117 Problemas de Polinomios del Programa de Verano AwesomeMath

Titu Adreescu, Navide Safei y Alessandro Ventullo

Traducido del inglés por Kenny J. Tinoco

Managua, 2023

Índice general

Capítulo 1

Propiedades básicas de los polinomios - Parte I

Un *polinomio* es una expresión de la forma

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i.$$

Los números a_i se dicen *coeficientes* del polinomio $P(x)$. Usualmente, consideramos a_i, en $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y decimos que el polinomio tiene coeficientes enteros, racionales, reales o complejos, respectivamente. Denotamos por $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ el conjunto de polinomios con coeficientes enteros, racionales, reales o complejos, respectivamente.

El coeficiente a_0 se dice el *término constante*. Por la definición, se sigue que dos polinomios

$$P(x) = \sum_{i=0}^{n} a_i x^i \quad \text{y} \quad Q(x) = \sum_{i=0}^{m} b_i x^i$$

son iguales si y solo si $a_i = b_i$ para todo i (si $m > n$, entonces $b_{n+1} = \ldots = b_m = 0$).

Definimos el *grado* del polinomio $P(x) = \sum_{i=0}^{n} a_i x^i$ como el mayor entero i tal que $a_i \neq 0$ y denotamos el grado por $\deg P(x)$. Si i es el mayor entero i tal que $a_i \neq 0$, decimos que a_i es el *coeficiente principal* de $P(x)$. Si el coeficiente principal es igual a 1, decimos que el polinomio es *mónico*. Observe que el grado de un polinomio constante $P(x) = a_0 \neq 0$ es cero. No damos ningún grado al *polinomio cero* $P(x) \equiv 0$ (i.e.el polinomio cuyos

coeficientes son todos ceros)[1]. Normalmente, omitimos los términos que tiene coeficiente cero. Por ejemplo, escribimos el polinomio $0x^3 + 1x^2 + 2x + 0$ como $x^2 + 2x$. Este es claramente un ejemplo de un polinomio mónico de grado 2.

Podemos realizar algunas operaciones sobre polinomios.

Por ejemplo, si $P(x) = \sum_{i=0}^{n} a_i x^i$ y $Q(x) = \sum_{i=0}^{m} b_i x^i$ son dos polinomios y $n \leq m$, entonces la suma y el producto de $P(x)$ y $Q(x)$ es definida por

$$P(x) + Q(x) = \sum_{h=0}^{m} (a_h + b_h) x^h \quad \text{y} \quad P(x)Q(x) = \sum_{h=0}^{n+m} \left(\sum_{i+j=h} a_i b_j \right) x^h,$$

respectivamente. Sabiendo lo anterior obtenemos lo siguiente.

Teorema 1.

Sea $P(x)$ y $Q(x)$ dos polinomios y sea k un entero positivo. Entonces,

1. $\deg[P(x)Q(x)] = \deg P(x) + \deg Q(x)$
2. $\deg[P(x) + Q(x)] \leq \text{máx}(\deg P(x), \deg Q(x))$
3. $\deg[P(x)^k] = k \cdot \deg P(x)$.

1.1. Identidades

El término *identidad* designa una igualdad que se cumple para todo valor permitido de las incognitas que contenga (normalmente todos los números reales o todos los números complejos). Cuando está claro por el contexto a menudo se omite especificar explícitamente el rango permitido de las incognitas. Por ejemplo, las siguientes ecuaciones son identidades:

$$\begin{aligned} a^2 - b^2 &= (a-b)(a+b), \\ a^3 - b^3 &= (a-b)(a^2 + ab + b^2), \\ (a+b+c)^2 &= a^2 + b^2 + c^2 + 2(a+b+c), \\ \frac{a^2}{a+b} + \frac{b^2}{b+c} + \frac{c^2}{c+a} &= \frac{b^2}{a+b} + \frac{c^2}{b+c} + \frac{a^2}{a+c}. \end{aligned}$$

Las primeras tres se cumplen para todos los valores reales (o complejos) a, b y c, mientras que el último solo se cumple si ninguno de los valores $a+b$, $b+c$ y $c+a$ es cero. Sin

[1] Por convección, también podemos asignar al polinomio cero el grado $-\infty$.

embargo, las ecuaciones a continuación no cumplen con este criterio, ya que no se cumplen universalmente:

$$\begin{aligned} 2x+1 &= 5, \\ \frac{1}{x-2}+\frac{1}{x} &= 3, \\ a^3+b^3+c^3 &= 3abc. \end{aligned}$$

Las identidades son los pilares de los cálculos matemáticos. Se encuentran comúnmente en las competiciones matemáticas, donde muchos problemas requieren de su conocimiento.

Aquí recopilamos algunas de las identidades más útiles. Es importante que, para mejorar tu fortaleza en el trabajo con expresiones algebraicas, te esforcés en aprender estas identidades.

Identidades útiles

(Diferencia de cuadrados)	$a^2-b^2=(a-b)(a+b)$
(Binomio al cuadrado)	$(a+b)^2=a^2+2ab+b^2$
(Trinomio al cuadrado)	$(a+b+c)^2=a^2+b^2+c^2+2(ab+bc+ca)$
(Identidad de Gauss)	$a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ca)$
(Diferencia de potencias)	$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$
(Suma de potencias)	$a^n+b^n=(a+b)(a^{n-1}-a^{n-2}b+\cdots+b^{n-1})$ con n impar
(Binomio de Newton)	$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\cdots+\binom{n}{k}a^{n-k}b^k+\cdots+b^n$

Observación 1. La *Identidad de Gauss* implica que si $a+b+c=0$, entonces $a^3+b^3+c^3=3abc$.

Observación 2. El *Binomio al cuadrado* tiene un caso general, esto es, sean x_1, x_2 , …, x_n n números, entonces

$$(x_1+\cdots+x_n)^2=x_1^2+\cdots+x_n^2+2\sum_{1\le i<j\le n}x_ix_j.$$

Por ejemplo, cuando $n=4$ tenemos

$$(a+b+c+d)^2=a^2+b^2+c^2+d^2+2(ab+ac+ad+bc+bd+cd).$$

Observación 3. El caso general del *Binomio de Newton* es de especial interés. Sean $x_1, x_2, \ldots, x_n$ n números y sea m un entero positivo, entonces

$$(x_1 + \cdots + x_n)^m = \sum_{0 \le i_1, i_2, \ldots, i_n \le m}^{i_1+i_2+\cdots+i_n=m} \binom{m}{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdot \ldots \cdot x_n^{i_n}.$$

Esta identidad es llamada *Identidad Multinomial*.

Por ejemplo, cuando $n = m = 3$ tenemos

$$(a+b+c)^3 = a^3 + b^3 + c^3 + 3(a^2b + b^2c + c^2a + b^2a + c^2b + a^2c) + 6abc.$$

Muchos problemas elementales de álgebra se simplifican enormemente con las identidades. No obstante, veremos algunas de las aplicaciones creativas en soluciones más complejas.

Ejemplo 1.1 (Olimpiada Matemática de San Petersburgo, 1999)**.** Sea $n \ge 3$ un entero positivo. Probar que n^{12} puede representarse como la suma de los cubos de tres números naturales.

Solución. Notemos que $(a-3b)^3 = a^3 - 9a^2b + 27ab^2 - 27b^3$. Multiplicando ambos lados de la ecuación por a, tenemos $a(a-3b)^3 = a^4 - 9b(a-b)^3 - 9b^4$. Ahora bien, haciendo $a = n^3$ y $b = 3m^3$, tendremos

$$n^{12} = n^3(n^3 - 9m^3)^3 + 27m^3(n^3 - 3m^3)^3 + 27m^3(3m^3)^3.$$

Esto es equivalente a

$$n^{12} = (n^4 - 9m^3n)^3 + (3mn^3 - 9m^4)^3 + (9m^4)^3. \qquad \blacksquare$$

Ejemplo 1.2 (Olimpiada Matemática de Serbia, 2012)**.** Si $x+y+z = 0$ y $x^2+y^2+z^2 = 6$, ¿cuál es el máximo valor de $|(x-y)(y-z)(z-x)|$?

Solución. Haciendo $z = -x - y$, encontramos que $2x^2 + 2xy + 2y^2 = 6$ es decir $x^2 + xy + y^2 = 3$. Asimismo, $y^2 + yz + z^2 = z^2 + zx + x^2 = 3$, así $xy + yz + zx = -3$. Ahora,

$$(x-y)^2 = x^2 - xy + y^2 - 3xy = 3 - 3xy,$$

por consiguiente,

$$[(x-y)(y-z)(z-x)]^2 = (3-3xy)(3-3yz)(3-3zx).$$

El lado derecho es igual a

$$27\left(1 - xy - yz - zx + xyz(x+y+z) - x^2y^2z^2\right) = 27(4 - x^2y^2z^2) \le 27 \cdot 4.$$

Por lo tanto, $|(x-y)(y-z)(z-x)| \le 6\sqrt{3}$. Ya que se alcanza este valor cuando $\{x, y, z\} = \{0, \sqrt{3}, -\sqrt{3}\}$, podemos decir que este es el máximo valor. $\blacksquare$

Ejemplo 1.3 (Revista Mathematics and Youth, 2003)**.** Resolver el sistema de ecuaciones

$$x^2(y+z)^2 = (3x^2+x+1)y^2z^2$$
$$y^2(z+x)^2 = (4y^2+y+1)z^2x^2$$
$$z^2(x+y)^2 = (5z^2+z+1)x^2y^2.$$

Solución. Si $x=0$, entonces las tres ecuaciones se reducen a $y^2z^2=0$ y encontramos las soluciones $(x,y,z)=(0,t,0)$ o $(0,0,t)$ para cualquier real t. Similarmente, los casos donde $y=0$ y $z=0$ añaden la otra familia de soluciones $(x,y,z)=(t,0,0)$. Ahora bien, asumamos que $xyz\neq 0$. Haciendo a $x=\frac{1}{a}$, $y=\frac{1}{b}$ y $z=\frac{1}{c}$, obtenemos el siguiente sistema de ecuaciones

$$(b+c)^2 = 3+a+a^2$$
$$(c+a)^2 = 4+b+b^2$$
$$(a+b)^2 = 5+c+c^2.$$

Al sumarlas, encontramos que $(a+b+c)^2-(a+b+c)-12=0$. Sustituimos $t=a+b+c$, y simplificar a $t^2-t-12=0$, lo que da $t=4$ o $t=-3$. Si $t=4$, entonces $a+b+c=4$ y sustituyendo en las ecuaciones anteriores, obtenemos $(4-a)^2=3+a+a^2$, es decir, $9a=13$, por tanto $x=\frac{9}{13}$. Por el mismo argumento $y=\frac{3}{4}$ y $z=\frac{9}{11}$, asi encontramos la solución $(x,y,z)=\left(\frac{9}{13},\frac{3}{4},\frac{9}{11}\right)$. Si $t=3$, entonces $a+b+c=3$, y por el mismo argumento encontramos la solución $(x,y,z)=\left(-\frac{5}{6},-1,-\frac{5}{4}\right)$. ■

Ejemplo 1.4 (Olimpiada Matemática de Bulgaria, 2008. Ivan Tonov)**.** Si la siguiente ecuación es una identidad

$$(x+y)^{2n+1}-x^{2n+1}-y^{2n+1} = xy(2n+1)(x+y)(x^2+xy+y^2)^{n-1},$$

hallar el valor de n.

Solución. Sea $x=y=1$. Entonces $2^{2n+1}-2=2(2n+1)3^{n-1}$, de este modo

$$2^{2n}-1=(2n+1)3^{n-1}.$$

Demostraremos que la igualdad no ocurre para $n>3$. Escribiendo la igualdad como

$$\left(\frac{4}{3}\right)^n = \frac{2n+1}{3}+\frac{1}{3^n}.$$

Entonces, para $n>3$ tenemos

$$\frac{2n+1}{3}+\frac{1}{3^n}=\left(\frac{4}{3}\right)^n=\left(1+\frac{1}{3}\right)^n=1+\frac{n}{3}+\frac{n(n-1)}{2\cdot 3^2}+\ldots+\frac{1}{3^n}$$

$$\frac{2n+1}{3}+\frac{1}{3^n}>1+\frac{n}{3}+\frac{n(n-1)}{2\cdot 3^2}+\frac{1}{3^n}.$$

Ahora bien,

$$\frac{2n+1}{3}>1+\frac{n}{3}+\frac{n(n-1)}{2\cdot 3^2},$$

lo que lleva a la desigualdad $n^2-7n+12=(n-3)(n-4)<0$, lo cual es falso para $n\geq 4$. Si $n\in\{1,2,3\}$, la ecuación es de hecho una identidad. ■

Nota. También podemos usar un argumento de teoría de números para refutar el caso de identidad: $2^{2n}-1=(2n+1)3^{n-1}$. Digamos que $v_3(N)$ denota el número exacto de veces que el primo 3 divide a N. Ya que $v_3(2^{2n}-1)=v_3(4^n-1)\geq n-1$, encontramos que $3^{n-2}\mid n$, lo cual es falso para $n>3$.

1.2. El coeficiente de x^d

Supongamos que buscamos calcular el coeficiente de x^{50} en el siguiente producto

$$(1+2x+3x^2+\cdots+101x^{100})(1+x+x^2+\cdots+x^{25}).$$

Para ello, es necesario estudiar de cuántas maneras un monomio del primer factor y monomio del segundo factor general el término x^{50}. Eso es

$$x^{50}=x^{50}\cdot 1=x^{49}\cdot x^1=\cdot=x^{25}\cdot x^{25}.$$

De aquí que, el coeficiente de x^{50} es la suma de los coeficientes de los monomios construidos y es igual a

$$51+50+\cdots+26=1001.$$

Ejemplo 1.5 (Navid Safaei)**.** Sea k un entero positivo tal que

$$1+x^k+x^{2k}=(1+a_1x+x^2)(1+a_2x+x^2)\cdots(1+a_kx+x^2).$$

Hallar el valor de $a_1^2+a_2^2+\cdots+a_k^2$.

Solución. Si $k=1$, entonces $a_1=1$ y valor deseado es 1. Si $k=2$, entonces

$$1+x^2+x^4=(1+a_1x+x^2)(1+a_2x+x^2).$$

Comparando los coeficientes de x^2 y x en ambos lados de la ecuación, encontramos que

$$a_1+a_2=0,\ a_1a_2=-1\quad\text{es decir}\quad a_1^2+a_2^2=(a_1+a_2)^2-2a_1a_2=2.$$

Por otra parte, podemos deducir que $\{a_1, a_2\} = \{-1, 1\}$. Por tanto,

$$1 + x^2 + x^4 = (1 - x + x^2)(1 + x + x^2).$$

Ahora, asumiendo que $k \geq 3$, entonces los coeficientes de x y x^2 en el producto

$$(1 + a_1 x + x^2)(1 + a_2 x + x^2) \cdots (1 + a_k x + x^2)$$

debe ser cero. Examinando los coeficientes antes mencionados, podemos deducir que $a_1 + \cdots + a_k = 0$ y

$$k + \sum_{1 \leq i < j \leq k} a_i a_j = 0 \quad \text{es decir} \quad \sum_{1 \leq i < j \leq k} a_i a_j = -k.$$

Por consiguiente, por la generalización del *Binomio al cuadrado*, tenemos que

$$(a_1 + \cdots + a_n)^2 = a_1^2 + \cdots + a_n^2 + 2 \sum_{1 \leq i < j \leq n} a_i a_j = 2k.$$

Por lo tanto, la respuesta es, si $k = 1$ o 2 el valor deseado es el valor de k, si $k \geq 3$ el valor es $2k$. ■

Ejemplo 1.6. Hallar el coeficiente de x^{100} en la expresión

$$(1 + x + x^2 + \cdots + x^{100})^3.$$

Solución. Notemos que

$$(1 + x + x^2 + \cdots + x^{100})^3 = (1 + x + \cdots + x^{100})(1 + x + \cdots + x^{100})(1 + x + \cdots + x^{100}).$$

De este modo, el término x^{100} debe surgir de un producto de al forma $x^a x^b x^c$ de los respectivos factores donde $a + b + c = 100$ y $a, b, c \geq 0$. Sea $a = 0$, entonces $b + c = 100$ y se tiene 101 casos. Si $a = 1$, entonces $b + c = 99$ y se tiene 100 casos. Similarmente, cuando $a = 100$, entonces $b + c = 0$ y solo se tiene un caso. Por tanto, el número total de casos es

$$1 + 2 + \cdots + 101 = 5151.$$ ■

Ejemplo 1.7 (Olimpiada Italiana de Matemáticas, 2013. Local Round. Federico Poloni)**.** Sean $P(x)$ y $Q(x)$ dos trinomios. ¿Al menos, cuántos monomios distintos de cero tiene el producto $P(x)Q(x)$?

Solución. Asumamos que $P(x) = Ax^R + Bx^S + Cx^T$ y $Q(x) = ax^r + bx^s + cx^t$ donde $A, B, C, a, b, c \neq 0$ y $R, S, T, r, s, t \geq 0$ son enteros, también $R \neq S \neq T$ y $r \neq s \neq t$. Sin perdida de generalidad, asumamos que $R > S > T$ y $r > s > t$. Entonces,

$$P(x)Q(x) = Aax^{R+r} + \cdots + Ccx^{T+t},$$

y es un producto con 9 términos. Es claro que los monomios x^{R+r} y x^{T+t} no se pueden cancelar debido a la mínimalidad y maximalidad. Es decir, el producto tiene al menos dos términos. Ahora daremos un ejemplo con exactamente dos términos, esto es, considerando el polinomio x^4+4. Si lo factorizamos, tendremos que

$$x^4+4=(x^2-2x+2)(x^2+2x+2).$$

Así, la respuesta es 2. ■

Ejemplo 1.8. Se define una familia de polinomios recursivamente por

$$\begin{aligned} P_0(x) &= x-2,\\ P_k(x) &= P_{k-1}^2(x)-2 \text{ si } k\geq 1. \end{aligned}$$

Hallar el coeficiente de x^2 en $P_k(x)$ es términos de k.

Solución. Notemos que para todo $k\geq 1$ tenemos que $P_k(0)=2$, de este modo

$$P_k(x)=2+a_kx+b_kx^2+\ldots,$$

por tanto $P_{k+1}(x)=2+a_{k+1}x+b_{k+1}x^2+\ldots=2(2+a_kx+b_kx^2+\ldots)^2-2$. Un cálculo sencillo muestra que $a_{k+1}=4a_k$ y $b_{k+1}=a_k^2+4b_k$. Ya que $a_1=-4$, encontramos que $a_k=-4^k$, entonces

$$b_k=4^{2k-2}+\ldots+4^{k-1}=4^{k-1}\left(1+4+\cdots+4^{k-1}\right)=\frac{4^{2k-1}-4^{k-1}}{3}.$$ ■

Ejemplo 1.9 (AIME, 2016)**.** Sea $P(x)=1-\frac{x}{3}+\frac{x^2}{6}$ y se define a

$$Q(x)=P(x)P(x^3)P(x^5)P(x^7)P(x^9)=\sum_{i=0}^{50}a_ix^i.$$

Hallar $\displaystyle\sum_{i=0}^{50}|a_i|$.

Solución. Notemos que todos los coeficientes del polinomio $P(-x)$ son no negativos. De hecho todos sus coeficientes son los valores absolutos de los coeficientes del polinomio $P(x)$. Así todos los coeficientes del polinomio

$$Q(x)=P(-x)P(-x^3)P(-x^5)P(-x^7)P(-x^9)$$

son no negativos y son los valores absolutos de los coeficientes del polinomio $Q(x)$. Por lo tanto,

$$\sum_{i=0}^{50}|a_i|=Q(-1)=P(-)^5=\left(\frac{3}{2}\right)^5.$$ ■

Ejemplo 1.10 (Olimpiada Rusa de Matemáticas, 2008. V. A. Senderov)**.** Hallar todos los enteros positivos n tal que existen números no negativos a, b, c, d tal que $(ax+b)^{1000} - (cx+d)^{100}$ tiene exactamente n coeficientes distintos de cero.

Solución. La respuesta es $n \in \{500, 1000, 1001\}$. De hecho para $n = 1001$ consideramos la expresión $(2x+2)^{1000} - (x+1)^{1000}$ y para $n = 1001$ consideramos la expresión $(2x+1)^{1000} - (x+1)^{1000}$. Si tenemos más de un coeficiente igual a cero entonces existen dos coeficientes, digamos los coeficientes de x^r y x^t tal que

$$a^r b^{1000-r} = c^r d^{1000-r}, \quad a^t b^{1000-t} = c^t d^{1000-t}.$$

En consecuencia,

$$\left(\frac{ad}{bc}\right)^r = \left(\frac{d}{b}\right)^{1000} = \left(\frac{ad}{bc}\right)^t, \quad \text{por tanto} \quad \left|\frac{ad}{bc}\right| = \left|\frac{d}{b}\right| = 1,$$

lo que da también $\left|\frac{a}{b}\right| = 1$.

Ahora, está claro que si remplazamos el polinomio $ax+b$ por $-ax-b$, la condición no cambia. De este modo, sin perdida de generalidad asumimos que $\frac{a}{b} = 1$ y tenemos dos casos. Si $\frac{d}{b} = 1$, entonces tenemos $(ax+b)^{1000} - (ax+b)^{1000}$ lo cuál solo da coeficientes iguales a cero, una contradicción. Si $\frac{d}{b} = -1$, entonces tenemos $(ax+b)^{1000} - (ax-b)^{1000}$, lo cual tiene exactamente 500 coeficientes distintos de cero. ■

Ejemplo 1.11 (Tournament of Towns, 2012)**.** Sea $P(0) = 1$ y

$$P(x)^2 = 1 + x + x^{100} Q(x).$$

Hallar el coeficiente de x^{99} en la expansión de $(1+P(x))^{100}$.

Solución. Notemos que la expansión de $(1+P(x))^{100} + (1-P(x))^{100}$ tenemos únicamente potencias pares de $P(x)$. En realidad, la expresión de arriba es un polinomio en $P(x)^2 = 1 + x + x^{100} Q(x)$ de grado 50. Tomando la ecuación en módulo x^{100}, el mayor coeficiente de la expresión es $2(1+x)^{50}$; de este modo no existe el término con x^{99} en la expansión. Por otra parte, ya que $P(0) = 1$ podemos encontrar que el polinomio $P(x) - 1$ es divisible por x. Por lo tanto, $(1-P(x))^{100} = x^{100} R(x)$, para algún polinomio $R(x)$, lo cual implica que no x^{99} en la expansión. En consecuencia, tampoco existe ningún x^{99} en la expansión de $(1+P(x))^{100}$. ■

Ejemplo 1.12 (Olimpiada Matemática de Moscow, 1997)**.** Sea

$$1 + x + x^2 + \ldots + x^{n-1} = F(x)G(x), \text{ donde } n > 1$$

siendo F y G polinomios cuyos coeficientes son ceros o unos. Probar que uno de los polinomios F y G puede expresarse en la forma $(1 + x + x^2 + \cdots + x^{k-1})T(x)$, donde $k > 1$ y T es también un polinomio cuyos coeficientes son ceros o unos.

Solución. Sea $F(x) = a_0 + a_1x + \cdots$ y $G(x) = b_0 + b_1x + \cdots$. Por el término constante obtenemos que $a_0b_0 = 1$ que implica $a_0 = b_0 = 1$. Por el coeficiente de x obtenemos $a_1b_0 + a_0b_1 = 1$, por lo tanto, $a_1 + b_1 = 1$. Sin perdida de generalidad, asumimos que $a_1 = 1$ y $b_1 = 0$. Si $G(x) = 1$, entonces hemos terminado, de esta manera podemos asumir que hay al menos un monomio distinto de cero en $G(x)$, digamos x^k, tal que $G(x) = 1 + x^k + \cdots$. Mirando a los coeficientes de x^i para $x = 1, 2, \ldots, k$ concluimos que $a_0 = a_1 = a_2 = \cdots = a_{k-1} = 1$ y $a_k = 0$.

Ahora mostraremos que cualquier monomio en G es de la forma x^{kr} para algún r (o en términos de polinomios $G(x) = Q(x^k)$ para algún polinomio Q con coeficientes ceros o unos) y que todo monomio distinto de cero en F ocurre en una serie de monomios distintos de cero de la forma $x^{kr} + x^{kr+1} + x^{kr+2} + \cdots + x^{kr+(k-1)}$ (o en términos de polinomios $F(x) = (1 + x + x^2 + \cdots + x^{k-1})P(x^k)$ para algún polinomio $P(x)$ con coeficientes ceros o unos). Tenga en cuenta que esto resolverá el problema haciendo $T(x) = P(x^k)$.

Supongamos, por el contrario, que este no es el caso. Entonces hay algún monomio de grado menor que falla. Hay dos maneras en lo que esto puede pasar.

Si el primer monomio malo está en G, entonces hay algún monomio x^{kr+s} en G donde $0 < s < k$. Ya que el producto $F(x)G(x)$ contiene el monomio x^{kr} debe haber un monomio x^a en F y un monomio x^b en G con $a + b = kr$. Donde $a, b < kr + s$ y el monomio x^{kr+s} el la primera desviación en nuestro patrón propuesto, resulta que $b = kr'$ para algún $r' \leq r$ y por consiguiente $a = k(r - r')$. De nuevo ya que x^{kr+s} fue el primer monomio malo, esto debe comenzar una racha de monomios $x^{k(r-r')} + x^{k(r-r')+1} + \cdots + x^{k(r-r')+(k-1)}$ en F. Pero entonces el coeficiente de x^{kr+s} en $F(x)G(x)$ obtiene una contribución de 1 desde $x^{k(r-r')+s} \cdot x^{kr'}$ y otra contribución de 1 desde $x^0 \cdot x^{kr+s}$. Ya que cualquier contribución adicional solo sería posible, el coeficiente de x^{kr+s} en el producto será al menos 2, una contradicción.

Si el primer monomio malo está en F, entonces hay algún r tal que F solo contenga un subconjunto propio de los monomios $x^{kr}, x^{kr+1}, \ldots, x^{kr+k-1}$. Digamos que contiene x^{kr+i} pero no a x^{kr+j} para algunos $0 \leq i, j < k$. El monomio x^{kr+j} debe ocurrir en $F(x)G(x)$, digamos $x^a \cdot x^b$. Puesto que la serie $x^{kr}, \ldots, x^{rk+k-1}$ contiene el monomio malo con menor grado, debemos tener $b = kr'$ para algún $1 \leq r' \leq r$ y por tanto $a = k(r - r') + j$. Como este es el menor, F debe contener la serie completa

$$x^{k(r-r')} + x^{k(r-r')+1} + \cdots + x^{k(r-r')+k-1}.$$

Ahora veamos cuántas veces el monomio x^{kr+i} aparece en $F(x)G(x)$. Este aparece una vez en $x^{k(r-r')+i} \cdot x^{kr'}$ y una vez en $x^{kr+i} \cdot x^0$. Esto es, aparece al menos dos veces, una contradicción. ■

Ejemplo 1.13 (Olimpiada Matemática de Moscow, 1994)**.** ¿Existe un polinomio $P(x)$ con un coeficiente negativo tal que para cualquier potencia $P(x)^n$ con $n > 1$ todos los coeficientes son positivos?

Solución. La respuesta es sí, Sea $P(x) = a_d x^d + \cdots + a_0$ que tiene coeficientes positivos. Entonces todas sus potencias tienen coeficientes positivos. Tomar a $f(x) = x^4 + x^3 + x + 1$ y sea $g(x) = f(x) - \epsilon x^2$ para algún $\epsilon > 0$ lo suficientemente pequeño. Entonces todos los coeficientes de $g(x)^2$ y $g(x)^3$ están cerca de los coeficientes de

$$f(x)^2 = x^9 + 2x^7 + x^6 + 2x^5 + 4x^4 + 2x^3 + x^2 + 2x + 1$$

y

$$f(x)^3 = x^{12} + 3x^{11} + 3x^{10} + 4x^9 + 9x^8 + 9x^7 + 6x^6 + 9x^5 + 9x^4 + 4x^3 + 3x^2 + 3x + 1.$$

Los coeficientes de $f(x)^2$ y $f(x)^3$ son todos positivos, por lo tanto, los coeficientes de $g(x)^2$ y $g(x)^3$ debe ser positivos. En consecuencia, ya que todos los enteros positivos n puede escribirse como $n = 2a + 3b$ para algunos enteros no negativos a, b todas las potencias $g(x)^n$ tiene solo coeficientes positivos. ■

1.3. Factorización y sus implicaciones

Factorizar una expresión algebraica significa descomponer la expresión original en un producto de expresiones con grados menores. Tenemos dos herramientas principales para esto: agrupar o usar identidades. La aplicación de la primera herramienta incluye dividir la expresión en grupos con factores comunes. Por ejemplo,

$$a^2 + ab + bc + ca = (a^2 + ab) + (ac + bc) = a(a + b) + c(a + b) = (a + c)(a + b).$$

Ejemplo 1.14. Factorizar la siguiente expresión

$$xyz + 3xy + 2xz - yz + 6x - 3y - 2z - 6.$$

Solución. Agrupamos la expresión de arriba como

$$(xyz + 3xy) + (2xz + 6x) - (yz + 3y) - (2z + 6).$$

Ahora podemos sacar el factor $z + 3$ para cada grupo,

$$(z + 3)(xy + 2x - y - 2).$$

Nuevamente, podemos agrupar la expresión $xy + 2x - y - 2$ como

$$x(y + 2) - (y + 2) = (x - 1)(y + 2).$$

Por tanto, nuestra expresión queda factorizada como

$$(x - 1)(y + 2)(z + 3).$$ ■

El segundo caso se refiere a identidades para factorizar,e.g., podemos factorizar la expresión

$$(a^2-b^2)^3+(b^2-c^2)^3+(c^2-a^2)^3.$$

Primero, notemos que $a^2-b^2+b^2-c^2+c^2-a^2=0$. Por lo tanto, por la *Identidad de Gauss*,

$$(a^2-b^2)^3+(b^2-c^2)^3+(c^2-a^2)^3=3(a^2-b^2)(b^2-c^2)(c^2-a^2).$$

Ahora por la identidad de *Diferencia de cuadrados*, encontramos que

$$3(a^2-b^2)(b^2-c^2)(c^2-a^2)=3(a-b)(b-c)(c-a)(a+b)(b+c)(c+a).$$

Ejemplo 1.15 (Revista Mathematics and Youth, 2004)**.** Resolver el sistema de ecuaciones

$$\begin{aligned} x^3+y^3&=4y^2-5y+3x+4\\ 2y^3+z^3&=4z^2-5z+6y+6\\ 3z^3+x^3&=4x^2-5x+9z+8. \end{aligned}$$

Solución. Escribamos el sistema como

$$\begin{aligned} x^3-3x-2&=-y^3+4y^2-5y+2\\ 2y^3-6y-4&=-z^3+4z^2-5z+2\\ 3z^3-9z-6&=-x^3+4x^2-5x+2. \end{aligned}$$

Ambos lados de cada ecuación puede ser factorizado, como se muestra a continuación

$$\begin{aligned} (x-2)(x+1)^2&=(2-y)(y-1)^2\\ 2(y-2)(y+1)^2&=(2-z)(z-1)^2\\ 3(z-2)(z+1)^2&=(2-x)(x-1)^2 \end{aligned}$$

Ahora, si $x=2$, entonces $y=2$ o $y=1$. Si $y=2$, entonces para la segunda y tercera ecuación, obtenemos $z=2$. Si $y=1$, entonces comparando la segunda y tercera ecuación, no tenemos soluciones. Esto significa que si una de las variables x,y,z es 2, entonces $x=y=z=2$. Asi, asumiendo que $x,y,z\neq 2$ y multiplicando todas las ecuaciones encontramos que

$$(x-1)^2(y-1)^2(z-1)^2+6(x+1)^2(y+1)^2(z+1)^2=0$$

lo cuál claramente no tiene soluciones. ■

Ejemplo 1.16 (Revista Mathematics and Youth, 2005)**.** Sean x,y,z,t números reales. Considere el polinomio

$$F(x,y,z,t)=9(x^2y^2+y^2z^2+z^2t^2+t^2x^2)+6xz(y^2+t^2)-6yt(x^2+z^2)-4xyzt.$$

1. Probar que el polinomio puede ser factorizado como el producto de dos polinomios cuadráticos.

2. Encontrar el mínimo valor del polinomio F si $xy+zt=1$.

Solución. 1. Es obvio que $F(x,y,z,t)=(3x^2+3z^2+2xz)(3y^2+3t^2-2yt)$.

2. Notemos que

$$F(x,y,z,t)=4\left((x+z)^2+\frac{(x-z)^2}{2}\right)\left(\frac{(y+t)^2}{2}+(y-t)^2\right),$$

entonces, por la desigualdad de Cauchy-Schwarz, tenemos

$$F(x,y,z,t)\geq 4\left(\frac{(x+z)(y+t)}{\sqrt{2}}+\frac{(x-z)(y-t)}{\sqrt{2}}\right)^2=2(2xy+2zt)^2=8.$$

Ya que $F\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}\right)=8$ esto es en efecto el mínimo. ■

Nota. Por el segundo punto, también se pudo haber escrito $F(x,y,z,t)$ como se sigue

$$F(x,y,z,t)=(3zy+xy-zt-3xt)^2+8(xy+zt)^2\geq 8.$$

Ejemplo 1.17. Dado los números naturales $m,n>2$, probar que el número

$$\frac{m^{2^n-1}-1}{m-1}-m^n$$

tiene un divisor de la forma m^k+1, donde k es un entero positivo.

Solución. Haciendo $n+1=2^r s$, donde $r\geq 0$ y s es un número impar. Sea

$$d_n=\frac{m^{2^n-1}-1}{m-1}-m^n.$$

Ahora,

$$md_n=\frac{m^{2^n}-m}{m-1}-m^{n+1}=\frac{m^{2^n}-1}{m-1}-\left(m^{n+1}+1\right).$$

Note que

$$\frac{m^{2^n}-1}{m-1}=(m+1)(m^2+1)\cdot\ldots\cdot(m^{2^{n-1}}+1).$$

Ya que $r\leq n-1$, entonces $m^{2^r}+1$ divide a $\dfrac{m^{2^n}-1}{m-1}$ y $m^{n+1}+1=(m^{2^r})^s+1$, entonces

$$(m^{2^r}+1)\mid md_n.$$

Como $mcd(m,m^{2^r}+1)=1$, encontramos que $(m^{2^r}+1)\mid d_n$ y hemos terminado. ■

Nota. Empleamos un enfoque similar al del problema anterior para resolver un que apareció en un TST Chino.

Encontrar todos los $m, n \geq 2$ tal que

1. $m+1$ es primo de la forma $4k-1$.
2. Existe un primo p y entero no negativo a tal que

$$\frac{m^{2^n-1}-1}{m-1} = m^n + p^a.$$

Decimos que un polinomio es *irreducible* si este no puede ser factorizado como productos de polinomios con grados menores. De lo contrario, llamamos al polinomio *reducible*. Estos dos conceptos son dependientes del contexto, esto es, el polinomio $1+x^2$ es irreducible sobre $\mathbb{R}[x], \mathbb{Q}[x]$ y $\mathbb{Z}[x]$ pero es reducible sobre $\mathbb{R}[x]$ porque

$$1+x^2 = (x+i)(x-i), \text{ donde } i^2 = -1.$$

Ejemplo 1.18. Sea F_n el n-ésimo término de la secuencia de Fibonacci. Probar que el polinomio

$$P(x) = F_n x^{n+1} + F_{n+1} x^n - 1$$

es reducible sobre $\mathbb{Z}[x]$

Solución. Es fácil ver que el polinomio es divisible por (x^2+x-1). En efecto, ya que $F_{k+1} = F_k + F_{k-1}$, entonces

$$\begin{aligned} F_n x^{n+1} + F_{n+1} x^n - 1 &= \sum_{k=1}^{n} F_k (x^{k+1} + x^k - x^{k-1}) \\ &= (x^2+x-1)(F_n x^{n-1} + F_{n-1} x^{n-2} + \cdots + F_2 x + F_1). \end{aligned}$$ ■

Ejemplo 1.19. Sea $P(x) = (x^2-12x+11)^4+23$. Probar que $P(x)$ no puede representarse como el producto de tres polinomios no constante con coeficientes enteros.

Solución. Asumamos que

$$P(x) = (x^2-12x+11)^4 + 23 = Q(x)H(x)R(x),$$

donde $Q(x), H(x)$ y $R(x)$ tienen coeficientes enteros. Ya que el producto de los coeficientes principales de Q, H y R debe ser igual al coeficiente principal de P, el cual es 1, cada uno de los coeficientes deben ser ± 1. Si uno de los coeficientes es -1, entonces un segundo coeficientes debe ser -1 y podemos multiplicar ambos por -1. En consecuencia podemos asumir que Q, H y R son mónicos. Ya que $P(x)$ no tiene raíces reales, entonces los

grados de los polinomios $Q(x)$, $H(x)$ y $R(x)$ deben ser pares (si por ejemplo Q tiene un grado impar, entonces Q tiene una raíz real, por lo tanto $P(x)$ debe tener una raíz real). Entonces dos de los polinomios Q, H y R deben ser cuadráticos. Sin perdida de generalidad, asumamos que $\deg Q(x) = \deg H(x) = 2$. Ya que $P(1) = P(11) = 23$ podemos encontrar que $Q(1), Q(11) \in \{\pm 1, \pm 23\}$. Así

$$(11-1) \mid Q(11) - Q(1).$$

El argumento anterior es cierto si y solo si $Q(1) = Q(11)$. Análogamente, $H(1) = H(11)$. Ahora ya que uno de los valores $Q(1)$ o $H(1)$ debe ser igual a ± 1, sin perdida de generalidad, asumimos que $Q(1) = \pm 1$, entonces $Q(11) = \pm 1$. Así,

$$Q(x) = (x-1)(x-11) \pm 1,$$

pero entonces $Q(x)$ tiene raíces reales, una contradicción. ■

Ejemplo 1.20 (Olimpiada Polaca de Matemáticas, 2014)**.** Para cualquier entero $n \geq 1$, determina el menor valor del polinomio

$$P_n(x) = x^{2n} + 2x^{2n-1} + 3x^{2n-2} + \cdots + (2n-1)x^2 + 2nx$$

en el conjunto de los números reales.

Solución. Notemos que

$$\begin{aligned} x^{2n} + 2x^{2n-1} + x^{2n-2} &= (x+1)^2 x^{2n-2} \\ 2x^{2n-2} + 4x^{2n-3} + 2x^{2n-4} &= 2(x+1)^2 x^{2n-4} \\ 3x^{2n-4} + 6x^{2n-5} + 3x^{2n-6} &= 3(x+1)^2 x^{2n-4} \end{aligned}$$

y de manera general $kx^{2n-2k+2} + 2kx^{2n-2k+1} + kx^{2n-2k} = k(x+1)^2 x^{2n-2k}$.

Finalmente, escribimos $nx^2 + 2nx = n(x+1)^2 - n$. Entonces podemos deducir la siguiente identidad

$$P_n(x) = (x+1)^2 \left(x^{2n-2} + 2x^{2n-4} + \cdots + (n-1)x^2 + n\right) - n.$$

Por tanto, $P_n(x) \geq P_n(-1) = -n$. ■

Con el fin de resolver el siguiente problema, necesitamos un criterio útil de irreducibilidad.

Definición 1.1 (Criterio de Eisenstein)**.** Supongamos que $P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ es un polinomio con coeficientes enteros y que existe un primo p tal que p no divide a_d, pero divide a todos los $a_{d-1}, \ldots, a_0$ y p^2 no divide a a_0. Entonces $P(x)$ es irreducible sobre los enteros.

Demostración. Supongamos, por el contrario, que $P(x) = f(x)g(x)$ donde $f(x) = b_0 + b_1x + \cdots$ y $g(x) = c_0 + c_1x + \cdots$ son polinomios no constantes con coeficientes enteros. Ya que el producto de los coeficientes principales de f y g es a_d el cuál no es múltiplo de p, los coeficientes principales de f y g no son múltiplos de p. Por lo tanto, hay un mínimo índice k tal que b_k no es múltiplo de p y hay un mínimo índice m tal que c_m no es múltiplo de p. Entonces por el coeficiente de x^{k+m} obtenemos

$$a_{k+m} = (b_0c_{m+k} + \cdots + b_{k-1}c_{m+1}) + b_kc_m + (b_{k+1}c_{m-1} + \cdots + b_{m+k}c_0).$$

Cada término en el lado derecho de la ecuación excepto el de en medio es múltiplo de p, porque $b_0, \cdots, b_{k-1}$ y $c_0, \cdots, c_{k-1}$ son múltiplos de p. Ya que el término de en medio no es múltiplo de p, se sigue que a_{m+k} no es múltiplo de p. Así $m + k = d$. Pero esto significa que b_kx^k y c_mx^m deben ser los términos principales de f y g. En particular, $k, m > 0$ por tanto b_0 y $b_0$son ambos múltiplos de p. Pero esto haría a a_0 un múltiplo de p^2, contradiciendo la hipótesis. Esto es una contradicción y por consiguiente $P(x)$ es irreducible sobre en los enteros. ■

Ejemplo 1.21 (Mathematical Reflections, S18. Titu Andreescu)**.** Encontrar el menor entero positivo n para el cual el polinomio

$$P(x) = x^{n-4} + 4n$$

puede ser escrito como un producto de cuatro polinomios no constantes con coeficientes enteros.

Solución. Probaremos que el menor números es 16. Demostraremos que los números desde 1 a 15 no cumplen. Para $10 \leq n \leq 15$ el polinomio $P(x) = x^{n-4} + 4n$ es irreducible sobre los racionales, como se puede comprobar usando el criterio de Eisenstein (ver arriba) para los primos 5, 11, 3, 13, 7, 5, respectivamente. Para $n = 9$, tenemos $P(x) = x^5 + 36$. Si podemos factorizar en la forma deseada entonces uno de los factores sería línea. Por lo tanto, $P(x) = x^5 + 36$ debería tener una raíz entera, los cual es imposible. Similarmente, cuando $n = 8$, $P(x) = x^4 + 32$ tiene una raíz entera e implica el mismo razonamiento. Para $n = 4, 5, 6, 7$ al menos uno de los factores debe se constante. Para $n = 16$, tenemos

$$\begin{aligned} x^{12} + 64 &= x^{12} + 16x^6 + 64 - 16x^6 \\ &= (x^6 + 8)^2 - (4x^3)^2 \\ &= (x^6 - 4x^3 + 8)(x^6 + 4x^3 + 8). \end{aligned}$$

Por otro lado,

$$\begin{aligned} x^{12} + 64 &= (x^4 + 4)(x^8 - 4x^4 + 16) \\ &= \left((x^2 + 2)^2 - 4x^2\right)(x^8 - 4x^4 + 16) \\ &= (x^2 + 2x + 2)(x^2 - 2x + 2)(x^8 - 4x^4 + 16). \end{aligned}$$

Ya que x^2+2x+2 y x^2-2x+2 no tiene raíces enteras, son irreducibles. Por consiguiente deben dividir a x^6-4x^3+8 y x^6+4x^3+8. En efecto, tenemos que

$$x^6-4x^3+8=(x^2+2x+2)(x^4-2x^3+2x^2-4x+4)$$

y

$$x^6+4x^3+8=(x^2-2x+2)(x^4+2x^3+2x^2+4x+4).$$

Por lo tanto para $n=16$ nuestro polinomio es el producto de cuatro polinomios no constantes con coeficientes enteros. ■

Ejemplo 1.22. Sea n un impar y $p>n^n$ un número primo. Probar que el polinomio

$$Q(x)=(x-1)\cdot\ldots\cdot(x-n)+p$$

es irreducible.

Solución. Asumamos que $Q(x)=f(x)g(x)$, donde $f(x)$ y $g(x)$ son polinomios no constantes con coeficientes enteros. Tenga en cuenta que siempre que $x>n$ o $x<0$ tenemos $Q(x)>0$. Además, para $x\in[0,n]$ tenemos

$$(x-1)\cdot\ldots\cdot(x-n)+p>-n^n+p>0.$$

En consecuencia para todo número real x, tenemos $f(x)g(x)>0$. Sin perdida de generalidad, asumamos que $f(x)>0$ y $g(x)>0$. Entonces, para todo $k=1,2,\ldots,n$ tenemos $f(k)g(k)=p$ que implica $f(k)$ y $g(k)\in\{1,p\}$. Definamos el polinomio $f(x)+g(x)-p-1$, el cual es cero en $k=1,2,\ldots,n$ pero el grado de este polinomio es a lo más $n-1$. Así este debe ser un polinomio cero y tenemos $f(x)+g(x)=p-1$ para todo x. Pero ya que f y g son positivos esto obliga $0<f(x),g(x)<p-1$ para todo x. Ya que $f(x)$ y $g(x)$ son no constantes, esto es imposible. ■

1.4. Valores de polinomios

Como hemos visto, cualquier polinomio $P(x)$ de grado no negativo tiene una representación *genérica* como la siguiente

$$P(x)=a_dx^d+a_{d-1}x^{d-1}+\ldots+a_1x+a_0,$$

donde $a_d,a_{d-1},\ldots,a_1,a_0$ son números complejos. El término a_dx^d es llamado el *término principal* y a_d es llamado el *coeficiente principal*. Además, a_0 es llamado el *término constante*. El valor del polinomio en $x=c$, el cual es denotado por $P(c)$, es

$$P(c)=a_dc^d+a_{d-1}c^{d-1}+\ldots+a_1c+a_0.$$

De especial interés son los casos de $P(1)$ y $P(-1)$, i.e.

$$P(1) = a_d + a_{d-1} + \ldots + a_0$$

el cual es llamado la *suma de coeficientes* y

$$P(-1) = a_0 - a_1 + \ldots + (-1)^d a_d.$$

Ejemplo 1.23. Sea

$$\left(\sqrt{2017}x - \sqrt{2027}\right)^{2017} = a_{2017}x^{2017} + a_{2016}x^{2016} + \ldots + a_1 x + a_0.$$

Hallar el valor de $(a_1 + a_3 + \cdots + a_{2017})^2 - (a_0 + a_2 + \cdots + a_{2016})^2$.

Solución. Si hacemos $x = 1$, tenemos

$$\left(\sqrt{2017} - \sqrt{2027}\right)^{2017} = a_{2017} + a_{2016} + \ldots + a_1 + a_0.$$

y si hacemos $x = -1$, tenemos

$$\begin{aligned}\left(-\sqrt{2017} - \sqrt{2027}\right)^{2017} &= -a_{2017} + a_{2016} + \ldots - a_1 + a_0 \\ &= (a_0 + a_2 + \ldots + a_{2016}) - (a_1 + a_3 + \ldots + a_{2017}).\end{aligned}$$

Multiplicando ambas ecuaciones obtenemos

$$\begin{aligned}&(a_1 + a_3 + \cdots + a_{2017})^2 - (a_0 + a_2 + \cdots + a_{2016})^2 \\ &= \left(\sqrt{2017} - \sqrt{2027}\right)^{2017} \cdot \left(\sqrt{2017} + \sqrt{2027}\right)^{2017} \\ &= -10^{2017}.\end{aligned}$$

■

Ejemplo 1.24 (Competición Mediterrania, 2015)**.** Probar que para el polinomio

$$P(x) = x^4 - x^3 - 3x^2 - x + 1$$

existen infinitos enteros positivos n para el cual $P(3^n)$ es compuesto.

Solución. Sea $x = 3^{2n-1}$, entonces

$$P(3^{2n-1}) = 81^{2n-1} - 27^{2n-1} - 3(9^{2n-1}) - 3^{2n-1} + 1.$$

Tomando la ecuación en módulo 5, encontramos que

$$P(3^{2n-1}) \equiv 1 - 2^{2n-1} - 3(-1)^{2n-1} - 3^{2n-1} + 1 \equiv (2^{2n-1} + 3^{2n-1}) \pmod 5.$$

Ya que $2^{2n-1} + 3^{2n-1}$ es divisible por 5, hemos terminado. ■

Ejemplo 1.25. Sea $P(x) = a_0 + \ldots + a_n x^n$ un polinomio con coeficientes enteros talque $P(-1) = 0$ y $P\left(\sqrt{2}\right) \in \mathbb{Z}$. Probar que existe un entero $0 \leq k \leq n$ talque $P(k) + a_k$ es par.

Solución. Tenemos $P(1) = \sum a_{2i} + \sum a_{2i+1}$. Ya que $P(-1) = 0$, encontramos que

$$\sum a_{2i} = \sum a_{2i+1}.$$

Ya que $P\left(\sqrt{2}\right) \in \mathbb{Z}$, encontramos que $\sum 2^i a_{2i} + \sqrt{2}\sum 2^i a_{2i+1} \in \mathbb{Z}$, por lo tanto

$$\sum 2^i a_{2i+1} = 0.$$

Entonces a_1 debe ser par. Así, $P(1) + a_1 = 2\sum a_{2i} + a_1$ es par. ■

Ejemplo 1.26 (Olimpiada Matemática de Zhautykov, 2014)**.** Encontrar todos los polinomios $P(x)$ con coeficientes enteros talque

$$P\left(1+\sqrt{3}\right) = 2+\sqrt{3}, \quad P\left(3+\sqrt{5}\right) = 3+\sqrt{5}.$$

Solución. Sea $Q(x) = P(x) - x$. Claramente, $Q\left(3+\sqrt{5}\right) = 0$. Además, ya que $Q(x)$ tiene coeficientes enteros, tenemos que si D no es un cuadrado perfecto, a, b son números racionales y $Q\left(a+b\sqrt{D}\right) = c + e\sqrt{D}$ para algunos números racionales c, e, entonces

$$Q\left(a-b\sqrt{D}\right) = c - e\sqrt{D}.$$

Esto implica que $Q\left(3-\sqrt{5}\right) = 0$. Entonces $Q(x)$ es divisible por

$$\left(x-\left(3-\sqrt{5}\right)\right)\left(x-\left(3+\sqrt{5}\right)\right) = x^2 - 6x + 4.$$

Ahora, $Q(x) = P(x) - x = (x^2 - 6x + 4)R(x)$. para algún polinomio $R(x)$ con coeficientes enteros. Entonces $P(x) = x + (x^2 - 6x + 4)R(x)$. Ahora, tomando $x = 1 + \sqrt{3}$, tenemos

$$1 = \left(2 - 4\sqrt{3}\right)R\left(1+\sqrt{3}\right).$$

Análogamente, $1 = \left(2 + 4\sqrt{3}\right)R\left(1-\sqrt{3}\right)$. Entonces

$$R\left(1+\sqrt{3}\right)R\left(1-\sqrt{3}\right) = \frac{1}{44}.$$

Pero $R(x)$ tiene coeficientes enteros, asi

$$R\left(1+\sqrt{3}\right) = a + b\sqrt{3} \quad \text{y} \quad R\left(1-\sqrt{3}\right) = a - b\sqrt{3},$$

para algunos enteros a, b. Entonces $R\left(1+\sqrt{3}\right)R\left(1-\sqrt{3}\right) = a^2 - 3b^2$ lo cuál es un entero, contradicción. ■

Una propiedad interesante de los polinomios con coeficientes enteros es que para todos los enteros arbitrarios r,s tenemos

$$\begin{aligned} P(r)-P(s) &= a_d r^d + a_{d-1}r^{d-1} + \ldots + a_0 - \left(a_d s^d + a_{d-1}s^{d-1} + \ldots + a_0\right) \\ &= a_d(r^d - s^d) + a_{d-1}(r^{d-1} - s^{d-1}) + \ldots + a_1(r-s). \end{aligned}$$

Ya que $r^k - s^k$ es divisible por $r-s$, encontramos

$$P(r)-P(s) = (r-s)\left(a_1 + a_2(r+s) + \ldots + a_d\left(\frac{r^d - s^d}{r-s}\right)\right).$$

Pues como $a_1, \ldots, a_d$ son todos enteros, vemos que

$$a_1 + a_2(r+s) + \ldots + a_d\left(\frac{r^d - s^d}{r-s}\right) = Q(r,s)$$

es un entero. En consecuencia, hallamos el siguiente teorema.

Teorema 2.

Sea $P(x)$ un polinomio con coeficientes enteros. Entonces, la razón $\dfrac{P(r)-P(s)}{r-s}$ es un entero para todo los enteros distintos r,s.

De acuerdo con el resultado de arriba, no existen un polinomio con coeficientes enteros talque

$$P(10) = 2017, \quad P(12) = 2018$$

ya que $\dfrac{P(12)-P(10)}{12-10} = \dfrac{1}{2}$ no es un entero.

Ejemplo 1.27. ¿Existe un polinomio $P(x)$ talque ninguno de sus coeficientes distintos de cero es un entero, $P(0) = 0$ y para cualquiera enteros distintos a, b tenemos que $\frac{P(a)-P(b)}{a-b}$ es un entero?

Solución. La respuesta es sí. Sea $P(x) = \dfrac{x^m + x^n}{2}$ donde $m > n > 1$ son enteros. Ahora,

$$\frac{P(a)-P(b)}{a-b} = \frac{1}{2}\left(\frac{a^m - b^m}{a-b} + \frac{a^n - b^n}{a-b}\right).$$

Note que

$$\frac{a^k - b^k}{a-b} = a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1} \equiv a + b + (k-2)ab \pmod 2.$$

Por tanto para todo $k \geq 2$

$$2 \cdot \frac{P(a)-P(b)}{a-b} \equiv (a+b+(m-2)ab)+(a+b+(n-2)ab) \equiv (m+n)ab \pmod 2.$$

Sean m, n números con la misma paridad. Por lo tanto $2 \cdot \dfrac{P(a)-P(b)}{a-b}$ es un entero par y hemos terminado. ■

Ejemplo 1.28. Si $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ tiene raíces x_1, x_2, …, x_n y $Q(x) = x^{n+1} + b_n x^n + \ldots + b_0$ tiene raíces $y_1, y_2, \ldots, y_{n+1}$, probar que

$$P(y_1) \cdot \ldots \cdot P(y_{n+1}) = Q(x_1) \cdot \ldots \cdot Q(x_n).$$

Solución. Escribamos

$$P(x) = (x-x_1) \cdot \ldots \cdot (x-x_n) \quad \text{y} \quad Q(x) = (x-y_1) \cdot \ldots \cdot (x-y_{n+1}).$$

Entonces

$$P(y_1) \cdot \ldots \cdot P(y_{n+1}) = [(y_1-x_1) \cdot \ldots \cdot (y_1-x_n)] \cdot \ldots \cdot [(y_{n+1}-x_1) \cdot \ldots \cdot (y_{n+1}-x_n)].$$

Este producto tiene $n(n+1)$ factores, lo cual siempre es un número par. Por consiguiente podemos reordenar el producto de arriba como

$$[(x_1-y_1) \cdot \ldots \cdot (x_1-y_{n+1})] \cdot \ldots \cdot [(x_n-y_1) \cdot \ldots \cdot (x_n-y_{n+1})] = Q(x_1) \cdot \ldots \cdot Q(x_n)$$

y tenemos la conclusión. ■

Nota. El ejemplo previo puede ser usado para resolver el siguiente problema de Titu Andreescu (Mathematical Reflections U451):

Sean x_1, x_2, x_3, x_4 las raíces del polinomio $2018x^4 + x^3 + 2018x^2 - 1$. Evaluar la expresión

$$(x_1^2 - x_1 + 1)(x_2^2 - x_2 + 1)(x_3^2 - x_3 + 1)(x_4^2 - x_4 + 1).$$

(**Pista.** Tomar $P(x) = x^3 + 1$ y $Q(x) = 2018x^4 + x^3 + 2018x^2 - 1$.)

Ejemplo 1.29. Sea P un polinomio de grado a lo más 10 con coeficientes enteros talque para todo $k \in \{1, 2, \ldots, 10\}$ existe un entero m talque $P(m) = k$ y se tiene además $|P(10) - P(0)| < 1000$. Probar que para todo entero k existe un entero m talque $P(m) = k$.

Solución. Asumamos que para todo $i = 1, 2, \ldots, 10$ existen enteros c_i talque $P(c_i) = i$. Para todo $i = 1, 2, \ldots, 9$ tenemos

$$(c_{i+1} - c_i) \mid (P(c_{i+1}) - P(c_i)) = 1.$$

Así $c_1, c_2, \ldots, c_{10}$ son consecutivos. Ya que siempre podemos reemplazar $P(x)$ por $P(-x)$ podemos asumir sin perdida de generalidad que $c_1, c_2, \ldots, c_{10}$ están en orden creciente, por consiguiente $c_i = c_1 - 1 + i$. Haciendo $Q(x) = 1 + x - c_1$. Entonces,

$$P(x) - Q(x) = R(x)(x - c_1) \cdot \ldots \cdot (x - c_{10})$$

para algún polinomio $R(x)$ con coeficientes enteros. Por lo tanto,

$$P(x) = 1 + x - c_1 + R(x)(x - c_1) \cdot \ldots \cdot (x - c_{10}).$$

Tomando la condición del grado encontramos que $R(x)$ es un polinomio constante, digamos $R(x) = C$. Si $C \neq 0$, tenemos

$$\begin{aligned} P(10) - P(0) &= 10 + C\left[(10 - c_1) \cdot \ldots \cdot (10 - c_{10}) - (0 - c_1) \cdot \ldots \cdot (0 - c_{10})\right] \\ &= 10 + (N + 20)(N + 19) \cdot \ldots \cdot (N + 11) - (N + 10) \cdot \ldots \cdot (N + 1), \end{aligned}$$

donde tomamos a $N = c_1 - 1$. Es fácil verificar que

$$(N + 20)(N + 19) \cdot \ldots \cdot (N + 11) \quad \text{y} \quad (N + 10) \cdot \ldots \cdot (N + 1)$$

son distintos (el primero es mayor para $N \geq -10$ y el segundo es mayor para $N \leq -11$) y ambos son divisibles por 10!. En consecuencia

$$|(N + 20)(N + 19) \cdot \ldots \cdot (N + 11) - (N + 10) \cdot \ldots \cdot (N + 1)| \geq 10!.$$

De aquí que $|P(10) - P(0)| > 10! - 10 > 1000$, una contradicción. Así $C = 0$ y

$$P(x) = 1 + x - c_1.$$

Por tanto, para todo entero k tomamos $m = k + c_1 - 1$ y obtenemos la conclusión. ■

Otra propiedad interesante de los polinomios con coeficientes enteros es la similitud entre $P(c)$ y la expansión de un número entero en base c. Si comenzamos con la expansión del entero $\overline{a_d a_{d-1} \ldots a_{0_c}}$ (donde como siempre $0 \leq a_i \leq c - 1$ para todo $0 \leq i \leq d$) podemos definir el polinomio

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0,$$

donde es fácil ver que

$$P(c) = \overline{a_d a_{d-1} \ldots a_{0_c}}.$$

En cambio, si tenemos el polinomio P y conocemos todos los coeficientes a_i que satisfacen $0 \leq a_i \leq c - 1$, entonces podemos decir que los coeficientes de P son la expansión en base c del entero $P(c)$.

Ejemplo 1.30. Todos los coeficientes del polinomio $P(x)$ son -1 o 1. Si $P(3) = 130$, hallar dicho polinomio.

Solución. Escribamos $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$, entonces

$$130 = P(3) \leq -3^d + 3^{d-1} + \ldots + 3 + 1 < 0.$$

Así debemos tener $a_d = 1$. Ahora

$$130 = P(3) \geq 3^d - \left(3^{d-1} + \ldots + 3 + 1\right) = \frac{1+3^d}{2}$$

implica que $d \leq 5$. Si $d < 5$ entonces $130 = P(3) \leq 3^4 + 3^3 + \ldots + 1 = 121$, asi que $d = 5$. Ahora ciertamente $a_4 = -1$, entonces

$$130 = P(3) = 3^5 - 3^4 + 27a_3 + 9a_2 + 3a_1 + a_0.$$

Por lo tanto

$$27a_3 + 9a_2 + 3a_1 + a_0 = -32.$$

Entonces $a_3 = a_2 = -1$, $a_1 = a_0 = 1$ y $P(x) = x^5 - x^4 - x^3 - x^2 + x + 1$. ■

Ejemplo 1.31 (Tournament of Towns, 2012)**.** Vlad afirma que un polinomio no constante $P(x)$ con coeficientes enteros no negativos es unívocamente determinado por los valores de $P(2)$ y $P(P(2))$. ¿Vlad tiene razón?

Solución. Vlad tiene razón. Sea $P(x) = a_d x^d + \ldots + a_0$ un polinomio no constante con coeficientes enteros no negativos. Haciendo

$$P(2) = b = a_d 2^d + \ldots + a_0 > a_d + \ldots + a_0.$$

Esto lleva que todos los coeficientes de $P(x)$ son enteros no negativos en el rango de 0 a $b-1$. Así podemos decir que los coeficientes de $P(x)$ es la expansión en base b del entero $P(P(2)) = P(b) = \overline{a_d a_{d-1} \ldots a_0}_b$. En consecuencia $P(x)$ está unívocamente determinado. ■

Ejemplo 1.32 (Olimpiada Koreana de Matemática, 2001)**.** Sea n y N dos enteros positivos y se define P_n como el conjunto de todos los polinomios $f(x) = a_0 + \cdots + a_n x^n$ tal que

1. Para todo $j = 0, 1, \ldots, n$ tenemos $|a_j| \leq N$.
2. El conjunto $\{j | 1 \leq j \leq n, a_j = N\}$ tiene a lo más dos elementos.

Encontrar el número de elementos en el conjunto $\{f(2N) | f(x) \in P_n\}$.

Solución. Sea $h(x) = N(1 + x + \ldots + x^n)$. Podemos contar el número de valores diferentes de $f(2N) + h(2N)$ para $f(x) \in P_n$. Si ninguno de los coeficientes de f es igual a N, entonces $f(2N) + h(2N)$ es un número de k dígitos en base $2N$ para algún $k \leq n + 1$.

Así $f(2N)+h(2N)$ puede tomar todos los valores enteros desde 0 hasta $(2N)^{n+1}-1$. Si solo $a_n = N$, entonces $f(2N)+h(2N) = (2N)^{n+1}+M$, donde M es número de k dígitos en base $2N$ para algún $k \leq n$. Así $f(2N)+h(2N)$ puede tomar todos los valores enteros desde $(2N)^{n+1}$ hasta $(2N)^{n+1}+(2N)^n-1$. Si $a_n = a_{n-1} = N$, entonces $f(2N)+h(2N) = (2N)^{n+1}+(2N)^n+M$, donde M es un número de k dígitos en base $2N$ para algún $k \leq k-1$. Así $f(2N)+h(2N)$ puede tomar todos los valores enteros desde $(2N)^{n+1}+(2n)^n$ a $(2N)^{n+1}+(2N)^n+(2N)^{n-1}-1$. Combinando estos tres casos, podemos ver que $f(2N)+h(2N)$ puede tomar todos los valores desde 0 hasta $(2N)^{n+1}+(2N)^n+(2N)^{n-1}-1$. Sin embargo, está claro que como a lo sumo dos coeficientes de $f+h$ son $2N$, el valor más grande posible de $f(2N)+h(2N)$ es

$$(2N-1)(1+2N+\cdots+(2N)^{n-2})+(2N)(2N)^{n-1}+(2N)(2N)^n$$

lo cual es igual a

$$(2N)^{n+1}+(2N)^n+(2N)^{n-1}-1.$$

Así estos valores son los únicos de $f(2N)+h(2N)$ que cumplen, por lo tanto, el número de elementos en el conjunto es $(2N)^{n-1}((2N)^2+2N+1)$. ■

Proporcionamos un maravilloso problema de la olimpiada Rusa del 2003 basado en la interpretación base c en el valor de polinomio $P(c)$.

Ejemplo 1.33 (Olimpiada Rusa de Matemáticas, 2003. Alexander Khrabrov)**.** Sea $P(x)$ y $Q(x)$ dos polinomios con coeficientes enteros no negativos tal que todos los coeficientes de $P(x)$ son menores o iguales a m. Si existen enteros $a < b$ talque $P(a) = Q(a)$, $P(b) = Q(b)$ y $b > m$, probar que $P(x) = Q(x)$.

Solución. Asumamos que

$$P(x) = \sum_{i=0}^{n} c_i x^i \quad \text{y} \quad Q(x) = \sum_{i=0}^{k} d_i x^i$$

y $0 \leq c_i \leq m < b$. En consecuencia, vemos que $P(b)$ escrito en base b es $\overline{c_n c_{n-1}\cdots c_0}_b$. Si todos los coeficientes de Q con menores a b hemos terminado. Si no, entonces existe un índice menor i talque $d_i \geq b$. En ese caso podemos escribir $d_i = bq+r$ con $0 = r < b$. Ahora construyamos el polinomio Q_1 desde Q cambiando d_{i+1} por $d_{i+1}+q$ y d_i por r. Entonces es obvio que $Q_1(b) = Q(b)$. Ahora, ¿qué pasa con $Q_1(a)$ y $Q(a)$? Podemos ver que

$$\begin{aligned} d_i a^i + d_{i+1}a^{i+1} &= (bq+r)a^i + d_{i+1}a^{i+1} \\ &> (aq+r)a^i + d_{i+1}a^{i+1} \\ &> ra^i + (d_{i+1}+r)a^{i+1} \end{aligned}$$

Esto implica que $Q_1(a) < Q(a)$. Si iteramos este proceso, entonces el índice donde d_i primero iguala o excede a b solo puede incrementar. Así en a los más n pasos, obtenemos el polinomio Q_s el cuál todo sus coeficientes son menores que b y con $P(b) = Q(b) = Q_s(b)$. La igualdad $P(b) = Q_s(b)$ implica que P y Q_s deben ser iguales, pero la desigualdad $Q_s(a) < Q(a)$ contradice la suposición. Por tanto, nuestra primera suposición es falsa y tenemos $P(x) = Q(x)$. ■

Ejemplo 1.34 (Tuymada[2], 2007. Aleksander Golovanov)**.** Se tiene dos polinomios de grado 100

$$f(x) = a_{100}x^{100} + a_{99}x^{99} + \ldots + a_1x + a_0$$

y

$$g(x) = b_{100}x^{100} + b_{99}x^{99} + \ldots + b_1x + b_0.$$

Sabiendo que los coeficientes de uno es la permutación del otro y para todo i tenemos $a_i \neq b_i$. ¿Existen dos polinomios tales que para todo real x tengamos $f(x) \geq g(x)$?

Solución. Sea $h(x) = (x-1)^{100} = c_{100}x^{100} + \ldots + c_0$. Sabemos que

$$h(1) = c_{100} + c_{99} + \ldots + c_0 = 0.$$

Sea $b_0 = 2$, $b_1 = 2 + c_0$, $b_2 = 2 + c_0 + c_1$, ... donde $b_k = 2 + c_0 + c_1 + \ldots + c_{k-1}$ y

$$b_{100} = 2 + c_0 + c_1 + \ldots + c_{99} = 2 - c_{100} = 1.$$

Ahora hagamos $a_k = b_k + c_k$. En ese caso para todo $0 \leq k \leq 99$ tenemos $a_k = b_{k+1}$ y $a_{100} = b_0 = 2$. Por tanto

$$f(x) - g(x) = h(x) \geq 0.$$ ■

1.5. División, MCD de polinomios

Sabemos que para cualquier entero positivo b y cualquier entero a, dividir a por b deja enteros únicos q, r talque

$$a = bq + r, \quad 0 \leq r \leq b - 1.$$

Usando la división de polinomios obtenemos un resultado similar. Primero consideremos polinomios con coeficientes racionales. Los mismos argumentos trabajan para coeficientes reales o complejos, aunque como veremos abajo los coeficientes enteros requiere un cuidado extra. Suponga $B(x)$ como cualquier polinomio no cero. Entonces para cualesquiera polinomios $A(x)$, existe polinomios único $Q(x)$, $R(x)$ talque

$$A(x) = B(x)Q(x) + R(x), \quad \deg R(x) < \deg B(x).$$

[2]Tuymada es una olimpiada que se realiza en la republica rusa de Sakha

Así que en lugar del resto con menor magnitud, es decir, satisface la desigualdad $0 \leq r \leq b-1$, tenemos una condición análoga del resto con el grado menor. El hecho de arriba es llamado *Teorema de la División Polinómica* Este puede probarse usando una inducción simple en el grado de $A(x)$ o equivalentemente por la división larga de polinomios. Cuando $R(x) = 0$, decimos que el polinomio $A(x)$ es divisible por el polinomio $B(x)$.

Por ejemplo, sea $A(x) = 3x^4 - x^3 + x^2 - x + 1$ y $B(x) = x^2 + x + 2$. Entonces la división larga nos da

$$3x^4 - x^3 + x^2 - x + 1 = (x^2 + x + 1)(3x^2 - 4x - 1) + 8x + 3.$$

En consecuencia $Q(x) = 3x^2 - 4x - 1$ y $R(x) = 8x + 3$. Además, si queremos dividir un polinomio arbitrario $P(x)$ por $x^2 + 2$, por el Teorema de la División Polinómica, encontramos que

$$P(x) = (x^2 + 2)Q(x) + R(x).$$

Ya que $\deg R(x) < \deg x^2 + 2 = 2$, podemos escribir que $R(x) = ax + b$, de donde,

$$P(x) = (x^2 + 2)Q(x) + ax + b.$$

Si $A(x)$ y $B(x)$ tiene coeficientes enteros, entonces no podemos encontrar siempre polinomios $Q(x)$ y $R(x)$ con coeficientes enteros tales que

$$A(x) = B(x)Q(x) + R(x) \quad \text{y} \quad \deg R(x) < \deg B(x).$$

Por ejemplo, si $B(x) = 2x^2 + 1$ y $Q \neq 0$ tiene enteros coeficientes, entonces el coeficiente principal de $B(x)Q(x) + R(x)$ siempre será múltiplo de 2. Por lo tanto, no podemos escribir $A(x) = x^3$ en esta forma. Sin embargo, si asumimos que $B(x)$ es un polinomio mónico, entonces este problema desaparece y tenemos el siguiente resultado.

Corolario 1.1. Si $A(x)$ es un polinomio con coeficientes enteros y $B(x)$ es un polinomio mónico con coeficientes enteros, entonces existen polinomios único $Q(x)$, $R(x)$ con coeficientes enteros tales que

$$A(x) = B(x)Q(x) + R(x), \quad \deg R(x) < \deg B(x).$$

Esto puede probarse imitando la demostración anterior y viendo que siempre que B sea mónico podemos realizar una división larga o derivar a un colorario del resultado para coeficientes racionales. Por este resultado, encontramos $A(x) = B(x)Q(x) + R(x)$ donde Q and R tiene coeficientes racionales. Ahora suponga $q_k x^k$ es el monomio con mayor grado en Q para el cual el coeficiente no es un entero. Entonces viendo el coeficiente de $x^{k+\deg B}$, obtenemos una contradicción. Por tanto Q y de ahí $R(x) = A(x) - B(x)Q(x)$ tiene coeficientes enteros.

Ejemplo 1.35. Sean $P(x)$ y $Q(x)$ polinomios de segundo grado con coeficientes enteros. Probar que hay un polinomio $R(x)$ con coeficientes enteros y grado a lo más dos tal que

$$R(8)R(12)R(2017) = P(8)P(12)P(2017)Q(8)Q(12)Q(2017).$$

Solución. Definamos, $T(x) = P(x)Q(x)$. Entonces, $\deg T(x) = 4$ y $T(x)$ tiene coeficientes enteros. Ahora debemos probar que hay un polinomio $R(x)$ con coeficientes enteros y grado a lo más dos tal que

$$R(8)R(12)R(2017) = T(8)T(12)T(2017).$$

Ahora, dividimos el polinomio $T(x)$ por un polinomio mónico

$$(x-8)(x-12)(x-2017),$$

i.e, escribimos

$$T(x) = (x-8)(x-12)(x-2017)H(x) + R(x),$$

donde $\deg R(x) < \deg(x-8)(x-12)(x-2017) = 3$, i.e., $\deg R(x) \leq 2$. Ahora, tomemos $x = 8$, 12, 2017 en la identidad anterior. Obtenemos

$$T(8) = R(8), \quad T(12) = R(12), \quad T(2017) = R(2017),$$

i.e.,

$$R(8)R(12)R(2017) = T(8)T(12)T(2017).$$

y hemos terminado. ■

Por el *Máximo Común Divisor* (MCD) de dos polinomios $A(x)$, $B(x)$ con coeficientes racionales queremos decir un polinomio mónico $D(x)$ del mayor grado que divide ambos polinomios.

Por el *Mínimo Común Múltiplo* (MCM) de dos polinomios $A(x)$, $B(x)$ con coeficientes racionales queremos decir un polinomio mónico $L(x)$ del menor grado divisible por ambos polinomios.

Ejemplo 1.36 (Olimpiada Italiana de Matemática, 2015. Ronda Distrital)**.** Sean $P(x)$, $Q(x)$ dos polinomios mónicos con coeficientes enteros tal que su MCD es $(x-1)(x-2)$ y su mínimo común múltiplo (LCM) es

$$(x-1)^2(x-2)^2(x-3)(x+1).$$

Si además asumimos $\deg P(x) < \deg Q(x)$, ¿Cuántos polinomios $P(x)$ existen para los cuales hay un $Q(x)$ que satisface estas condiciones?

Solución. Sea $D(x) = mcd(P(x), Q(x))$ y $L(x) = mcm(P(x), Q(x))$. Análogamente, paro el caso de enteros, encontramos que

$$L(x) = \frac{P(x)Q(x)}{D(x)},$$

i.e.

$$L(x)D(x) = P(x)Q(x).$$

Por tanto,

$$P(x)Q(x) = (x-1)^3(x-2)^4(x-3)(x+1).$$

El polinomio $(x-1)(x-2)$ es divisor común para ambos polinomio $P(x)$ y $Q(x)$. Después cancelando esos factores, vemos que

$$\frac{P(x)}{(x-1)(x-2)} \cdot \frac{Q(x)}{(x-1)(x-2)} = (x-1)(x-2)^2(x-3)(x+1).$$

Los factores de la derecha deben repartirse entre $P(x)$ y $Q(x)$, y ya que los factores de la izquierda son primos relativos debemos dar ambos factores de $(x-2)^2$ al mismo polinomio. Así, esto es posible en $2^4 = 16$ maneras. Como el producto $P(x)Q(x)$ es de grado 9, encontramos que $\deg P(x) \neq \deg Q(x)$, de esta manera en exactamente $\frac{16}{2} = 8$ caso tenemos $\deg P(x) < \deg Q(x)$. ■

Para encontrar el MCD de dos polinomios con coeficientes racionales, asumamos que $\deg A(x) \geq \deg B(x)$. Entonces, por el teorema de División Polinómica, encontramos que hay polinomios $Q_1(x)$, $R_1(x)$ talque

$$A(x) = B(x)Q_1(x) + R_1(x), \quad \deg R_1(x) < \deg B(x).$$

Si $R_1(x) = 0$, entonces $B(x)$ divide a $A(x)$ y por tanto $B(x)$ (dividido por su coeficiente principal) es el mayor común divisor. Si $R_1(x) \neq 0$, entonces cualquier común divisor de $A(x)$ y $B(x)$ también divide a $R_1(x)$. Asi $B(x)$ y $R_1(x)$ tiene el mismo *MCD*. Continuando, dividimos $B(x)$ por $R_1(x)$, entonces

$$B(x) = R_1(x)Q_2(x) + R_2(x), \quad \deg R_2(x) < \deg R_1(x) < \deg B(x).$$

Iterando este proceso, ya que el grado siempre decrece, eventualmente debe obtener el caso donde $R_{n+1}(x) = 0$. En este caso , $R_n(x)$ (dividido por su coeficiente principal) es el mayor común divisor de $A(x)$, $B(x)$. Si $R_n(x)$ es un polinomio constante, entonces los polinomios $A(x)$, $B(x)$ no debe tener divisores no constantes comunes, esto se llaman *primos relativos* o *coprimo*. Por otra parte, ya que

$$R_1(x) = A(x) - B(x)Q_1(x)$$

tenemos

$$R_2(x) = B(x) - R_1(x)Q_2(x) = -Q_2(x)A(x) + (1 + Q_2(x)Q_1(x))B(x).$$

Continuando de esta manera, encontraremos eventualmente que hay polinomios $R(x)$, $S(x)$, talque

$$R_n(x) = R(x)A(x) + S(x)B(x).$$

El caso interesante es cuando $A(x), B(x)$ son coprimos. En este caso dividiendo a través del polinomio constante R_n muestra que hay polinomios $R(x)$, $S(x)$ talque

$$1 = R(x)A(x) + S(x)B(x).$$

Así acabamos de demostrar el siguiente colorario.

Corolario 1.2 (Identidad de Bezout para polinomios)**.** Para cualquiera dos polinomios coprimo $P(x)$, $Q(x)$ con coeficientes racionales, existen polinomios $R(x)$, $S(x)$ con coeficientes racionales tales que

$$1 = R(x)P(x) + S(x)Q(x)$$

Un número complejo α es llamado *algebraico* si existe un polinomio no cero $P(x)$ con coeficientes enteros talque $P(\alpha) = 0$. Por ejemplo, $\sqrt{2} + \sqrt{3}$ es un número algebraico ya que $P\left(\sqrt{2} + \sqrt{3}\right) = 0$, donde

$$P(x) = x^4 - 10x^2 + 1.$$

Un polinomio no cero $P(x)$ con coeficientes enteros de grado mínimo para el cual $P(\alpha) = 0$ es llamado un *polinomio mínimo* del número algebraico α. Por la condición de mínimalidad del grado, tenemos que este polinomio es irreducible sobre $\mathbb{Q}[x]$, y por tanto sobre $\mathbb{Z}[x]$. Además, haciendo $R(\alpha) = 0$ para algún polinomio arbitrario $R(x)$ con coeficientes enteros. Por la suposición del grado mínimo, $\deg P(x) \leq \deg R(x)$. Entonces por el teorema de División Polinómica, se puede escribir

$$R(x) = P(x)Q(x) + S(x)$$

para algunos polinomios $Q(x), S(x)$ con coeficientes racionales, donde $\deg S(x) < \deg P(x)$. Multiplicando ambos lados por el mínimo común denominador de los coeficientes de los polinomios $Q(x), S(x)$ podemos asumir que $Q(x)$, $S(x)$ tiene coeficientes enteros. Ahora tomando $x = \alpha$ encontramos que $S(\alpha) = 0$. Por tanto, la condición de grado mínimo implica que $S(x) = 0$, i.e., $R(x)$ es divisible por $P(x)$. Asi todos los polinomios con α como raíz son múltiplos del polinomio mínimo.

Ejemplo 1.37. Determine todos los enteros positivos n tales que el polinomio

$$P(x) = x^{4n} + x^{4(n-1)} + \ldots + x^4 + 1$$

es divisible por

$$Q(x) = x^{2n} + x^{2(n-1)} + \ldots + x^2 + 1.$$

Solución. Si $x \neq 1$, entonces

$$\frac{P(x)}{Q(x)} = \frac{(x^4-1)P(x)}{(x^4-1)Q(x)}$$

$$= \frac{x^{4(n+1)}-1}{(x^2+1)(x^{2(n+1)}-1)}$$

$$= \frac{(x^{2(n+1)}-1)(x^{2(n+1)}+1)}{(x^2+1)(x^{2(n+1)}-1)}$$

$$= \frac{x^{2(n+1)}+1}{x^2+1}.$$

Si $Q(x)$ divide a $P(x)$, entonces el último cociente debe ser un polinomio. Si $(n+1)$ es impar, entonces $x^{2(n+1)}+1$ es divisible por x^2+1 y hemos terminado. Si $(n+1)$ es par, entonces x^2+1 divide a $x^{2(n+1)}-1$. Así, el resto de dividir $x^{2(n+1)}+1$ por x^2+1 es 2 y vemos que $Q(x)$ no divide a $P(x)$. Por lo que n debe ser par y todos los números pares cumplen la propiedad deseada. ■

Ejemplo 1.38. Sea $f(x) = a_0 + a_1x + \cdots + a_4x^4$ donde $a_4 \neq 0$. Los restos de f cuando es dividido por $(x-2003)$, $(x-2004)$, $(x-2005)$, $(x-2006)$ y $(x-2007)$ son 24, -6, 4, -6, 24. Hallar el valor de $f(2008)$.

Solución. El resto cuando el polinomio $f(x)$ es dividido por $(x-a)$ es[3] $f(a)$. De este modo la hipótesis puede reformularse como

$$f(2023) = f(2007) = 24, \quad f(2004) = f(2006) = -6, \quad \text{y} \quad f(2005) = 4.$$

Haciendo $f(x) = g(x-2005)$, necesitamos encontrar un polinomio cuártico g con $g(0) = 4$, $g(1) = g(-1) = -6$ y $g(2) = g(-2) = 24$. Ya que los valores de g son simétricos, buscamos un polinomio de la forma $g(x) = 4 + ax^2 + bx^4$. Entonces tenemos $-6 = g(1) = 4 + a + b$ y $24 = g(2) = 4 + 4a + 16b$. Resolviendo esas dos ecuaciones encontramos los valores de $a = -15$ y $b = 5$. En consecuencia $g(x) = 4 - 15x^2 + 5x^4$ es una posibilidad. Esta es la única solución, porque si $h(x)$ es cualquier otro polinomio cuártico con los mismos valores en 0, ±1, ±2, entonces $g(x) - h(x)$ tiene, como máximo, grado 4, pero tiene esos cinco puntos como raíces, por lo tanto, debe ser un polinomio cero. Así

$$f(x) = 4 - 15(x-2005)^2 + 5(x-2005)^4$$

y

$$f(2008) = 4 - 15 \cdot 9 + 5 \cdot 81 = 274.$$ ■

En la solución de arriba encontramos un polinomio de grado cuatro $f(x)$ con valores prescritos en cinco puntos específicamente para este fin. Cabría preguntarse si existe una forma más sistemática de hacer esto. Uno de esos métodos es la Fórmula de Interpolación de Lagrange. Supongamos que queremos hallar un polinomio de grado a lo más n para lo cual tenemos los valores prescritos de $(n+1)$ puntos, digamos $f(x_i) = a_i$ para $i = 0, \ldots, n$.

[3] Esta es una reformulación del hecho que $(x-a)$ divide a $f(x) - f(a)$.

Como se indicó anteriormente, solo existe un polinomio, ya que la diferencia de dos polinomios sería un polinomio de grado como máximo n con $(n+1)$ raíces.

El polinomio $(x-x_0)(x-x_1)\cdots(x-x_{k-1})(x-x_{k+1})\cdots(x-x_0)$ desaparece en x_0, x_1, …, x_{k-1}, x_{k+1}, …, x_n, esto es, en cualquiera de los x_i excepto x_k. Por lo tanto, el polinomio

$$\frac{(x-x_0)(x-x_1)\cdots(x-x_{k-1})(x-x_{k+1})\cdots(x-x_0)}{(x_k-x_0)(x_k-x_1)\cdots(x_k-x_{k-1})(x_k-x_{k+1})\cdots(x_k-x_0)}$$

desaparece en cualquier x_i como x_k y tomas los valores de 1 a x_k. Por lo tanto

$$f(x)=\sum_{k=0}^{n} a_k \frac{\prod_{i\neq k}(x-x_i)}{\prod_{i\neq k}(x_k-x_i)}$$

es un polinomio de grado a lo máximo n (porque, cada sumando tiene grado a lo máximo n) que toma los valores a_k en $x=x_k$. Esta es la extremadamente poderosa Fórmula de Interpolación de Lagrange.

Como ejemplo de su utilidad cabe señalar que este demuestra que un polinomio $f(x)$ de grado n toma valores racionales en $(n+1)$ valores racionales de x tiene coeficientes racionales. (Si todos los x_i y a_i son racionales, entonces la fórmula de arriba es un polinomio con coeficientes racionales, pero este es el único polinomio de grado a lo máximo n con $f(x_i)=a_i$.)

Para el problema de anterior la fórmula de Interpolación de Lagrange nos da

$$\begin{aligned} f(x) &= \frac{(x-2004)(x-2005)(x-2006)(x-2007)}{(-1)(-2)(-3)(-4)}\cdot 24 \\ &+ \frac{(x-2003)(x-2005)(x-2006)(x-2007)}{(1)(-1)(-2)(-3)}\cdot(-6) \\ &+ \frac{(x-2003)(x-2004)(x-2006)(x-2007)}{(2)(1)(-1)(-2)}\cdot 4 \\ &+ \frac{(x-2003)(x-2004)(x-2005)(x-2007)}{(3)(2)(1)(-1)}\cdot(-6) \\ &+ \frac{(x-2003)(x-2004)(x-2005)(x-2006)}{(4)(3)(2)(1)}\cdot 24 \end{aligned}$$

Luego volvemos a calcular $f(2008)=274$.

Ejemplo 1.39. Sea $P(x)$ un polinomio mónico de grado cuatro tal que $f(1+2^n)=1+8^n$ para todo $n=1,2,3,4$. Hallar el valor de $P(1)$.

Solución 1. Es claro que $P(2)=9$, $P(5)=65$, $P(9)=513$ y $P(17)=4097$. Asumamos que $P(1)=a$. Entonces,

$$P(x)=\frac{(x-2)(x-5)(x-9)(x-17)}{512}\cdot a$$

$$+\frac{(x-1)(x-5)(x-9)(x-17)}{-315}\cdot 9$$
$$+\frac{(x-1)(x-2)(x-9)(x-17)}{576}\cdot 65$$
$$+\frac{(x-1)(x-2)(x-5)(x-17)}{-1792}\cdot 513$$
$$+\frac{(x-1)(x-2)(x-5)(x-9)}{23040}\cdot 4097.$$

Como $P(x)$ es mónico, examinando el coeficiente de x^4 en ambos lados, obtenemos

$$1=\frac{a}{512}-\frac{9}{315}+\frac{65}{576}-\frac{513}{1792}+\frac{4097}{23040}.$$

Entonces, $a=513$. ■

Solución 2. La declaración del problema nos dice que el polinomio

$$P(x)-(x-1)^3-1=P(x)-x^3+3x^2-3x$$

tiene cuatro raíces reales, i.e. $x=2,4,9,17$. Como el polinomio es mónico podemos encontrar que $P(x)-x^3+3x^2-3x$ es también un polinomio mónico. Por consiguiente,

$$P(x)-x^3+3x^2-3x=(x-2)(x-5)(x-9)(x-19).$$

Haciendo $x=1$, hallamos que $P(1)=1+512=513$. ■

Ejemplo 1.40 (Sebian TST 2016. Dusan Djukic)**.** Definida una familia de polinomios como

$$P_0(x)=x^3-4x \quad \text{y} \quad P_{n+1}(x)=P_n(1+x)P_n(1-x)-1.$$

Probar que x^{2016} divide a $P_{2016}(x)$.

Solución. Claramente, $P_n(x)=P_n(-x)$. Ahora, vemos que tenemos

$$\begin{aligned}P_{n+2}(x)&=P_{n+1}(1+x)P_{n+1}(1-x)-1\\&=[P_n(2+x)P_n(-x)-1][P_n(2-x)P_n(x)-1]-1\\&=P_n(2+x)P_n(2-x)P_n(x)^2-(P_n(2+x)+P_n(2-x))\,P_n(x).\end{aligned}$$

Encontramos que $P_{n+2}(x)$ es divisible por $P_n(x)$. Así, como $P_0(2)=0$, entonces $P_n(2)=0$, para todo número natural par n. Haciendo $x=0$ en el polinomio $P_n(2+x)+P_n(2-x)$, obtenemos $P_n(2)+P_n(2)=0$ para todos los números naturales impares n. En consecuencia $P_n(2+x)+P_n(2-x)$ es divisible por x, por tanto, el término x^1 se cancela en la división por x^2. Ahora, si existe algún $k\geq 2$ tal que $x^k(x-2)$ divide a $P_n(x)$, tenemos que $x^{k+2}(x-2)$ divide a $P_{n+2}(x)$. Como $P_2(x)$ es divisible por $x^2(x-2)$, obtenemos por inducción que $x^{2n}(x-2)$ divide a $P_{2n}(x)$, lo que da la conclusión. ■

Ejemplo 1.41. Definida una familia de polinomios como

$$P_1(x) = 2x, \quad P_2(x) = 2(x^2+1)$$

y para todo $n \geq 3$,

$$P_n(x) = (2x)P_{n-1}(x) - (x^2-1)P_{n-2}(x).$$

Probar que $P_n(x)$ es divisible por (x^2+1) si y solo si $n \equiv 2 \pmod 4$.

Solución. Dado que el polinomio característico de esta recursividad de coeficiente constante es

$$T^2 - 2xT + (x^2-1) = (T-x-1)(T-x+1),$$

vemos que la solución general es $P_n(x) = c_1(x+1)^n + c_2(x-1)^n$ para algunas constantes c_1, c_2. Reemplazando los valores iniciales dados, encontramos que

$$P_n(x) = (x+1)^n + (x-1)^n.$$

Haciendo $n = r + 4k$, donde $0 \leq r \leq 3$. Entonces,

$$P_n(x) = (x+1)^r[(x+1)^4]^k + (x-1)^r[(x-1)^4]^k.$$

Escribiendo la expresión anterior como

$$(x+1)^r[(1+x^2)(x^2+4x+5)-4]^k + (x-1)^r[(1+x^2)(x^2-4x+5)-4]^k.$$

Luego el resto de tal polinomio cuando es dividido por $(1+x^2)$ es el mismo que el resto de $(-4)^k[(x+1)^r + (x-1)^r]$. Probando $r = 0, 1, 2, 3$ encontramos que solo en $r = 2$ la expresión anterior es divisible por $(1+x^2)$. ■

Índice alfabético