Polinomios (parte 2)

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Segundo cuatrimestre de 2020

Reapaso de la clase anterior

En la clase anterior vimos como sumar, restar y multiplicar polinomios.

Más formalmente: Vimos que si A es un anillo conmutativo (un lugar donde podemos sumar, restar y multiplicar con las reglas usuales), los polinomios en una indeterminada X con coeficientes en A forman otro anillo conmutativo $A[X]$.

Por ejemplo, podemos tomar $A = \mathbb{Z}$ (enteros), $A = \mathbb{Q}$ (racionales), $A = \mathbb{R}$ (reales), $A = \mathbb{C}$ (complejos), $A = \mathbb{Z}_n = Z/nZ$ (enteros módulo n).

¡En la computadora!

Operaciones con polinomios usando SageMath

```
sage: R=PolynomialRing(ZZ,"x")
sage: p=R(1+x+x^2)
sage: p.coefficients()
[1, 2, 1]
sage: p.degree()
2
sage: q=R(x^3-1)
sage: p+q
x^3 + x^2 + 2*x + 2
sage: p-q
-x^3 + x^2 + 2*x + 4
sage: p*q
x^5 + 2*x^4 + 3*x^3 - x^2 - 2*x - 3
```

El algoritmo de división para polinomios

Si repazamos como hicimos en $\mathbb{Z}$ para demostrar los resultados fundamentales, que condujeron al teorema de factorización única, veremos que en la base de la aritmética de $\mathbb{Z}$ estaba el algoritmo de división. Por ello, tiene sentido preguntarse si existirá un concepto análogo para polinomios.
Dados dos polinomios P y D con $D \neq 0$, aunque D no divida a P, podríamos preguntarnos si es posible escribirlo en la forma

$$P = QD + R$$

donde el resto es "pequeño" en relación con D. Pero dado que entre los polinomios no hay orden, utilizaremos el grado para compararlos. Este es el contenido del siguiente teorema.

El algoritmo de división para polinomios (2)

Teorema

Sea K un cuerpo. Entonces, dados polinomios $P, D \in K[X]$ con $D \neq 0$, existen únicos polinomios Q (cociente) y R (resto) de la división de polinomios de P por D, tales que

$$P = QD + R$$

y $R = 0$ (el polinomio nulo) o sino $gr(R) < gr(D)$.

División de polinomios: Un ejemplo

Dividimos a $P = X^6 - 1$ por $D = X^2 + 2X + 1$.

$$
\begin{array}{r|l}
 & x^4 - 2x^3 + 3x^2 - 4x + 5 \\
\hline
x^2 + 2x + 1 & x^6 - 1 \\
 & -x^6 - 2x^5 - x^4 \\
\cline{2-2}
 & \quad -2x^5 - x^4 \\
 & \quad 2x^5 + 4x^4 + 2x^3 \\
\cline{2-2}
 & \qquad 3x^4 + 2x^3 \\
 & \qquad -3x^4 - 6x^3 - 3x^2 \\
\cline{2-2}
 & \qquad\quad -4x^3 - 3x^2 \\
 & \qquad\quad 4x^3 + 8x^2 + 4x \\
\cline{2-2}
 & \qquad\qquad 5x^2 + 4x - 1 \\
 & \qquad\qquad -5x^2 - 10x - 5 \\
\cline{2-2}
 & \qquad\qquad\quad -6x - 6
\end{array}
$$

¡En la computadora!

La función quo_rem en Sagemath nos permite obtener el cociente y el resto (*quotient and remainder*) en una división de polinomios

División de polinomios usando SageMath

```
sage: R=PolynomialRing(ZZ,"x")
sage: p=R(x^6-1)
sage: d=R(x^2+2*x+1)
sage: p.quo_rem(d)
(x^4 - 2*x^3 + 3*x^2 - 4*x + 5, -6*x - 6)
```

Demostración del algoritmo de división: Existencia (1)

Demostremos primero la existencia: Para ello, hacemos inducción en el grado del dividendo, P.
Si $P = 0$ o si $\text{gr}(P) = 0$ (polinomios contantes), claramente podemos tomar $Q = 0$, y $R = P$.
Hagamos ahora el paso inductivo: Supongamos pues que $grP = n$ y que ya hemos demostrado el teorema cuando el grado del dividendo es menor que n. Sean pues:

$$P = \sum_{i=0}^{n} a_i X^i \text{ con } a_n \neq 0 \ (\text{gr}(P) = n)$$

$$D = \sum_{j=0}^{m} b_j X^j \text{ con } b_m \neq 0 \ (\text{gr}(D) = m)$$

Nuevamente si $n < m$, podemos tomar $Q = 0$ y $R = P$.

Demostración del algoritmo de división: Existencia (2)

Supongamos pues que $n \geq m$. Entonces podemos determinar un primer cociente aproximado Q_0, dividiendo el monomio principal de P, $a_n X^n$, por el monomio principal $b_m X^m$ de Q, obteniendo:

$$Q_0 = \frac{a_n}{b_m} X^{n-m}$$

(Aquí hacemos uso de la hipótesis de que en K podemos dividir, es decir que K es un cuerpo).

Entonces, definiendo $R_0 = P - Q_0 D$, obtenemos un primer resto aproximado. Si fuera $R_0 = 0$ o $\text{gr}(R_0) < \text{gr}(D)$, hemos terminado: tomando $Q = Q_0$ y $R = R_0$ obtenemos lo que queremos.

Demostración del algoritmo de división: Existencia (3)

Si no, hemos de repetir el proceso. Para ello notamos que $\text{gr}(R_0) < \text{gr}(P)$, ya que en la forma que hemos elegido Q_0 los términos correspondientes a la potencia X^n se cancelan. Entonces, en virtud de la hipótesis de inducción, existirán Q_1 y R_1, cociente y resto respectivamente en la división de R_0 por D, de modo que:

$$R_0 = Q_1 D + R_1$$

donde $R_1 = 0$ o $\text{gr}(R_1) < \text{gr}(D)$. Entonces,

$$P = Q_0 D + R_0 = Q_0 D + Q_1 D + R_1 = (Q_0 + Q_1) D + R_1$$

Entonces tomando $R = R_1$ y $Q = Q_0 + Q_1$ obtenemos lo que queremos. Esto demuestra la parte de existencia.

Demostración del algoritmo de división: Unicidad (1)

Queda por demostrar la unicidad: Para ello supongamos que tenemos dos cocientes Q y $\tilde{Q}$, y dos restos R y $\tilde{R}$ de modo que:

$$P = QD + R \text{ y } R = 0 \text{ o } \text{gr}(R) < \text{gr}(D)$$

$$P = \tilde{Q}D + \tilde{R} \text{ y } \tilde{R} = 0 \text{ o } \text{gr}(\tilde{R}) < \text{gr}(D)$$

Entonces obtenemos que:

$$QD + R = \tilde{Q}D + \tilde{R}$$

o sea:

$$(Q - \tilde{Q})D = \tilde{R} - R$$

Si $R = \tilde{R}$ tendríamos que $(Q - \tilde{Q})D = 0$ y por lo tanto como $D \neq 0$, $Q - \tilde{Q} = 0$; o sea, $Q = \tilde{Q}$.
Hemos pues de probar que no puede suceder que $R \neq \tilde{R}$.

Demostración del algoritmo de división: Unicidad (2)

Pero si esto ocurriera sería $R - \tilde{R} \neq 0$, $Q - \tilde{Q} \neq 0$ y comparando los grados obtenemos una contradicción pues:

$$\text{gr}[(Q - \tilde{Q})D] = \text{gr}(Q - \tilde{Q}) + \text{gr}(D) \geq \text{gr}(D)$$

y por otra parte:

$$\text{gr}(\tilde{R} - R) \leq \text{máx}(\text{gr}(R), \text{gr}(\tilde{R}) < \text{gr}(D)$$

Esta contradicción provino de suponer que $R \neq \tilde{R}$. Así pues, debe ser $R = \tilde{R}$, y consecuentemente, $Q = \tilde{Q}$. Esto prueba la unicidad del cociente y el resto.

La Regla de Ruffini

Un caso importante de la división de polinomios, es la división de polinomios por polinomios de la forma $X - a$. En este caso la regla de Ruffine proporciona un esquema simplificado para efectuar la división

$$
\begin{array}{r|l}
X-3 & X^2+4X+12 \\
\hline
X^3+X^2-1 & \\
-X^3+3X^2 & \\
\hline
4X^2-1 & \\
-4X^2+12X & \\
\hline
12X-1 & \\
-12X+36 & \\
\hline
35 &
\end{array}
$$

$$
\begin{array}{c|cccc}
 & 1 & 1 & 0 & -1 \\
3 & & 3 & 12 & 36 \\
\hline
 & 1 & 4 & 12 & 35
\end{array}
$$

El teorema del resto

Teorema (Teorema del Resto)

El resto de la división de un polinomio $P \in K[X]$ por $X - a$ $(a \in K)$, coincide con el valor $P(a)$ del polinomio P especializado cuando $X = a$.

Demostración.

Diviendo P por $X - a$ lo escribimos como:

$$P(X) = Q(X) \cdot (X - a) + R$$

donde el resto R debe ser un polinomio constante. Luego, especializando esta expresión en $X = a$, obtenemos que: $P(a) = R$ □

Corolario

Sea $P \in K[X]$ un polinomio. Entonces P es divisible por $X - a$ $(a \in K)$ si y sólo si a es raíz de P.

Ejemplo

Consideremos la ecuación cúbica:

$$P(X) = X^3 - 6X^2 + 11X - 6 = 0$$

Se ve a ojo que $X = 1$, es raíz. Entonces el polinomio P será divisible (en $\mathbb{Q}[X]$) por $X - 1$. Efectuando la división de polinomios,

$$\begin{array}{c|cccc} & 1 & -6 & 11 & -6 \\ 1 & & 1 & -5 & 6 \\ \hline & 1 & -5 & 6 & 0 \end{array}$$

obtenemos la factorización:

$$P(X) = (X - 1)(X^2 - 5X + 6) = (X - 1)Q(X)$$

Entonces, para que X sea raíz de P debe ser $X - 1 = 0$ o

$$Q(X) = X^2 - 5X + 6 = 0$$

Ejemplo (continuación)

Esta es la ecuación cuadrática que resolvimos en la clase anterior, y sus raíces son $X = 2$ y $X = 3$, con lo que Q se factoriza en la forma:

$$Q(X) = (X - 2)(X - 3)$$

Por lo tanto, las raíces de P son $X = 1$, $X = 2$ y $X = 3$, y su factorización es:

$$P(X) = (X - 1)(X - 2)(X - 3)$$

Vemos que en general el corolario 1, es útil a la hora de resolver ecuaciones, porque significa que una vez que encontramos alguna raíz a del polinomio P, el problema se reduce al de resolver una ecuación de un grado menor, efectuando la división de P por $X - a$.

Otrac consecuencias

Recordamos la definición de polinomio irreducible. Que es el concepto análogo al de número primo para el anillo de polinomios $K[X]$.

Definición

Sea $P \in K[X]$ un polinomio no constante. Diremos que el polinomio P es irreducible en $K[X]$ si no es posible factorizarlo en la forma $P = Q \cdot S$ donde Q y S son polinomios en $K[X]$ no contantes.

Corolario

Si un polinomio P es irreducible en $K[X]$, no puede tener raíces en K.

Obs: ¡No vale la vuelta! El polinomio
$P = (x^2 + 1)^2 = x^4 + 2\,x^2 + 1 \in \mathbb{R}[X]$ no tiene raíces en $\mathbb{R}$ pero no es irreducible en $\mathbb{R}[X]$.

Ireducibilidad en polinomios de grado 2 y 3

Corolario

Si $P \in K[X]$ es un polinomio de grado 2 o 3, entonces P es irreducible en $K[X]$ si y sólo si P no tiene raíces en K.

Demostración.

Por el corolario anterior, basta probar la afirmación recíproca: a saber, que si P es irreducible, no puede tener raíces. Pero si tuviéramos que $P = RS$ con R, S no constantes, entonces alguno de los factores R o S sería de primer grado (pues $\mathrm{gr}(P) = \mathrm{gr}(R) + \mathrm{gr}(S)$), y entonces P tendría una raíz. □

Consideremos el polinomio $P(X) = X^3 - 2 \in \mathbb{Q}[X]$. Como $\sqrt[3]{2}$ son irracionales, P no tiene raíces en $\mathbb{Q}$. Luego es irreducible en $\mathbb{Q}[X]$.

Otras consecuencias

Razonando inductivamente (por inducción en r) podemos demostrar lo siguiente:

Corolario

Si $P \in K[X]$ es un polinomio, y $\alpha_1, \alpha_2, \ldots, \alpha_r$ son raíces distintas de P, entonces P admite la factorización siguiente:

$$P(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_r)Q(X)$$

Comparando los grados de ambos miembros en esta ecuación, obtenemos la siguiente consecuencia importante:

Corolario

Si K es un cuerpo y $P \in K[X]$ es un polinomio de grado n, P no puede tener más de n raíces en K.

Igualdad como funciones implica igualdad como polinomios si el cuerpo es infinito

de aquí deducimos en particular

Corolario

Si K es un cuerpo infinito, y $P, Q \in K[X]$ son dos polinomios que originan la misma función polinómica ($f_P = f_Q$ o sea $P(a) = Q(a)$ para todo $a \in K$), entonces son iguales.

Pues en efecto, $P - Q$ debe anularse para todo los elementos de K, y como K es infinito, por el corolario anterior; esto sólo puede suceder si $P - Q$ es el polinomio nulo. Es decir si $P = Q$.

Factorización de un polinomio con tantas raices cono su grado

Corolario

Si K es un cuerpo, y $P \in K[X]$ es un polinomio de grado n que tiene exactamente n raíces distintas $\alpha_1, \alpha_2, \ldots, \alpha_n$ en K, tenemos que:

$$P(X) = a_n(X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n)$$

siendo a_n el coenficiente principal de P (el que acompaña a X^n).

Demostración.

Comparando los grados en el corolario sobre un polinomio que tiene varias raíces, vemos que en este caso, Q debe ser de grado cero, es decir un polinomio constante. Igualnado entonces los coeficientes principales, vemos que $Q = a_n$. □

Un ejemplo con las raíces de la unidad

Volvamos a mirar el ejemplo del polinomio $P = X^n - 1 \in \mathbb{C}[X]$, cuyas raíces son las n raíces n-ésimas de la unidad:

$$\omega_k = e^{\frac{2\pi ik}{n}} \ (0 \leq k < n)$$

Entonces P admite la factorización:

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \omega_k) \tag{1}$$

Esto permite usar ideas de polinomios para resolver ejercicios sobre raíces de la unidad. Por ejemplo, haciendo la distributiva y comparando los coeficientes de X^{n-1} tenemos otra demostración de que

$$S(n) = \sum_{\omega \in G_n} \omega = \sum_{k=0}^{n-1} \omega_k = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases}$$

Un ejemplo en $\mathbb{Z}_p$

Sea p un número primo, y consideremos el polinomio $Q = X^{p-1} - 1$, sobre el cuerpo $K = \mathbb{Z}_p$. Por el teorema de Fermat, cualquier elemento no nulo de $\mathbb{Z}_p$ es una raíz de este polinomio. Deducimos que su factorizaciòn en $\mathbb{Z}_p$ es[1]

$$X^{p-1} - 1 = (X-1)(X-2)(X-3)\dots(X-(p-1)) \quad \text{en } \mathbb{Z}_p[X]$$

Comparando los términos independientes se otra demostración de una de las implicaciones del teorema de Wilson:

$$(p-1)! \equiv -1 \pmod{p}$$

[1] Para simplificar la notación, escribirmos aquí por ejemplo 3 y no $\overline{3}$, pero recordamos que los elementos de $\mathbb{Z}_p$ no son enteros, sino clases de enteros congruéntes módulo p

Máximo común divisor

Como en el anillo de polinomios $K[X]$, tenemos un algoritmo de división, podemos extender a los polinomios el algoritmo de Euclides para el cálculo del máximo común divisor. Comenzamos definiendo esta noción, por analogía con la caracterización del máximo común divisor que teníamos en los enteros:

Definición

Sean A, B dos polinomios en $K[X]$. Diremos que un polinomio $D \in K[X]$ es un máximo común divisor entre A y B, si cumple las siguientes condiciones:

i) *D es un divisor común de A y B, es decir $D|A$ y $D|B$.*

ii) *Si $\tilde{D}$ es otro divisor común de A y B, o sea $\tilde{D}|A$ y $\tilde{D}|B$ entonces $\tilde{D}|D$.*

Estas condiciones no determinan unívocamente al máximo común divisor, ya que si D y $\tilde{D}$ son dos máximo comunes divisores entre A y B, lo mejor que podemos decir es que se dividen recíprocamente, o sea $D|\tilde{D}$ y $\tilde{D}|\tilde{D}$, y por lo tanto difieren en una constante no nula de K como factor.

Máximo común divisor (2)

Ejemplo: Consideremos (en $\mathbb{Q}[X]$) los polinomios

$$A(X) = (X-1)(X-2) = X^2 - 3X + 2$$

$$B(X) = (X-1)(X-3) = X^2 - 4X + 3$$

entonces $D = X - 1$ es un máximo común divisor entre A y B, pero $\tilde{D} = 2X - 2 = 2(X-1)$ es otro.

Para eliminar esta ambigüedad, a veces se requiere una condición adicional:

iii) D es mónico

Si pedimos esta condición, el máximo común divisor (si existe, lo cual vamos a ver que siempre ocurre) queda unívocamente determinado.

El algoritmo de Euclides

Ahora podemos enunciar el algoritmo de Euclides, en completa analogía con la aritmética de $\mathbb{Z}$. Dados dos polinomios $A, B \in K[X]$ (y supongamos que $\text{gr}(A) \geq \text{gr}(B)$), para hallar su máximo común divisor, se divide $R_0 = A$ por $R_1 = B$, obteniendo un primer cociente Q_1 y un primer resto R_2, de modo que[2]:

$$A = Q_1 B + R_2 \text{ donde } R_2 = 0 \text{ o } \text{gr}(R_2) < \text{gr}(B)$$

Si $R_2 \neq 0$, podemos volver a dividir $R_1 = B$ por R_2, obteniendo un nuevo cociente Q_2 y un nuevo resto R_3, de modo que se verifica:

$$B = Q_2 R_2 + R_3 \text{ donde } R_3 = 0 \text{ o } \text{gr}(R_3) < \text{gr}(R_2)$$

Mientras $R_i \neq 0$ podemos continuar este proceso (inductivamente), dividimos a R_{i-1} por R_i obteniendo un nuevo cociente Q_i y un nuevo resto R_{i+1},

$$R_{i-1} = Q_i R_i + R_{i+1} \text{ donde } R_{i+1} = 0 \text{ o } \text{gr}(R_{i+1}) < \text{gr}(R_i)$$

[2]Utilizamos esta notación procurando ser coherentes con la que utilizamos antes al exponer el algoritmo de Euclides en los números enteros.

El algoritmo de Euclides (2)

Dado que la sucesión de los restos tiene grado estrictamente decreciente:

$$\mathrm{gr}(A) \geq \mathrm{gr}(B) > \mathrm{gr}(R_2) > \ldots > \mathrm{gr}(R_i) > \mathrm{gr}(R_{i+1}) > \ldots$$

y que los grados son enteros, en virtud del principio del mínimo entero, tarde o temprano debemos tener que $R_n = 0$, es decir que el algoritmo de Euclides termina después de un número finito de pasos. Cuando esto ocurre, podemos demostrar (repitiendo exactamente la cuenta que hicimos para la aritmética de $\mathbb{Z}$), que $R_{n-1} = \mathrm{mcd}(A, B)$,

El algoritmo de Euclides (3)

Además exactamente igual que en los enteros, se obtiene el teorema siguiente:

Teorema

Sean $A, B \in K[X]$ dos polinomios. Entonces su máximo común divisor $D = mcd(A, B)$ siempre existe, y se puede calcular utilizando el algoritmo de Euclides. Además, existen polinomios $\alpha, \beta \in K[X]$ tales que:

$$\alpha A + \beta B = D$$

Es decir que el máximo común divisor se escribe como una combinación lineal de A y B, pero los coeficientes α y β no son ahora números sino polinomios.

Un ejemplo

Calculemos el máximo común divisor entre $A = X^5 - 1$ y $B = X^3 - 1$.
Comenzamos dividiendo A por B:

$$X^5 - 1 = X^2(X^3 - 1) + (X^2 - 1)$$

luego $Q_1 = X^2$, $R_2 = X^2 - 1$. Ahora dividimos a B por R_2:

$$X^3 - 1 = X(X^2 - 1) + (X - 1)$$

luego $Q_2 = X$, $R_3 = X - 1$. Finalmente, dividimos a R_2 por R_3:

$$X^2 - 1 = (X + 1)(X - 1)$$

luego $Q_3 = X + 1$ y $R_3 = 0$. En consecuencia, en este caso
$D = \text{mcd}(A, B) = X - 1$

Un ejemplo (2)

Para encontrar los coeficientes α, β tales que $\alpha A + \beta B = D$, procedemos como sigue; de las ecuaciones anteriores obtenemos que:

$$D = (X - 1) = 1 \cdot (X^3 - 1) + (-X) \cdot (X^2 - 1)$$

pero

$$X^2 - 1 = 1 \cdot (X^5 - 1) + (-X^2) \cdot (X^3 - 1)$$

Sustituyendo:

$$X - 1 = 1(X^3 - 1) + (-X)\left[1 \cdot (X^5 - 1) + (-X^2) \cdot (X^3 - 1)\right]$$

$$= (-X) \cdot (X^5 - 1) + (X^3 + 1) \cdot (X^3 - 1)$$

Luego $\alpha(X) = -X$ y $\beta(X) = X^3 + 1$.

El método matricial

Usando un programita en Sagemath

```
sage: Euclides_matricial_con_polinomios(x^5-1,x^3-1)
paso  0
[      1         0 x^5 - 1]
[      0         1 x^3 - 1]
paso  1
[      1     -x^2 x^2 - 1]
[      0         1 x^3 - 1]
paso  2
[      1     -x^2 x^2 - 1]
[     -x x^3 + 1   x - 1]
paso  3
[     x^2 + x + 1     -x^4 - x^3 - x^2 - x - 1    0     ]
[     -x                x^3 + 1                   x - 1]
(-x, x^3 + 1, x - 1)
```

Máximo común divisor y raíces en común

Observación

Sean $A, B \in K[X]$ y $D = mcd(A, B)$ su máximo común divisor. Entonces $a \in K$ es una raíz en común de A y B, si y sólo si a es raíz de D.

Demostración.

Por el corolario 1, a es raíz de D si y sólo sí $X - a$ divide a D, lo cual ocurre si y sólo si $X - a$ divide simultáneamente a A y B, lo cual a su vez sucede si y sólo si a es raíz de ambos polinomios. □

Ejemplo: En el ejemplo anterior vimos que $\text{mcd}(X^3 - 1, X^5 - 1) = X - 1$, esto significa precisamente que 1 es la única raíz en común entre estos polinomios (ya que $G_3 \cap G_5 = \{1\}$).

Ejercicio: Probar que en general

$$\text{mcd}(X^n - 1, X^m - 1) = X^d - 1$$

donde $d = \text{mcd}(n, m)$ (en $\mathbb{Z}$)

Polinomios coprimos

Definición

Dos polinomios $P, Q \in K[X]$ se dicen coprimos si $mcd(P, Q) = 1$. En otras palabras: si los únicos divisores comunes de P y Q son los polinomios constantes.

Corolario

Sean $P, Q, R \in K[X]$. Si $P|QR$ y P es coprimo con Q, entonces $P|R$.

Corolario

Sean $P, Q, R \in K[X]$. Si $P|QR$ y P es irreducible en $K[X]$, entonces $P|Q$ o $P|R$.

Teorema de factorización única como producto de irreducibles

Entonces, podemos obtener (imitando el razonamiento que hicimos en los enteros), el siguiente teorema de factorización única:

Teorema

Cada polinomio $P \in K[X]$ se puede factorizar de manera única en la forma:

$$P = kP_1P_2 \cdots P_r$$

siendo k una constante no nula de K, y los P_i polinomios irreducibles en $K[X]$.
La factorización es única en el sentido de que cualquier otra factorización sólo puede diferir en el orden de los factores, en el valor de la constante k y en la multiplicación de alguno de los factores P_i por una constante no nula de K (ajustando adecuadamente el valor de la constante k).