Facultad
de
Ciencias

El cálculo del máximo común divisor de polinomios sobre cuerpos de números

(Computing the greatest common divisor of polynomials over number fields)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Adrián Sansiñena Rodríguez
Director: Luis Felipe Tabera Alonso

Junio 2022

Agradecimientos

En primer lugar, quiero dar las gracias a mi director, Luis, por su paciencia, amabilidad y dedicación. Gracias también al resto de mis profesores del grado por haber sabido inculcarnos su pasión por las matemáticas a lo largo de toda la carrera.

Quiero agradecer a mi familia su apoyo durante estos cinco años. Me hubiese gustado haber podido compaginar todo mejor para haber pasado más tiempo con vosotros.

Por último, me gustaría mencionar a mis amigos de Laredo, sobretodo a mis compañeros de piso con los que he compartido estos años y quienes han hecho más amena mi estancia en Santander.

Índice general

1. Introducción **1**

2. Requisitos algebraicos **3**
2.1. La resultante de dos polinomios 3
2.2. Teoría de subresultantes 7
2.3. Teorema de Praga de Dedekind 15

3. Escogiendo los primos correctos **18**
3.1. Una cota para el máximo común divisor 18
3.2. Los anillos finitos $R/(p)$ 24
3.3. Cálculo de h^* 30

4. Reconstrucción del máximo común divisor sobre $\mathbb{Z}[\alpha]$ **36**
4.1. Sobre la condición de parada 37
4.2. Algoritmo 38
4.3. Posibles mejoras del algoritmo 39
4.4. Tiempo de ejecución 40

Resumen

Al aplicar el algoritmo de Euclides tal y como hemos visto en el grado en el caso de polinomios con coeficientes racionales ocurre el fenómeno llamado explosión de coeficientes. El tamaño de los coeficientes de los polinomios intermedios hace que este algoritmo no sea eficiente en la práctica para polinomios de grado moderado.

En esta memoria trabajaremos con polinomios con coeficientes en un cuerpo de números. Presentamos y analizamos un algoritmo alternativo propuesto por Langemyr y McCallum, basado en una algoritmo similar propuesto por Brown en el caso de polinomios con coeficientes racionales, que realiza el cálculo del máximo común divisor sobre varios anillos finitos para luego reconstruir el máximo común divisor original usando el Teorema Chino de los Restos.

Palabras clave: Máximo común divisor, Teorema Chino de los Restos, Resultante, Discriminante, Subresultante, Entero algebraico.

Abstract

When applying Euclid's algorithm to the case of polynomials with rational coefficients, the phenomenon known as coefficient explosion arises. The size of the coefficients of the intermediate polynomials makes this algorithm unfeasible in practice for polynomials of moderate degree.

In this report, we study the case of polynomials with coefficients in a number field. We present and analyze an alternative algorithm proposed by Langemyr and McCallum, based on an algorithm proposed by Brown for the case of rational coefficients, that computes greatest common divisor over several finite rings and then reconstructs the original greatest common divisor using the Chinese Remainder Theorem.

Key words: Greatest common divisor, Chinese Remainder Theorem, Resultant, Discriminant, Subresultant, Algebraic Integer.

Capítulo 1

Introducción

El algoritmo de Euclides, que aparece en la proposición segunda del séptimo libro de *los Elementos*, es un sencillo método para el cálculo del máximo común divisor de dos números enteros. Se puede extender de manera natural para el cálculo del máximo común divisor sobre dominios euclídeos. En el caso particular de polinomios con coeficientes en $\mathbb{Q}$ no es un método eficiente. Esto se debe al crecimiento, también conocido como *explosión*, del tamaño de los coeficientes de los restos intermedios. Brown y Collins desarrollaron de manera independiente en 1971 un algoritmo modular para el caso de polinomios con coeficientes en $\mathbb{Q}$, que conseguía evitar el problema del crecimiento de los factores [2]. Otra alternativa a estos algoritmos modulares es usar el llamado método de las subresultantes. Este método fue propuesto por el propio Collins [4] en 1967 y consiste a grandes rasgos en seguir el algoritmo que se utiliza para el cálculo de subresultantes. Cada cierto número de pasos, se dividen los restos intermedios por un divisor de sus contenidos, reduciendo así el tamaño de los coeficientes. Este método resulta, no obstante, menos eficiente que el algoritmo modular.

En 1987 Langemyr y McCallum [7] propusieron un algoritmo modular basado en el de Brown y Collins pero que funciona para polinomios con coeficientes en un cuerpo de números algebraicos. Dados dos polinomios f y $g \in \mathbb{Q}(\alpha)[x]$, este algoritmo calcula el máximo común divisor de sus clases módulo diversos cuerpos finitos $\mathbb{F}_q$. Posteriormente, se recupera el máximo común divisor de f y g aplicando el Teorema Chino de los Restos. Obsérvese que, de esta manera, sobre cada cuerpo finito, no se da el fenómeno de explosión de coeficientes.

Claramente, esta estrategia no se puede implementar de una manera ingenua. Para poder reducir un polinomio módulo un cuerpo finito $\mathbb{F}_q$, deberemos considerar asociados a los polinomios f y g que tengan coeficientes en un subanillo de $\mathbb{Q}(\alpha)$ donde tengan sentido estas reducciones. Por esto, asumiremos que α es un entero algebraico, el subanillo será $\mathbb{Z}[\alpha]$ y tomaremos las clases de f y g en $\mathbb{Z}[\alpha]/(p)[x]$. Pero, para que $\mathbb{Z}[\alpha]/(p)$ sea un cuerpo necesitamos que el polinomio mínimo de α sobre $\mathbb{Z}$ sea irreducible módulo p. Conocemos polinomios irreducibles sobre $\mathbb{Z}$ pero reducibles módulo cualquier primo p, por lo que esto no es siempre posible. Además, incluso en el caso de que $\mathbb{Z}[\alpha]/(p)$ sea un cuerpo, el cálculo del máximo común divisor puede no

conmutar con la reducción módulo p. Finalmente, recordemos que el máximo común divisor está definido salvo asociados. Querremos, por tanto, definir unos asociados privilegiados $h \sim \gcd(f, g)$ y $h_q \sim \gcd(\bar{f}, \bar{g})$ de manera que h tenga coeficientes en $\mathbb{Z}[\alpha]$ y su reducción a $\mathbb{F}_q$ sea h_q.

Recordemos que en $\mathbb{Z}[x]$, si f es un polinomio primitivo, el lema de Gauss nos asegura que la factorización en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ coincide. En particular, el máximo común divisor de dos polinomios primitivos tiene de manera natural coeficientes en $\mathbb{Z}[x]$. Puede ocurrir que $\mathbb{Z}[\alpha]$ no sea un dominio de factorización única y no podamos aplicar el Lema de Gauss. No obstante, demostraremos que los coeficientes de un factor de f pertenecen al anillo de enteros que, pese a que puede no ser un dominio de factorización única, cumplirá una versión del Lema de Gauss. Véase el Lema 3.1.7.

En la presente memoria, comenzamos en el Capítulo 2 dando un breve resumen de la teoría de resultantes y subresultantes que nos va a permitir controlar cuándo el máximo común divisor conmuta con la reducción módulo p. Seguidamente damos una versión del Lema de Gauss conocida como el Teorema de Praga de Dedekind para la relación del máximo común divisor de dos polinomios sobre $\mathbb{Q}(\alpha)$ y el anillo de enteros. En el Capítulo 3 analizamos con detalle qué tipo de anillos aparecen al calcular la reducción de $\mathbb{Z}(\alpha)$ módulo p, para lo cual lo escribiremos como producto de cuerpos utilizando el Teorema Chino de los Restos cuando sea posible. También veremos qué tipo de fenómenos pueden aparecer al comparar el máximo común divisor de $\bar{f}$ y $\bar{g}$ y la reducción de $\gcd(f, g)$ módulo p. Finalmente, en el Capítulo 4, discutimos el algoritmo.

Se ilustrarán los distintos detalles y casos discutidos sobre el algoritmo mediante distintos ejemplos. Estos ejemplos han sido elaborados con la ayuda del programa *SageMath*.

Capítulo 2

Requisitos algebraicos

La teoría de subresultantes puede entenderse como una generalización de la noción de resultante. Permite establecer una relación entre el máximo común divisor de dos polinomios y los determinantes de unas matrices definidas a partir de sus coeficientes. Además, el valor de estos determinantes guardan un estrecho paralelismo con los grados de los restos que aparecen en el algoritmo de Euclides y, bajo ciertas condiciones, conmuta con la reducción módulo p. En estos casos se dice que la subresultante especializa bien.

2.1. La resultante de dos polinomios

En primer lugar, vamos a recordar brevemente la noción de resultante de dos polinomios y algunas de sus propiedades.

Definición 2.1.1. Sea $\mathbb{K}$ un cuerpo. Sean $f = \sum_{i=0}^{n} a_i x^i$ y $g = \sum_{i=0}^{m} b_i x^i$ dos polinomios con coeficientes en $\mathbb{K}$. Se define la matriz de Sylvester de f y g, $Syl(f,g)$ como la matriz cuadrada de tamaño $n+m$ de la forma:

$$Syl(f,g) = \begin{pmatrix} a_n & a_{n-1} & \dots & \dots & \dots & \dots & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & \dots & \dots & \dots & \dots & \dots & a_1 & a_0 & \dots & 0 \\ & & \ddots & & & & & & & \ddots & \\ 0 & 0 & & a_n & \dots & \dots & \dots & \dots & \dots & \dots & a_0 \\ b_m & b_{m-1} & \dots & \dots & \dots & b_0 & 0 & \dots & \dots & \dots & 0 \\ 0 & b_m & \dots & \dots & \dots & b_1 & b_0 & \dots & \dots & \dots & 0 \\ & & & \ddots & & & & & \ddots & & \\ 0 & 0 & \dots & \dots & b_m & b_1 & b_0 & \dots & \dots & \dots & b_0 \end{pmatrix}.$$

La matriz de Sylvester es la matriz asociada a la siguiente aplicación $\mathbb{K}$-lineal:

$$\begin{array}{rcl} \Psi : \mathbb{K}[x]_{<m} \times \mathbb{K}[x]_{<n} & \longrightarrow & \mathbb{K}[x]_{<n+m} \\ (u(x), v(x)) & \mapsto & u(x)f(x) + v(x)g(x). \end{array}$$

Definición 2.1.2. Se denomina resultante de dos polinomios $Res(f,g)$ al determinante de $Syl(f,g)$.

En la siguiente proposición se enuncian algunas propiedades de las resultantes ya estudiadas en el grado que utilizaremos más adelante:

Proposición 2.1.3. *Sean f y g dos polinomios con coeficientes en $\mathbb{K}$. Entonces la resultante de f y g cumple las siguientes propiedades:*

- $Res(f,g) = (-1)^{nm} Res(g,f)$.
- *Si* $f = a \in K^*$, $\deg(g) > 0$, $Res(f,g) = a^m$.
- *Si* $g = b \in K^*$, $\deg(f) > 0$, $Res(f,g) = b^n$.
- $Res(f,g) = 0$ *si y solo si* $\deg(\gcd(f,g)) > 0$.

El interés por la noción de resultante en este trabajo proviene fundamentalmente de la última de las propiedades enunciadas en la proposición.

A partir de los siguientes resultados, que pueden encontrarse en [1], demostraremos cómo se relaciona el determinante de dos polinomios y los determinantes de sus factores.

Lema 2.1.4. *Sean f y g dos polinomios en $\mathbb{K}[x]$ no nulos de grados n y m, $n \geq m$. Podemos escribir $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$. Sea r, $\deg(r) = p < m$, el resto de dividir f entre g, $f = qg + r$. Supongamos que r es no nulo. Entonces:*

$$Res(f,g) = (-1)^{nm} b_m^{n-p} Res(g,r).$$

Demostración. Sea $r = \sum_{i=0}^{p} c_i x^i$. En primer lugar, $Res(f,g) = (-1)^{nm} Res(g,f)$. Por lo tanto es suficiente probar $Res(g,f) = b_m^{n-p} Ref(g,r)$.

A partir de la igualdad $f = qg + r$ es posible hacer ceros en la matriz $Syl(g,f)$ ya que $\deg(r) < g$. Podemos escribir $q = \sum_{i=0}^{n-m} d_i x^i$. Entonces $f = \sum_{i=0}^{n-m} d_i x^i g + r$. Por lo tanto, restando a una fila con los coeficientes de f como entradas, múltiplos de filas de g, pasamos de tener los coeficientes de f en dicha fila a los coeficientes de r sin que el determinante de la matriz cambie. Escribiendo $r = \sum_{i=0}^{p} c_i x^i$, la matriz tendrá la forma:

$$\begin{pmatrix}
b_m & \dots & b_{m-(n-p)+1} & \dots & & & & \\
 & \ddots & & & & & & \\
0 & \dots & b_m & \dots & & & & \\
0 & \dots & 0 & b_m & \dots & b_0 & \dots & 0 \\
 & \ddots & & & \ddots & & \ddots & \\
0 & \dots & 0 & & & b_m & \dots & b_0 \\
0 & \dots & 0 & c_p & \dots & c_0 & \dots & 0 \\
 & \ddots & & & \ddots & & \ddots & \\
0 & \dots & 0 & & & c_p & \dots & c_0
\end{pmatrix}.$$

En las primeras $n-p$ columnas tenemos sólo una submatriz triangular superior con b_m en la diagonal. Desarrollando el determinante por estas columnas obtenemos:

$$Res(g,f) = b_m^{n-p} \begin{vmatrix} b_m & \dots & b_0 & \dots & 0 \\ & \ddots & & \ddots & 0 \\ & & b_m & \dots & b_0 \\ c_p & \dots & c_0 & \dots & 0 \\ & \ddots & & \ddots & 0 \\ & & c_p & \dots & c_0 \end{vmatrix} = b_m^{n-p} Res(g,r).$$

Entonces $Res(f,g) = (-1)^{nm} Res(g,f) = (-1)^{nm} Res(g,r)$ como queríamos probar. □

Lema 2.1.5. *Sea $\mathbb{K}$ un cuerpo y sean f y g dos polinomios no nulos en $\mathbb{K}[x]$. Sea*

$$f = a_n \prod_{i=1}^{n} (x - \alpha_i), \qquad g = b_m \prod_{i=1}^{m} (x - \beta_i),$$

la factorización de f y g en alguna clausura algebraica de $\mathbb{K}$ donde alguno de los factores pueden aparecer repetidos. Entonces:

$$Res(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Demostración. Denotemos $Diff(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$ y veamos por inducción sobre la longitud en la sucesión de restos del algoritmo de Euclides aplicado a f y g para calcular $\gcd(f,g)$ que $Res(f,g) = Diff(f,g)$.

En el caso base, la longitud de restos es mínima $\Longrightarrow g = \gcd(f,g)$. En este caso se tiene que si g es constante entonces $Res(f,g) = b_m^n$ ya que $Syl(f,g)$ es una matriz diagonal con n filas y columnas, el grado de n y los elementos de la diagonal son $b_m = g$. Por lo tanto en se cumple $Res(f,g) = Diff(f,g)$. Si por otro lado ni f ni g son constantes, tanto la resultante como $Diff(f,g)$ se anulan porque tienen raíces en común en la extensión algebraica.

Supongamos ahora que es cierto para pares f y g tales que la sucesión de restos del algoritmo de Euclides para llegar hasta su gcd tiene longitud menor o igual que $k-1$ y probemos la igualdad para un par cuya la longitud sea k. Sea f y g dicho par. La primera división del algoritmo será $f = gq + r$. Como f y g necesitan k divisiones, g y r necesitan $k-1$ ya que son las mismas que para f y g salvando la primera. Entonces, por hipótesis de inducción, $Diff(g,r) = Res(g,r)$. Sea $p < m$ el grado de r y $r = c_p \prod_{i=1}^{p} (x - \gamma_i)$ su factorización. Con esto y teniendo en cuenta que $Res(f,g) = (-1)^{nm} b_m^{n-p} Res(g,r)$ se llega a la igualdad deseada desarrollando $Diff(f,g)$:

$$Diff(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) = (-1)^{nm} a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\beta_j - \alpha_i) =$$

$$= (-1)^{nm} b_m^n \prod_j = 1^m f(\beta_j) = (-1)^{nm} b_m^n \prod_{j=1}^{m} (qg + r)(\beta_j) =$$

$$= (-1)^{nm} b_m^{n-p} b_m^p \prod_{j=1}^{m} r(\beta_j) = (-1)^{nm} b_m^n - p b_m^p c_p^m \prod_{j=1}^{m} \prod_{i=1}^{p} (\beta_j - \gamma_i) =$$

$$= (-1)^{nm} b_m^{n-p} Diff(g, r) = (-1)^{nm} b_m^{n-p} Res(g, r) = Res(f, g).$$

□

La igualdad que establece el lema que acabamos de demostrar suele utilizarse a menudo como la propia definición de resultante de dos polinomios.

Lema 2.1.6. *Sean f y g dos polinomios con factorización $f = a_n \prod_{i=1}^{n}(x - \alpha_i)$ y $g = b_m \prod_{i=1}^{m}(x - \beta_i)$ en una clausura algebraica, entonces*

$$Res(f, g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j).$$

Demostración. Es inmediato a partir del lema anterior. En la primera igualdad basta con observar que $g(\alpha) = b_m \prod_{i=1}^{m}(\alpha - \beta_i)$ y, para la segunda, $f(\beta) = a_n \prod_{i=1}^{n}(\beta - \alpha_i) = (-1)^n \prod_{i=1}^{n}(\alpha_i - \beta)$. □

Teorema 2.1.7. *Sean $f,\ g \in \mathbb{K}[x]$ dos polinomios no nulos y $f = f_1 \cdots f_r$, $g = g_1 \cdots g_s$ factorizaciones de f y g en $\mathbb{K}[x]$ no necesariamente en factores irreducibles o distintos. Entonces*

$$Res(f, g) = \prod_{i=1}^{r} \prod_{j=1}^{s} Res(f_i, g_j).$$

Demostración. Es suficiente con demostrar, sin pérdida de generalidad, que

$$Res(f, g) = \prod_{i=1}^{r} Res(f_i, g),$$

ya que en ese caso, para cada $1 \leq i \leq r$ se tendría

$$Res(f_i, g) = \prod_{j=1}^{s} Res(f_i, g_j).$$

y por lo tanto,

$$Res(f, g) = \prod_{i=1}^{r} \left(\prod_{j=1}^{s} Res(f_i, g_j) \right) = \prod_{i=1}^{r} \prod_{j=1}^{s} Res(f_i, g_j).$$

Sea $\overline{\mathbb{K}}$ la clausura algebraica de f y g. Sean $f = a_n \prod_{i=1}^{n}(x - \alpha_i)$ y $g = b_m \prod_{j=1}^{m}(cx - \beta_j)$ las factorizaciones en $\overline{\mathbb{K}}$. Cada g_i tendrá una factorización $g_j = b_j(x - \alpha_{j1}) \cdots (x - \alpha_{jt(j)})$ sobre $\overline{\mathbb{K}}$, de forma que

$$g = b_m \prod_{j=1}^{m}(x - \beta_j) = \prod_{j=1}^{s} \left(b_j(x - \alpha_{j1}) \cdots (x - \alpha_{jt(j)}) \right).$$

$Res(f,g) = a_n^m \prod_{i=1}^n g(\alpha_i)$ y, en particular, para cada g_j,

$$Res(f,g_j) = a_n^{t(j)} \prod_{i=1}^n g_j(\alpha_i).$$

Entonces:

$$Res(f,g) = a_n^m \prod_{i=1}^n g(\alpha_i) = a_n^m \prod_{i=1}^n \left(\prod_{j=1}^s g_j(\alpha_i) \right) =$$

$$= \prod_{j=1}^s \left(a_n^{t(j)} \prod_{i=1}^n g_j(\alpha_i) \right) = \prod_{j=1}^s Res(f,g_j).$$

□

2.2. Teoría de subresultantes

La teoría de subresultantes amplía la de resultantes y la usaremos explícitamente para caracterizar los pirmos p para los cuales el algoritmo de Euclides fallará en un anillo $(\mathbb{Z}(\alpha)/(p))$ que no sea cuerpo o los casos en los que el máximo común divisor no conmute con la reducción módulo p.

Sea $\mathbb{K}$ un cuerpo, f y g polinomios de grados n y m respectivamente en $\mathbb{K}[x]$.

$$f = \sum_{i=0}^n a_i x^n, \qquad\qquad g = \sum_{i=0}^m b_i x^n.$$

Se define la siguiente aplicación lineal:

$$\begin{array}{rcl} \Psi_j : \mathbb{K}[x]_{<m-j} \times \mathbb{K}[x]_{<n-j} & \longrightarrow & \mathbb{K}[x]_{<n+m-j}/\mathbb{K}[x]_{<j} \\ (u(x),v(x)) & \mapsto & (u(x)f(x)+v(x)g(x))//x^j. \end{array}$$

Donde $z//y$ representa el cociente de la división de z entre y. Observamos en primer lugar que si $j=0$, Ψ_0 es la aplicación lineal que define la matriz de Sylvester de f y g.

Tomando las bases

$$B_S = [x^{m-j-1}, \ldots, 1; x^{n-j-1}, \ldots, 1], \qquad B_{LL} = [x^{n+m-1}, \ldots, x^j],$$

la matriz de Ψ_j es la matriz cuadrada de tamaño $(m+n-2j)$ de la forma siguiente:

$$\Psi_j = \begin{pmatrix} a_n & a_{n-1} & \ldots & \ldots & \ldots & \ldots & \ldots & a_0 & 0 & \ldots & 0 \\ 0 & a_n & \ldots & \ldots & \ldots & \ldots & \ldots & a_1 & a_0 & \ldots & 0 \\ & & \ddots & & & & & & & \ddots & \\ 0 & 0 & \ldots & a_n & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & a_j \\ b_m & b_{m-1} & \ldots & \ldots & \ldots & b_0 & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & b_m & \ldots & \ldots & \ldots & 0 & b_0 & \ldots & \ldots & \ldots & 0 \\ & & & \ddots & & & & & & \ddots & \\ 0 & 0 & \ldots & \ldots & b_m & \ldots & \ldots & \ldots & \ldots & \ldots & b_j \end{pmatrix}.$$

Ψ_j resulta por tanto de eliminar las primeras j filas y j columnas, las siguientes j filas a la fila m y las últimas j columnas de la matriz de Sylvester.

Definición 2.2.1. Se denomina j-ésimo coeficiente subresultante principal de f y g al determinante de Ψ_j. Lo denotaremos por $\mathrm{sRes}_j(f,g)$.

La resultante es un caso particular de coeficiente subresultante principal, en concreto, ambas nociones coinciden uando $j=0$. Recordemos que el interés por el estudio de las propiedades de las resultantes provenía de su relación con el máximo común divisor de dos polinomios, en la primera parte de esta sección vamos a ver cómo generalizar esta propiedad al resto de coeficientes subresultantes.

El siguiente teorema nos permite conocer bajo qué condiciones la subresultante de dos polinomios conmuta con un homomorfismo, especializa bien.

Teorema 2.2.2. *Sean $f,\ g \in \mathbb{K}[x]$. $\deg(f)=n$, $\deg(g)=m\leq n$. Sea $\phi:\mathbb{K}\longrightarrow\mathbb{K}'$ que se extiende a $\phi:\mathbb{K}[x]\longrightarrow\mathbb{K}'[x]$ definiendo $\phi(x)=x$ y tal que $\deg(\phi(f))=n$, $\deg(\phi(g))=p\leq m$. Entonces si $0\leq j<p$:*

$$\phi(sRes_j(f,g))=\phi(a_n^{m-p})sRes_j(\phi(f),\phi(g)).$$

Demostración. Sean $a_n,\ldots,a_0$ y $b_m,\ldots,b_0$ los coeficientes de f y g respectivamente con $a_n\neq 0$ y $b_m\neq 0$. Dada la matriz de Sylvester (Ψ_0) de f y g,

$$\begin{pmatrix}
a_n & \ldots & \ldots & \ldots & & & & & \\
 & \ddots & & & & & & & \\
0 & \ldots & a_n & \ldots & & & & & \\
0 & \ldots & \ldots & a_n & \ldots & & \ldots & & \\
 & \ddots & & & \ddots & & \ldots & & \\
0 & \ldots & 0 & \ldots & & & a_n & \ldots & a_0 \\
b_m & \ldots & b_{p+1} & b_p & \ldots & & \ldots & & \\
 & \ddots & & & \ddots & & \ddots & & \\
0 & \ldots & b_m & b_{m-1} & \ldots & b_p & \ldots & & \\
 & \ldots & & \ddots & & & \ddots & & \\
0 & \ldots & & & b_m & \ldots & & b_p \quad \ldots & b_0
\end{pmatrix}.$$

Llamando $\alpha_i=\phi(a_i)$, $\beta_j=\phi(b_j)$. Sabemos que $\beta_j=0$ para $j=p+1,\ldots,m$. Entonces

$$\begin{pmatrix}
\alpha_n & \dots & \dots & \dots & & & & & & \\
 & \ddots & & & & & & & & \\
0 & \dots & \alpha_n & \dots & & & & & & \\
0 & \dots & \dots & \alpha_n & \dots & & \dots & & & \\
 & \ddots & & & \ddots & & \dots & & & \\
0 & \dots & 0 & \dots & & & \alpha_n & \dots & & \alpha_0 \\
0 & \dots & 0 & \beta_p & \dots & & \dots & & & \\
 & \ddots & & & \ddots & & \ddots & & & \\
0 & \dots & 0 & 0 & \dots & \beta_p & \dots & & & \\
 & \dots & & \ddots & & & \ddots & & & \\
0 & \dots & & & 0 & \dots & & \beta_p & \dots & b_0
\end{pmatrix},$$

es la matriz $\phi(\Psi_0(f,g))$. Si quitamos las j primeras filas y columnas con $j < p$, así como las filas $m+1$ a la $m+j$ y la última columna, se tendrá $\phi(\Psi_0(f,g))$. Esta matriz, de tamaño $m+n-2j$ tiene un primer bloque triangular superior de tamaño $m-p$. Desarrollando el determinante de esta matriz por los elementos de la diagonal de este primer bloque se tiene:

$$\det(\phi(\Psi_0(f,g)) = \phi(sRes_j(f,g)) = \alpha_n^{m-p} \cdot \det(H).$$

Donde H es la submatriz compuesta por las últimas $n+p-2j$ filas y columnas que es precisamente $sRes_j(\phi(f),\phi(g))$. Por lo tanto:

$$\phi(sRes_j(f,g)) = \phi(a_n^{m-p}) sRes_j(\phi(f),\phi(g)),$$

como queríamos ver. □

Lema 2.2.3. *$sRes_j(f,g) = 0$ si y solo si existen $u, v \in \mathbb{K}[x]$ no nulos, $\deg(u) < m-j$, $\deg(v) < n-j$ tales que $\deg(fu+gv) < j$.*

Demostración. $\mathrm{sRes}_j(f,g) = 0$ si y solo si el núcleo de la aplicación Ψ_j es no trivial, es decir, si y solo si existen $u, v \in \mathbb{K}[x]$ no nulos, $\deg(u) < m-j$, $\deg(v) < n-j$ tales que $\Psi_j(u,v) = 0$ si y solo si $\deg(fu+gv) < j$. □

Lema 2.2.4. *Supongamos $\deg(f) = n \leq m = \deg(g)$. Sea $h = \gcd(f,g)$ y d su grado. Son equivalentes:*

- *$j \leq d$.*
- *Existen $u, v \in \mathbb{K}[x]$ no nulos, $\deg(u) \leq m-j$, $\deg(v) \leq n-j$ con $fu+gv = 0$.*

Demostración. Supongamos que $j \leq d$. Sean $u = g/h$ y $v = -f/h$. Entonces se tiene $fu+gv = 0$ con $\deg(u) = m-d \leq m-j$ y $\deg(v) = n-d \leq n-j$.

Supongamos ahora que existen $u, v \in \mathbb{K}[x]$ no nulos, $\deg(u) \leq m-j$, $\deg(v) \leq n-j$ con $fu+gv = 0$. Sea r el grado de u, entonces $\deg(fu) = n+r$ y, como $fu+gv = 0$, $\deg(gv) = n+r$. Por lo tanto, $\deg(v) = \deg(gv) - \deg(g) = n+r-m$. Por otro lado, f divide a $-gv$ y $\deg(\gcd(f,v)) \leq \deg(v) = n+r-m$, luego $d = \deg(\gcd(f,g)) \geq n-(n+r-m) = m-r \geq m-(m-j) = j$. □

Teorema 2.2.5. *En las condiciones anteriores,* $d = \deg(\gcd((f,g))$ *si y solo si*

- *para* $0 \leq j < d$, $sRes_j(f,g) = 0$.
- $sRes_d(f,g) \neq 0$.

Demostración. Por el lema anterior, tomando $j = d$, existen u y v no nulos tales que $\deg(u) \leq m - d$ y $\deg(v) \leq n - d$ con $fu + gv = 0$. Si ahora $j < d$, $\deg(u) < m - jy\deg(v)n - j$ con $fu + gv = 0$ y, luego $(u, v) \in \ker(\Psi_j)$ y su determinante se anula.

Veamos ahora que $\mathrm{sRes}_d(f,g) \neq 0$. Supongamos por reducción al absurdo que $\mathrm{sRes}_d(f,g) = 0$, entonces existen u, v no nulos $\deg(u) < m - d$, $\deg(v) < n - d$ con $\deg(fu + vg) < d$. Como $h = \gcd(f,g)$, $fu + vg$ es múltiplo de h, tiene que ser $fu + vg = 0$. Por lo tanto, $\deg(u) \leq m - d - 1$, $\deg(v) \leq n - d - 1$ con $fu + vg = 0$. Por el lema anterior, esto implica que $d + 1 \leq d$ lo cual es absurdo. Así se tiene que $\mathrm{sRes}_d(f,g) \neq 0$.

Sea ahora $d \geq 0$ tal que para $0 \leq j < d$, $\mathrm{sRes}_j(f,g) = 0$ y $\mathrm{sRes}_d(f,g) \neq 0$. Esto es equivalente a decir que d es el menor para el cual $\mathrm{sRes}_d(f,g)$ no se anula. Por la implicación anterior, esto equivale a que d sea el grado del $\gcd(f,g)$.

□

Corolario 2.2.6. *Sea* $0 \leq j \leq m$ *si* $m < n$ *y* $0 \leq j \leq m - 1$ *si* $m = n$.
$\deg(\gcd(f,g)) \geq j$ *si y solo si* $sRes_0(f,g) = \cdots = sRes_{j-1}(f,g) = 0$

Demostración. Como $\mathrm{sRes}_j(f,g) = 0$ para $0 \leq j \leq \deg(\gcd(f,g))$ y, como $d = \deg(\gcd(f,g))$, $\mathrm{sRes}_d(f,g) \neq 0$, se tiene el resultado. □

Los coeficientes subresultantes permiten entonces conocer el grado del gcd de dos polinomios: será el primer número natural j tal que el j-ésimo coeficiente subresultante principal es no nulo.

En cada paso del algoritmo extendido de Euclides se expresa el resto de dividir dos polinomios como una combinación lineal de los mismos de la forma

$$r = uf + gv,$$

con r el resto de dividir f entre g y u y v los polinomios proporcionados por el algoritmo que cumplen la relación. El siguiente teorema permite describir los grados de u y v a partir del grado del resto correspondiente.

Teorema 2.2.7. *Sean* f, g, $\deg(f) = n \geq m = \deg(g)$. *Sean* $r_0 = f$, $r_1 = g$, …, $r_k = \gcd(f,g)$ *la sucesión de restos del algoritmo de Euclides para el cálculo del* gcd. *Sean*

$$r_i = fu_i + gv_i,$$

los polinomios que aparecen en el algoritmo extendido de Euclides. Sea $2 \leq j \leq k$, *entonces* $\deg(u_j) = m - \deg(r_{j-1})$ *y* $\deg(v_j) = n - \deg(r_{j-1})$.

Demostración. Vamos a probarlo por inducción en j, para $j \leq 2$. En primer lugar, dado que $r_0 = f$ y $r_1 = g$:

$$r_0 = fu_0 + gv_0; \quad f = f \cdot 1 + g \cdot 0,$$

$$r_1 = fu_1 + gv_1; \quad g = f \cdot 0 + g \cdot 1.$$

Sea $2 \leq j$, la división con resto r_{j-2} es $r_{j-2} = r_{j-1}q + r_j$. Entonces, por el propio algoritmo de Euclides extendido se tiene:

$$\begin{array}{rcl} r_j & = & r_{j-2} - r_{j-1}q, \\ u_j & = & u_{j-2} - u_{j-1}q, \\ v_j & = & v_{j-2} - v_{j-1}q. \end{array}$$

En el caso base $j = 2$, $r_2 = f \cdot 1 - g \cdot q$, y por lo tanto $\deg(q) = n - m$. Así

$$\begin{array}{rccccccc} u_2 = 1; & \deg(u_2) & = & 0 & = & m - \deg(g) & = & m - \deg(r_1), \\ v_2 = -q; & \deg(v_2) & = & n - m & = & n - \deg(g) & = & n - \deg(r_1). \end{array}$$

Por lo tanto el enunciado se cumple para $j = 2$.

Tomemos ahora $j > 2$ y supongámoslo cierto hasta $j - 1$, se tiene por un lado las expresiones del par de restos previo:

$$\begin{array}{rcl} r_{j-2} & = & fu_{j-2} + gu_{j-2}, \\ r_{j-1} & = & fu_{j-1} + gu_{j-1}. \end{array}$$

Ahora $r_{j-2} = r_{j-1}q + r_j$ con $\deg(q) = \deg(r_{j-2}) - \deg(r_{j-1}) > 0$, ya que $\deg(r_{j-2}) > \deg(r_{j-1})$ pues $j > 2$. Por tanto, sumando las expresiones anteriores

$$r_j = f(u_{j-2} - qu_{j-1}) + g(v_{j-2} - qv_{j-1})$$

Por hipótesis de inducción, $\deg(u_{j-1}) = m - \deg(r_{j-2})$, $\deg(v_{j-1}) = n - \deg(r_{j-2})$. Ahora $u_j = u_{j-2} - qu_{j-1}$, $v_j = v_{j-2} - qv_{j-1}$. Distinguimos dos casos:

Si $j = 3$, $u_3 = u_1 - qu_2 = -qu_2$ y $v_3 = v_1 - qv_2 = 1 - qv_2$. Así,

$$\deg(u_3) = \deg(qu_2) = \deg(q)\deg(u_2) = \deg(r_1) - \deg(r_2) + m - \deg(r_1) = m - \deg(r_2),$$

$$\deg(qv_2) = \deg(r_1) - \deg(r_2) + n - \deg(r_1) = n - \deg(r_2) > 0 = \deg(v_1),$$

luego

$$\deg(v_3) = \deg(1 - qv_2) = \deg(qv_2) = n - \deg(r_2).$$

Si $j > 3$

$$u_j = u_{j-2} - qu_{j-1},$$

por inducción se tiene por un lado $\deg(u_{j-2}) = m - \deg(r_{j-3})$ y, por el otro, $\deg(qu_{j-1}) = \deg(r_{j-2}) - \deg(r_{j-1}) + m - \deg(r_{j-2}) = m - \deg(r_{j-1})$. Necesitamos ver que al sumar u_{j-2} y $-qu_{j-1}$, el grado de la suma es el grado de $-qu_{j-1}$, esto

es, $m-\deg(r_{j-1})$. Para ello basta con ver que $m-\deg(r_{j-1}) > n-\deg(r_{j-3})$. Pero como $\deg(r_{j-1}) > \deg(r_{j-3})$, $\deg(qu_{j-1}) = m-\deg(r_{j-1}) > m-\deg(r_{j-3}) = \deg(u_{j-2})$ y $\deg(u_j) = m-\deg(r_{j-1})$.

De la misma manera, $\deg(v_{j-2}) = n-\deg(r_{j-3})$ y $\deg(qv_{j-1}) = \deg(r_{j-2}) - \deg(r_{j-1}) + n - \deg(r_{j-2}) = n - \deg(r_{j-1})$. Como $\deg(r_{j-1}) > \deg(r_{j-3})$, se tiene finalmente $\deg(v_j) = n - \deg(r_{j-1})$.

□

La propiedad de los grados de u y v aquí encontrada permite aplicar el Lema 2.2.3 para relacionar u y v con los coeficientes subresultantes. Esto es, establecer una relación entre la sucesión de restos de f y g y los posibles valores de $sRes_j(f,g)$.

Teorema 2.2.8. *Si $j < m$ es el grado de uno de los restos de la sucesión de Euclides, entonces existen polinomios u y v de grado exactamente $m-j$ y $n-j$ respectivamente tales que*

$$\deg(fu+gv) < j.$$

Demostración. Sea a con $\deg(r_a) = j$. Entonces, por el teorema anterior $r_{a+1} = fu_{a+1} + gv_{a+1}$, con $\deg(r_{a+1}) < d(r_a) = j$, $\deg(u_{a+1}) = m-j$, $\deg(v_{a+1}) = n-j$. En el caso $j = \deg(\gcd(f,g))$, $r_{a+1} = 0$ y los polinomios son los cofactores de f y g. □

Teorema 2.2.9. *Sea $\deg(\gcd(f,g)) < j < m$. Si el grado j no aparece en la sucesión de restos de Euclides, existen u, v no nulos, $\deg(u) < m-j$, $\deg(v) < n-j$ tales que $\deg(fu+gv) < j$. En particular, la subresultante se anula.*

Demostración. Sea a con $\deg(r_a) > j > \deg(r_{a+1})$. Entonces

$$r_{a+1} = fu_{a+1} + gv_{a+1},$$

con $\deg(r_{a+1}) < j$, $\deg(u_{a+1}) = m-\deg(r_a) < m-j$, $\deg(v_{a+1}) = n-\deg(r_a) < n-j$. Aplicando ahora el lema 2.2.3, se tiene que $sRes_j(f,g) = 0$. □

Por lo tanto, la sucesión de restos del algoritmo de Euclides aporta información sobre cómo serán las subresultantes. En concreto, si no aparece el grado j en la sucesión, el j-ésimo coeficiente subresultante principal j se anula. Veamos que realmente es una relación bidireccional.

Teorema 2.2.10. *Sea r_i uno de los restos de la sucesión de Euclides, $\deg(r_i) = j$. Sean $r_{i+1} = fu+gv$, con $\deg(u) = m-j$, $\deg(v) = n-j$ la expresión del siguiente resto. Sean t y s dos polinomios no nulos con $\deg(t) \le m-j$ y $\deg(s) \le n-j$ tales que $\deg(ft+gs) < j$. Entonces $\deg(t) = m-j$, $\deg(s) = n-j$ y existe una constante k con $t = ku$ y $s = kv$.*

Demostración. Escribiremos (t,s) para referirnos al vector con t en su primera coordenada y s en la segunda.

Por inducción en la longitud de la sucesión de restos. El caso base es si g divide a f. Entonces $0 = f - gq$. Si $ft+gs = 0$, $\deg(t) \le m-m = 0$ y $t \neq 0$, $\deg(s) \le n-m$,

y por el teorema de unicidad de cociente y resto, $gs = -ft = -qgt \Longrightarrow s = -qt$. Por lo tanto, $(1, -q) = k(t, s)$ con $k = t^{-1}$ y $\deg(t) = m - m = 0$, $\deg(s) = n - m$.

Supongamos ahora que el enunciado es cierto para secuencias de restos de longitud $k-1$ y veamos que se cumple para longitud k. Sean f y g con una secuencia de restos de longitud k, sea $r_2 = f - q_1 g$ el primer resto y sea r_i uno de los restos de la sucesión de Euclides de f y g. Entonces r_i también es un resto de la sucesión de Euclides de g y r_2, que en este caso será de longitud $k-1$. Supongamos ahora que tenemos t y s. Entonces se puede escribir:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}.$$

Ahora, sea a_i, b_i los coeficientes del algoritmo extendido de Euclides, con g y r_2.

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{pmatrix} \begin{pmatrix} g \\ r_2 \end{pmatrix} = \begin{pmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}.$$

Entonces: $tf + sg = t(gq + r_2) + sg = (tq + s)g + tr_2$ donde $\deg(t) \leq m - j$. Veamos que $\deg(tq + s) \leq \deg(r_2) - j$:

Como t y s cumplen las condiciones del teorema, en particular $\deg(tf + sg) = \deg((tq+s)g+tr_2) < j$. Tomando el segundo sumando, $\deg(tr_2) = \deg(t)+\deg(r_2) \leq m + \deg(r_2) - j$. Ahora bien, $\deg((tq + s)g) = \deg(tq + s) + m$, por lo tanto, necesariamente $\deg(tq + s) \leq \deg(r_2) - j$ ya que en caso contrario, $\deg((tq + s)g) > m + \deg(r_2) - j > j$ por ser j el grado de un resto posterior a r_2 en la secuencia de restos del algoritmo. De esta manera, $\deg(tq + s) > \deg(r_2) - j$ contradice que el grado de $tf + sg$ sea estrictamente menor que j.

Por lo tanto,g y r_2 tienen una secuencia de restos del algoritmo de Euclides de longitud $k-1$ y $tq + s$ y t, $\deg(tq + s) \leq \deg(r_2) - j$ y $\deg(t) \leq m - j$, tales que $(tq + s)g + tr_2 < j$. Aplicando la hipóteis de inducción a g y r_2 tenemos que $(tq + s, t) = c(a_{i+1}, b_{i+1})$. Pero entonces:

$$(t, s) = (tq_1 + s, t) \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} =$$

$$= c(a_{i+1}, b_{i+1}) \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} = c(u_{i+1}.v_{i+1}).$$

La última igualdad se prueba observando que

$$\begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{pmatrix} = \prod_{j=1}^{i} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-j+1} \end{pmatrix}.$$

Para ello procedemos por inducción sobre i teniendo en cuenta las igualdades que definen el algoritmo extendido de Euclides:

$$u_i = u_{i-2} - q_{i-1} u_{i-1},$$

$$v_i = v_{i-2} - q_{i-1}v_{i-1}.$$

En el caso $i = 1$, se tiene la igualdad buscada de manera inmediata

$$\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}.$$

En el caso i = 2,

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} =$$

$$= \begin{pmatrix} u_2 & v_2 \\ u_1 - q_2u_2 & v_1 - q_2v_2 \end{pmatrix} = \begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix}.$$

Supuesta cierta la igualdad hasta i, vemos que también se da para i:

$$\prod_{j=1}^{i}\begin{pmatrix} 0 & 1 \\ 1 & -q_{i-j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}\prod_{j=2}^{i}\begin{pmatrix} 0 & 1 \\ 1 & -q_{i-j+1} \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}\begin{pmatrix} u_{i-1} & v_{i-1} \\ u_i & v_i \end{pmatrix} = \begin{pmatrix} u_i & v_i \\ u_{i-1} - q_iu_i & v_{i-1} - q_iv_i \end{pmatrix} = \begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{pmatrix}.$$

Por lo tanto, tenemos

$$\begin{pmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{pmatrix} = \prod_{j=1}^{i-1}\begin{pmatrix} 0 & 1 \\ 1 & -q_{i-j+1} \end{pmatrix},$$

con lo que finalmente,

$$\begin{pmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} = \prod_{j=1}^{i}\begin{pmatrix} 0 & 1 \\ 1 & -q_{i-j+1} \end{pmatrix} = \begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{pmatrix}.$$

□

Corolario 2.2.11. *Si r es uno de los restos de la sucesión de Euclides,* $\deg(r) = j$*, no existen t y s no nulos,* $\deg(t) < m - j$*,* $\deg(s) < n - j$ *tales que* $\deg(tf + sg) < j$*. En particular, la subresultante no se anula.*

Demostración. Supongamos que existen t y s de grados $\deg(t) < m - j$ y $\deg(s) < n - j$ tales que $\deg(tf + sg) < j$. Sean u y v los polinomios que definen el siguiente resto en la sucesión, $\deg(u) = m - j$, $\deg(v) = n - j$, y por el teorema anterior, existirá una constante k tal que $(t, s) = k(u, v)$. Pero $\deg(u) = m - j > \deg(t)$ y $\deg(v) = n - j > \deg(s)$ así que el único k que satisface la igualdad es $k = 0$.
Aplicando ahora el lema 2.2.3, se tiene que $sRes_j(f, g) \neq 0$. □

Teorema 2.2.12. *Sea $f = r_0$, $g = r_1, \ldots, r_k = \gcd(f, g)$ la sucesión de restos de Euclides de f y g $n \leq m$. Entonces un resto de grado i aparece en la sucesión si y solo si $sRes_i(f, g) \neq 0$.*

Demostración. Es consecuencia directa de los resultados 2.2.9 y 2.2.11: Si un resto de grado i aparece en la sucesión, por 2.2.11, $sRes_i(f,g) \neq 0$, mientras que si no aparece $sRes_i(f,g) = 0$ aplicando 2.2.9. □

Con esto sabemos que, dados dos polinomios f y g, si $sRes(f,g) = 0$, al aplicar el algoritmo de Euclides a f y g no aparecerá un resto de grado j. Del mismo modo, si se tiene la sucesión de restos, se conoce qué coeficientes subresultantes principales son nulos y cuáles no. Durante la ejecución del algoritmo modular, se empleará el algoritmo de Euclides para calcular el gcd de dos polinomios en distintos cuerpos y será útil conocer de antemano si la sucesión de grados que aparece en el algoritmo de Euclides es la misma en cada caso. Esta relación nos permitirá caracterizar dicha sucesión.

2.3. Teorema de Praga de Dedekind

En esta sección recordamos las nociones de entero algebraico y anillo de enteros de un cuerpo de números. El motivo de trabajar con el anillo de enteros de $\mathbb{Q}(\alpha)$ en nuestro contexto es porque nos va a permitir acotar cómo son los coeficientes del máximo común divisor de dos polinomios.

Tratar de calcular la clausura entera de $\mathbb{Z}$ puede resultar muy costoso arruinando la eficiencia del método. Dedicamos esta primera parte a dar cotas de cómo deben ser los denominadores que pueden aparecer al calcular el máximo común divisor. Recordemos en primer lugar la noción de entero algebraico y fijemos la notación.

Definición 2.3.1. Dado un número $\delta \in \mathbb{C}$, se dice que δ es un entero algebraico sobre $\mathbb{Z}$ si es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$.

Proposición 2.3.2. *El conjunto de los enteros algebraicos sobre $\mathbb{Z}$ forma un subanillo de $\mathbb{C}$.*

Definición 2.3.3. Denotaremos por $\mathfrak{o}$ al anillo de los enteros algebraicos sobre $\mathbb{Z}$.

Sea $K \subseteq \mathbb{C}$ un cuerpo que contiene a $\mathbb{Z}$, denotaremos por $\mathfrak{o}_K = \mathfrak{o} \cap K$ los enteros algebraicos sobre $\mathbb{Z}$ en K.

Proposición 2.3.4. *Los únicos enteros algebraicos sobre $\mathbb{Z}$ racionales son los números enteros. Es decir, $\mathfrak{o}_{\mathbb{Q}} = \mathbb{Z}$.*

Los siguientes resultados nos permitirán demostrar la versión del lema de Gauss para anillos de enteros algebraicos conocida como el Teorema de Praga de Dedekind que aparece en el libro de Pollar [9].

Lema 2.3.5. *Sea $f = a_0 + a_1 x + \ldots + a_n x^n$, $n \geq 1$ un polinomio cuyos coeficientes son enteros algebraicos. Sea p una raíz de f. Entonces los coeficientes de $\frac{f}{x-p}$ son enteros algebraicos.*

Demostración. Por inducción en el grado del polinomio.

Si $n = 1$, $f = a_0 + a_1 x$, $p = \frac{-a_0}{a_1}$, $\frac{f}{x+(a_0/a_1)} = a_1 \frac{a_0+a_1 x}{a_0+a_1 x} = a_1$ es un entero algebraico.

Supongamos ahora que el enunciado es cierto para polinomios de grado $n-1$ y probémoslo para polinomios de grado n.

Primeramente, como $f(a_n x/a_n) = f(p) = 0$, tenemos que $a_n p$ es raíz de:

$$\sum_{i=0}^{n} a_i \left(\frac{x}{a_n}\right)^i,$$

si multiplicamos por a_n^{n-1} tenemos que $a_n p$ es raíz de:

$$x^n + \sum_{i=0}^{n-1} a_i a_n^{n-1-i} x^i,$$

y $a_n p$ es raíz de un polinomio mónico con coeficientes enteros algebraicos, tenemos que $a_n p$ es, a su vez, un entero algebraico.

Sea ahora

$$g = f - a_n x^{n-1}(x-p).$$

Tenemos que g es un polinomio de grado $n-1$ con coeficientes enteros algebraicos y p es una raíz de g ya que ambos sumandos se aunlan en $x = p$. Por hipótesis de inducción, los coeficientes de $g/(x-p)$ son enteros algebraicos. Pero

$$\frac{g}{x-p} = \frac{f - a_n x^{n-1}(x-p)}{x-p} = \frac{f}{x-p} - a_n x^{n-1},$$

luego

$$\frac{f}{x-p} = \frac{g}{x-p} + a_n x^{n-1},$$

tiene también coeficientes enteros algebraicos. □

Lema 2.3.6. *Sea $f = a_0 + a_1 x + \ldots + a_n x^n$, $n \geq 1$ un polinomio cuyos coeficientes son enteros algebraicos. Escribamos*

$$f = a_n(x - p_1) \cdots (x - p_n),$$

la factorización de f. Entonces para cada subconjunto $\{i_1, \ldots, i_j\} \subseteq \{1, \ldots, n\}$ tenemos que

$$a_n p_{i_1} \cdots p_{i_j},$$

es un entero algebraico.

Demostración. Sin pérdida de generalidad, reordenando las raíces, basta probar que $a_n p_1 \cdots p_j$ es un entero algebraico.

Aplicando el lema anterior, los coeficientes de $\frac{f}{x-p_n}$ son enteros algebraicos y $p_1, p_2, \dots p_{n-1}$ son sus raíces. Aplicando de nuevo el lema, $\frac{f}{(x-p_n)(x-p_{n-1})}$ es un polinomio cuyos coeficientes son enteros algebraicos y cuyas raíces son $p_1, p_2, \dots p_{n-2}$. Aplicando el lema $n-j$ veces se llega a que los coeficientes de:

$$\frac{f}{(x-p_{j+1})\cdots(x-p_n)} = a_n(x-p_1)\cdots(x-p_j),$$

son enteros algebraicos. En particular, su término independiente

$$(-1)^j a_n p_1 \cdots p_j,$$

es un entero algebraico. □

Teorema 2.3.7. *[Teorema de Praga de Dedekind] Sean g y h con coeficientes en un cuerpo $K \subseteq \mathbb{C}$, $g = \sum_{i=0}^{n} g_i x^i$, $h = \sum_{i=0}^{m} h_i x^i$. Sea $\mathfrak{o}_K$ el anillo de enteros de K. Supongamos que $\delta \in \mathfrak{o}_K$, que $f = gh \in \mathfrak{o}_K[x]$ y $\frac{f}{\delta} \in \mathfrak{o}_K[x]$. Entonces, para cada par de índices i, j tenemos que $\frac{g_i h_j}{\delta} \in \mathfrak{o}_K$. (Si δ divide a cada coeficiente de f en $\mathfrak{o}_K$, entonces δ divide a cada producto cruzado $g_i h_j$ en $\mathfrak{o}_K$).*

Demostración. Sea E un cuerpo de escisión de f sobre K y sea $\mathfrak{o}_E$ el anillo de enteros de E. En $E[x]$ podemos escribir

$$g = g_n(x-p_1)\cdots(x-p_n), \quad h = h_m(x-q_1)\cdots(x-q_m), \quad p_t, q_s \in E,$$

$$f = g_n h_m (x-p_1)\cdots(x-p_n)(x-q_1)\cdots(x-q_m) \in \mathfrak{o}_E[x],$$

por hipótesis

$$\frac{f}{\delta} = \frac{g_n h_m}{\delta}(x-p_1)\cdots(x-p_n)(x-q_1)\cdots(x-q_m) \in \mathfrak{o}_E[x],$$

por el lema anterior aplicado a este polinomio, tenemos que todos los posibles productos:

$$\frac{g_n h_m}{\delta} p_{t_1} \cdots p_{t_k} q_{s_1} \cdots q_{s_l} \in \mathfrak{o}_E.$$

Ahora

$$\frac{g_i h_j}{\delta} = \frac{1}{\delta}\left((-1)^{n-i} g_n \sum_{|I|=n-i} \prod_{t\in I} p_t\right)\left((-1)^{m-j} h_m \sum_{|J|=m-j} \prod_{s\in J} q_s\right) =$$

$$= (-1)^{n+m-i-j} \sum_{\substack{|I|=n-i \\ |J|=m-j}} \left(\frac{g_n h_m}{\delta} \prod_{t\in I} p_t \prod_{s\in J} q_s\right).$$

Como cada sumando de esta última expresión pertenece a $\mathfrak{o}_E$, tenemos que $\frac{g_i h_j}{\delta} \in \mathfrak{o}_E$.

Ahora $\frac{g_i h_j}{\delta} \in K$ y es un entero algebraico, tenemos que $\frac{g_i h_j}{\delta} \in \mathfrak{o}_K$ y, por tanto, $g_i h_j \in \mathfrak{o}_K$ y δ divide a $g_i h_j$ en $\mathfrak{o}_K$.

□

Capítulo 3

Escogiendo los primos correctos

3.1. Una cota para el máximo común divisor

Sea $\alpha \in \mathbb{C}$ un entero algebraico con polinomio mínimo $r(y)$ perteneciente a $\mathbb{Z}[y]$. A partir de $r(y)$ se tiene el siguiente dominio

$$R = \mathbb{Z}[\alpha] \simeq \frac{\mathbb{Z}[y]}{(r(y))}.$$

Sea $\mathbb{Q}(\alpha)$ su cuerpo de fracciones.

Dado $f \in R[x]$. Sea δ su coeficiente principal, entonces $\delta^{-1}f \in \mathbb{Q}(\alpha)[x]$ es el polinomio mónico asociado a f. Si escribimos sus coeficientes en la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ tendremos

$$f = \sum_{i=0}^{s} \left(\sum_{j=0}^{n-1} \frac{f_{ij}}{a_{ij}} \right) x^i.$$

Tomando $a = \operatorname{lcm}(a_{ij}) \in \mathbb{Z}$, $a\delta^{-1}f \in \mathbb{Z}[\alpha][x]$ y su coeficiente principal es el número entero a.

Podemos suponer por tanto, sin pérdida de generalidad, que vamos a calcular el máximo común divisor de dos f y g con coeficientes en $R[x]$ y coeficientes directores a y $b \in \mathbb{Z}$.

Si $z = \gcd(f, g)$ mónico en $\mathbb{Q}(\alpha)[x]$ buscamos una cota de un entero c que dependa de a, b y α y tal que $cz \in R[x]$. La dependencia de c respecto de α viene dada por el discriminante.

Definición 3.1.1. Dado r un polinomio sobre un dominio de integridad. Sean n su grado y d su coeficiente director. Se define el discriminante de r a partir de la siguiente expresión:

$$\operatorname{disc}(r) = (-1)^{n(n-1)/2} Res(r, r')/d,$$

donde r' es la derivada de r.

Sea Δ el discriminante de r, nuestro próximo objetivo es demostrar que basta tomar como cota $c = \Delta \cdot \gcd(a, b)$.

Definición 3.1.2. Dado un dominio X, sea Y su cuerpo de fracciones y $x \in X$ un elemento cualquiera no nulo. Escribiremos $(1/x)X$ para referirnos al siguiente conjunto:

$$\frac{1}{x}X = (1/x)X = \{y \in Y : x \cdot y \in X\}.$$

Este conjunto es un subgrupo de Y con la operación suma heredada, pero no es un subanillo de Y ya que no es cerrado para el producto. Por otro lado, contiene a X y es un X-módulo.

Definición 3.1.3. Sea α raíz del polinomio mínimo r de grado n. Sean $\alpha = \alpha_1$, α_2, ..., $\alpha_n \in \mathbb{C}$ sus conjugados.Definimos la matriz de Vandermonde de α como la matriz:

$$V(\alpha) = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix}.$$

La demostración de la siguiente proposición puede encontrarse en [3]. La igualdad establecida entre el determinante de la matriz de Vandermonde de un elemento entero algebraico y el discriminante de su polinomio mínimo permite interpretar el discriminante, que es un número racional, como el cuadrado de un elemento en un cuerpo de números

Proposición 3.1.4. *Se tiene la relación* $discr(r) = \Delta = \det(V(\alpha))^2$.

Demostración. Sean $\alpha = \alpha_1, \dots, \alpha_n$ las raíces de r en su cuerpo de escisión. Como r es el polinomio mínimo de α, todas las ráices son distintas. Sea ahora la factorización de r,

$$r = \prod_{i=1}^{n}(x - \alpha_i).$$

La derivada de r, r', se puede escribir en términos de esta factorización sin más que aplicar la derivada del producto:

$$r' = \sum_{i=1}^{n}\prod_{j\neq i}(x - \alpha_j).$$

Por otro lado, por el Lema 2.1.6, $\Delta = (-1)^{n(n-1)/2}\prod_{i=1}^{n} r'(\alpha_i)$. Desarrollando esta igualdad a partir de la expresión que define r' se obtiene:

$$\Delta = (-1)^{n(n-1)/2}\prod_{i=1}^{n}\left(\sum_{j=1}^{n}\prod_{k\neq j}(\alpha_i - \alpha_k)\right).$$

Dado un i fijo, $1 \leq i \leq n$, se tiene que $\sum_{j=1}^{n} \prod_{k \neq j}(\alpha_i - \alpha_j) = \prod_{k \neq i}(\alpha_i - \alpha_k)$ ya que el resto de sumandos son nulos. Así,

$$\Delta = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \left(\prod_{k \neq i} (\alpha_i - \alpha_k) \right) = (-1)^{n(n-1)} \prod_{i<k} (\alpha_i - \alpha_k)^2 = \prod_{i<k} (\alpha_i - \alpha_k)^2.$$

Bastaría ahora con ver que, salvo signo,

$$\det(V(\alpha)) = \prod_{1 \leq i < k \leq n} (\alpha_i - \alpha_k).$$

Procedamos por inducción en el tamaño de la matriz n. En el caso base, $n = 2$, $V(\alpha)$ es una matriz 2x2 y su determinante es $\det(V(\alpha)) = \alpha_2 - \alpha_1$, satisfaciendo la igualdad que deseamos probar.

Supongamos ahora como hipótesis de inducción que la igualdad se satisface hasta $n-1$ y probemos que, entonces, también se cumple para n. Es posible hacer ceros en la primera fila de $V(\alpha)$ sumando a la columna i, α_1 veces la columna $i-1$, con i descendiendo desde n hasta 2, sin que cambie el determinante. De esta forma:

$$\det(V(\alpha)) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & \alpha_2 - \alpha_1 & \alpha_2(\alpha_2 - \alpha_1) & \dots & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n - \alpha_1 & \alpha_n(\alpha_n - \alpha_1) & \dots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix} =$$

$$= \begin{vmatrix} \alpha_2 - \alpha_1 & \alpha_2(\alpha_2 - \alpha_1) & \dots & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & & \vdots \\ \alpha_n - \alpha_1 & \alpha_n(\alpha_n - \alpha_1) & \dots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix}.$$

Dado j, $2 \leq j \leq n$, todas las entradas de la fila j de la última matriz tienen como factor común $\alpha_j - \alpha_1$. Por lo tanto,

$$\det(V(\alpha)) = \left(\prod_{2 \leq j \leq n} (\alpha_j - \alpha_1) \right) \begin{vmatrix} 1 & \alpha_2 & \dots & \alpha_2^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-2} \end{vmatrix}.$$

Por hipótesis de inducción, salvo signo, se tiene que

$$\begin{vmatrix} 1 & \alpha_2 & \dots & \alpha_2^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-2} \end{vmatrix} = \prod_{2 \leq j < k \leq n} (\alpha_j - \alpha_k)$$

y, por lo tanto,

$$\det(V(\alpha)) = \left(\prod_{2\leq j\leq n}(\alpha_j - \alpha_1)\right)\cdot\left(\prod_{2\leq j<k\leq n}(\alpha_j - \alpha_k)\right) = \prod_{1\leq j<k\leq n}(\alpha_j - \alpha_k),$$

□

En el siguiente teorema construiremos un subgrupo de $\mathbb{Q}(\alpha)$ a partir de R que contenga a todos los elementos enteros.

Teorema 3.1.5. *Sea $\theta \in \mathfrak{o}_K$ donde $K = \mathbb{Q}(\alpha)$, entonces $\theta \in (1/\Delta)R$.*

Demostración. Como $\theta \in K$ y $\alpha \in K$, $\theta\alpha^k \in K$ y podemos escribirlo en función de los elementos de la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ de K:

$$\theta\alpha^k = a_1 + a_2\alpha + \ldots + a_n\alpha^{n-1}, \qquad a_i \in \mathbb{Q}.$$

Las ecuaciones conjugadas forman un sistema lineal $\mathbf{b} = \mathbf{V}(\alpha)\mathbf{a}$ donde

$$\mathbf{b} = \left(\theta^{(1)}\alpha^{(1)^k}, \ldots, \theta^{(n)}\alpha^{(n)^k}\right)^T \text{ y } \mathbf{a} = (a_1, \ldots, a_n)^T.$$

Aplicando la regla de Cramer se tiene que $a_j = \delta_j/\det(\mathbf{V}(\alpha))$ donde δ_j es el determinante de la matriz que aparece al sustituir en $\mathbf{V}(\alpha)$ la columna j por $\mathbf{b}$. Como $\Delta = \det(\mathbf{V}(\alpha))^2$,

$$a_j = \frac{\delta_j}{\det(\mathbf{V}(\alpha))} = \frac{\det(\mathbf{V}(\alpha))\delta_j}{\Delta}.$$

Δa_j es racional ya que ambos miembros del producto lo son. Por lo tanto, si se prueba que $\Delta a_j \in \mathfrak{o}$, necesariamente $\Delta a_j \in \mathbb{Z}$.

Como cada entrada de la matriz de Vandermonde es un entero algebraico y los enteros algebraicos forman un anillo, $\det(V) = \sqrt{\Delta}$ es un entero algebraico.

Desarrollando los determinantes δ_j por adjuntos se puede escribir

$$\delta_j = \pm\theta^{(1)}\alpha^{(1)^k}\xi_{1,j} \pm \ldots \pm \theta^{(n)}\alpha^{(n)^k}\xi_{n,j},$$

donde $\xi_{i,j}$ es el determinante de la submatriz obtenida al eliminar la fila i y la columna j de $\mathbf{V}(\alpha)$. Como $\theta \in \mathfrak{o}$, $\theta^{(i)} \in \mathfrak{o}$ $\forall i$, falta entonces probar que cada $\alpha^{(i)^k}\xi_{i,j}$ es un entero algebraico. Por la definición de determinante $\xi_{i,j}$ es suma de productos de elementos de la forma $\alpha^{(t)}$ con t entre 1 y n. Por lo tanto, $\alpha^{(i)^k}\xi_{i,j} \in \mathfrak{o}$ por ser suma de productos entre enteros algebraicos. Esto implica que $\Delta a_j \in \mathbb{Z}$ y, por lo tanto, $\theta\alpha^k \in (1/\Delta)R$ □

Corolario 3.1.6. *$\mathfrak{o}_K$ es un grupo libre de rango $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.*

Demostración. $(1/\Delta)\mathbb{Z}[\alpha]$ es un grupo abeliano libre de rango n con base

$$\{1/\Delta, \alpha/\Delta, \ldots, \alpha^{n-1}/\Delta\}.$$

Como $\mathfrak{o}_K \subseteq (1/\Delta)\mathbb{Z}[\alpha]$, tenemos que es un grupo libre de rango a lo sumo n. Como $1, \alpha, \ldots, \alpha^{n-1}$ son independientes, el rango es como mínimo n. Entonces tiene que ser n. □

Lema 3.1.7. *Sea $f \in (1/a)\mathfrak{o}_K[x]$ mónico con $a \in \mathbb{Z}$ y supongamos que $f(x) = g(x)h(x)$ con $g(x)$ y $h(x)$ mónicos en $K[x]$. Entonces $g(x)$ y $h(x)$ pertenecen a $(1/a)\mathfrak{o}_K[x]$.*

Demostración. Como $f \in (1/a)\mathfrak{o}_K[x]$, por definición $af(x) \in \mathfrak{o}_K[x]$ y como $a \in \mathbb{Z}$, $a^2 \in \mathfrak{o}_K[x]$. Se tiene entonces que a es tal que $a^2 f(x) = ag(x)ah(x)$ y $a^2 f(x)/a = af(x) \in \mathfrak{o}_K[x]$. Por el Teorema de Praga de Dedekind, se cumple que para cada par de índices i, j $a^2 g_i h_j / a = a g_i h_j \in \mathfrak{o}_K[x]$. Pero, como $g(x)$ es mónico, tomando como $g_i = 1$ el coeficiente principal de g, se tiene que, para cada j, $ah_j \in \mathfrak{o}_k$. Por simetría, se prueba que, para cada i, $ag_i \in \mathfrak{o}_k$. De esta manera, $g(x)$ y $h(x)$ pertenecen a $(1/a)\mathfrak{o}_K[x]$, como se quería demostrar. □

Finalmente, con el siguiente teorema encontramos la cota buscada para los denominadores de los coeficientes del máximo común divisor mónico de f y g.

Teorema 3.1.8. *Sean $f_{1/a} \in \frac{1}{a}R[x]$ y $g_{1/b} \in \frac{1}{b}R[x]$ mónicos con a y $b \in \mathbb{Z}$. Sea $\hat{z} = \gcd(f_{1/a}, g_{1/b})$ mónico sobre $K = \mathbb{Q}(\alpha)$. Entonces $\hat{z}(x) \in \frac{1}{c}R[x]$ con $c = \Delta \cdot \gcd(a, b)$. Además, los cofactores $f^*_{1/a} = f_{1/a}/\hat{z}$ y $g^*_{1/b} = g_{1/b}/\hat{h}$ pertenecen a $\frac{1}{a\Delta}R[x]$ y $\frac{1}{b\Delta}R[x]$ respectivamente.*

Demostración. Como $f_{1/a} = f^*_{1/a}\hat{z}$ y $g_{1/b} = g^*_{1/b}\hat{z}$, por el lema anterior $\hat{z} \in (1/a)\mathfrak{o}_K$ y $\hat{z} \in (1/b)\mathfrak{o}_K$, por lo tanto $a\hat{z} \in \mathfrak{o}_K[x]$ y $b\hat{z} \in \mathfrak{o}_K[x]$. Como $\mathfrak{o}_K \subseteq \frac{1}{\Delta}R$, $\Delta a\hat{z} \in R[x]$ y $\Delta b\hat{z} \in R[x]$. Sean u y v los coeficientes de Bezout de a y de b, $au + bv = \gcd(a, b)$. Multiplicando esta identidad por $\Delta\hat{z}$ se tiene que

$$\Delta \gcd(a, b)\hat{z}u + \Delta \gcd(a, b)\hat{z}v = \Delta \gcd(a, b)\hat{z}.$$

Como los dos sumandos pertenecen a $R[x]$,

$$\Delta \gcd(a, b)\hat{z} \in R[x].$$

La otra parte del enunciado se demuestra aplicando de nuevo el lema anterior que afirma que $f^*_{1/a} \in \frac{1}{a}\mathfrak{o}_K[x]$ y $g^*_{1/b} \in \frac{1}{b}\mathfrak{o}_K[x]$. Finalmente, como $\mathfrak{o}_K \subseteq \frac{1}{\Delta}R$,

$$f^*_{1/a} \in \frac{1}{a\Delta}R[x] \text{ y } g^*_{1/b} \in \frac{1}{b\Delta}R[x].$$

□

En el caso general, dados f y $g \in R[x]$ podemos suponer que sus coeficientes directores son enteros racionales a y b. Se tiene que $a^{-1} \cdot f \in (1/a)R[x]$ y, del mismo modo, $b^{-1} \cdot g \in (1/b)R[x]$. Por el último teorema, el máximo común divisor mónico $\gcd(a^{-1}f, b^{-1}g) \in (1/c)R[x]$. Así, $cz \in R[x]$ como queríamos ver.

El polinomio $h = cz$ es el asociado privilegiado de z que calcularemos con nuestro algoritmo.

Ejemplo 3.1.9. Tomemos el polinómio mónico $r = y^3 - 2$ y sea α una de sus raíces. Sean f y g los polinomios sobre $R = \mathbb{Z}[\alpha]$ siguientes:

$$\begin{aligned} f =& 10x^7 + (30\alpha^2 - 10\alpha + 2)x^5 + (\alpha^2 + 10\alpha + 10)x^4 + (-2\alpha - 50)x^3 \\ &+ (-10\alpha^2 - 10\alpha - 2)x^2 + (30\alpha^2 + 2)x + \alpha^2 + 10\alpha + 10, \end{aligned}$$

$$\begin{aligned} g =& 130x^6 - 65\alpha x^5 + (390\alpha^2 + 65\alpha + 26)x^4 + (8\alpha^2 + 117\alpha - 260)x^3 \\ &+ (-65\alpha^2 - 52\alpha + 377)x^2 + (64\alpha^2 + 35\alpha + 13)x - 5\alpha^2 - \alpha - 10. \end{aligned}$$

Se tiene entonces que los coeficientes directores de f y g son 10 y 130 respectivamente, de manera que su máximo común divisor es 10. Por otro lado, $\Delta = \text{discr}(r) = 108$. Entonces $c = 1080$. El máximo común divisor mónico de f y g sobre el cuerpo de fracciones es:

$$\gcd(f, g) = x^3 + (3\alpha^2 + 1/5)x + (1/10)\alpha^2 + \alpha + 1.$$

Por lo tanto, claramente $\gcd(f, g) \in (1/c)R[t]$ y $h = c \cdot \gcd(f, g) \in R[t]$.

Ejemplo 3.1.10. En el ejemplo anterior c ha cumplido que $h = c \cdot \gcd(f, g) \in R[x]$, pero realmente habría bastado con tomar $c = \gcd(a, b)$. Veamos que existen ejemplos en los que no es suficiente con tomar $c = \gcd(a, b)$, necesitando Δ. Para ello, es necesario que R no sea DFU ya que, en estos dominios, el contenido del máximo común divisor de dos polinomios es el máximo común divisor de sus contenidos.

Tomemos $\alpha = \sqrt{7} + \sqrt{10}$, su polinomio mínimo es $r = x^4 - 34x^2 + 9$, entonces $R = \mathbb{Z}[\sqrt{7}, \sqrt{10}] = \mathbb{Z}[\sqrt{7} + \sqrt{10}]$ y $\Delta = 180633600$. Tomando los polinomios

$$f = x^2 - 806a^2 + 215 \quad ,$$

$$g = x^2 - 6x + 5a^3 - 806a^2 + a + 215,$$

se tiene que su máximo común divisor es

$$\gcd(f, g) = x - \frac{5}{6}a^3 - \frac{1}{6}a.$$

Claramente $\gcd(a, b) = 1$ porque f y g son mónicos. Como $\gcd(f, g) \notin R[x]$, no se cumple que $\gcd(a, b)\gcd(f, g) \in R[x]$, pero sí que $c\gcd(f, g) = \Delta\gcd(f, g) \in R[x]$.

3.2. Los anillos finitos $R/(p)$

En las condiciones anteriores, sea p un número primo. Vamos a estudiar el anillo cociente:

$$\bar{R} = \frac{R}{(p)} = \frac{\mathbb{Z}[\alpha]}{(p)} \simeq \frac{(\mathbb{Z}/(p))[y]}{(\bar{r})},$$

con $\bar{r} = r \mod p$. Si bien r es irreducible sobre $\mathbb{Z}$ por hipótesis, se puede dar el caso de que $\bar{r}$ no lo sea sobre $\mathbb{Z}/(p)$. En este caso, $\bar{r}$ factorizará en irreducibles como $\bar{r}_1^{i_1} \cdot \bar{r}_2^{i_2} \cdots \bar{r}_t^{i_t}$. Como los r_j son irreducibles, si $j \neq q$, $\gcd(\bar{r}_j^{i_j}, \bar{r}_q^{i_q}) = 1$ y los factores son comaximales. Aplicando el Teorema Chino de los Restos obtenemos:

$$\bar{R} = \frac{(\mathbb{Z}/(p))[y]}{(\bar{r})} = \frac{(\mathbb{Z}/(p))[y]}{(\bar{r}_1^{i_1} \cdots \bar{r}_t^{i_t})} \simeq \frac{(\mathbb{Z}/(p))[y]}{(\bar{r}_1^{i_1})} \times \ldots \times \frac{(\mathbb{Z}/(p))[y]}{(\bar{r}_t^{i_t})}.$$

Como $\bar{R}$ no es dominio de integridad, la noción de máximo común divisor de dos polinomios no está definida sobre $\bar{R}$. Sin embargo, si $\bar{R}$ fuese un producto de cuerpos, en cada uno de ellos sí se podría calcular el máximo común divisor de dos polinomios. No obstante, el anillo finito $\bar{R}$ así construido es producto de anillos que pueden no ser dominios de integridad: Si la multiplicidad de un factor $\bar{r}_j$ es $i_j > 1$, entonces $\bar{r}_j$ es nilpotente en su correspondiente factor y $\bar{R}$ no es producto de cuerpos. Tenemos así que $\bar{R}$ será producto de cuerpos cuando la multiplicidad de cada factor de $\bar{r}$ sea 1 ($\bar{r}$ es libre de cuadrados). Denotaremos en este caso por ψ el isomorfismo dado por el Teorema Chino de los Restos:

$$\begin{aligned} \psi : \bar{R} &\longrightarrow \bar{R}_1 \times \ldots \times \bar{R}_t \\ k + \bar{r} &\longrightarrow (k + \bar{r}_1, \ldots, k + \bar{r}_t). \end{aligned}$$

Donde cada R_i representa el cuerpo dado por el cociente $(\mathbb{Z}/(p))[y]/(\bar{r}_i)$ para $1 \leq i \leq t$. Este isomorfismo se extiende de manera natural a un isomorfismo entre los correspondientes anillos de polinomios, que seguiremos denotando por ψ:

$$\begin{aligned} \psi : \bar{R}[x] &\longrightarrow \bar{R}_1[x] \times \ldots \times \bar{R}_t[x] \\ f + \bar{r} &\longrightarrow (f + \bar{r}_1, \ldots, f + \bar{r}_t). \end{aligned}$$

Sean ψ_i $i \in \{1, \ldots t\}$ los homomorfismos de $\bar{R}[x]$ a $\bar{R}_i[x]$ que componen ψ. Al ser los $\bar{R}_i$ cuerpos, $\psi_i(\bar{f})$ y $\psi_i(\bar{g})$ tendrán un máximo común divisor en $\bar{R}_i[x]$. De esta forma, definimos $h^*(x)$ como el único polinomio de $\bar{R}[x]$ que satisface $\psi_i(h^*) = \gcd(\psi_i(\bar{f}), \psi_i(\bar{g}))$ para todo $i \in \{1, \ldots t\}$.

Con el siguiente teorema se establece la condición que debe cumplir p para que $\bar{R}$ sea producto de cuerpos y con ello se pueda definir h^*.

Teorema 3.2.1. *Sea $r \in \mathbb{Z}$ no nulo, mónico e irreducible, sea Δ el discriminante de r y sea $p \in \mathbb{Z}$ un número primo. Entonces, si $p \nmid \Delta$, $\bar{r}$ es libre de cuadrados.*

Demostración. Un polinomio es libre de cuadrados cuando su discriminante no se anula. Como r es mónico e irreducible sobre $\mathbb{Z}$, $\Delta = Res(r, r') \neq 0$. Al realizar la reducción mód p de r, r no baja de grado al ser mónico y por lo tanto $\bar{\Delta} = \overline{Res(r, r')} = Res(\bar{r}, \bar{r}') = \text{Disc}(\bar{r})$. Por lo tanto, si $p \not| \Delta$, $\text{Disc}(\bar{r}) = \bar{\Delta} \neq 0$, y $\bar{r}$ es libre de cuadrados. □

En consecuencia, debemos descartar los primos p que dividan a Δ para poder definir el polinomio h^* sobre el anillo finito $\bar{R}$.

Ejemplo 3.2.2. Sea r como en el Ejemplo 3.1.9. Tomemos $p = 3$. Como $\Delta = 108$, p divide a Δ. Sea $\bar{r}$ la reducción módulo p de r, $\bar{r}$ deja de ser irreducible y factoriza como $\bar{r} = (1+x)^3$. Entonces, $\bar{R}$ no es producto de cuerpos. Por lo tanto, no es posible calcular un h^* para $\bar{f}$ y $\bar{g}$.

Ejemplo 3.2.3. Sean f, g y r como en el Ejemplo 3.1.9. Tomemos ahora $p = 11$. p no divide a 108 lo que asegura que $\bar{r} = r \mod p$ es libre de cuadrados sobre $\mathbb{Z}/(p)$. Efectivamente, su factorización en irreducibles es $\bar{r} = (y+4)(y^2+7y+5)$. Por el teorema Chino de los Restos,

$$\bar{R} = \frac{\mathbb{Z}[y]/(p)}{(\bar{r})} \simeq \frac{\mathbb{Z}[y]/(p)}{(y+4)} \times \frac{\mathbb{Z}[y]/(p)}{(y^2+7y+5)}.$$

$\bar{R}$ es por lo tanto isomorfo a un producto de cuerpos.

Denotemos $R_1 = (\mathbb{Z}[y]/(p))/(y+4)$ y $R_2 = (\mathbb{Z}[y]/(p))/(y^2+7y+5)$. Como son cuerpos, $\bar{R}_1[x]$ y $\bar{R}_2[x]$ son dominios euclídeos y se puede calcular el máximo común divisor de las imágenes de f y g aplicando el algoritmo de Euclides en cada uno de ellos.

Comencemos por calcular el máximo común divisor sobre $\bar{R}_1$. Se tiene que $\bar{R}_1$ es el cuerpo finito $\mathbb{Z}/(11)$. Las imágenes de f y g en $\bar{R}_1[x]$, f_1 y g_1, se pueden calcular reduciendo los polinomios módulo 11 y sustituyendo las variables indeterminadas y por -4, raíz de $(y+4)$. Se tiene entonces

$$f_1 = 10x^7 + 5x^5 + 8x^4 + 2x^3 + 10x^2 + 9x + 8,$$

$$g_1 = 9x^6 + 7x^5 + 5x^3 + 7x^2 + 6x + 2.$$

Ahora se puede calcular fácilmente el máximo común divisor de f_1 y g_1 sin más que aplicar el algoritmo de Euclides sabiendo que no va a surgir el inconveniente del crecimiento de los coeficientes al estar trabajando sobre un cuerpo finito. Se obtiene:

$$h_1 = \gcd(f_1, g_1) = y^4 + 2y^3 + 2y^2 + 7y + 6.$$

R_2 será isomorfo a $\mathbb{Z}/(p)[\mu]$ con μ una de las dos raíces de y^2+7y+5 en su cuerpo de escisión sobre $\mathbb{Z}/(p)$. Las imágenes de f y g son

$$f_2 = 10x^7 + 6x^5 + (10\mu+2)x^4 + (8\mu+7)x^3 + (2\mu+10)x^2 + (4\mu+7)x + 10\mu + 2,$$

$$g_2 = 9x^6 + (7\mu + 10)x^5 + (\mu + 4)x^4 + (9\mu + 2)x^3 + (5\mu + 2)x^2 + (2\mu + 7)x + 7\mu + 3.$$

Su gcd es:

$$h_2 = x^3 + (7\mu + 4)x + \mu + 9.$$

Para calcular ahora h^* es necesario resolver el sistema de congruencias

$$\begin{aligned} h^*(y)(x) \equiv & h_1(y)(x) \mod (y+4), \\ h^*(y)(x) \equiv & h_2(y)(x) \mod (y^2+7y+5). \end{aligned}$$

El resultado es:

$$h^* = (3y^2+10y+4)x^4+(3y^2+10y+5)x^3+(6y^2+9y+8)x^2+(7y^2+6y+7)x+8y^2+9y+2.$$

Se comprueba fácilmente, sin más que sustituir y por -4 o por μ, que se obtienen h_1 y h_2 respectivamente y el resultado es correcto.

El objetivo de calcular h^* es poder recuperar posteriormente h. Está claro que, en general, como se ha realizado la reducción módulo p, no es posible hacerlo directamente a partir de un único h^*. No obstante, si se realiza el cálculo varias veces con distintos primos, obteniendo así varios polinomios h^*, se podría utilizar de nuevo el Teorema Chino de los Restos para tratar de recuperar h. Sean p_i $1 \leq i \leq m$ cada uno de los primos empleados y h_i^* los correspondientes $\gcd(f \mod p_i, g \mod p_i)$ calculados sobre los anillos finitos $R/(p_i)$ $1 \leq i \leq m$. Entonces debemos resolver el siguiente sistema de congruencias dado por el Teorema Chino:

$$\begin{aligned} h' \equiv & c h_1^*(x) \bmod p_1 \\ & \vdots \\ h' \equiv & c h_m^*(x) \bmod p_m. \end{aligned}$$

donde h' es un polinomio con coeficientes en $\mathbb{Z}[\alpha]/(\omega)$ siendo $\omega = \prod p_i$. Podemos tomar un representante de h' que sea un polinomio de dos variables en $(\mathbb{Z}/(\omega))[y, x]$ sustituyendo α por y.

Este sistema de congruencias es realmente un sistema de congruencias enteras, una por cada coeficiente de los polinomios $h_i^*(y, x)$. Por este motivo, para poder resolver efectivamente este sistema y que el h' sea el buscado $h \mod \omega$, es necesario que ninguno de los h_i^* tenga grado en x mayor a h ya que de ser así, el grado de h' también lo será y no podrá ser por tanto nunca h. Tampoco podremos calcular h correctamente si todos los h_i^* tienen grado menor pues en ese caso $\deg(h') < \deg(h)$. La idea de resolver este sistema es que si ω es lo suficientemente grande, entonces el propio representante balanceado de la clase de h es el propio de h (véase el Capítulo 4). Veamos bajo qué condiciones se puede asegurar que el polinomio h' solución a este sistema sea realmente la imagen de h en $\mathbb{Z}[\alpha]/(\omega)$.

Mediante el siguiente resultado se demuestra que si p no divide a a ni a b entonces $\deg(h^*(x)) \leq \deg(h(x))$.

Lema 3.2.4. *Sea p un número primo tal que no divida a a a b ni a Δ. Entonces $\bar{h} = h \mod p$ divide a h^* en $\bar{R}[x]$.*

Demostración. En primer lugar, el coeficiente director de h es un número entero c, su clase módulo p es no nulo porque p no divide ni a a ni a b ni a Δ luego tampoco a c. Así $\bar{c}$ es una unidad en $\bar{R}$ y poemos dividir h^* por $\bar{h}$.

Por el Teorema 3.1.8, $\hat{h} \in \frac{1}{c}R[x]$, $f^*_{1/a} \in \frac{1}{a\Delta}R[x]$ y $g^*_{1/b} \in \frac{1}{b\Delta}R[x]$. Por lo tanto

$$(ca\Delta)f_{1/a} = (c\hat{h}) \cdot (a\Delta f^*_{1/a}) \Longrightarrow c\Delta f = h \cdot (a\Delta f^*_{1/a}),$$

$$(cb\Delta)g_{1/b} = (c\hat{h}) \cdot (b\Delta g^*_{1/b}) \Longrightarrow c\Delta g = h \cdot (b\Delta g^*_{1/b}).$$

f, g, h, $a\Delta f$ y $b\Delta g$ están en $R[x]$ por lo que reduciendo mod p a ambos lados de las igualdades queda

$$\overline{c\Delta}\,\bar{f} = \bar{h}\bar{\Delta}\overline{f^*_{1/a}},$$

$$\overline{c\Delta}\bar{g} = \bar{h}\bar{\Delta}\overline{g^*_{1/b}}.$$

p no divide a $c\Delta$ porque no divide a a ni a b ni a Δ. Además es un número entero así que es unidad en $\bar{R}$. De esta manera, $\bar{h}$ es un divisor común de $\bar{f}$ y $\bar{g}$ sobre $\bar{R}[x]$. Por lo tanto, $\bar{h}$ divide a h^*. □

Ejemplo 3.2.5. Tomemos α raíz de $r = y^3 - 2$, y f y g los siguientes polinomios en $\mathbb{Z}[\alpha][x]$:

$$f = 45x^7 - 15x^6 - 9\alpha x^5 + 3\alpha x^4 + 15\alpha x^3 - 5\alpha x^2 - 3\alpha^2 x + \alpha^2,$$

$$g = 21x^6 + (42\alpha - 3)x^5 - 6\alpha x^4 + 7\alpha x^2 + (14\alpha^2 - \alpha)x - 2\alpha^2.$$

Su máximo común divisor sobre $\mathbb{Q}(\alpha)$ es el polinomio $3x^4 + \alpha$. Si tomamos $p = 7$, g reducido módulo p cae de grado. Se tiene además $h^* = 1$, que claramente no es divisible por $\bar{h}$ de grado 4.

De esta manera, se ha encontrado otra condición para poder descartar rápidamente los p para los que el algoritmo dará malos resultados: p no debe dividir ni a a ni a b ni a Δ.

Por otro lado, se ha demostrado que, de cumplir p esta condición, el grado de h^* debe ser igual o mayor que el grado de h. Como se ha comentado previamente, se necesita tener $\deg(h^*) = \deg(h)$. En este contexto se realiza la siguiente distinción:

Definición 3.2.6. Dado p un primo que no divide a a ni a b ni a Δ, si el grado de h^* es mayor que el de h, p se denomina *unlucky* y, si es igual, p es un primo *lucky*.

Ejemplo 3.2.7. En el ejemplo 3.2.3, el máximo común divisor de las imágenes de f y g en uno de los cuerpos ha resultado tener grado mayor que h de manera que el grado de h^* también ha sido mayor. Por lo tanto se tiene que 11 es un primo *unlucky*.

Los primos *unlucky* deben de ser descartados. Sin embargo, no es fácil detectar directamente si cierto primo es *lucky* o *unlucky* sin conocer el grado de h. El algoritmo propone el siguiente método:

Supongamos que se han utilizado ya i primos, $p_1, \ldots, p_i$ de manera que se han calculado $h_1^*, \ldots, h_i^*$ todos de igual grado (siempre puede encontrarse i cumpliendo esta condición, basta con tomar $i = 1$). Sea ahora un primo p_{i+1} para el cual se calcula h_{i+1}^*. Por definición si p_{i+1} es *unlucky*, sabemos que $\deg(h_{i+1}^*) \geq \deg(h)$, mientras que $\deg(h_j^*) \geq \deg(h)\ \forall j$. De esta forma, si el grado de h_{i+1}^* es mayor que el de los anteriormente calculados, entonces seguro que p_{i+1} es *unlucky* y se descarta h_{i+1}^*. Si, por el contrario, el grado de h_{i+1}^* es menor que el de los anteriores, entonces todos estos serán *unlucky* y, por ello, se deben descartar. La última opción es que el grado del nuevo polinomio sea igual al de sus predecesores, en ese caso no podemos descartar nada y se continúa ejecutando el algoritmo.

Para garantizar que este método es válido, siempre se debe poder encontrar un primo *lucky* en un número finito de iteraciones con el que poder descartar cualquier *unlucky* hallado previa o posteriormente. De lo contrario, el algoritmo podría no converger al no ser capaz de calcular un h' con el grado correcto. Dicha validez se puede demostrar viendo que existe sólo una cantidad finita de primos *unlucky*. El siguiente teorema determina cuándo un primo es *unlucky* aplicando los resultados sobre teoría de subresultantes vistos en el capítulo 2.

Teorema 3.2.8. *Sea p primo tal que no divida a a ni a b ni a Δ. Entonces $deg(h^*) > k$ si y solo si divide a $W = Res(r(y), sRes_k(f,g)(y))$. Es decir, p es unlucky si y solo si es divisor de W.*

Demostración. En primer lugar, se observa que $W \neq 0$ ya que $\mathrm{sRes}_k(f,g)) \neq 0$ por ser k el grado del máximo común divisor de f y g y, además, $r(y)$ es irreducible, por lo que no tiene factores comunes con $\mathrm{sRes}_k(f,g)(y)$, que es de grado estrictamente menor.

Como $W \neq 0$, p divide a W si y solo si $\overline{W} = 0$. r es mónico de forma que $\bar{r}$ conserva el grado y así $\overline{W} = \mathrm{Res}(r, \mathrm{sRes}_k(f,g))\mod p = \mathrm{Res}(\bar{r}, \mathrm{sRes}_k(f,g) \mod p) = 0$. Como p no divide a los coeficientes directores de f y g, estos no caen de grado. Entonces, por el Teorema 2.2.2, la subresultante especializa bien, luego $\overline{W} = \mathrm{Res}(\bar{r}, \mathrm{sRes}_k(\bar{f}, \bar{g})) = 0$. Ahora bien, $\bar{r} = \bar{r}_1 \cdots \bar{r}_t$ con cada $\bar{r}_i$ irreducible, por lo tanto,

$$\begin{aligned} p|W &\iff \prod_{i=1}^{t} \mathrm{Res}(\bar{r}_i, \mathrm{sRes}(\bar{f}, \bar{g})) = 0 \\ &\iff \exists j \in \{1, \ldots t\} :\ \mathrm{Res}(\bar{r}_j, \mathrm{sRes}(\bar{f}, \bar{g})) = 0. \end{aligned}$$

Como $\bar{r}_j$ es irreducible y no nulo, $\mathrm{Res}(\bar{r}_j, \mathrm{sRes}(\bar{f}, \bar{g})) = 0$ si y solo si $\bar{r}_j$ divide a $\mathrm{sRes}(\bar{f}, \bar{g})$ si y solo si $\psi_j(\mathrm{sRes}(\bar{f}, \bar{g})) = \mathrm{sRes}(\psi_j(\bar{f}), \psi_j(\bar{g})) = 0$ ya que $\deg(\psi_j(\bar{f})) = deg(\bar{f})$ y $\deg(\psi_j(\bar{g})) = deg(\bar{g})$ al ser a y b números enteros y r_j un polinomio de grado positivo. Como sabemos que para todo $0 \leq l < k$ $\mathrm{sRes}_l(f,g) = 0$ al ser $\deg(\gcd(f,g)) = k$, se demuestra que $\mathrm{sRes}_l(\psi_j(\bar{f}), \psi_j(\bar{g})) = 0$ sin más que seguir el

razonamiento anterior. De esta forma, se tiene finalmente que $\mathrm{sRes}_k(\psi_j(\bar{f}), \psi_j(\bar{g})) = 0$ si y solo si $\deg(\gcd(\psi_j(\bar{f}), \psi_j(\bar{g}))) > k$ si y solo si $\deg(h^*) > k$. □

Corolario 3.2.9. *El número de primos unlucky es finito.*

Demostración. Por lo discutido anteriormente, se tiene que el grado de h^* es mayor que k, es decir, p es *unlucky*, si y solo si p es divisor de W. Como $W \in \mathbb{Z}$ puede tener únicamente un número finito de divisores, se tiene el resultado. □

Ejemplo 3.2.10. Como hemos visto antes, 11 es un primo *unlucky*. Veamos que divide a W:

$$W = \mathrm{Res}(y^3 - 2, \mathrm{sRes}_3(f, g)(y)) = 31136134420257908593750000000000000.$$

La factorización en primos de W es $2^{14} \cdot 5^{21} \cdot 11 \cdot 4349 \cdot 833091244757$ y por lo tanto $11|W$. De los factores primos de W, 2 y 5 dividen a los coeficientes directores de f y g y por lo tanto serían descartados directamente. Por lo tanto, el 11, el 4349 y el 833091244757 son todos los primos *unlucky*.

Ahora que tenemos W factorizado podemos tomar un primo que no divida a a ni b ni a Δ ni a W, como por ejemplo $p = 17$. Como p cumple estas condiciones, el polinomio h^* correspondiente debería ser de grado 3. Sea $\bar{r} = r \mod p$, este polinomio factoriza sobre $\mathbb{Z}/(p)$ como $\bar{r} = (y + 9)(y^2 + 8y + 13)$. $\bar{R}$ es por lo tanto isomorfo al producto de dos cuerpos. Calculando los gcd, $\bar{h}_1$ y $\bar{h}_2$, de las imágenes de f y g en los cuerpos correspondientes se obtiene:

$$\bar{h}_1 = 3x^3 + 2x + 2,$$

$$\bar{h}_2 = (9\eta + 4)x^3 + (15\eta + 7)x + 2\eta + 10.$$

donde η es una de las raíces de $y^2 + 8y + 13$ en su cuerpo de escisión sobre $\mathbb{Z}/(p)$.

Resolviendo el sistema de congruencias, se obtiene $h^* = x^3 + (3\alpha^2 + 7)x + 12\alpha^2 + \alpha + 1$ de manera que $\deg(h^*) = 3 = \deg(h)$ y el 17 es un primo *lucky*.

Finalmente, el siguiente resultado justifica la presencia de los c_i congruentes con c en el sistema de congruencias a resolver para recuperar h.

Lema 3.2.11. *Sea p un primo que no divide a a, a b ni a Δ. Si p es lucky, entonces $\bar{h} = \bar{c}h^*$.*

Demostración. Por el lema 3.2.4, $h^* = q\bar{h}$ para algún $q \in \bar{R}[x]$. Como p no divide a c, el coeficiente director de $\bar{h}$ es $\bar{c}p$, una unidad de $\bar{R}$. Por lo tanto,

$$\deg(h^*) = \deg(q) + \deg(\bar{h}).$$

Si p es lucky, $\deg(q)$=0 porque $\deg(h^*) = \deg(\bar{h})$. Además, h^* es mónico ya que el grado del $gcd(\psi_j(\bar{f}), \psi_j(\bar{g}))$ es k en todos los j y cada $\bar{R}_j$ es un cuerpo. Por lo tanto, $1 = q\bar{c}$. □

Ejemplo 3.2.12. Veamos que se cumple c satisface la congruencia a resolver $\bar{h} = h$ mód $17 = \bar{c}h^*$.

$$h = c \cdot \gcd(f, g) = 1080 \cdot \left(t^3 + (3\alpha^2 + 1/5)t + (1/10)\alpha^2 + \alpha + 1\right)$$

$$\Longrightarrow \bar{h} = 9x^3 + (10\alpha^2 + 12)x + 6\alpha^2 + 9\alpha + 9.$$

Por otro lado, $\bar{c} = 1080 \mod 17 = 9$. Entonces,

$$\bar{c} \cdot h^* = 9 \cdot (x^3 + (3\alpha^2 + 7)x + 12\alpha^2 + \alpha + 1) =$$

$$= 9x^3 + (10\alpha^2 + 12)x + 6\alpha^2 + 9\alpha + 9.$$

Por lo tanto se cumple la congruencia $h \equiv \bar{c}h^* \mod p$.

3.3. Cálculo de h^*

Dado p, si queremos obtener el correspondiente h^* podríamos calcular el gcd de las imágenes de $\bar{f}$ y $\bar{g}$ en cada cuerpo para, después, recuperar el h^* resolviendo el sistema de congruencias dado por el Teorema Chino de los Restos. Esto requeriría calcular los cuerpos, aplicar el algoritmo de Euclides tantas veces como cuerpos compongan el producto y ejecutar el levantamiento de los máximos común divisores encontrados. Existe una alternativa a este método que consiste en intentar llevar a cabo el algoritmo de Euclides aplicado a $\bar{f}$ y $\bar{g}$ sobre $\bar{R}[x]$. Este método puede no funcionar siempre ya que $\bar{R}$ no es un dominio, y por lo tanto, podría suceder que en cierto punto del algoritmo no sea posible realizar la división en el caso de encontrar un resto no nulo cuyo coeficiente director no sea una unidad. En este caso, no se podría realizar la siguiente división lo que impediría continuar con el algoritmo de Euclides. No obstante, en el caso de que se pueda completar el algoritmo, obtendríamos h^* aplicándolo una única vez.

Poder o no calcular h^* de esta forma dependerá del primo p. Si el número de primos para los cuales este método falla es finito, será posible calcular tantos h^* como sea necesario y el algoritmo modular acabará convergiendo en un número finito de iteraciones. Veamos en qué casos podemos encontrar un resto con un coeficiente director que no sea unidad en $\bar{R}$.

Asumamos, sin pérdida de generalidad, que $\deg(f) \geq \deg(g)$ y, por lo tanto, como p no divide a a ni a b, $\deg(\bar{f}) \geq \deg(\bar{g})$. El coeficiente director de $\bar{g}$, $\bar{b} \in \mathbb{Z}/(p)$, es una unidad en $\bar{R}$. Para ver esto basta con observar que su inverso está en $\mathbb{Z}/(p) \subseteq \bar{R}$ al ser $\mathbb{Z}/(p)$ un cuerpo. Otra forma de verlo, y que vamos a poder aplicar posteriormente a otros elementos de $\bar{R}$, es probar que su imagen por el isomorfismo dado por el Teorema Chino de los Restos, al que denominamos ψ, es $(b_1, \ldots, b_t)$ con $b_i = \psi_i(\bar{b})$ y $b_i \neq 0$, $1 \leq i \leq t$, ya que de esta forma, cada coordenada b_i tendrá un inverso b_i^{-1} en el cuerpo correspondiente al no ser 0. Por lo tanto, $\bar{b}^{-1}$ será la contraimagen (única) por ψ de $(b_1^{-1}, \ldots, b_t^{-1})$. Como se tiene $\bar{b} \in \mathbb{Z}/(p)$ no nulo y el grado de cada factor r_i es mayor o igual que 1, la imagen de $\bar{b}$ en cada cuerpo no es nula y, por lo discutido

antes, $\exists \bar{b}^{-1} \in \bar{R}$, luego $\bar{b}$ es unidad. Consecuentemente, podemos dividir $\bar{f}$ y $\bar{g}$ para encontrar q y s en $\bar{R}[x]$ tales que

$$\bar{f} = \bar{g}q + s,$$

con $\deg(s) < \deg(g)$. Ahora s puede no tener un coeficiente director invertible. En ese caso no sería posible dividir g y s y no podríamos seguir con el Algoritmo de Euclides. Si, por el contrario, es invertible, será posible seguir.

Proposición 3.3.1. *Si la secuencia de grados de $\psi_i(\bar{f})$ y $\psi_i(\bar{g})$ sobre R_i es la misma para cada i, $1 \leq i \leq t$, entonces es posible completar el algoritmo de Euclides en $\bar{R}[x]$ hasta llegar a h^**

Demostración. Procedamos por inducción en el número de divisiones realizadas con éxito al tratar de llevar a cabo el Algoritmo de Euclides:

El caso base es 0 divisiones, la secuencia de grados obtenida hasta esta división es $n_0 = \deg(f)$ y $n_1 = \deg(g)$ que es la misma en todos los cuerpos porque f y g no caen de grado. Como se ha demostrado antes, es posible realizar la división euclidea de f entre g.

Supongamos ahora que la secuencia de restos es igual para cada $\bar{R}_i[x]$, $1 \leq i \leq t$, hasta el resto $s+1$ obteniendo en todos ellos la secuencia $n_0 = \deg(f)$, $n_1 = \deg(g)$, ..., n_{s+1} sin haber alcanzado todavía el gcd, es decir, siendo el resto $s+1$, r_{s+1}, no nulo, ya que en ese caso no haría falta realizar más divisiones. Supongamos además que ha sido posible realizar las correspondientes divisiones en $\bar{R}$. Como ψ es un isomorfismo coeficiente a coeficiente y el grado de los restos esentonces las divisiones realizadas en $\bar{R}[x]$ se corresponden a través de ψ con las realizadas en $\bar{R}_i[x]$, $1 \leq i \leq t$. Particularmente, si el resto de la división número s en $\bar{R}$ es $\bar{r}_{s+1}$, el resto de la división número s en $\bar{R}_i$ es $\psi_i(\bar{r}_{s+1})$, $1 \leq i \leq t$. Como cada $\psi_i(\bar{r}_{s+1})$ tiene el mismo grado, tiene el mismo grado que $\bar{r}_{s+1}$ por ser ψ un isomorfismo coeficiente a coeficiente y por la unicidad de la división euclídea. Veamos que es posible realizar entonces la siguiente división, la $s+1$.

Como la imagen de $\bar{r}_{s+1}$ tiene el mismo grado en cada cuerpo y es no nulo, su coeficiente director no es nulo en ninguno y, por lo tanto, es unidad en $\bar{R}$. Al ser unidad, puede realizarse la división euclídea entre $\bar{r}_s$ y $\bar{r}_{s+1}$ para obtener $\bar{r}_{s+2}$ y seguir con el Algoritmo de Euclides un paso más. Si $s+1$ es la longitud de la secuencia de restos, entonces $\bar{r}_{s+2} = 0$ y se ha encontrado $h^* = \bar{r}_{s+1}$.

□

Definición 3.3.2. Sea p un primo en $\mathbb{Z}$ tal que no divide a a ni a b ni a c. Si no es posible completar el Algoritmo de Euclides para encontrar h^* en $\bar{R} = R/(p)$, diremos que p es un primo *fail*.

La proposición 3.3.1 establece una condición suficiente sobre la secuencia de restos en los distintos cuerpos para poder calcular h^* mediante el algoritmo de Euclides sobre $\bar{R}$. El siguiente teorema aprovecha la relación entre subresultantes y sucesión de restos para demostrar la finitud de primos *fail*.

Teorema 3.3.3. *Sea p primo que no divida a a ni a b ni a Δ. Entonces, en alguno de los cuerpos no aparece un resto de grado j en la sucesión de restos del algoritmo de Euclides entre las correspondientes imágenes de $\bar{f}$ y $\bar{g}$ si y solo si*

$$p|W_j = Res(r, sRes_j(f, g)).$$

Demostración. En primer lugar, si $sRes_j(f, g) = 0$ entonces en la sucesión de restos del algoritmo de Euclides de f y g en R no aparece un resto de grado j. En ese caso, $W_j = 0$ y por lo tanto es múltiplo de p. Como p no divide a a ni a b y a y b son números enteros, los polinomios no bajan de grado y se tiene $\forall i$, $1 \leq i \leq t$

$$0 = \psi_i\left(\overline{sRes_j(f, g)}\right) = sRes_j(\psi(\bar{f}), \psi_i(\bar{g})).$$

Por lo tanto, si $sRes_j(f, g) = 0$ en ningún cuerpo aparece un resto de grado j en la sucesión de restos del algoritmo de Euclides.

Supongamos ahora $sRes_j(f, g) \neq 0$, entonces $W_j \neq 0$ ya que r es un polinomio irreducible. Como $\bar{r}$ es mónico y $p \not| a, b$,

$$\overline{W_j} = Res\left(\bar{r}, \overline{sRes_j(f, g)}\right) = Res(\bar{r}, sRes_j(\bar{f}, \bar{g})) = \prod_{i=1}^{t} Res(r_i, sRes_j(\bar{f}, \bar{g})).$$

Por lo tanto, $p|W_j \iff \overline{W_j} = 0 \iff Res(r_i, sRes_j(\bar{f}, \bar{g})) = 0$ para uno o varios i con $1 \leq i \leq t$. En este punto hay dos casos posibles:

- Si $sRes_j(\bar{f}, \bar{g}) = 0$, entonces, por ser los coeficientes directores de $\bar{f}$ y $\bar{g}$ números enteros, $0 = \psi_i(sRes_j(\bar{f}, \bar{g})) = sRes_j(\psi_i(\bar{f}), \psi_l(\bar{g}))$ $\forall 1 \leq i \leq t$ y así, en ninguno de los cuerpos aparece un resto de grado j en la sucesión de restos de $\psi_i(\bar{f})$ y $\psi_i(\bar{g})$. No obstante, como $sRes_j(f, g) \neq 0$, en la sucesión de restos del algoritmo de Euclides aplicado a f y g en R sí aparecería un resto de grado j.

- Si $sRes_j(\bar{f}, \bar{g}) \neq 0$, tomemos l, $1 \leq i \leq t$, tal que $Res(r_i, sRes_j(\bar{f}, \bar{g})(y)) = 0$. Como r_i es irreducible,

  $$Res(r_i, sRes_j(\bar{f}, \bar{g})(y)) = 0 \iff r_i \text{ divide a } sRes_j(\bar{f}, \bar{g})(y)$$

  $$\iff \psi_j(sRes_j(\bar{f}, \bar{g})) = sRes_j(\psi_i(\bar{f}), \psi_i(\bar{g})) = 0.$$

  Esto último es equivalente a que en la sucesión de restos de $\psi_i(\bar{f})$ y $\psi_i(\bar{g})$ no aparezca un resto de grado j.

□

De la demostración de este teorema se desprende que si $W_j = 0$, entonces no aparecerá en ningún cuerpo un resto de grado j. Mientras que si $W_j \neq 0$ el resto de grado j no aparecerá en alguno de los cuerpos (o en todos) si W_j es divisible por p. Es en este último caso en el que puede ocurrir que p sea *fail* si p divide a W_j. Pero, como los grados j tienen que estar entre 0 y mín$\{\deg(f), \deg(g)\}$ y, para cada

uno hay un $W_j \in \mathbb{Z}$, se tiene que hay una cantidad finita de primos p que dividan a alguno de los W_j. Por lo tanto, el número de primos *fail* también es finito.

Puede ocurrir que aún p dividiendo a algún W_j sea posible llegar a calcular h^* si en ningún cuerpo aparece un resto de grado j. En particular, si p es *unlucky*, para $j = \deg(\gcd(f, g))$, se tiene $\bar{W}_j = 0$ por el teorema 3.2.8, pero se puede llegar a calcular h^* como ilustra el siguiente ejemplo.

Ejemplo 3.3.4. Veamos un ejemplo de cada caso, analizando la sucesión de subresultantes en los respectivos anillos.

- Veamos en primer lugar el caso de un primo *lucky* pero *fail*, de manera que el h^* correspondiente sería válido pero no podríamos calcularlo mediante el algoritmo de Euclides aplicado a $\bar{f}$ y $\bar{g}$. Para buscarlo directamente, vamos a calcular cada uno de los W_j con $0 \leq j \leq 6$. Esto no se hace en el algoritmo ya que no es necesario: si cierto p es *uncharming* no se podría llevar a cabo el algoritmo de Euclides, se descartaría y se volvería a intentar con el siguiente primo.

$\boldsymbol{j}$	W_j
6	$2^3 \cdot 5^3 \cdot 13^3$
5	$-1 \cdot 2^5 \cdot 5^9 \cdot 13^6 \cdot 107$
4	$2^9 \cdot 3 \cdot 5^{15} \cdot 13^3 \cdot 1957478407$
3	$2^{14} \cdot 5^{21} \cdot 11 \cdot 4349 \cdot 833091244757$
2	0
1	0
0	0

  Como $\deg(h) = 3$ $W_j = 0$ si $j < 3$ como se esperaba. Recordemos que $a = 10$, $b = 130$ y $\Delta = 108$ y por lo tanto, los primos descartados inicialmente son 2, 3, 5 y 13. Los primos *fail* serán a lo sumo aquellos que dividan a algún W_j no nulo y no estén descartados. Estos son el 11, el 107, el 4349, el 1957478407 y el 833091244757. Los primos que se obtienen para $j = 3$ ya aparecieron en un ejemplo anterior y es que son precisamente los primos *unlucky*.

  Para comprobar qué pasa con uno de estos primos, tomemos por ejemplo $p = 107$. Se esperaría en principio encontrar problemas a la hora de tratar de llevar a cabo el algoritmo de Euclides aplicado a $\bar{f}$ y $\bar{g}$. A partir de la factorización de $\bar{r}$ se tiene:

$$\frac{\mathbb{Z}[y]/(p)}{(\bar{r})} \simeq \frac{\mathbb{Z}[y]/(p)}{(y+101)} \times \frac{\mathbb{Z}[y]/(p)}{(y^2+6y+36)}.$$

  Al calcular los máximos común divisor de las imágenes de f y g en los respectivos cuerpos obtenemos:

$$h_1 = 31y^3 + 80y + 29 \quad \text{y} \quad h_2 = (45\beta + 51)y^3 + (5\beta + 8)y + 20\beta + 67$$

donde β una de las raíces de $y^2 + 6y + 36$ en su cuerpo de escisión sobre $(\mathbb{Z}/(p))[y]$.

En la tabla siguiente se muestra el valor de los coeficientes subresultantes principales calculados sobre $\bar{R}$, $\bar{R}_1 = \frac{\mathbb{Z}[y]/(p)}{(y+101)}$ y $\bar{R}_2 = \frac{\mathbb{Z}[y]/(p)}{(y^2+6y+36)}$.

$\boldsymbol{j}$	$\text{sRes}_j\ (\bar{R})$	$\text{sRes}_j\ (\bar{R}_1)$	$\text{sRes}_j\ (\bar{R}_2)$
6	23	23	23
5	$92\alpha^2 - 17\alpha$	**0**	$4\beta + 99$
4	$-26\alpha^2 + 63\alpha + 87$	10	$55\beta + 69$
3 = k	$18\alpha^2 + 41\alpha$ - 102	43	$96\beta + 8$
2	0	0	0
1	0	0	0
0	0	0	0

Vemos que, como p es *lucky*, $sRes_j$ se anula para $j < 3$ en cada anillo pero es no nulo para $j = 3$. Para $j = 5$, la subresultante en uno de los dos cuerpos se anula pero en el otro no. Por lo tanto, la sucesión de restos no es la misma en ambos cuerpos y por ello no es posible llevar a cabo el algoritmo de Euclides en $\bar{R}$. En concreto, sabemos que por ser $j = 5$ y $\deg(g) = 6$, el coeficiente director del resto de dividr f entre g será divisor de 0. Este coeficiente es $56\alpha^2 + 92\alpha$.

- Tomemos ahora

$$f = x^{10} + 4x^7 + (-\alpha - 3)x^6 + (\alpha^2 + 1)x^4 + (-4\alpha - 12)x^3 + (4\alpha^2 + 4)x,$$

$$g = x^6 + 7x^5 + (-3\alpha - 4)x^4 + (-21\alpha - 24)x^3 + 28x^2 + (-12\alpha - 16)x - 84\alpha - 112,$$

manteniendo α como hasta ahora, ráiz de $r = x^3 - 2$. El máximo común divisor de estos dos polinomios es $y^3 + 4$, por lo tanto $k = \deg(h) = 3$. Tomemos $p = 7$. En $\mathbb{Z}(p)$, la reducción módulo p de r, $\bar{r}$, sigue siendo irreducible. Por lo tanto, se tiene que $\bar{R}$ es un cuerpo lo cual nos asegura el poder calcular h^* mediante el Algoritmo de Euclides. Entonces p no podrá ser un primo *fail*. No obstante, se llega a que

$$h^* = \gcd(\bar{f}, \bar{g}) = (\alpha^2 + 5\alpha + 2)x^4 + (4\alpha^2 + 6\alpha + 1)x.$$

Pero entonces, $\deg(h^*) > \deg(h)$ y p es un primo *unlucky*. Veamos la sucesión de subresultantes:

$\boldsymbol{j}$	$\text{sRes}_j(\bar{R})$
6	1
5	0
4	$\alpha^2 + \alpha + 3$
3 = k	0
2	0
1	0
0	0

Se tiene que el tercer coeficiente subresultante principal se anula, condición para que, efectivamente, p sea *unlucky*. En un caso como este, sería posible calcular h^* con el algoritmo de Euclides, pero este polinomio no sería útil y acabaría siendo desechado en el momento que se encuentre otro con grado menor.

- Veamos por último un ejemplo de primo *lucky* y no *fail* que es el que desearíamos encontrarnos al ejecutar el algoritmo. Retomemos los previos f y g:

$$\begin{aligned} f =& 10x^7 + (30\alpha^2 - 10\alpha + 2)x^5 + (\alpha^2 + 10\alpha + 10)x^4 + (-2\alpha - 50)x^3 \\ &+ (-10\alpha^2 - 10\alpha - 2)x^2 + (30\alpha^2 + 2)x + \alpha^2 + 10\alpha + 10, \end{aligned}$$

$$\begin{aligned} g =& 130x^6 - 65\alpha x^5 + (390\alpha^2 + 65\alpha + 26)x^4 + (8\alpha^2 + 117\alpha - 260)x^3 \\ &+ (-65\alpha^2 - 52\alpha + 377)x^2 + (64\alpha^2 + 35\alpha + 13)x - 5\alpha^2 - \alpha - 10. \end{aligned}$$

Vimos en un ejemplo anterior que $p = 17$ es *lucky*. Además, al tratar de aplicar el algoritmo de Euclides sobre $\bar{R}$ se logra alcanzar el resto 0 y, por lo tanto, no es *fail*. Se vio también que $\bar{R}$ es producto producto de dos cuerpos, a los que denominamos $\bar{R}_1$ y $\bar{R}_2$. Observemos la sucesión de subresultantes:

j	$\text{sRes}_j(\bar{R})$	$\text{sRes}_j(\bar{R}_1)$	$\text{sRes}_j(\bar{R}_2)$
6	11	11	11
5	$5\alpha^2 + 13\alpha$	12	12η+5
4	$11\alpha^2 + 4\alpha + 3\alpha$	8	$11\eta + 12$
3 = k	$13\alpha^2 + 9\alpha + 11$	14	9η+5
2	0	0	0
1	0	0	0
0	0	0	0

Recordemos que η representaba una de las dos raíces del factor de segundo grado de $\bar{r}$. Se tiene que no se anula ningún coeficiente subresultante principal en $\bar{R}_1$ o $\bar{R}_2$ tal que el correspondiente en $\bar{R}$ no se anule. Además, el primero no nulo es el tercero en todos los casos. Las condiciones impuestas sobre la sucesión para poder asegurar que el primo es *lucky* y no *fail* se cumplen.

Capítulo 4

Reconstrucción del máximo común divisor sobre $\mathbb{Z}[\alpha]$

Resumamos el análisis realizado en el Capítulo 3. Por un lado, se tienen dos polinomios f y g en $\mathbb{Z}[\alpha][x] = R[x]$ cuyo máximo común divisor en $\mathbb{Q}(\alpha)[x]$ nos interesa calcular. En realidad, calculamos primero el asociado $h = c\,\gcd(f, g) \in R[x]$. Para ello, se realiza la reducción módulo un primo p y se trata de aplicar el algoritmo de Euclides en $\bar{R}[x]$ sobre $\bar{f}$ y $\bar{g}$ para encontrar un polinomio h^*. Para todos salvo para un número finito de primos, será posible calcular h^* que servirá para recuperar el máximo común divisor de f y g. En este caso, sabemos que el polinomio h^* calculado satisface $c\,\gcd(f, g) \mod p = (c \mod p)h^*$. Los primos para los que esto no es posible, son:

- Aquellos divisores de Δ, a o b. Estos primos son descartados directamente.
- Los primos *fail*, que no permiten completar el algoritmo de Euclides sobre $\bar{R}$ al aparecer divisores de cero en el cálculo.
- Los primos *unlucky*, que provocarán que el grado del h^* calculado sea mayor que el de h, por lo que no son útiles a la hora de recuperar el máximo común divisor de f y g.

Debemos repetir este procedimiento varias veces empleando distintos primos para obtener así una serie de polinomios h_i^* con los que realizar el levantamiento para tratar de calcular h. Pero, ¿cómo podemos asegurar que vamos a recuperar el asociado h al $\gcd(f, g)$?

4.1. Sobre la condición de parada

Asumiendo que, tras calcular el máximo común divisor de $\bar{f}$ y $\bar{g}$ para distintos anillos $\bar{R}$, tendremos que resolver el sistema de congruencias

$$\begin{aligned} h' \equiv & ch_1^*(y,x) \bmod p_1 \\ & \vdots \\ h' \equiv & ch_m^*(y,x) \bmod p_m, \end{aligned}$$

donde $ch_i^* \in (\mathbb{Z}/(p))[y,x]$, $\deg_y(ch_i^*) < n$, y todos tienen el mismo grado en x. Por el Teorema Chino de los Restos aplicados a los coeficientes, existe una única clase $h' \in (\mathbb{Z}/(\omega))[y,x]$ solución del sistema, donde $\omega = \prod p_i$. Ahora bien, los coeficientes de h pueden ser positivos o negativos, por lo que a la hora de tomar un representante canónico de un coeficiente $\bar{e}_{j\ell} \in \mathbb{Z}/(\omega)$ de h', tomaremos el único $e_{j\ell} \in \mathbb{Z}$ tal que

$$-\omega/2 < e_{j\ell} \leq \omega/2.$$

Si $h = \sum_{\ell=0}^{k} \left(\sum_{j=0}^{n-1} e_{j\ell} y^j \right) x^\ell$, entonces podremos recuperar h a partir de h' cuando

$$2 \cdot \text{máx}\{|e_{j\ell}| \ : \ 0 \leq j \leq n-1, \ 0 \leq \ell \leq k\} + 1 < \omega.$$

Langemyr y McCallum [7] calculan una cota de máx$\{|e_{j\ell}|\}$:

$$K = 2^k |\Delta|^{1/2} \, \text{mín}(\|f(x)\|_2, \|g(x)\|_2) n (n-1)^{(n-1)/2} \|r(y)\|_2^{n-1},$$

donde k es el grado del máximo común divisor, Δ es el discriminante del polinomio mínimo r, $n = \deg(r)$. Para $r(y) \in \mathbb{Z}[y]$, $\|r\|_2 = \sqrt{\sum_{j=0}^{n-1} r_i^2}$ es la norma euclídea del vector de coeficientes. Dado un polinomio $u(x)$ en $R[x]$, se define $\|u(x)\|_2 = \text{máx}_{i=1}^{n} (\sum_{i=0}^{s} | \sum_{j=0}^{n-1} u_{i,j} \alpha_l^j |^2)^{1/2}$ donde s es el grado de $u(x)$, $u_{i,j}$ es el coeficiente en $\mathbb{Z}$, que acompaña a α^j en el término de grado j y $\alpha = \alpha_1, \ldots, \alpha_n$ son los conjugados de α. Es decir, el máximo de las normas de todos los posibles embebimientos del vector de coeficientes de u en $\mathbb{C}^{s+1}$.

No obstante, existen alternativas heurísticas para intentar recuperar h antes de alcanzar la cota, de manera que, en la práctica, nunca necesitemos alcanzarla. Obsérvese que si en un momento dado el polinomio h' balanceado que resuelve el sistema de congruencias divide a f y a g, necesariamente h' será un $\gcd(f,g)$. Como los h^* que se van calculando tienen grado mayor o igual al grado de h, el grado de h' también será mayor o igual al de h. Esto asegura que no podemos recuperar nunca un divisor común de f y g no asociado a h ya que todos los divisores comunes no asociados tienen un grado menor que h por ser éste el máximo común divisor. Entonces, si al dividir f y g por h' el resto se anula, se tiene $h = h'$, ya que h es el único polinomio que satisface la congruencia y es divisor de f y g, entonces finalizaría el algoritmo pues ya hemos dado con el máximo común divisor. En el caso de que el polinomio h' calculado no divida a f o a g se continuaría con el algoritmo, utilizando

otro primo para calcular h^* y volviendo a resolver sistema de congruencias con una congruencia más.

Una posible estrategia en este sentido es calcular h' balanceado cada vez que tengamos una cierta cantidad de polinomios h^* y comprobar si h' divide a f y a g. Una segunda estrategia es calcular h' balanceado cada vez que se añade un nuevo primo. Si h' es igual al anterior, es un candidato razonable y se comprueba entonces si divide a f y a g. Ambas estrategias podrían incluso combinarse.

Veamos una cota y comparémosla con el máximo común divisor.

Ejemplo 4.1.1. Tomemos r, f y g de nuevo como en el Ejemplo 3.1.9. Entonces $n = 3$, $k = 3$, $\Delta = 108$ y, calculando la cota, obtenemos:

$$2K = 399901{,}31225743203\ldots.$$

Por otro lado,

$$h = 108x^3 + (3240\alpha^2 + 216)x + 108\alpha^2 + 1080\alpha + 1080.$$

El máximo coeficiente $h_{i,j} \in \mathbb{Z}$ en valor absoluto de h es 3240, por lo tanto, bastaría con que ω fuese mayor que 6480 para poder realizar el levantamiento con éxito.

4.2. Algoritmo

A continuación se resume el algoritmo modular que se ha venido analizando paso a paso.

En primer lugar, supongamos que f y g vienen dados con coeficientes en un cuerpo de números N. Como estamos en carácteristica 0, por el Teorema del Elemento Primitivo, podemos encontrar un elemento β tal que $N = \mathbb{Q}(\beta)$. Ahora, si β no es entero sobre $\mathbb{Z}$, sea r' el polinomio mínimo de β. $r' = x^n + \sum_{i=0}^{n-1} \frac{r'_i}{d} x^i$, donde d es el denominador común de los coeficientes de r'. Entonces el pónimio mínimo de $d\beta$ es

$$x^n + \sum_{i=0}^{n-1} r'_i d^{n-1-i},$$

y $\mathbb{Q}(\beta) = \mathbb{Q}(d\beta)$ y $\alpha = d\beta$ es entero.

El algoritmo trabaja con tres listas: una lista infinita de números primos, que serán los p que se irán probando para obtener los polinomios h^*; una lista H, al principio vacía, que contiene a los h^* válidos ya calculados; y una lista P, al principio vacía, que contiene los primos empleados para obtener los polinomios en H.

La densidad de números primos *unlucky* o *fail* es esperable que sea mayor para valores bajos. Además, en algunas implementaciones prácticas de anillos finitos, excepto para primos especiales como el 2, no hay diferencias de cómputo mientras el número de bits del primo sea menor que 32. Por ello, es una estrategia inteligente hacer que los primos de la lista comiencen en un número relativamente alto, por ejemplo, el mínimo entre Δ y 2^{30}.

El algoritmo recibe como entrada un entero algebraico α que define $\mathbb{Q}(\alpha)$ y dos polinomios $f(x)$ y $g(x)$ en $\mathbb{Q}(\alpha)[x]$.

El algoritmo devuelve como salida el polinomio $h(x)$ asociado al máximo común divisor de $f(x)$ y $g(x)$ sobre el cuerpo de fracciones de R con coeficiente director $c = \gcd(a, b)\Delta$, siendo Δ el discriminante de $r(y)$.

Paso 0: Hacer f y g mónicos y limpiar denominadores. Tomar a y $b \in \mathbb{Z}$ como los coeficientes directores de f y g respectivamente. Calcular $c = \Delta \cdot \gcd(a, b)$.

Paso 1: Iniciar las listas P y H vacías.

Paso 2: Tomar p el siguiente primo de la lista de primos que no divida a a ni a b ni a Δ. Sea $\bar{r}(y) = r(y) \mod p$ y $\bar{R} = \mathbb{Z}[y]/(p)/(\bar{r}(y))$. Denotemos $\bar{f}(x) = f(x)$ mód p y $\bar{g}(x) = g(x) \mod p$.

Paso 3: Tratar de aplicar el algoritmo de Euclides a $\bar{f}(x)$ y $\bar{g}(x)$. Si finaliza con éxito, tomar $h^*(x)$ igual al último resto no nulo. En caso contrario, descartar p y volver al Paso 1.

Paso 4: Comparar el grado de $h^*(x)$ con el grado de los elementos en H:

- Si H es vacía, añadir $h^*(x)$ a H y p a P.
- Si el grado de $h^*(x)$ es mayor, descartar p de la lista y volver al Paso 2.
- Si el grado de $h^*(x)$ es igual, añadir $h^*(x)$ a H y p a P.
- Si el grado de $h^*(x)$ es menor, vaciar H y P y añadir $h^*(x)$ a H y p a P.

Paso 5: Calcular $\omega = \prod p_i$ el producto de todos los primos en P. Resolver el sistema de congruencias

$$\begin{aligned} h'(y,x) &\equiv c h_1^*(y,x) \bmod p_1 \\ &\vdots \\ h'(y,x) &\equiv c h_m^*(y,x) \bmod p_m, \end{aligned}$$

para un elemento $h'(x) \in \mathbb{Z}[y, x]/(\omega)$.

Paso 6: Considerar $h'(y, x)$ en $\mathbb{Z}[y, x]$ balanceado. Comprobar si su asociado mónico divide a $f(y, x)$ y a $g(y, x)$. Si es así, $h = h'$ y el algoritmo finaliza. Si no, continuar al Paso 2.

4.3. Posibles mejoras del algoritmo

El algoritmo de Langemyr y McCallum se basa en el algoritmo modular para calcular el máximo común divisor de dos polinomios con coeficientes en $\mathbb{Q}$ propuesto por Brown [2]. Posteriormente, han surgido diversas mejoras a este método.

En [5], se elimina la necesidad de que el generador α de la extensión $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ sea un elemento primitivo. Además, calcula el máximo común divisor mónico a partir de los residuos. Para esto, usa técnicas de reconstrucción racional. Dada una

clase $\overline{e} \in \mathbb{Z}/(\omega)$, en lugar de tomar un representante balanceado $e \in (-\omega/2, \omega/2]$, se buscan enteros e_n, e_d de tamaño pequeño tales que $\overline{e}_n \overline{e}_d^{-1} = \overline{e}$.

En [6], se hace una revisión de la bibliografía asociada a este problema y se proponen diversas heurísticas que mezclan las estrategias de Langemyr-McCallum y Encarnacion, para determinar cuándo es razonable intentar reconstruir el polinomio h sin necesidad de alcanzar la cota de coeficientes esperados.

En [8], los autores proponen diversas mejoras, las más destacables en el contexto de esta memoria son la adaptación del algoritmo a extensiones algebraicas $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ que no estén representadas por un elemento primitivo y en la que no se exige que los generadores α_i sean elementos algebraicos. Y, por otro lado, los autores demuestran que no es necesario calcular el discriminante Δ ni comprobar que un primo p sea divisor de Δ para que el algoritmo siga siendo correcto.

Como mejora alternativa, en el cálculo del máximo común divisor sobre $\bar{R}$, si los grados de f y g son altos, se pueden implementar algoritmos de complejidad subcuadrática, asintóticamente mejores que el algoritmo de Euclides.

4.4. Tiempo de ejecución

En esta sección vamos a comparar, mediante unos ejemplos sencillos, el desempeño del algoritmo estudiado con el del algoritmo de Euclides clásico. Para ello, medimos los tiempos de ejecución de ambos algoritmos en función de los grados de f, g y h para dos extensiones concretas. Aportamos también el máximo de los coeficientes de f y h considerados como polinomios en $\mathbb{Z}[x, y]$. Estos resultados se muestran a modo de ejemplo. Tener una buena batería de tests para el cálculo de gcd en esta situación no es un problema trivial.

Tabla 4.1: Ejemplos en $\mathbb{Q}(\alpha)$ con $r(y) = y^2 - 2$.

	$\deg(f)$	$\deg(g)$	$\deg(h)$	máx(f_i)	máx(h_i)	*tiempo*
Euclides	10	10	0	101	1	1.12 ms
Modular	10	10	0	101	1	0.983 μs
Euclides	50	50	0	78	1	1.03 s
Modular	50	50	0	78	1	10 ms
Euclides	50	50	25	1222	19	141 ms
Modular	50	50	25	1222	19	7 ms

Tabla 4.2: Ejemplo $\mathbb{Q}(\alpha)$ con $r(y) = y^4 - 34y^2 + 9$.

	$\deg(f)$	$\deg(g)$	$\deg(h)$	máx(f_i)	máx(h_i)	*tiempo*
Euclides	10	10	0	$3 \cdot 10^8$	1	39.5 ms
Modular	10	10	0	$3 \cdot 10^8$	1	1.95ms
Euclides	50	50	0	$7 \cdot 10^{24}$	1	733 ms
Modular	50	50	0	$7 \cdot 10^{24}$	1	2.51 ms
Euclides	50	50	25	$4 \cdot 10^{27}$	10^{22}	10.7 s
Modular	50	50	25	$4 \cdot 10^{27}$	10^{22}	34.3 ms
Euclides	100	100	12	$5 \cdot 10^{362}$	$9 \cdot 10^{95}$	$>$ 180 s
Modular	100	100	12	$5 \cdot 10^{362}$	$9 \cdot 10^{95}$	457 ms

Bibliografía

[1] S. Basu, R. Pollack, M.F. Roy (2006). Algebra. In: *Algorithms in Real Algebraic Geometry*. Algorithms and Computation in Mathematics, vol 10. Springer, Berlin, Heidelberg . https://doi.org/10.1007/3-540-33099-2_5

[2] W. S. Brown. 1971. *On Euclid's algorithm and the computation of polynomial greatest common divisors*. In Proceedings of the second ACM symposium on Symbolic and algebraic manipulation (SYMSAC '71). Association for Computing Machinery, New York, NY, USA, 195–211. https://doi.org/10.1145/800204.806288

[3] H. Cohen (1993). Algorithms on Polynomials. In: *A Course in Computational Algebraic Number Theory*, vol 138. . Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-02945-9_3 948/9781614440093

[4] G. E. (Collins). 1967. *Subresultants and Reduced Polynomial Remainder Sequences.* J. ACM 14, 1 (Jan. 1967), 128–142. https://doi.org/10.1145/321371.321381

[5] M.J. Encarnación (1995). *Computing GCDs of Polynomials over Algebraic Number Fields*. J. Symb. Comput., 20, 299-313. doi:10.1006/jsco.1995.1052

[6] D. Huelse & M. Hemmer (2009). *Generic implementation of a modular gcd over algebraic extension fields*. Paper presented at 25th European Workshop on Computational Geometry, Brussels, Belgium.

[7] L. Langemyr, S. McCallum (1989). *The computation of polynomial greatest common divisors over an algebraic number field.* In: Davenport, J.H. (eds) Eurocal '87. EUROCAL 1987. Lecture Notes in Computer Science, vol 378. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-51517-8_129

[8] M. Monagan & M. Van Hoeij. (2005). *A Modular Algorithm for Computing Polynomial GCDs over Number Fields presented with Multiple Extensions.*

[9] H. Pollard & H. Diamond (1975). *The Theory of Algebraic Numbers* (2nd ed.). Mathematical Association of America. doi:10.5