Capítulo 3

Base Espectral Para $K[x]_h$

El presente Capítulo se aparta de la interpolación para abordar el tema de las bases espectrales para el anillo polinomial módulo h, $K[x]/ < h(x) >:= K[x]_h$ sobre el campo K. Posteriormente se verá la manera de emplear bases espectrales para calcular ciertos polinomios de interpolación con mayor simplicidad y generalizar algunos conceptos. Por ahora, se enunciarán unos cuantos resultados básicos para el desarrollo de estas bases y después ver cómo se conforman en el caso del anillo modular $\mathbb{Z}_h$ y para anillos polinomiales modulares $K[x]_h$.

3.1. Preliminares

El propósito de esta sección es enunciar y probar un teorema que proporciona una importante relación entre números primos relativos, que será fundamental en el desarrollo de la idea de las bases espectrales en anillos modulares $\mathbb{Z}_h$. Posteriormente, se demostrará el análogo de dicho teorema, sólo que ahora en el caso del anillo polinomial modular $K[x]_h$. El teorema se enuncia a continuación.

Teorema 3.1. *Dados r enteros positivos $h_1, h_2, \ldots, h_r \in \mathbb{N}$ cuyo máximo común divisor sea $1 \in \mathbb{N}$, existen enteros $b_1, b_2, \ldots, b_r \in \mathbb{Z}$ tales que*

$$b_1h_1 + b_2h_2 + \ldots + b_rh_r = 1\,. \tag{3.1}$$

Demostración. Para probar el Teorema 3.1, se hará uso de los siguientes lemas:

Lema 3.2. *Si $a_1, a_2, \ldots, a_r$ son enteros positivos y $d = a_1s_1 + a_2s_2 + \ldots + a_rs_r$ es su combinación lineal positiva mínima, entonces d divide a cada a_i para $i = 1, 2, \ldots, r$.*

Demostración. Por el algoritmo de la división, se tiene que

$$a_i = dq_i + t_i, \qquad 0 \leq t_i < d\,.$$

Entonces

$$a_i = (a_1 s_1 + a_2 s_2 + \ldots + a_i s_i + \ldots + a_r s_r) q_i + t_i$$

y

$$t_i = (1 - s_i q_i) a_i - (s_1 q_i) a_1 - (s_2 q_i) a_2 - \ldots - (s_r q_i) a_r \,,$$

por lo que t_i es combinación lineal de a_i, $i = 1, 2, \ldots, r$, y como $0 \leq t_i < d$ y por hipótesis d es la combinación lineal positiva mínima de a_i, $i = 1, 2, \ldots, r$, se sigue que $t_i = 0$ y así $d|a_i$. Este procedimiento se repite para cada $i = 1, 2, \ldots, r$ y el lema queda demostrado. □

Lema 3.3. *El máximo común divisor de* $a_1, a_2, \ldots, a_r \in \mathbb{Z}_+$ *es la combinación lineal positiva mínima de* $a_1, a_2, \ldots, a_r$.

Demostración. Sea $D = (a_1, a_2, \ldots, a_r)$ el máximo común divisor de los a_i, $i = 1, 2, \ldots, r$, y $d = a_1 s_1 + a_2 s_2 + \ldots + a_r s_r$ la combinación lineal positiva mínima de ellos.

Como $D|a_1$, $D|a_2$, ..., $D|a_r$, es claro que $D|a_1 s_1 + a_2 s_2 + \ldots + a_r s_r = d$, por lo que $D \leq d$. Por otro lado, el Lema 3.2 garantiza que $d|a_1$, $d|a_2$, ..., $d|a_r$ debido a que d es la combinación lineal positiva mínima de los a_i, $i = 1, 2, \ldots, r$, y como D es el máximo común divisor de ellos, se tiene que $d \leq D$. Entonces $d = D$ y el Lema 3.3 queda probado. □

Regresando a la demostración del Teorema 3.1, como $1 \in \mathbb{N}$ es el máximo común divisor de $h_1, h_2, \ldots, h_r$, el Lema 3.3 asegura que existen enteros $b_1, b_2, \ldots, b_r$ tales que se cumple la ecuación 3.1, con lo que termina la demostración del Teorema 3.1 [1]. □

El Teorema 3.1 tiene un análogo en el anillo de polinomios modulares $K[x]_h$, sin embargo su demostración hace uso de algunos conceptos de la teoría de anillos que se exponen de manera breve a continuación.

Definición 3.1. Un *grupo* es un conjunto no vacío G dotado de una operación $*$ tal que

1. Si $a, b \in G$, entonces $a * b \in G$.
2. Dados $a, b, c \in G$, se cumple que $a * (b * c) = (a * b) * c$.
3. Existe $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$.
4. Para todo $a \in G$ existe $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$.

Definición 3.2. Un subconjunto no vacío H de un grupo G se llama *subgrupo* de G si H forma un grupo relativo a la operación de G.

En la práctica no es necesario probar los cuatro axiomas de un grupo en el subconjunto H para demostrar que éste es un subgrupo, dado que la asociatividad se da en cualquier subconjunto del grupo; además, la cerradura en H junto con la existencia del inverso para todo elemento de H garantizan la presencia de la identidad en H. Por lo tanto, para probar que un subconjunto no vacío $H \subset G$ es un subgrupo de G basta con verificar que se cumplen 2 y 4 de la Definición 3.1 dentro de H con respecto a la operación del grupo [5].

Definición 3.3. Un *anillo* es un conjunto no vacío R dotado de dos operaciones $+$ y $\cdot$ tales que

1. Si $a, b \in R$, entonces $a + b \in R$.
2. Dados $a, b, c \in R$, se cumple que $a + (b + c) = (a + b) + c$.
3. $a + b = b + a$ para $a, b \in R$.
4. Existe $e \in R$ tal que $a + e = a$ para todo $a \in R$.
5. Para todo $a \in R$ existe $b \in R$ tal que $a + b = e$; b se expresará como $-a$.
6. Si $a, b \in R$, entonces $a \cdot b \in R$.
7. Dados $a, b, c \in R$, se cumple que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
8. Dados $a, b, c \in R$, se cumple $a \cdot (b + c) = a \cdot b + a \cdot c$.
9. Dados $a, b, c \in R$, se cumple $(a + b) \cdot c = a \cdot c + b \cdot c$.

Definición 3.4. Sea R un anillo. Un subconjunto no vacío I de R es un *ideal* de R si

1. I es un subgrupo aditivo de R.
2. Dados $r \in R$, $a \in I$, se tiene que $ra \in I$ y $ar \in I$.

Si K es un campo, es posible formar el anillo de polinomios en x sobre K, expresado como $K[x]$; éste será el conjunto de todos los $p(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$, donde los a_i están en K. La igualdad, adición y producto de polinomios se define como de costumbre.

Definición 3.5. $f(x) \in K[x]$ es un *polinomio mónico* si el coeficiente de su potencia más alta es 1.

Definición 3.6. El *máximo común divisor* de $f_1(x), f_2(x), \ldots, f_n(x) \in K[x]$ se define como el polinomio mónico $d(x) \in K[x]$ tal que

1. $d(x) | f_i(x)$ para cada $i = 1, 2, \ldots, n$.
2. Si $h(x) | f_i(x)$ para cada $i = 1, 2, \ldots, n$, entonces $h(x) | d(x)$.

Por último, se prueba el teorema de existencia del máximo común divisor de polinomios en $K[x]$, que además proporciona la forma de éste. El resultado análogo al Teorema 3.1 será un corolario del siguiente.

Teorema 3.4. *Dados $f_1(x), f_2(x), \ldots, f_n(x) \in K[x]$ no todos cero, su máximo común divisor $d(x) \in K[x]$ existe y además $d(x) = a_1(x)f_1(x) + a_2(x)f_2(x) + \ldots + a_n(x)f_n(x)$ para $a_i(x) \in K[x]$, $i = 1, 2, \ldots, n$, adecuados.*

Demostración. Sea I el conjunto de todos los $r_1(x)f_1(x) + r_2(x)f_2(x) + \ldots + r_n(x)f_n(x)$, con $r_i(x)$, $i = 1, 2, \ldots, n$, variando en $K[x]$. Se tiene que I es un ideal de $K[x]$, puesto que

$$(r_1(x)f_1(x) + \ldots + r_n(x)f_n(x)) + (s_1(x)f_1(x) + \ldots + s_n(x)f_n(x)) =$$

$$(r_1(x) + s_1(x))f_1(x) + \ldots + (r_n(x) + s_n(x))f_n(x)\,,$$

y evidentemente existe el inverso de cada elemento de I en el mismo conjunto, por lo que I es un subgrupo aditivo de $K[x]$. Ahora se toma $t(x) \in K[x]$ y entonces

$$t(x)(r_1(x)f_1(x) + \ldots + r_n(x)f_n(x)) = (t(x)r_1(x))f_1(x) + \ldots + (t(x)r_n(x))f_n(x)$$

el cual sigue en I, lo cual dice que I es un ideal de $K[x]$. Además $I \neq 0$ ya que al menos uno de los $f_i(x)$ es distinto de cero. Entonces I consiste de los múltiplos de un polinomio mónico $d(x)$ por los elementos de $K[x]$; esto gracias a una consecuencia del algoritmo euclidiano para polinomios. Dado que $f_i(x)$, $i = 1, 2, \ldots, n$, están en I, deben ser múltiplos de $d(x)$ por elementos de $K[x]$, por lo que $d(x)|f_i(x)$ para cada $i = 1, 2, \ldots, n$.

Finalmente, como $d(x) \in I$, debe poder expresarse como

$$d(x) = a_1(x)f_1(x) + a_2(x)f_2(x) + \ldots + a_n(x)f_n(x)$$

para $a_i(x) \in K[x]$, $i = 1, 2, \ldots, n$, adecuados. Entonces si $h(x)|f_i(x)$ para $i = 1, 2, \ldots, n$, se tiene que $h(x)|a_1(x)f_1(x) + a_2(x)f_2(x) + \ldots + a_n(x)f_n(x) = d(x)$. Esto demuestra que $d(x)$ es el máximo común divisor de los polinomios dados [5]. □

Corolario 3.5. *Si el máximo común divisor de $f_1(x), f_2(x), \ldots, f_n(x) \in K[x]$ (no todos cero) es $1 \in K[x]$, entonces existen $b_1(x), b_2(x), \ldots, b_n(x) \in K[x]$ tales que*

$$1 = b_1(x)f_1(x) + b_2(x)f_2(x) + \ldots + b_n(x)f_n(x)\,.$$

Demostración. Basta con poner $d(x) = 1$ en el Teorema 3.4 para obtener el resultado. □

3.2. Base Espectral para el Anillo Modular $\mathbb{Z}_h$

Después de probar el Teorema 3.5, el siguiente paso es definir el concepto de base espectral, y esto se hará en el contexto de los anillos modulares $\mathbb{Z}_h$, para después extender esta idea al caso de los anillos de polinomios modulares en la siguiente sección.

Sea $h \in \mathbb{N}$ y fórmese el anillo $\mathbb{Z}$ módulo h: $\mathbb{Z}_h = \{0, 1, \ldots, h-1\}$, con la adición y multiplicación definidas módulo h. Así, en lo que resta de esta sección, $a + b \equiv c\ mod(h)$ y $ab \equiv c\ mod(h)$ se escribirán como $a + b = c$ y $ab = c$ en Z_h respectivamente. Naturalmente, todo número en Z_h representa una clase de equivalencia módulo h.

Por otra parte, el teorema de factorización única en números primos garantiza que h puede escribirse en la forma $h = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$, donde $p_1, \dots, p_r$ son números primos. Ahora se definen $h_i := h/p_i^{m_i}$ para $i = 1, 2, \dots, r$. Por su definición, es claro que el máximo común divisor de los h_i es 1, por lo que es posible aplicar el Teorema 3.1 y así obtener

$$b_1 h_1 + b_2 h_2 + \ldots + b_r h_r = 1$$

en $\mathbb{Z}_h$ para $b_1, b_2, \dots, b_r$ enteros. Lo siguiente es definir los números $s_i := b_i h_i$ y $q_i := p_i s_i$, $i = 1, 2, \dots, r$, todos en $\mathbb{Z}_h$, y entonces se dice que la *Base Espectral Completa* de $\mathbb{Z}_h$, denotada por $csb(\mathbb{Z}_h)$, es

$$csb(\mathbb{Z}_h) := \left\{ s_1, q_1, \dots, q_1^{m_1-1}, s_2, q_2, \dots, q_2^{m_2-1}, \dots, s_r, q_r, \dots, q_r^{m_r-1} \right\} .$$

En el siguiente teorema se enuncian algunas de las propiedades de los elementos de $csb(\mathbb{Z}_h)$, [9], [10].

Teorema 3.6. *Se cumplen las siguientes relaciones en* $\mathbb{Z}_h$*:*

1. $s_1 + s_2 + \ldots + s_r = 1.$
2. $s_i \cdot s_j = 0 \qquad$ *para* $i \neq j.$
3. $s_i^2 = s_i \qquad$ *para* $i = 1, 2, \dots, r.$
4. $q_i^{m_i} = 0, \quad q_i^{m_i-1} \neq 0 \qquad$ *para* $i = 1, 2, \dots, r.$
5. $q_i s_i = q_i \qquad$ *para* $i = 1, 2, \dots, r.$

Demostración. La propiedad 1 se sigue inmediatamente de la ecuación 3.1 y de la definición de s_i. Para probar la propiedad 2, basta calcular directamente el producto

$$s_i \cdot s_j = b_i h_i \cdot b_j h_j = b_i b_j (h/p_i^{m_i})(h/p_j^{m_j}) = b_i b_j (h/p_i^{m_i} p_j^{m_j}) \cdot h = 0 .$$

Por otro lado, si se multiplica la expresión en 1 de ambos lados por s_i, se tiene

$$\begin{aligned} & s_i(s_1 + s_2 + \ldots + s_r) = 1(s_i) \\ & s_1 s_i + s_2 s_i + \ldots + s_i^2 + \ldots + s_r s_i = s_i \\ & s_i^2 = s_i \end{aligned}$$

en virtud de la propiedad 2. La primera parte de la propiedad 4 es directa:

$$q_i^{m_i} = p_i^{m_i} s_i^{m_i} = p_i^{m_i} s_i = p_i^{m_i} b_i h_i = b_i \cdot h = 0 ,$$

mientras que para la segunda el procedimiento es similar al empleado con la propiedad 2, es decir,

$$q_i^{m_i-1}(s_1 + s_2 + \ldots + s_r) = q_i^{m_i-1} \quad \Rightarrow \quad 0 \neq q_i^{m_i-1} s_i = q_i^{m_i-1} .$$

Finalmente, para la propiedad 5 se tiene que

$$\begin{aligned} &q_i(s_1 + s_2 + \ldots + s_r) = q_i \\ &p_i s_i(s_1 + s_2 + \ldots + s_r) = q_i \\ &p_i s_i s_i = q_i \\ &q_i s_i = q_i \end{aligned}$$

y con esto queda completa la demostración. □

Las propiedades 1, 2 y 3 dicen que los s_i son idempotentes que se anulan dos a dos y que conforman una partición de la unidad, mientras que 4 y 5 indican que los q_i son nilpotentes con índice de nilpotencia m_i [9].

Ahora supóngase que $x \in \mathbb{Z}_h$; multiplicando ambos lados de la igualdad 1 del Teorema 3.6 por x resulta que

$$x = x_1 s_1 + x_2 s_2 + \ldots + x_r s_r \,, \tag{3.2}$$

donde $x_i \equiv x \; mod(p_i^{m_i})$.

Por último, empleando las propiedades del Teorema 3.6 es posible encontrar fácilmente los valores de los idempotentes s_i. Tan sólo hay que multiplicar por h_i en ambos lados de la expresión en 1 para obtener $h_i s_i = h_i$ en $\mathbb{Z}_h$, de donde

$$s_i = (h_i^{-1} \; mod \; p_i^{m_i}) h_i$$

para $i = 1, 2, \ldots, r$. Resulta claro que conociendo los valores de los s_i no existe mayor problema en calcular los nilpotentes q_i y sus potencias.

Ejemplo 3.1. Sea $h = 450 = 2 \cdot 3^2 \cdot 5^2$, y fórmese el anillo modular $\mathbb{Z}_{450}$, del cual se calculará la base espectral. Entonces $p_1 = 2$, $p_2 = 3$ y $p_3 = 5$, y por la definición se tiene que $h_1 = 225$, $h_2 = 50$ y $h_3 = 18$. Ahora se usa la igualdad 1 del Teorema 3.6 y se multiplica por h_1 de ambos lados para obtener

$$225 s_1 \; mod \; 2 = 225 \qquad \Rightarrow \qquad s_1 = 225.$$

En seguida se repite el proceso para h_2:

$$50 s_2 \; mod \; 3^2 = 50 \qquad \Rightarrow \qquad 5 s_2 = 50 \,,$$

y ahora se multiplica la ecuación anterior por el inverso de 5 módulo 9; así, $s_2 = 100$.

Finalmente se hace lo mismo para h_3 y entonces

$$18 s_3 \; mod \; 5^2 = 18 \qquad \Rightarrow \qquad s_3 = 126.$$

La suma $s_1 + s_2 + s_3 = 451$, pero como se está trabajando módulo 450 el resultado es 1. Debido a las potencias de los p_i en la factorización de h, sólo hay q_2 y q_3, que se calculan por medio de su definición:

$$s_2 p_2 = q_2 = 300 \; mod \; 450 = 300 \,; \qquad s_3 p_3 = q_3 = 630 \; mod \; 450 = 180 \,.$$

En vista de lo anterior, la Base Espectral Completa de $\mathbb{Z}_{450}$ es

$$csb(\mathbb{Z}_{450}) := \{s_1, s_2, q_2, s_3, q_3\} = \{225, 100, 300, 126, 180\}$$

3.3. Base Espectral para el Anillo Polinomial $K[x]_h$

El caso de los anillos de polinomios modulares es análogo al de los enteros módulo h. Ahora se toma un polinomio $h \equiv h(x)$ de grado m sobre un campo arbitrario K y se forma el anillo polinomial modular $K[x]_h := K[x] / < h(x) >$. Entonces las operaciones de adición y producto de polinomios se hacen módulo $h(x)$ mediante el algoritmo de la división de polinomios, el cual dice que para $f(x), g(x) \in K[x]_h$ se tiene que

$$f(x) \cdot g(x) = q(x)h(x) + r(x)\,,$$

donde $r(x)$ es idénticamente cero o de grado menor que $h(x)$. Así, el producto de dos polinomios módulo $h(x)$ es simplemente $r(x)$.

Bajo la adición, $K[x]_h$ posee la estructura de un espacio vectorial de dimensión m, y una base para $K[x]_h$ es $\{1, x, x^2, \ldots, x^{m-1}\}$, conocida como base estándar. Así, todo polinomio $f(x) \in K[x]_h$ puede expresarse mediante una combinación lineal de los elementos de la base estándar. La base espectral que se está buscando pretende servir el mismo propósito, cambiando la sencillez de los miembros de la base estándar por otras propiedades que serán de utilidad para simplificar diferentes aspectos.

Por el teorema de factorización de polinomios, $h(x)$ puede escribirse en la forma

$$h(x) = (x - x_1)^{m_1}(x - x_2)^{m_2} \cdots (x - x_r)^{m_r}\,,$$

y haciendo $p_i^{m_i} = (x - x_i)^{m_i}$, la expresión resultante es

$$h(x) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}\,.$$

Es evidente que, dado que $x_i \neq x_j$ para $i \neq j$, cada $p_i^{m_i}$ es un factor primo de $h(x)$. Así, se definen los polinomios $h_i := h/p_i^{m_i}$, los cuales tienen como máximo común divisor al $1 \in K[x]$; de esta manera, se puede emplear el Corolario 3.5 para afirmar que existen polinomios $b_i(x) \in K[x]$, $i = 1, 2, \ldots, r$, tales que se cumple

$$b_1(x)h_1(x) + b_2(x)h_2(x) + \ldots + b_r(x)h_r(x) = 1 \tag{3.3}$$

en $K[x]_h$. Siguiendo con el esquema desarrollado en la Sección 3.2, se definen los polinomios $s_i(x) := b_i(x)h_i(x) \in K[x]_h$ y $q_i(x) := (x - x_i)s_i(x) = p_i s_i(x) \in K[x]_h$ para $i = 1, 2, \ldots, r$. La *Base Espectral Completa* de $K[x]_h$, denotada por $csb(K[x]_h)$, es

$$csb(K[x]_h) := \left\{s_1, q_1, \ldots, q_1^{m_1-1}, s_2, q_2, \ldots, q_2^{m_2-1}, \ldots, s_r, q_r, \ldots, q_r^{m_r-1}\right\}\,. \tag{3.4}$$

Los polinomios $s_i(x)$ y $q_i(x)$ en $K[x]_h$ mantienen las mismas propiedades enunciadas en el Teorema 3.6 que los números s_i y q_i en $\mathbb{Z}_h$ respectivamente, por lo que los $s_i(x)$ son idempotentes que se anulan dos a dos y que conforman una partición de la unidad, mientras que los $p_i(x)$ son nilpotentes con índice de nilpotencia m_i.

Hay dos expresiones importantes que se obtienen mediante el uso de la base espectral en $K[x]_h$. En primer lugar, si se multiplica la ecuación 3.3 de ambos lados por $f(x) \in K[x]_h$, resulta que

$$f(x) = f_1(x)s_1(x) + f_2(x)s_2(x) + \ldots + f_r(x)s_r(x) = \sum_{i=1}^{r} f_i(x)s_i(x)\,, \tag{3.5}$$

donde $f_i(x) \equiv f(x)\ mod\ (x-x_i)^{m_i}$. Estos $f_i(x)$ son los primeros m_i términos de la expansión de Taylor de $f(x)$ alrededor de $x = x_i$, puesto que a partir del término m_{i+1} todos serán cero módulo $(x - x_i)^{m_i}$, entonces lo que se está haciendo mediante esta representación de $f(x)$ empleando la base espectral del anillo es simplemente expandir la función en su serie de Taylor alrededor de las distintas raíces de $h(x)$.

La otra expresión relevante es la llamada *Descomposición Espectral Generalizada*, la cual se obtiene empleando la ecuación 3.5 y la definición de los nilpotentes $q_i(x)$. Así, basta con tomar $f(x) = x \in K[x]_h$ y posteriormente usar 3.5, con lo que

$$x = \sum_{i=1}^{r}((x - x_i) + x_i)s_i(x) = \sum_{i=1}^{r}(x_i + q_i(x))s_i(x)\,, \tag{3.6}$$

donde $x_i \equiv x\ mod\ (x - x_i)^{m_i}$.

Finalmente se añade que, igual que en el caso de $\mathbb{Z}_h$, los idempotentes $s_i(x)$ se encuentran multiplicando la ecuación 3.3 de ambos lados por $h_i(x)$ y empleando las propiedades de $s_i(x)$:

$$h_i(x)s_i(x) = h_i(x)\,,$$

de donde $s_i(x) = \left[h_i^{-1}(x)\ mod\ (x - x_i)^{m_i}\right] h_i(x)$ para $i = 1, 2, \ldots, r$, [9].

Ejemplo 3.2. Se desea encontrar la base espectral para el anillo polinomial modular $K[x]_h$, donde $K = \mathbb{R}$ y $h(x) = (x-1)^2(x-4)^2(x-9)^2$. Entonces $p_1(x) = (x-1)$, $p_2(x) = (x-4)$ y $p_3(x) = (x-9)$, y por otra parte $h_1(x) = (x-4)^2(x-9)^2$, $h_2(x) = (x-1)^2(x-9)^2$ y $h_3(x) = (x-1)^2(x-4)^2$.

Siguiendo el método del Ejemplo 3.1, se toma $s_1(x) + s_2(x) + s_3(x) = 1$ y se multiplica de ambos lados por $h_1(x)$, con lo que se consigue la igualdad $h_1(x)s_1(x) = h_1(x)$; hay que recordar que el miembro izquierdo está en módulo $(x-1)^2$ y el derecho es en módulo $h(x)$. Entonces

$$(x-4)^2(x-9)^2 s_1(x) = (x-4)^2(x-9)^2\,.$$

Se puede simplificar el miembro izquierdo de la ecuación anterior escribiendo los términos de manera conveniente para aprovechar el hecho de que se trabaja módulo $(x-1)^2$ y varios términos se eliminarán:

$$\begin{aligned}
[(x-1)-3]^2[(x-1)-8]^2 s_1(x) &= (x-4)^2(x-9)^2 \\
[-6(x-1)+9][-16(x-1)+64]s_1(x) &= (x-4)^2(x-9)^2 \\
[-528(x-1)+576]s_1(x) &= (x-4)^2(x-9)^2 \\
-331776 s_1(x) &= (x-4)^2(x-9)^2[-528(x-1)-576]
\end{aligned}$$

y finalmente

$$s_1(x) = \frac{(x-4)^2(x-9)^2(11x+1)}{6912}\,.$$

La forma de encontrar $s_2(x)$ y $s_3(x)$ es análoga al procedimiento anterior, y los cálculos arrojan que

$$s_2(x) = -\frac{(x-1)^2(x-9)^2(4x-31)}{3375}$$

y

$$s_3(x) = -\frac{(x-1)^2(x-4)^2(13x-137)}{32000}\,.$$

Calcular los nilpotentes $q_i(x)$ es fácil después de haber obtenido los $s_i(x)$. Tan solo basta multiplicar $s_i(x)$ por $p_i(x)$ módulo $h(x)$; por ejemplo,

$$\begin{aligned}
q_1(x) = p_1(x)s_1(x) &= \frac{(x-4)^2(x-9)^2(11x+1)(x-1)}{6912} \\
&= \frac{(x-4)^2(x-9)^2(x-1)[11(x-1)+12]}{6912} = \frac{(x-4)^2(x-9)^2(x-1)}{576}\,.
\end{aligned}$$

Similiarmente,

$$q_2(x) = \frac{(x-1)^2(x-9)^2(x-4)}{225}$$

y

$$q_3(x) = \frac{(x-1)^2(x-4)^2(x-9)}{1600}\,.$$