TEMA 3

Aritmética entera y polinomial

3.1 Números naturales: División y bases de numeración.

Definición 1. Denotamos al conjunto de los números naturales mediante el símbolo $\mathbb{N}$. En los naturales tenemos definidas dos operaciones conocidas por todos que son la suma y el producto, operaciones cuyas propiedades son sobradamente conocidas y que explicitaremos en el apartado de números enteros.

Definición 2 (Orden)**.** Decimos que $n \leq m$ si existe $c \in \mathbb{N}$ tal que $m = n + c$.

Proposición 3. *La relación $\leq$ satisface las propiedades siguientes:*

Reflexiva: *$n \leq n$ para cualquier natural n.*

Antisimétrica: *si $n \leq m$ y $m \leq n$ entonces $n = m$.*

Transitiva: *si $n \leq m$ y $m \leq p$ entonces $n \leq p$.*

Proposición 4. *Para cualesquiera $a, b, c \in \mathbb{N}$ con $a \leq b$ se tiene $a + c \leq b + c$ y $ac \leq bc$.*

Proposición 5. *1. La relación $\leq$ es un orden total, es decir, para cualesquiera $n, m \in \mathbb{N}$ se tiene $n \leq m$ o $m \leq n$.*

2. La relación $\leq$ es un buen orden, es decir, todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo.

Teorema 6 (Algoritmo de la división)**.** *Para cualesquiera $a, b \in \mathbb{N}$ con $b \neq 0$ existen únicos $c, r \in \mathbb{N}$ con $0 \leq r < b$ tales que $a = c \cdot b + r$.*

Teorema 7. *Dado un natural $b \geq 2$ y $k \geq 1$, todo $n < b^k$ se representa de manera única como*

$$n = d_{k-1} \cdot b^{k-1} + d_{k-2} \cdot b^{k-2} + \cdots + d_1 \cdot b + d_0$$

donde $0 \leq d_i < b$ para todo $i = 0, \ldots, k-1$.

Busquemos b símbolos que representen a cada uno de los números naturales comprendidos entre 0 y $b-1$. En virtud del Teorema 7 todo natural n se representa de manera única como $n = d_{k-1}d_{k-2}\ldots d_1 d_0)_b$ donde los d_i son los símbolos anteriores. La representación nos dice que

$$n = d_{k-1} \cdot b^{k-1} + \cdots + d_1 \cdot b + d_0.$$

Si $n = d_{k-1}d_{k-2}\ldots d_1 d_0)_b$ con $d_{k-1} \neq 0$ decimos que n es un número de exactamente k dígitos en base b. Observemos que n tiene exactamente k dígitos en base b si y sólo si $b^{k-1} \leq n < b^k$, lo que nos permite comprobar que el número de dígitos en base b de n es $\lfloor \log_b n \rfloor + 1$, donde $\lfloor \_ \rfloor$ representa la función *parte entera*.

Para pasar de base b a base 10 basta con utilizar la aritmética usual en la base 10. Para pasar de base 10 a base b el Teorema 7 nos da la clave, hay que realizar divisiones e ir tomando los restos. Por ejemplo, para convertir 25 a binario realizamos divisiones sucesivas entre 2, la base, y nos quedamos con los restos:

$$\begin{aligned} 25 &= 2 \times 12 + 1 \\ 12 &= 2 \times 6 + 0 \\ 6 &= 2 \times 3 + 0 \\ 3 &= 2 \times 1 + 1 \\ 1 &= 2 \times 0 + 1 \end{aligned}$$

Por tanto $25 = 11001)_2$

Existe una situación en la que es especialmente sencillo hacer cambios de base. Vamos a cambiar de base b a base b^s y viceversa. Todo natural comprendido entre 0 y $b^s - 1$ se escribe como $d_{s-1}b^{s-1} + \cdots + d_1 b + d_0$ donde los símbolos $d_0, \ldots d_{s-1}$ son dígitos en base b. Así, todo dígito en base b^s se escribe mediante s dígitos en base b. Así, si $n = (D_{k-1} \ldots D_1 D_0)_{b^s}$, y $D_i = (d_{s-1}^{(i)} \ldots d_1^{(i)} d_0^{(i)})_b$ tenemos que

$$\begin{aligned} n &= D_{k-1}(b^s)^{k-1} + \cdots + D_1 b^s + D_0 \\ &= (d_{s-1}^{(k-1)} b^{s-1} + \cdots + d_1^{(k-1)} b + d_0^{(k-1)})(b^s)^{k-1} + \\ &\quad \cdots + (d_{s-1}^{(1)} b^{s-1} + \cdots + d_1^{(1)} b + d_0^{(1)}) b^s + (d_{s-1}^{(0)} b^{s-1} + \cdots + d_1^{(0)} b + d_0^{(0)}) \\ &= d_{s-1}^{(k-1)} b^{(k-1)s+(s-1)} + \cdots + d_1^{(k-1)} b^{(k-1)s+1} + d_0^{(k-1)} b^{(k-1)s} + \\ &\quad \cdots + d_{s-1}^{(1)} b^{s+s-1} + \cdots + d_1^{(1)} b^{s+1} + d_0^{(1)} b^s + d_{s-1}^{(0)} b^{s-1} + \cdots + d_1^{(0)} b + d_0^{(0)}, \end{aligned}$$

es decir,

$$(D_{k-1} \ldots D_1 D_0)_{b^s} = (d_{s-1}^{(k-1)} \ldots d_1^{(k-1)} d_0^{(k-1)} \ldots d_{s-1}^{(1)} \ldots d_1^{(1)} d_0^{(1)} d_{s-1}^{(0)} \ldots d_1^{(0)} d_0^{(0)})_b.$$

Cada dígito en base b^s se sustituye por su representación mediante s dígitos en base b. El proceso inverso es completamente análogo.

Ejemplo 8. Convertimos

$$n = 10010010111010010011100 1010)_2$$

a base $16 = 2^4$. Para ello agrupamos n en bloques de cuatro bits,

$$n = \underline{100}\,\underline{1001}\,\underline{0111}\,\underline{0100}\,\underline{1001}\,\underline{1100}\,\underline{1010})_2$$

como $100)_2 = 4 = 4)_{16}$, $1001)_2 = 9 = 9)_{16}$, $0111)_2 = 7 = 7)_{16}$, $1100)_2 = 12 = C)_{16}$ y $1010)_2 = 10 = A)_{16}$,

$$n = 49749CA)_{16}.$$

Recíprocamente, convertimos $m = 74051)_8$ a base 2. Ya que $7)_8 = 111)_2$, $4)_8 = 100)_2$, $0)_8 = 000)_2$, $5)_8 = 101)_2$ y $1_8 = 001)_2$, tememos que $m = 111\,100\,000\,101\,001)_2$. Este es el motivo por el que las bases 8 y 16 se utilizan mucho en diversos campos de la informática.

3.2 Números enteros

En el conjunto $\mathbb{Z}$ de los números enteros conocemos dos operaciones, la suma y el producto, que satisfacen las propiedades que vamos a describir a continuación

Proposición 9. *La suma de números enteros es*

conmutativa, *es decir, para cualesquiera $x, y \in \mathbb{Z}$, $x + y = y + x$,*

asociativa, *es decir, para cualesquiera $x, y, z \in \mathbb{Z}$, $x + (y + z) = (x + y) + z$,*

tiene elemento neutro, *es decir, existe un elemento $0 \in \mathbb{Z}$ (necesariamente único) tal que para cualquier $x \in \mathbb{Z}$, $x + 0 = 0 + x = x$,*

tiene elemento simétrico, *es decir, para cualesquiera $x \in \mathbb{Z}$ existe $-x \in \mathbb{Z}$ (llamado opuesto) tal que $x + (-x) = (-x) + x = 0$.*

Proposición 10. *El producto de números enteros es*

conmutativo, *es decir, para cualesquiera $x, y \in \mathbb{Z}$, $xy = yx$,*

asociativo, *es decir, para cualesquiera $x, y, z \in \mathbb{Z}$, $x(yz) = (xy)z$,*

tiene elemento neutro, *es decir, existe un elemento $1 \in \mathbb{Z}$ (necesariamente único) tal que para cualquier $x \in \mathbb{Z}$, $x1 = 1x = x$*

distributivo respecto de la suma, *es decir, para cualesquiera* $x, y, z \in \mathbb{Z}$, $(x+y)z = xz+yz$ *y* $x(y+z) = xy+xz$.

Es decir, $\mathbb{Z}$ es un anillo conmutativo. Además es lo que se conoce como **dominio**, es decir, si $a, b \in \mathbb{Z} \setminus \{0\}$ entonces $ab \neq 0$

Definición 11 (Orden)**.** El orden en $\mathbb{Z}$ se define igual que en $\mathbb{N}$, es decir, decimos que $p \leq q$ si existe $n \in \mathbb{N}$ tal que $q = p + n$.

Muchas de las propiedades son análogas

Proposición 12. *La relación* $\leq$ *es reflexiva, antisimétrica y transitiva.*

Proposición 13. *Para cualesquiera* $a, b, c \in \mathbb{Z}$ *con* $a \leq b$ *se tiene* $a + c \leq b + c$*. Además, si* $c \geq 0$ *se tiene que* $ac \leq bc$*, y si* $c \leq 0$ $bc \leq ac$.

Definición 14 (Valor absoluto)**.** Para todo $p \in \mathbb{Z}$ se define el valor absoluto de p como

$$|p| = \begin{cases} p & \text{si } p \geq 0 \\ -p & \text{si } p < 0 \end{cases}$$

Teorema 15 (Algoritmo de la división)**.** *Para cualesquiera* $a, b \in \mathbb{Z}$ *con* $b \neq 0$*, existen únicos* $q, r \in \mathbb{Z}$ *tales que* $a = q \cdot b + r$ *y* $0 \leq r < |b|$.

En la división el resto se denota a mód b y el cociente suele representarse por a quo b.

3.3 Divisibilidad

Definición 16. Dados $a, b \in \mathbb{Z}$, decimos que a divide a b si existe $c \in \mathbb{Z}$ tal que $ac = b$. Se denota $a \mid b$. Es inmediato comprobar que

$$a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b,$$

por lo que para estudiar la divisibilidad podemos restringirnos siempre a los valores absolutos de los enteros implicados.

Proposición 17. *Para cualesquiera* $a, b \in \mathbb{Z}$*,*

1. $a \mid a$,
2. $1 \mid a$,
3. $a \mid 0$,
4. *si* $a, b \neq 0$ *y* $a \mid b$ *entonces* $|a| \leq |b|$.

Definición 18. Dados $a, b \in \mathbb{Z}$, decimos que d es el máximo común divisor de a y b ($d = \text{mcd}(a, b)$) si

1. $d \mid a$ y $d \mid b$,
2. si $e \mid a$ y $e \mid b$ entonces $e \leq d$.

Lema 19. *Si* $a = cb + r$ *entonces* $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración. Sean $d_1 = \text{mcd}(a, b)$ y $d_2 = \text{mcd}(b, r)$. Dado que d_2 divide a b y a r, también divide a a, por lo que $d_2 \leq d_1$. Análogamente, como $r = a - cb$ y d_1 divide a a y a b tenemos que d_1 divide a r, por lo que $d_1 \leq d_2$. Por tanto $d_1 = d_2$. □

Algoritmo de Euclides

procedure MCD(a, b)
  $a \leftarrow |a|$, $b \leftarrow |b|$
  repeat
    $r \leftarrow a$ mód b

$a \leftarrow b$
$b \leftarrow r$
until $r = 0$
return a
end procedure

El algoritmo termina porque los restos son todos mayores o iguales que 0 y cada vez menores.

Observación 20. Supongamos que $x = u_x a + v_x b$ e $y = u_y a + v_y b$, es decir, x, y son combinaciones lineales de a y b. Si $x = cy + r$ entonces, sustituyendo los valores de x e y, tenemos:

$$\begin{aligned} r &= x - cy \\ &= (u_x a + v_x b) - c(u_y a + v_y b) \\ &= (u_x - cu_y)a + (v_x - cv_y)b, \end{aligned}$$

por lo que r también puede escribirse como combinación lineal de a y b. En vista de esta propiedad en cada repetición del algoritmo de Euclides podemos expresar el resto como combinación lineal de a y b.

La Observación 20 tiene dos consecuencias. En primer lugar sirve para demostrar la Propiedad Lineal:

Proposición 21 (Propiedad lineal). *Si $d = \mathrm{mcd}(a, b)$ entonces existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$.*

Demostración. Cada resto calculado puede escribirse como combinación lineal entera de a y b. □

Corolario 22. *Si $c \mid a$ y $c \mid b$ entonces $c \mid \mathrm{mcd}(a, b)$.*

Demostración. Por hipótesis tenemos que $a = sc$ y $b = tc$ para ciertos $s, t \in \mathbb{Z}$. Llamemos $d = \mathrm{mcd}(a, b)$, por la Proposición 21 existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$. Por tanto

$$d = ua + vb = usc + vtc = (us + vt)c,$$

luego $c \mid d$ como queríamos. □

En segundo lugar la Observación 20 también es la clave del conocido como Algoritmo de Euclides extendido:

Algoritmo 23 (Algoritmo de Euclides extendido). **procedure** MCDEX(a, b)
$s \leftarrow \frac{a}{|a|}$, $t \leftarrow \frac{b}{|b|}$
$a \leftarrow |a|$, $b \leftarrow |b|$
$u'' \leftarrow 1$, $v'' \leftarrow 0$
$u' \leftarrow 0$, $v' \leftarrow 1$
repeat
$r \leftarrow a$ mód b
$q \leftarrow a$ quo b
$a \leftarrow b$
$b \leftarrow r$
$u \leftarrow u'' - qu'$, $u'' \leftarrow u'$, $u' \leftarrow u$
$v \leftarrow v'' - qv'$, $v'' \leftarrow v'$, $v' \leftarrow v$
until $r = 0$
return a, su'', tv''
end procedure

Teorema 24 (Bezout). *Sean $a, b \neq 0$. $\mathrm{mcd}(a, b) = 1$ si y sólo si existen $u, v \in \mathbb{Z}$ tales que $1 = ua + vb$.*

Demostración. Una implicación es aplicación directa de la Proposición 21. Si $d \mid a$, $d \mid b$ y $1 = ua + vb$ entonces $d \mid 1$, de donde $d = \pm 1$, lo que nos dice que $\mathrm{mcd}(a, b) = 1$. □

Definición 25. Dados $a, b \in \mathbb{Z}$, decimos que $m \geq 0$ es el mínimo común múltiplo de a y b ($m = \mathrm{mcm}(a, b)$) si

1. $a \mid m$ y $b \mid m$,
2. si $a \mid n$ y $b \mid n$ entonces $m \leq |n|$.

Proposición 26. *Para cualesquiera $a, b \in \mathbb{Z}$*

$$|ab| = \mathrm{mcd}(a, b)\,\mathrm{mcm}(a, b)$$

3.4 Ecuaciones Diofánticas

Una ecuación diofántica es una ecuación del tipo

$$ax + by = c, \text{ donde } a, b, c \in \mathbb{Z}, \tag{2}$$

y de la que queremos encontrar sus soluciones enteras, es decir, encontrar valores $x_0, y_0 \in \mathbb{Z}$ que satisfagan la ecuación.

Proposición 27. *La ecuación* (2) *tiene solución si y sólo si* $\text{mcd}(a, b) \mid c$.

Proposición 28. *Si* (x_0, y_0) *es una solución de* (2) *y* $d = \text{mcd}(a, b)$*, entonces todas las soluciones se calculan mediante las fórmulas*

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n \tag{3}$$

con $n \in \mathbb{Z}$.

3.5 Congruencias y aritmética modular

Definición 29. Sea $m \in \mathbb{Z}$ $m \neq 0, \pm 1$. Sean $a, b \in \mathbb{Z}$. Decimos que a es congruente con b módulo m si $m \mid a - b$. Este hecho se denota

$$a \equiv b \pmod{m}$$

Proposición 30. *La congruencia módulo* m *es una relación de equivalencia, es decir,*

1. (reflexiva) $a \equiv a \pmod{m}$,
2. (simétrica) *si* $a \equiv b \pmod{m}$ *entonces* $b \equiv a \pmod{m}$,
3. (transitiva) *si* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$ *entonces* $a \equiv c \pmod{m}$.

Proposición 31. *Si* $a \equiv a' \pmod{m}$ *y* $b \equiv b' \pmod{m}$*, entonces* $a + b \equiv a' + b' \pmod{m}$ *y* $ab \equiv a'b' \pmod{m}$

Observación 32. Hay otras propiedades sencillas referentes a congruencias

1. si $a \equiv b \pmod{m}$ y $d \mid m$ entonces $a \equiv b \pmod{d}$,
2. si $d \mid a, b, m$ y $a \equiv b \pmod{m}$ entonces $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$,
3. si $a \equiv b \pmod{m_1}$ y $a \equiv b \pmod{m_2}$ entonces $a \equiv b \pmod{\text{mcm}(m_1, m_2)}$.

Definición 33. Sea $m \in \mathbb{Z}$ con $m \neq 0, 1$. No perdemos generalidad con suponer que $m \geq 0$, ya que podemos sustituir m por $|m|$ para estudiar divisibilidad. Llamamos $\mathbb{Z}_m$ al conjunto cociente $\mathbb{Z}$ sobre la relación de equivalencia ser congruente módulo m. Tenemos entonces que $\mathbb{Z}_m = \{[0], \ldots, [m-1]\}$. Vamos a definir dos operaciones en $\mathbb{Z}_m$,

Suma $[a] + [b] = [a + b]$,

Producto $[a][b] = [ab]$.

Estas definiciones están bien hechas (es decir, no dependen del representante) en virtud de la Proposición 31. Vamos a identificar normalmente $\mathbb{Z}_m$ con $\{0, \ldots, m-1\}$. Vía esta identificación, las operaciones en $\mathbb{Z}_m$ quedan de la siguiente forma para $0 \leq a, b, c \leq m - 1$,

Suma $a + b = c$ si y sólo si $a + b \equiv c \pmod{m}$,

Producto $ab = c$ si y sólo si $ab \equiv c \pmod{m}$.

Lema 34. *La ecuación* $ax \equiv b \pmod{m}$ *tiene solución si y sólo si* $\text{mcd}(a, m) \mid b$*. Si* x_0 *es una solución de la ecuación anterior entonces todas las soluciones son de la forma* $x = x_0 + \frac{m}{\text{mcd}(a,m)}n$ *con* $n \in \mathbb{Z}$.

3.6 Sistemas de congruencias

Lema 35. *Sean $m, n, k \in \mathbb{Z}$ con* $\text{mcd}(m, n) = \text{mcd}(m, k) = 1$. *Entonces* $\text{mcd}(m, nk) = 1$.

Teorema 36 (Teorema chino del resto)**.** *Si $m_1, \ldots, m_k$ son enteros primos relativos dos a dos, entonces el sistema de ecuaciones*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{4}$$

tiene solución única módulo $M = m_1 m_2 \ldots m_k$.

Demostración. Para cada j sea $M_j = \frac{m_1 \ldots m_k}{m_j} = \frac{M}{m_j}$ y b_j un entero que satisface $M_j b_j \equiv 1 \pmod{m_j}$, el cual existe porque $\text{mcd}(m_j, M_j) = 1$ en virtud del Lema 35. La solución del sistema es $x = a_1 M_1 b_1 + \cdots + a_k M_k b_k$. La unicidad es consecuencia de que $\text{mcm}(m_i, m_j) = m_i m_j$ si $i \neq j$ y de la Observación 32. □

Analicemos el caso general. Vamos a dar un procedimiento iterativo para resolver sistemas de ecuaciones en congruencias del tipo

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \quad \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases} \tag{5}$$

sin restricciones en los posibles valores de $m_1, \ldots, m_k$. En primer lugar resolvemos la primera ecuación mediante el Lema 34, que en caso de tener solución será de la forma

$$x \equiv c_1 \pmod{m_1'}.$$

Consideremos las dos primeras ecuaciones,

$$\begin{cases} x \equiv c_1 \pmod{m_1'} \\ a_2 x \equiv b_2 \pmod{m_2} \end{cases}$$

La primera ecuación puede describirse como $x = c_1 + m_1' s$ donde $s \in \mathbb{Z}$. Sustituyendo dicho valor de x en la segunda ecuación tenemos

$$a_2(c_1 + m_1' s) \equiv b_2 \pmod{m_2},$$

o lo que es lo mismo

$$a_2 m_1' s \equiv b_2 - a_2 c_1 \pmod{m_2}.$$

Hallamos los valores de s para los que dicha ecuación es cierta, es decir, resolvemos la ecuación anterior de nuevo mediante el Lema 34. La solución será de la forma $s = s_0 + m_2' n$ para cualquier $n \in \mathbb{Z}$. Susituyendo s tenemos la solución $x = c_1 + m_1'(s_0 + m_2' n) = c_1 + m_1' s_0 + m_1' m_2' n$ para cualquier $n \in \mathbb{Z}$, o equivalentemente

$$x \equiv c_1 + m_1' s_0 \pmod{m_1' m_2'}.$$

Nuestro sistema (5) se ha convertido en el sistema

$$\begin{cases} x \equiv c_2 \pmod{m_1' m_2'} \\ a_3 x \equiv b_3 \pmod{m_3} \\ \quad \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases},$$

que es un sistema del mismo tipo que (5) pero con una ecuación menos. Podemos reiterar el proceso hasta alcanzar una única ecuación que nos dará la solución, si existe.

3.7 Números primos

Definición 37. Un número entero $p \in \mathbb{Z}$ $p \neq \pm 1$ se dice primo si satisface algunas de las siguientes afirmaciones equivalentes:

1. sus únicos divisores son ± 1 y $\pm p$,
2. para cualquier $1 \leq a < p$ se tiene que $\text{mcd}(a, p) = 1$,
3. $\mathbb{Z}_p$ es un cuerpo, es decir, todo elemento no nulo de $\mathbb{Z}_p$ tiene inverso,
4. para cualesquiera $a, b \in \mathbb{Z}$, $p \mid ab$ implica $p \mid a$ o $p \mid b$.

Proposición 38. *Hay infinitos números primos.*

Teorema 39 (Fundamental de la aritmética). *Todo entero m se escribe de manera única como $m = \pm p_1^{\alpha_1} \dots p_k^{\alpha_k}$ donde $p_1 < \dots < p_k$ son primos positivos y $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$.*

Teorema 40 (Pequeño de Fermat). *Sea p un entero primo. Si p no divide a a entonces $a^{p-1} \equiv 1$ (mód p).*

3.8 Polinomios y aritmética

Definición 41. Sea A un anillo conmutativo y x una variable. Un polinomio sobre A es una expresión formal

$$a_0 + a_1 x + \dots + a_n x^n$$

donde $a_0, \dots a_n \in A$. Salvo que el polinomio sea cero la representación se suele presentar normalizada para que $a_n \neq 0$. En este caso decimos que el grado es n, y el coeficiente líder a_n. Si $p(x)$ es un polinomio cualquiera representamos el grado por $\deg(p)$ o $\deg(p(x))$. Al polinomio cero no se le asigna grado o se dice que tiene grado $-\infty$. El conjunto de los polinomios sobre A se denota $A[x]$.

Definición 42. Si $a(x) = a_0 + a_1 x + \dots a_n x^n$ y $b(x) = b_0 + b_1 x + \dots b_m x^m$, definimos la suma de $a(x)$ y $b(x)$ como

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_p + b_p)x^p$$

donde $p = \text{máx}\{n, m\}$, $a_i = 0$ si $i > n$ y $b_j = 0$ si $j > m$.

Definición 43. Igualmente, si $a(x) = a_0 + a_1 x + \dots a_n x^n$ y $b(x) = b_0 + b_1 x + \dots b_m x^m$, definimos el producto de $a(x)$ y $b(x)$ como

$$a(x)b(x) = c_0 + c_1 x + \dots + c_{n+m} x^{n+m}, \text{ con } c_k = \sum_{i+j=k} a_i b_j.$$

Observación 44. Si $p, q \in A[x]$, $\deg(p+q) \leq \text{máx}\{\deg(p), \deg(q)\}$ y $\deg(pq) \leq \deg(p) + \deg(q)$.

Proposición 45. *$(A[x], +, \cdot)$ es un anillo conmutativo.*

Demostración. Mecánica, sólo hay que tener cuidado en manipular subíndices. □

3.9 Divisibilidad

Teorema 46. *Sea $\Bbbk$ un cuerpo. Para cualesquiera $p, q \in \Bbbk[x]$ con $q \neq 0$ existen únicos $c, r \in \Bbbk[x]$ tales que $p = cq + r$ y $\deg(r) < \deg(q)$.*

Definición 47. Sean $a, b \in \Bbbk[x]$. Decimos que d es un *máximo común divisor* de a y b si $d \mid a$, $d \mid b$ y para cualquier elemento c con $c \mid a$ y $c \mid b$ se tiene que $c \mid d$. Denotamos $\text{MCD}(a, b)$ al conjunto de los elementos que son máximo común divisor de a y b.

Proposición 48. *Para cualesquiera $a, b \in \Bbbk[x]$, $d \in \text{MCD}(a, b)$ si y sólo si*

$$\text{MCD}(a, b) = \{ud \mid u \in \Bbbk \setminus \{0\}\}$$

Lema 49. *Sean $a, b \in \Bbbk[x]$. Si $a = cb + r$. Entonces* $\mathrm{MCD}(b, r) = \mathrm{MCD}(a, b)$

Demostración. Sea $d \in \mathrm{MCD}(a, b)$. Dado que $r = a - cb$, tenemos que cualquier divisor de a y b también divide a r, en particular $d \mid r$. Por otra parte, si $e \mid b$ y $e \mid r$, dado que $a = cb + r$ tenemos que $e \mid a$, de donde $e \mid d$ por la definición de máximo común divisor. Por tanto $d \in \mathrm{MCD}(b, r)$. La otra inclusión se obtiene análogamente. □

Teorema 50 (Algoritmo de Euclides)**.** *Si $a, b \in \Bbbk[x]$ entonces* $\mathrm{MCD}(a, b) \neq \varnothing$.

Demostración. El siguiente procedimiento permite justificar la existencia y calcular el máximo común divisor de a y b. Podemos suponer que tanto a como b son distintos de cero.

1. Realizamos la división, es decir, calculamos q, r tales que $a = qb + r$ con $r = 0$ o $\deg(r) < \deg(b)$.
2. Si $r = 0$ entonces $b \in \mathrm{MCD}(a, b)$, si no asignamos a el valor de b, a b el de r y repetimos el paso 1.

El proceso debe terminar porque los restos tienen norma cada vez menor. Además, por el Lema 49 el resultado es el correcto. □

Proposición 51 (Propiedad lineal)**.** *Sean $a, b \in \Bbbk[x]$. Si $d \in \mathrm{MCD}(a, b)$ entonces existen $u, v \in \Bbbk[x]$ tales que $d = ua + vb$.*

Demostración. Esencialmente la misma que la de la Proposición 21. □

El Algoritmo Extendido de Euclides que se presenta en el Algoritmo 23 del Tema 3 funciona exactamente igual para $\Bbbk[x]$. De la misma manera tenemos el siguiente teorema:

Teorema 52 (Bezout)**.** *Sean $a, b \in \Bbbk[x] \setminus \{0\}$. $1 \in \mathrm{MCD}(a, b)$ si y sólo si existen polinomios u, v tales que $1 = ua + vb$.*

Observación 53. Algunas consecuencias directas del Teorema de Bezout son las siguientes:

1. Si $d \in \mathrm{MCD}(a, b)$ entonces $1 \in \mathrm{MCD}(\frac{a}{d}, \frac{b}{d})$.
2. Si $1 \in \mathrm{MCD}(a, b)$ y $a \mid bc$, como $1 = ua + vb$ tenemos que $c = uac + vbc$, de donde $a \mid c$.
3. Es sencillo comprobar que $\mathrm{MCD}(a, b) = \Bbbk \setminus \{0\}$ si y sólo si $\mathrm{MCD}(a, b) \cap \Bbbk \setminus \{0\} \neq \varnothing$.

Terminamos la sección con un resultado que relaciona el máximo común divisor y el mínimo común múltiplo, que se define de forma natural.

Proposición 54. *Sean $a, b \in \Bbbk[x]$ y sea $d, m \in \Bbbk[x]$ tales que $dm = ab$. Entonces $d \in \mathrm{MCD}(a, b)$ si y sólo si $m \in \mathrm{MCM}(a, b)$.*

Demostración. Supongamos que $d \in \mathrm{MCD}(a, b)$ y escribamos $a = a'd$ y $b = b'd$. Necesariamente $m = a'b = ab'$, por lo que m es múltiplo de a y de b. Supongamos que c es múltiplo de a y b. Tenemos entonces que $c = a''a'd = b''b'd$. Así $b' \mid a''a'$, y en vista de la Observación 53 tenemos que $b' \mid a''$, es decir, $a'' = a'''b'$. Por tanto $c = a'''b'a'd = a'''m$ y $m \mid c$, lo que implica que $m \in \mathrm{MCM}(a, b)$.

Supongamos ahora que $m \in \mathrm{MCM}(a, b)$. Podemos escribir $m = a'a = b'b$, y dado que m es un mínimo común múltiplo podemos deducir que $1 \in \mathrm{MCD}(a', b')$. Dado que $dm = ab$ tenemos que $a'dm = a'ab = mb$, por lo que $b = a'd$ y $d \mid b$. Análogamente $a = b'd$ y $d \mid a$. Supongamos que $c \mid a$ y $c \mid b$. Como $1 = ua' + vb'$ tenemos que $d = ua'd + vb'd = ub + va$, de donde $c \mid d$ y $d \in \mathrm{MCD}(a, b)$. □

3.10 Congruencias

Todas las definiciones y propiedades de la Sección 3.5 del Tema 3 se pueden extender a $\Bbbk[x]$ de manera directa.

Definición 55. Sean $a, b, m \in \Bbbk[x]$. Decimos que a es congruente con b módulo m si $m \mid a - b$. Este hecho se denota

$$a \equiv b \pmod{m}$$

Proposición 56. *La congruencia módulo m es una relación de equivalencia, es decir,*

1. (reflexiva) $a \equiv a \pmod{m}$,
2. (simétrica) *si* $a \equiv b \pmod{m}$ *entonces* $b \equiv a \pmod{m}$,
3. (transitiva) *si* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$ *entonces* $a \equiv c \pmod{m}$.

Proposición 57. *Si* $a \equiv a' \pmod{m}$ *y* $b \equiv b' \pmod{m}$, *entonces* $a + b \equiv a' + b' \pmod{m}$ *y* $ab \equiv a'b' \pmod{m}$

Demostración. La misma que la Proposición 31 □

Observación 58. Las propiedades descritas en la Observación 32 también son ciertas para un anillo de polinomios:

1. si $a \equiv b \pmod{m}$ y $d \mid m$ entonces $a \equiv b \pmod{d}$,
2. si $d \mid a, b, m$, tenemos que $a \equiv b \pmod{m}$ si y sólo si $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$,
3. $a \equiv b \pmod{m_1}$ y $a \equiv b \pmod{m_2}$ si y sólo si $a \equiv b \pmod{m}$, donde $m \in \mathrm{MCM}(m_1, m_2)$.

Definición 59. Sea $m \in \Bbbk[x]$ con $\deg(m) > 0$. Llamamos $\Bbbk[x]_m$ al conjunto cociente $\Bbbk[x]$ sobre la relación de equivalencia ser congruente módulo m. De nuevo tenemos dos operaciones en $\Bbbk[x]_m$,

Suma $[a] + [b] = [a + b]$,

Producto $[a][b] = [ab]$.

Estas definiciones están bien hechas (es decir, no dependen del representante) en virtud de la Proposición 57. Como en el caso de $\mathbb{Z}$ podemos identificar $\Bbbk[x]_m$ con el conjunto de los restos de las divisiones por m. Vía esta identificación las operaciones en $\Bbbk[x]_m$ quedan de la siguiente forma para a, b, c restos módulo m,

Suma $a + b = c$ si y sólo si $a + b \equiv c \pmod{m}$,

Producto $ab = c$ si y sólo si $ab \equiv c \pmod{m}$.

Lema 60. *La ecuación* $ax \equiv b \pmod{m}$ *tiene solución si y sólo si* $\mathrm{MCD}(a, m) \mid b$.

Demostración. Se obtiene a partir de la Proposición 51 tal y como el Lema 34 se obtiene a partir de la Proposición 21 □

Teorema 61 (Teorema chino del resto)**.** *Si* $m_1, \ldots, m_k \in A$ *tales que* $1 \in \mathrm{MCD}(m_i, m_j)$ *para toda pareja* i, j, *entonces el sistema de ecuaciones*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{6}$$

tiene solución única módulo $M = m_1 m_2 \ldots m_k$.

Demostración. Análoga al Teorema 36 del Tema 3, utilizando una versión para anillos de polinomios del Lema 35 del mismo Tema. □

3.11 Irreducibilidad y Teorema Fundamental de la Aritmética

Definición 62. Decimos que $a, b \in \Bbbk[x]$ son asociados (abreviadamente $a \sim b$) si $a = ub$ con $u \in \Bbbk \setminus \{0\}$. Un polinomio $p \in \Bbbk[x]$ se dice *irreducible* si no es una constante y sus únicos divisores no constantes son sus asociados, es decir, si $q \mid p$ y $q \notin \Bbbk$, entonces $q = up$ con $u \in \Bbbk \setminus \{0\}$.

Lema 63. *Un polinomio* $p \in \Bbbk[x]$ *es irreducible si y sólo si para cualesquiera* $a, b \in \Bbbk[x]$, *si* $p \mid ab$ *entonces* $p \mid a$ *o* $p \mid b$.

Demostración. Sea p irreducible. Si $p \mid ab$ entonces $ab = cp$. Sea $d \in \mathrm{MCD}(a, p)$, si $d \notin \mathcal{U}(A)$ entonces d tiene que ser asociado a p, de donde $p \mid a$. Así pues, si suponemos que $p \nmid a$ tenemos que $1 \in \mathrm{MCD}(a, p)$, de donde $1 = ua + vp$. Así $uab = ucp$, por lo que $b = ucp - vpb = (uc - vb)p$, es decir, $p \mid b$.

Recíprocamente, supongamos que $p \mid ab$ implica $p \mid a$ o $p \mid b$. Si $a \mid p$ tenemos que $p = ac$ para algún c. Así $p \mid ac$, de donde $p \mid a$ o $p \mid c$. En el primer caso $a \sim p$, y en el segundo $p \sim c$ de donde $a \in \Bbbk \setminus \{0\}$. □

Proposición 64. *$p \in \Bbbk[x]$ es irreducible si y sólo si $\Bbbk[x]_p$ es un cuerpo.*

Lema 65. *Si $a \mid b$ y $\deg(a) = \deg(b)$ entonces $a \sim b$.*

Lema 66. *Si $\varnothing \neq B \subseteq \Bbbk[x]$, existe $b \in B$ tal que para todo $a \in B$, $a \mid b$ implica $a \sim b$.*

Demostración. Supongamos que el resultado es falso. Podemos construir una sucesión $\{a_i \mid i \in \mathbb{N}\}$ tal que $a_{i+1} \mid a_i$ y $a_{i+1} \nsim a_i$. A partir de la sucesión anterior tenemos una nueva sucesión $\{\delta(a_i) \mid i \in \mathbb{N}\} \subseteq \mathbb{N}$ tal que $\delta(a_{i+1}) \leq \delta(a_i)$. Como $\{\delta(a_i) \mid i \in \mathbb{N}\} \subseteq \{0, \ldots, \delta(a_0)\}$ que es un conjunto finito, existe un natural n tal que $\delta(a_n) = \delta(a_{n+k})$ para todo k. En particular $\delta(a_n) = \delta(a_{n+1})$, y por el Lema 65 tenemos que $a_n \sim a_{n+1}$, lo que contradice nuestra hipótesis sobre las propiedades de la sucesión $\{a_i \mid i \in \mathbb{N}\}$. Por lo tanto el Lema es verdadero. □

Teorema 67 (Fundamental de la Aritmética)**.** *Todo polinomio $a \in \Bbbk[x]$ se descompone como $a = p_1 \cdots p_s$ con p_i irreducible. Además si $a = p_1 \cdots p_s = q_1 \cdots q_t$ son dos descomposiciones como producto de irreducibles entonces $s = t$ y salvo reordenación $p_i \sim q_i$.*

Demostración. Demostramos la existencia de descomposiciones. Sea B el subconjunto de A formado por todos los elementos que no se descomponen como producto de irreducibles. Supongamos que B es no vacío. Sea b el elemento dado por el Lema 66. Como $b \in B$ tenemos que b no es irreducible, así que $b = b_1 b_2$ y con $b_i \nsim b$. Como $b_i \mid b$ y $b_i \nsim b$ tenemos que $b_i \notin B$. Entonces tanto b_1 como b_2 tienes descomposiciones como producto de irreducibles, es decir, $b_1 = p_1 \cdots p_s$ y $b_2 = q_1 \cdots q_t$, de donde $b = b_1 b_2 = p_1 \cdots p_s q_1 \cdots q_t$ tiene una descomposición como producto de irreducibles, es decir, $b \notin B$, lo que contradice la elección de b. Así $B = \varnothing$ y todo elemento de A se escribe como producto de irreducibles.

Vayamos con la unicidad. Si $a = p_1 \cdots p_s = q_1 \cdots q_t$, entonces $p_1 \mid q_1 \cdots q_t$. Por el Lema 63 p_1 divide a algún q_i, que podemos suponer q_1 después de reordenar. Como q_1 es irreducible tenemos que $p_1 \sim q_1$. La reiteración del proceso nos da la unicidad. □

3.12 Criterios de Irreducibilidad de Polinomios

Proposición 68 (Criba de Eratóstenes)**.** *Sea $p \in \mathbb{Z}$. p es primo si y sólo si para todo natural n con $2 \leq n \leq \sqrt{|p|}$, $n \nmid p$.*

Demostración. Basta observar que si $p = ab$ el valor absoluto de alguno de los factores debe ser menor o igual que $\sqrt{|p|}$. □

Observación 69. La Criba de Eratóstenes proporciona un algoritmo para determinar si un natural p dado es irreducible o no, calcular las divisiones de p entre todos los naturales menores que $\sqrt{p}$. De esta forma tenemos un procedimiento para determinar sin ningún género de duda si un entero es primo o no. Por otra parte la Criba de Eratóstenes tiene complejidad exponencial, aunque existen algoritmos que determinan la primalidad de un entero en tiempo polinomial.

Observación 70. Lamentablemente la situación no es tan cómoda en $\Bbbk[x]$. Por ejemplo todos los polinomios de la forma $x - \alpha$ con $\alpha \in \Bbbk$ son irreducibles (lo que se argumenta fácilmente con el grado) y no asociados (el coeficiente de x es uno). Así pues, si $\Bbbk$ es infinito un algoritmo tipo Criba de Eratóstenes parece no funcionar a priori.

Vamos a estudiar cuándo un polinomio tiene como factor a un polinomio de grado uno.

Definición 71. Sea $p(x) = a_0 + \cdots + a_n x^n \in \Bbbk[x]$. Denotamos también por p a la aplicación

$$\begin{aligned} p : \Bbbk &\longrightarrow \Bbbk \\ \alpha &\longmapsto a_0 + a_1\alpha + \cdots + a_n\alpha^n \end{aligned}$$

Esta aplicación se llama *evaluación*.

Lema 72. *Sea p un polinomio y $a \in \Bbbk$. Existe un único $q \in \Bbbk[x]$ tal que*

$$p(x) = q(x)(x - a) + p(a).$$

Demostración. Por la división $p(x) = q(x)(x - a) + b$ con $b \in \Bbbk$ (el resto tiene grado cero porque el divisor tiene grado uno). Así

$$p(a) = q(a)(a - a) + b = q(a)0 + b = b.$$

□

Proposición 73. *$(x-a) \mid p(x)$ si y sólo si $p(a)=0$.*

Si $p(a)=0$ se dice que a es una raíz de p. Este resultado permite comprobar si un polinomio tiene raíces, o equivalentemente factores de grado uno.

Algoritmo de Horner–Ruffini

Sea el polinomio $p(x)=a_0+a_1x+\cdots+a_nx^n\in\Bbbk[x]$, y sea $a\in\Bbbk$. Sean

$$\begin{aligned} b_n &= a_n \\ b_{n-1} &= a_{n-1}+b_na \\ &\vdots \\ b_j &= a_j+b_{j+1}a \qquad \text{y} \qquad q(x)=b_1+b_2x+\cdots+b_nx^{n-1} \\ &\vdots \\ b_0 &= a_0+b_1a \end{aligned}$$

Entonces

$$p(x)=q(x)(x-a)+b_0 \quad \text{y} \quad p(a)=b_0$$

Observación 74. Si $\Bbbk$ es un cuerpo finito, la evaluación en todos los elementos de $\Bbbk$ permite determinar si cierto polinomio tiene factores de grado uno. A partir de este algoritmo, y dado que hay un número finito de polinomios de un grado fijo, podemos construir TODOS los polinomios irreducibles del grado que queramos. Por ejemplo, serán irreducibles aquellos de grado dos que no tengan raíces. Lo mismo podemos decir de los de grado tres. Para los de grado cuatro basta estudiar sus raíces y si tienen algún factor irreducible de grado dos, que ya son conocidos. Podemos reiterar este procedimiento hasta el grado que queramos. Lamentablemente la complejidad es horrorosa, y mucho peor si $\Bbbk$ es grande.

Observación 75. Los casos $\Bbbk=\mathbb{R},\mathbb{Q}$ no pueden estudiarse a priori de la misma manera ya que son infinitos. Vamos a estudiar en primer lugar $\mathbb{Q}[x]$. Todo polinomio con coeficientes racionales tiene como asociado otro en $\mathbb{Z}[x]$, es decir, otro cuyos coeficientes son enteros. Comprobamos primeramente que las posibles raíces son un conjunto finito.

Proposición 76. *Sea $p(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$ donde $a_n\neq 0$. Sea $\frac{a}{b}\in\mathbb{Q}$ tal que $\operatorname{mcd}(a,b)=1$. Si $p(\frac{a}{b})=0$ entonces $a\mid a_0$ y $b\mid a_n$.*

Demostración. Si $p(\frac{a}{b})=0$ entonces

$$a_0+a_1\frac{a}{b}+\cdots+a_n\left(\frac{a}{b}\right)^n=0$$

y multiplicando por b^n tenemos

$$a_0b^n+a_1ab^{n-1}+\cdots+a_na^n=0.$$

Por tanto $a\mid a_0b^n$, y al ser a y b primos relativos necesariamente $a\mid a_0$. Análogamente $b\mid a_n$. □

Observación 77. Por tanto las posibles raíces de $p(x)=a_0+a_1x+\cdots+a_nx^n$ hay que buscarlas en el conjunto $\{\frac{a}{b}\mid a\mid a_0, b\mid a_n\}$, que es un conjunto finito.

3.13 Cuerpos Finitos

Terminamos el tema con una de las principales aplicaciones de los polinomios irreducibles, la construcción de los cuerpos finitos. A lo largo de esta sección $\mathbb{F}$ representa un cuerpo con un número finito de elementos. Vamos a tratar de analizar cuántos elementos puede tener $\mathbb{F}$.

Proposición 78. *Si $\mathbb{F}$ es un cuerpo finito entonces $\mathbb{F}$ tiene p^f elementos con p un número primo.*

El siguiente teorema es una de las piezas clave en la clasificación de los cuerpos con un número finito de elementos.

Teorema 79. *Dados $p \in \mathbb{Z}$ primo y $f \geq 1$, existe un polinomio irreducible de grado f sobre $\mathbb{Z}_p[x]$.*

Dados un primo p y un natural f, el Teorema 79 permite construir un cuerpo finito con p^f elementos. Dicho cuerpo se denota por $\mathbb{F}$, y podemos verlo como $\mathbb{Z}_p[x]_\phi$, el conjunto de los restos obtenidos al dividir entre ϕ, donde ϕ es un polinomio irreducible de grado f en $\mathbb{Z}_p[x]$ (el problema de encontrar dicho polinomio no lo vamos a considerar por ahora). La suma y el producto se realizan conforme a la Definición 59, y el inverso se calcula con la versión extendida del algoritmo de Euclides que proporciona los coeficientes de Bezout, de manera totalmente análoga al algoritmo 23 del Tema 3.