Álgebra Lineal y Estructuras Matemáticas

J. C. Rosales y P. A. García Sánchez

Departamento de Álgebra, Universidad de Granada

Capítulo 2

Aritmética entera y modular

1. Los números enteros

Dado un entero z, $-z$ es su opuesto, y denotamos por $|z| = \text{máx}\{z, -z\}$ al valor absoluto de z.

Propiedades de la suma. La suma de enteros es

- asociativa,
- tiene elemento neutro (el cero sumado a cualquier elemento da de nuevo ese elemento),
- todo elemento tiene inverso (si sumamos un entero con su opuesto obtenemos el cero),
- conmutativa,
- cancelativa ($a + b = a + c$ implica $b = c$; esto es consecuencia inmediata de la existencia de elemento inverso).

El conjunto de los números enteros con la suma es por tanto un grupo abeliano.

Propiedades del producto. El producto de números enteros es

- conmmutativo,
- asociativo,
- tiene elemento neutro (el uno),
- es cancelativo para elementos no nulos,
- distributivo ($a(b + c) = ab + ac$, que nos permite además sacar factor común).

Así el conjunto de los números enteros es un anillo conmutativo.

Propiedad de la división. Dados $a, b \in \mathbb{Z}$, con $b \neq 0$, existen $q, r \in \mathbb{Z}$ únicos de forma que $a = qb + r$ y $0 \leq r < |b|$.

A q y r los llamaremos cociente y resto de dividir a entre b, y los denotaremos por a div b y a mód b, respectivamente.

Dados a y b enteros, decimos que a divide a b, o que b es un múltiplo de a, si existe $c \in \mathbb{Z}$ tal que $b = ac$. Usaremos $a \mid b$ para denotar que a divide a b.

Ejercicio 15: Sean $a, b, c \in \mathbb{Z}$. Demuestra que si $c \mid a$ y $c \mid b$, entonces para todo $x, y \in \mathbb{Z}$, $c \mid xa + yb$.

Sea $p \in \mathbb{Z} \setminus \{-1, 1\}$. Diremos que p es primo si los únicos enteros que dividen a p son 1, -1, p y $-p$.

Decimos que dos enteros son primos relativos si los únicos enteros que dividen a ambos son 1 y -1. (Nótese que 1 y -1 dividen a cualquier número entero.)

Teorema de Bézout. Sean $a, b \in \mathbb{Z}$. Entonces a y b son primos relativos si y sólo si existen $u, v \in \mathbb{Z}$ tales que $au + bv = 1$.

Teorema fundamental de la aritmética. Todo número entero mayor que uno se puede expresar de forma única (salvo reordenaciones) como producto de números primos positivos.

1.1. Consequencia. Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ es la descomposición en primos del entero positivo n, entonces el número de divisores positivos de n es $(\alpha_1 + 1) \cdots (\alpha_r + 1)$.

Ejercicio 16: Calcula el número de divisores enteros positivos de 120.

Sean $a, b \in \mathbb{Z}$, con $a \neq 0$ o $b \neq 0$. Un entero d es un máximo común divisor de a y b si
1) $d \mid a$ y $d \mid b$,
2) si $c \mid a$ y $c \mid b$, con c un entero, entonces $c \mid d$.

Análogamente, un entero m es un mínimo común múltiplo de a y b si
1) $a \mid m$ y $b \mid m$,
2) si $a \mid c$ y $b \mid c$, con c un entero, entonces $m \mid c$.

De forma similar se puede definir el máximo común divisor y el mínimo común múltiplo de un conjunto de enteros $\{a_1, \ldots, a_n\}$ con n un entero positivo.

- Si d es un máximo común divisor de a y b, también lo es $-d$, y éstos son los únicos máximos divisores comunes de a y b. Lo mismo ocurre con el mínimo común múltiplo. Esto se debe a que si $a \mid b$, entonces $-a \mid b$. Cuando escribamos $\gcd\{a, b\}$ nos referiremos al máximo común divisor positivo de a y b. Para el mínimo común múltiplo utilizaremos $\operatorname{lcm}(a, b)$.
- Sean $a = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $b = vp_1^{\beta_1} \cdots p_r^{\beta_r}$, con $u, v \in \{1, -1\}$, $p_1, \ldots, p_r$ primos distintos y $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r$ enteros no negativos (algunos pueden ser cero, pues los primos que aparecen en a no tienen por qué aparecer en b). Entonces
$$\gcd\{a, b\} = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}},$$
$$\operatorname{lcm}\{a, b\} = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}.$$
- $\gcd\{a, b\}\operatorname{lcm}\{a, b\} = |ab|$.

Algoritmo de Euclides.
Entrada: a, b enteros positivos.
Salida: $\gcd\{a, b\}$.

$(a_0, a_1) := (a, b)$.
Mientras $a_1 \neq 0$
    $(a_0, a_1) := (a_1, a_0 \bmod a_1)$.
Devuelve a_0.

Ejercicio 17: Calcula el máximo común divisor de 237 y 99.

Maxima 9: Veamos algunos ejemplos de cálculo con `maxima`.

```
(%i1) primep(38129);

(%o1)                          false

(%i2) next_prime(38129);

(%o2)                          38149

(%i3) prev_prime(38129);

(%o3)                          38119

(%i4) factor(38129);

(%o4)                      7  13  419
```

```
(%i5) 7*13*419;
```

(%o5) 38129

```
(%i6) gcd(15,18);
```

(%o6) 3

```
(%i7) quotient(101,34);
```

(%o7) 2

```
(%i8) remainder(101,34);
```

(%o8) 33

```
(%i9) 2*34+33;
```

(%o9) 101

Hay que tener cuidado con estas funciones, pues el resto no se define como nosotros lo hemos hecho.

```
(%i10) quotient(-150,17);remainder(-150,17);
```

(%o10) −8

(%o11) −14

Si queremos un resto y cociente acordes a nuestra definición de división podemos hacer lo siguiente.

```
(%i12) cociente(a,b):=(a-mod(a,b))/b;
```

(%o12) $$\text{cociente}\,(a,b) := \frac{a - \text{mod}\,(a,b)}{b}$$

```
(%i13) cociente(-150,17);mod(-150,17);
```

(%o13) −9

(%o14) 3

```
(%i15) is(-8*17+-14=-9*17+3);
```

(%o15) true

Maxima 10: Una alternativa a `factor` es el comando `ifactor`, que devuelve una lista con pares de la forma (primo,exponente) para cada uno de los primos que aparecen en la factorización de un entero.

```
(%i1)  ifactors(12);
```
(%o1) [[2, 2], [3, 1]]

Un entero es libre de cuadrados si no es divisible por un cuadrado (distinto de 1), o lo que es lo mismo, en su factorización los exponentes de todos los primos que aparecen son uno.

```
(%i2)  libre_cuadradosp(x):=every(lambda([x],is(x[2]=1)),ifactors(x))$
(%i3)  libre_cuadradosp(12);
```
(%o3) false

```
(%i4)  libre_cuadradosp(2*3*5*7);
(%o4)  true

(%i5)  sublist(makelist(i,i,1,100),libre_cuadradosp);
(%o5)  [1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 33, 34, 35, 37, 38, 39, 41,
42, 43, 46, 47, 51, 53, 55, 57, 58, 59, 61, 62, 65, 66, 67, 69, 70, 71, 73, 74, 77, 78, 79, 82, 83, 85, 86,
87, 89, 91, 93, 94, 95, 97]
```

Maxima 11: Un entero positivo es perfecto si es suma de sus divisores propios.

```
(%i1)  divisors(10);
(%o1)  {1, 2, 5, 10}

(%i2)  perfectop(x):=is(2*x=apply("+",listify(divisors(x))))$
(%i3)  perfectop(28);
(%o3)  true

(%i4)  sublist(makelist(i,i,1,500),perfectop);
(%o4)  [6, 28, 496]
```

2. Ecuaciones diofánticas lineales

Una ecuación diofántica lineal es una expresión de la forma $a_1x_1 + \cdots + a_nx_n = b$, con $a_1, \ldots, a_n, b \in \mathbb{Z}$. Una solución a dicha ecuación es una n-upla $(c_1, \ldots, c_n)$ de elementos enteros de forma que $a_1c_1 + \cdots + a_nc_n = b$.

Teorema de Bézout generalizado. Sea $\{a_1, \ldots, a_n\}$ un conjunto de enteros, y d su máximo común divisor. Entonces existen $u_1, \ldots, u_n \in \mathbb{Z}$ tales que $a_1u_1 + \cdots + a_nu_n = d$.

Así la ecuación diofántica $a_1x_1 + \cdots + a_nx_n = b$ tiene solución si y sólo si $d \mid b$. Las soluciones de $a_1x_1 + \cdots + a_nx_n = b$ son las mismas que las de las ecuación $\frac{a_1}{d}x_1 + \cdots + \frac{a_n}{d}x_n = \frac{b}{d}$.

Para $n = 2$, tenemos ecuaciones en dos variables. Usamos las incógnitas x e y por comodidad. Si x_0, y_0 es una solución particular de $ax+by = c$, con $\gcd\{a, b\} = 1$, entonces todas las soluciones de esa ecuación son de la forma

$$\begin{cases} x = x_0 + bk, \\ y = y_0 - ak, \end{cases}$$

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

Algoritmo extendido de Euclides.
Entrada: a, b enteros positivos.
Salida: $s, t, d \in \mathbb{Z}$ tales que $d = \gcd\{a, b\}$ y $as + bt = d$.

$(a_0, a_1) := (a, b)$.
$(s_0, s_1) := (1, 0)$.
$(t_0, t_1) := (0, 1)$.
Mientras $a_1 \neq 0$
  $q := a_0$ div a_1.
  $(a_0, a_1) := (a_1, a_0 - a_1q)$.
  $(s_0, s_1) := (s_1, s_0 - s_1q)$.
  $(t_0, t_1) := (t_1, t_0 - t_1q)$.
$d := a_0$, $s := s_0$, $t := t_0$.

Devuelve s, t, d.

Maxima 12: Resolvamos la ecuación $40x + 15y = 30$. Usando `gcdex` obtenemos lo siguiente.

```
(%i1) gcdex(40,15);
```

$$(\%o1) \qquad [-1, 3, 5]$$

Lo que significa que $40 \times (-1) + 15 \times 3 = 5$. Como 5 divide a 30, la ecuación tiene solución. Multiplicamos por 6 ($6 \times 5 = 30$) y obtenemos lo siguiente.

```
(%i2) %*6;
```

$$(\%o2) \qquad [-6, 18, 30]$$

Que equivale a multiplicar la igualdad $40 \times (-1) + 15 \times 3 = 5$ por 6. Por tanto, una solución de nuestra ecuación $30 \times (-6) + 15 \times 18 = 30$.

Nótese que la ecuación $40x + 15y = 30$ es equivalente a $8x + 3y = 6$ (hemos dividido por el máximo común divisor de 40 y 15). Si x_0, y_0 es una solución de dicha ecuación, $x = x_0 + 3k$ e $y = y_0 - 8k$ es una solución de $8x + 3y = 6$ para todo $k \in \mathbb{Z}$.

```
(%i3) gcdex(8,3);
```

$$(\%o3) \qquad [-1, 3, 1]$$

```
(%i4) %*6;
```

$$(\%o4) \qquad [-6, 18, 6]$$

Así todas las soluciones de $40x + 15y = 30$ son

$$\begin{cases} x = -6 + 3k, \\ y = 18 - 8k. \end{cases}$$

Maxima 13: Resolvamos ahora la ecuación $121x - 77y = 88$.

```
(%i1)  gcd(121,-77);
```

$$(\%o1) \qquad 11$$

Al dividir por 11, la ecuación queda reducida a $11x - 7y = 8$.

```
(%i2)  l:gcdex(11,-7);
```

$$(\%o2) \qquad [2, 3, 1]$$

```
(%i3)  8*l;
```

$$(\%o3) \qquad [16, 24, 8]$$

Por lo que tenemos que una solución particular es $x_0 = 16$ e $y_0 = 24$. Siendo además todas las soluciones de la forma $x = x_0 - 7k,\ y = y_0 - 11k$ con k un entero cualquiera.

3. Ecuaciones en congruencias de grado uno

Sean $a, b, m \in \mathbb{Z}$. Escribimos $a \equiv b \pmod{m}$, que se lee "a es congruente con b módulo m", para indicar que $m \mid a - b$.

Una ecuación en congruencias de grado uno (o lineal) es una expresión de la forma $ax \equiv b \pmod{m}$. Una solución para dicha ecuación es un entero c de forma que $ac \equiv b \pmod{m}$. Nótese que las soluciones de $ax \equiv b \pmod{m}$ son las posibles x de la ecuación diofántica $ax + my = b$.

- La ecuación $ax \equiv b \pmod{m}$ tiene solución si y sólo si $\gcd\{a, m\} \mid b$.
- Si $d = \gcd\{a, m\}$ y $d \mid b$, entonces las ecuaciones $ax \equiv b \pmod{m}$ y $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ tienen las mismas soluciones.
- Si $\gcd\{a, m\} = 1$, y x_0 es una solución de $ax \equiv b \pmod{m}$, entonces el conjunto de todas las soluciones de la ecuación es $\{x_0 + km$ tales que $k \in \mathbb{Z}\}$.
- La ecuación $ax + c \equiv b \pmod{m}$ tiene las mismas soluciones que la ecuación $ax \equiv b - c \pmod{m}$.
- La ecuación $ax \equiv b \pmod{m}$ tiene las mismas soluciones que la ecuación $(a \bmod m)x \equiv (b \bmod m) \pmod{m}$.
- Si $au + mv = 1$, con $u, v \in \mathbb{Z}$, entonces bu es una solución de $ax \equiv b \pmod{m}$.

Maxima 14: Veamos si tiene solución la ecuación $54x \equiv 6 \pmod{34}$, y en caso de tener, vamos a describir su conjunto de soluciones.

```
(%i1) remainder(54,34);
```

$$(\%o1) \qquad 20$$

Al ser 54 mód 34 igual a 20, la ecuación anterior es equivalente a $20x \equiv 6 \pmod{34}$.

```
(%i2) gcd(20,34);
```

$$(\%o2) \qquad 2$$

Como $2|6$, la ecuación tiene solución, y es equivalente a $10x \equiv 3 \pmod{17}$. Usando `gcdex` obtenemos los coeficientes de Bézout para 10 y 17.

```
(%i2) gcdex(10,17);
```

$$(\%o2) \qquad [-5, 3, 1]$$

Lo que viene a decir que $(-5) \times 10 + 3 \times 17 = 1$. Así una solución de $10x \equiv 3 \pmod{17}$ es $(-5)3$, que vale -15. Así todas las soluciones de nuestra ecuación son de la forma $-15 + 17k$ con $k \in \mathbb{Z}$.

Ejercicio 18: Encuentra todas las soluciones enteras de

$$121x \equiv 2 \pmod{196}.$$

Maxima 15: Vamos a resolver el sistema

$$\begin{cases} x \equiv 5495 \pmod{7643} \\ x \equiv 7569 \pmod{8765} \end{cases}$$

Por la primera ecuación, sabemos que x es de la forma $x = 5495 + 7643k$ con k un entero cualquiera. Substituimos en la segunda y k se convierte en la nueva incógnita: $5495 + 7643k \equiv 7569 \pmod{8765}$. Como

```
(%i1)  7569-5495;
```
(%o1) 2074

tenemos que resolver $7643k \equiv 2074 \pmod{8765}$. El inverso de 7643 módulo 8765 lo calculamos (de existir) con el algoritmo extendido de Euclides.

```
(%i2)  gcdex(7643,8765);
```
(%o2) $[2617, -2282, 1]$

Despejamos

```
(%i3)  mod(2617*2074,8765);
```
(%o3) 2123

y obtenemos que $k = 2123 + 8765t$ para cualquier entero t. Substituyendo k en la expresión de x, llegamos a $x = 5495 + 7643(2123 + 8765t)$.

```
(%i4)  expand(5495+7643*(2123+8765*t));
```
(%o4) $66990895\,t + 16231584$

Por lo que $x = 66990895t + 16231584$ para todo $t \in \mathbb{Z}$ es una solución del sistema de congruencias. Lo podemos comprobar como sigue.

```
(%i6)  mod(16231584,[7643,8765]);
```
(%o6) $[5495, 7569]$

Ejercicio 19: Resuelve los siguientes sistemas de congruencias.

$$\left.\begin{array}{ll} 2x \equiv 3 & (\text{mód } 5) \\ 3x \equiv 1 & (\text{mód } 4) \end{array}\right\} \qquad \left.\begin{array}{ll} 2x \equiv 2 & (\text{mód } 4) \\ 6x \equiv 3 & (\text{mód } 9) \\ 2x \equiv 3 & (\text{mód } 5) \end{array}\right\}$$

$$\left.\begin{array}{ll} 2x \equiv 2 & (\text{mód } 4) \\ 3x \equiv 6 & (\text{mód } 12) \end{array}\right\} \qquad \left.\begin{array}{ll} x \equiv 1 & (\text{mód } 2) \\ 3x \equiv 2 & (\text{mód } 6) \\ 5x \equiv 1 & (\text{mód } 7) \end{array}\right\}$$

4. El anillo de los enteros módulo un entero positivo

Dado un entero positivo m, denotamos por $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ (que es el conjunto de restos posibles de la división por m), y por eso este conjunto se conoce a veces como el conjunto de los enteros módulo m.

En $\mathbb{Z}_m$ definimos una suma y un producto de la siguiente forma. Dados $a, b \in \mathbb{Z}_m$,

- $a \oplus b = (a + b) \bmod m$,
- $a \otimes b = (ab) \bmod m$.

Propiedades de la suma. Conmutativa, asociativa, elemento neutro y elemento inverso.

Propiedades del producto. Conmutativa, asociativa, elemento neutro y distributiva.

- Un elemento $a \in \mathbb{Z}_m$ tiene inverso para el producto si y sólo si $\gcd\{a, m\} = 1$. Si $au + mv = 1$, entonces $u \bmod m$ es el inverso de a en $\mathbb{Z}_m$.

Ejercicio 20: Calcula el inverso para el producto de 121 en $\mathbb{Z}_{196}$.

Si $a_1, \ldots, a_k$ y m son números enteros, entonces

- $(a_1 + \cdots + a_k) \mod m = (a_1 \mod m + \cdots + a_k \mod m) \mod m$,
- $(a_1 \times \cdots \times a_k) \mod m = (a_1 \mod m \times \cdots \times a_k \mod m) \mod m$,

Ejercicio 21: Calcula el resto de dividir 4225^{1000} entre 7.

Ejercicio 22: Prueba que dado un número entero m o bien se verifica que $m^2 \equiv 0 \pmod 8$, o $m^2 \equiv 1 \pmod 8$, o $m^2 \equiv 4 \pmod 8$.

Maxima 16: Escribamos una función para calcular $\mathbb{Z}_m$, para m un entero positivo.

```
(%i1) Z(m):=setify(makelist(i,i,0,m-1));
```

$$(\%o1)\quad Z(m) := \mathrm{setify}(\mathrm{makelist}(i, i, 0, m-1))$$

```
(%i2) Z(10);
```

$$(\%o2)\quad \{0,1,2,3,4,5,6,7,8,9\}$$

```
(%i3) tieneinverso(x,m):=is(gcd(x,m)=1);
```

$$(\%o3)\quad \mathrm{tieneinverso}(x, m) := \mathrm{is}(\gcd(x, m) = 1)$$

El inverso lo podemos calcular con la función `inv_mod`.

```
(%i4) inv_mod(3,10);
```

$$(\%o4)\quad 7$$

```
(%i5) inv_mod(2,10);
```

$$(\%o5)\quad \mathrm{false}$$

Veamos los elementos que tienen inverso en $\mathbb{Z}_{12}$.

```
(%i6) subset(Z(12),lambda([x],tieneinverso(x,12)));
```

$$(\%o6)\quad 1, 5, 7, 11$$

Como 11 es primo, todo elemento no nulo de $\mathbb{Z}_{11}$ tiene inverso:

```
(%i7) every(lambda([x],tieneinverso(x,11)),disjoin(0,Z(11)));
```

$$(\%o7)\quad \mathrm{true}$$

Por último, resolvamos la ecuación $137x \equiv 26 \pmod{155}$, que es equivalente a resolver la ecuación $137x = 26$ en $\mathbb{Z}_{155}$.

```
(%i9)  inv_mod(137,155);
```

$$(\%o9)\quad 43$$

```
(%i10) mod(43*26,155);
```

$$(\%o10)\quad 33$$

5. Sistemas de numeración

Sean $a, b \in \mathbb{N}$ con $a \neq 0$ y $b \geq 2$. Entonces existen únicos $m \in \mathbb{N}$ y $a_0, a_1, \ldots, a_m \in \mathbb{N}$ tales que:

- $a_m \neq 0$.
- $a = \sum_{k=0}^{m} a_k b^k = a_m b^m + \cdots + a_1 b + a_0$
- $a_i < b$.

Diremos entonces que $a_m a_{m-1} \ldots a_1 a_0$ es una representación del número a en base b, y escribiremos

$$a = (a_m a_{m-1} \ldots a_1 a_0)_b.$$

Para expresar un número en base b, lo dividimos entre b y tomamos el resto. El cociente de la división lo dividimos entre b y volvemos a tomar el resto, y así, hasta que el cociente sea menor que b. En la expresión anterior, $a = a_m b^m + \cdots + a_1 b + a_0$, nótese que $a_0 = a$ mód b y que a div $b = (a - a_0)/b = a_m b^{m-1} + \cdots + a_2 b^1 + a_1$.

Maxima 17: Para pasar de base 10 a base b, podemos utilizar esta función.

```
(%i1)  abase(x,b):=if is(x < b) then [x]
       else append(abase((x-mod(x,b))/b,b),[mod(x,b)]) $
(%i2)  abase(9,2);
(%o2)  [1,0,0,1]

(%i3)  abase(9,4);
(%o3)  [2,1]
```

Para pasar de base b a base 10, simplemente tenemos que utilizar la expresión en base b del número dado, y hacer las operaciones (en base 10).

```
(%i4)  debase(ls,b):=sum(ls[i]*b^(length(ls)-i), i,1,length(ls))$
(%i5)  debase([1,0,0],2);
(%o5)  4

(%i6)  debase(abase(10,2),2);
(%o6)  10
```

Si queremos pasar de base b a base b' podemos pasar de b a 10 y luego de 10 a b'.

```
(%i7)  debaseb1abaseb2(ls,b1,b2):=abase(debase(ls,b1),b2)$
(%i8)  debaseb1abaseb2([1,0,0,1],2,4);
(%o8)  [2,1]

(%i9)  debase([1,0,0,1],2);
(%o9)  9

(%i10) abase(9,4);
(%o10) [2,1]
```

Para pasar de base b a base b^r, primero agrupamos las cifras en base b en grupos de r (contando de derecha a izquierda), y cada uno de los grupos de r cifras los pasamos a base b^r.

Maxima 18: Veamos un ejemplo con $b = 2$ y $r = 2$.

```
(%i11) debaseb1abaseb2([1,0,1,0,1,1,1],2,8);
(%o11) [1,2,7]
```

Nótese que $(111)_2 = (7)_8$, $(010)_2 = (2)_8$ y $(1)_2 = (1)_8$.

Recíprocamente, para pasar un número de base b^r a base b es suficiente expresar cada cifra del número en base b (completando con ceros a la izquierda para que nos de r cifras).

Maxima 19:

```
(%i12) debaseb1abaseb2([1,2,7],8,2);
(%o12) [1,0,1,0,1,1,1]
```

Los algoritmos que conocemos para sumar, restar, multiplicar o dividir números escritos en base 10 son válidos para realizar estas operaciones para números escritos en una base b cualquiera.

Así, por ejemplo, para la suma, si $m, n \in \mathbb{N}$; $m = (m_k m_{k-1} \dots m_1 m_0)_b$ y $n = (n_k n_{k-1} \dots n_1 n_0)_b$ (hemos supuesto que los dos números tienen igual número de cifras. De no ser así, añadimos "cero" al que tenga menos), entonces $m + n = (c_{k+1} c_k \dots c_1 c_0)_b$ donde:

- $c_0 = (m_0 + n_0) \bmod b$
- $c_{i+1} = (m_{i+1} + n_{i+1} + a_i) \bmod b$, donde $a_i = (m_i + n_i + a_{i-1}) \operatorname{div} b$ (hemos tomado $a_{-1} = 0$).

Es fácil comprobar que el número $(c_{k+1} c_k \dots c_1 c_0)_b$ aquí descrito corresponde con la suma de m y n.

Ejercicio 23: Encuentra la base b (si existe) en que $(41)_b \times (14)_b = (1224)_b$.

Ejercicio 24: Demuestra que un número en base 10 es múltiplo de 5 si y sólo si termina en 0 ó 5.

Ejercicio 25: Demuestra que un número en base 10 es múltiplo de 3 si la suma de sus dígitos es un múltiplo de 3.

Ejercicio 26: Prueba que un número en base 8 es múltiplo de 7 si la suma de sus dígitos es un múltiplo de 7.

Ejercicio 27: Demuestra que un número expresado en base 10 es múltiplo de 11 si la suma de las cifras que ocupan una posición par menos la suma de las que ocupan un lugar impar es un múltiplo de 11.

Índice alfabético