$$

  con lo que tiene una raíz simple y la otra doble.

- Dadas x, y raíces de f determinadas por su multiplicidad, determine cuál es mayor.

  Denotamos por x a la raíz simple y por y a la raíz doble. Buscamos la derivada de orden $0 \leq k < 5$ mayor tal que $f^{(k)}(x) \neq f^{(k)}(y)$. Empezamos con $k = 4$. Se cumple que,

  $$|\{c \in \mathbb{R} : f(c) = 0, f^{(4)}(c) < 0\}| = 1$$
  $$|\{c \in \mathbb{R} : f(c) = 0, f^{(4)}(c) > 0\}| = 1$$

  y debe ser $f^{(4)}(x) \neq f^{(4)}(y)$. Podemos calcular el signo en la derivada $f^{(5)}$ en x e y como

  $$|\{c \in \mathbb{R} : f(c) = 0, f^{(5)}(c) > 0\}| = 2,$$

  con lo que $\text{sig}(f^{(5)}(x)) = \text{sig}(f^{(5)}(y)) = 1$ y aplicando el Ejercicio 11, se cumple

  $$x < y \leftrightarrow f^{(4)}(x) < f^{(4)}(y).$$

  Tenemos que $|\{c \in \mathbb{R} : f(c) = 0, f'(c)f^{(4)} < 0\}| = 1$. Lo podemos escribir como

  $$|\{c \in \mathbb{R} : f(c) = 0, f'(c) < 0, f^{(4)} > 0\}| + |\{c \in \mathbb{R} : f(c) = 0, f'(c) > 0, f^{(4)}(c) < 0\}|.$$

  Ademas, $|\{c \in \mathbb{R} : f(c) = 0, f'(c)f^{(4)}(c) > 0\}| = 0$, que coincide con la suma

  $$|\{c \in \mathbb{R} : f(c) = 0, f'(c) > 0, f^{(4)} > 0\}| + |\{c \in \mathbb{R} : f(c) = 0, f'(c) < 0, f^{(4)}(c) < 0\}|.$$

  Los dos últimos sumandos deben ser 0, pero como f tiene una raíz simple y otra doble, tenemos $|\{c \in \mathbb{R} : f(c) = 0, f'(c) > 0, f^{(4)}(c) < 0\}| = 1$, lo que implica que $f^{(4)}(x) < 0$.
  Tenemos que $|\{c \in \mathbb{R} : f(c) = 0, f^{(4)}(c) > 0\}| = 1$ y se cumple

  $$|\{c \in \mathbb{R} : f(c) = 0, f'(c) = 0, f^{(4)}(c) > 0\}| = |\{c \in \mathbb{R} : f(c) = 0, f^{(4)}(c) > 0\}| - \\ -|\{c \in \mathbb{R} : f(c) = 0, f'(c) < 0, f^{(4)}(c) > 0\}| - |\{c \in \mathbb{R} : f(c) = 0, f'(c) > 0, f^{(4)}(c) > 0\}| = 1.$$

  Por lo tanto, $f^{(4)}(x) < 0 < f^{(4)}(y)$ y la raíz simple es menor que la doble.