Tema 1

Aritmética entera

1.1 Los números enteros

1.1.1 Relaciones de orden

Una relación en un conjunto A es un subconjunto R del producto cartesiano AxA. Se dice que dos elementos $a,b \in A$ están relacionados, aRb, si el par (a,b) pertenece al subconjunto R.
Las propiedades que puede tener una relación son:

- *reflexiva*: aRa para todo a de A,
- *simétrica*: $aRb \Rightarrow bRa$,
- *antisimétrica*: aRb y $bRa \Rightarrow a = b$,
- *transitiva*: aRb y $bRc \Rightarrow aRc$.

Definición 1.1 *Una relación que verifique las propiedades reflexiva, antisimétrica y transitiva se denomina* ***relación de orden****. Esta relación se suele denotar por* $\leq$.

Ejemplo 1.2

- *La relación de inclusión en* $\mathcal{P}(A)$ *para un conjunto A.*
- *La relación* $\leq$ *en* $\mathbb{Z}$, $\mathbb{Q}$ *o* $\mathbb{R}$.
- *La relación de divisibilidad en el conjunto de los enteros positivos.*

Las relaciones de orden sirven para establecer una prelación entre elementos de un conjunto.
Un conjunto con una relación de orden en la que dos elementos cualesquiera están siempre relacionados se dice **totalmente ordenado**. Si no, se dice **parcialmente ordenado**. $\mathbb{Z}$ con la relación de orden habitual es un conjunto totalmente ordenados, para cada par de elementos siempre hay uno menor que otro. $\mathbb{Z}^+$ con la relación de divisibilidad es un conjunto parcialmente ordenado, para 3 y 5, ni 3 divide a 5 ni 5 divide a 3.

En un conjunto con una relación de orden, algunos elementos reciben nombres especiales:

- ***Mínimo***: a $\in A$ tal que $a \leq x$ para todo $x \in A$
- ***Máximo***: a $\in A$ tal que $x \leq a$ para todo $x \in A$

Por ejemplo, el conjunto de los números enteros positivos posee mínimo para la relación de orden habitual, el 1, mientras que no posee máximo. En el caso de las partes de un conjunto A con la inclusión como relación de orden, se tiene el que conjunto vacío es mínimo y el propio conjunto A es máximo.

Por otro lado, en relación a un subconjunto X de A se dice que $a \in A$ es:

- ***Cota inferior*** *de* X: si $a \leq x$ para todo $x \in X$

- ***Cota superior*** *de X:* si $x \leq a$ para todo $x \in X$

Cuando se tiene una relación de orden ≤, la notación $a < b$ significa que $a \leq b$ y $a \neq b$.

1.1.2 Principio de inducción

Consideraremos el conjunto de los números naturales como el conjunto de los enteros positivos junto con el 0, lo denotaremos por $\mathbb{N}$.

Proposición 1.3 *Supongamos que para cada natural $n \geq n_0$ se tiene una proposición $P(n)$ que puede ser cierta o falsa. Si*

i) *$P(n_0)$ es cierta y*

ii) *para todo $n \geq n_0$, $P(n)$ cierta $\Rightarrow P(n+1)$ es cierta.*

Entonces, $P(n)$ es cierta para todo $n \geq n_0$.

Proposición 1.4 *Supongamos que para cada natural $n \geq n_0$ se tiene una proposición $P(n)$ que puede ser cierta o falsa. Si*

i) *$P(n_0)$ es cierta y*

ii) *para todo $n \geq n_0$, $P(n)$ cierta para todo m con $n_0 \leq m \leq n \Rightarrow P(n+1)$ es cierta.*

Entonces, $P(n)$ es cierta para todo $n \geq n_0$.

Ejemplo 1.5 *Demostrar, utilizando el principio de inducción, la fórmula que nos da la suma de los n primeros números naturales.*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Esta fórmula representa una serie de afirmaciones, una por cada número natural, y queremos demostrar que es cierto.

Se verifica para 1, es cierto que $1 = \frac{1.2}{2}$

Supongamos que se verifica para *n*, esto es, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

veamos que también se verifica para $n + 1$,

$1 + 2 + \cdots + n + (n+1) = (1 + 2 + \cdots + n) + (n+1) = \frac{n(n+1)}{2} + (n+1)$

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

Por tanto se verifica para todo $n \geq 1$ ■

1.1.3 Los números enteros

En el conjunto de los números enteros $\mathbb{Z}$ hay dos operaciones internas, suma y producto que le dan estructura de anillo conmutativo con identidad y una relación de orden, que verifican las siguientes propiedades:

Z1. $(\mathbb{Z},+)$ tiene estructura de grupo conmutativo:

- La operación suma es interna: $a + b \in \mathbb{Z}$ para todo $a, b \in \mathbb{Z}$

- Asociativa: $(a + b) + c = a + (b + c)$ para todo $a, b, c \in \mathbb{Z}$
- Elemento neutro (0 es el elemento neutro): $a + 0 = 0 + a = a$ para todo $a \in \mathbb{Z}$
- Elemento inverso (opuesto) de $a \in \mathbb{Z}$,$-a$: $a + (-a) = (-a) + a = 0$

Por verificar estas cuatro propiedades $(\mathbb{Z},+)$ tiene estructura de grupo.

- Conmutativa: $a + b = b + a$ para todo $a, b \in \mathbb{Z}$

$(\mathbb{Z},+)$ tiene estructura de grupo conmutativo.

Z2. El producto es asociativo, tiene elemento identidad y es conmutativo.

- La operación producto es interna: $a . b \in \mathbb{Z}$ para todo $a, b \in \mathbb{Z}$
- Asociativa: $(a . b) . c = a . (b . c)$ para todo $a, b, c \in \mathbb{Z}$
- Elemento identidad (1): $a . 1 = 1 . a = a$ para todo $a \in \mathbb{Z}$
- Conmutativo: $a . b = b . a$ para todo $a, b \in \mathbb{Z}$

Z3. El producto es distributivo respecto de la suma.

a. $(b + c) = a . b + a . c$ para todo $a, b, c \in \mathbb{Z}$

El hecho de que el producto sea una operación interna, asociativa y distributiva respecto de la suma dotan a $(\mathbb{Z}, +, .)$de estructura de **anillo**.

Z4. $a . b = 0 \Rightarrow a =$ ó $b = 0$.

Por verifica esta propiedad junto con $1 \neq 0$ se dice que $(\mathbb{Z}, +, .)$ es un **dominio de integridad**.

Z5. En el conjunto de los enteros hay una relación de orden, es decir, una relación $\leq$ con las propiedades reflexiva, antisimétrica y transitiva.

Z6. Es un orden total, es decir, $a, b \in \mathbb{Z}$, $a \leq b$ o $b \leq a$

El orden es compatible con las operaciones aritméticas:

Z7. $a \leq b$ y $c \in \mathbb{Z} \Rightarrow a + c \leq b + c$

Z8. $a \leq b$ y $c \geq 0 \Rightarrow a . c \leq b . c$

y el conjunto de los enteros no negativos está bien ordenado:

Z9. Todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo.

Observación 1.6 *Estas propiedades pueden considerarse como los axiomas que definen los números enteros.*

Proposición 1.7 *Todo subconjunto no vacío de $\mathbb{Z}$ que este acotado superiormente tiene un máximo.*

1.2 Divisibilidad

Definición 1.8 *Dados dos números enteros a y b, con b ≠0, se dice que b divide a a o que a es múltiplo de b o que b es divisor de a, si existe otro entero q tal que a = bq. Se escribe $b \mid a$*

Todo número entero *a* distinto de 1 y -1 tiene, al menos, cuatro divisores, a saber, ±1 y ± *a*. A estos divisores se les conoce como divisores triviales de *a*. Otras propiedades de la divisibilidad se recogen en la siguiente proposición:

Proposición 1.9 *En las siguientes propiedades todos los números serán enteros y |a| denotará el valor absoluto de a:*

1) $d \mid a \Leftrightarrow -d \mid a \Leftrightarrow d \mid -a$,
2) $d \mid a,\ a \neq 0 \ y\ d > 0 \Rightarrow 1 \leq d \leq |a|$,
3) $d \mid 1 \Rightarrow d = 1 \ o\ d = -1$,
4) $a \mid b \ y\ b \mid a \Rightarrow b = a \ o\ b = -a$,
5) $a \mid b \ y\ b \mid c \Rightarrow a \mid c$,
6) $a \mid b \ y\ a \mid c \Rightarrow a \mid b + c$,
7) $a \mid b \ y\ c \in \mathbb{Z} \Rightarrow a \mid bc$,
8) $a \mid b \ y\ c \in \mathbb{Z} \Rightarrow ac \mid bc$,
9) $a \mid b \ y\ c \mid d \Rightarrow ac \mid bd$,
10) $ac \mid bc \ y\ c \neq 0 \Rightarrow a \mid b$.

La prueba de estas propiedades requiere el uso de la Definición 1.8 y de los axiomas que definen los números enteros. Se deja como ejercicio.

Definición 1.10 *Se define **valor absoluto** de a de la forma siguiente:*

$$|a| = \begin{cases} a & si \quad a \geq 0 \\ -a & si \quad a < 0 \end{cases}$$

Teorema 1.11 (División euclídea) *Si a y b son dos enteros, b ≠ 0, existe un único par de enteros q y r tales que:*

$$a = bq + r \quad y \quad 0 \leq r < |b|$$

*A q y a r se les conoce, respectivamente, como **cociente** y **resto** de la **división euclídea** de a por b.*

Demostración. Vamos a demostrar primero la existencia de cociente y resto.
Supongamos, primero, que $b > 0$ y sea $S = \{x \in \mathbb{Z} : bx \leq a\}$.
Este conjunto *S* es no vacío ($b > 0 \Rightarrow b \geq 1 \Rightarrow b(-|a|) \leq -|a| \Rightarrow -b|a| \leq -|a| \leq a$, por lo que $-|a|$ pertenece a *S*), y está acotado superiormente (por ejemplo, por |*a*|: $x \leq bx \leq a \leq |a|$).

Por tanto, tiene máximo. Llamaremos q al máximo de S y $r = a - bq$. Por construcción, se tiene que $a = bq + r$. Veamos que r verifica lo exigido. En efecto,

- $r \geq 0$ (por pertenecer q a S)
- $r < |b| = b$. Si $r \geq b$, se tendría $b(q+1) = bq+b \leq bq+r = a$ y, en consecuencia, $q+1$ pertenecería a S contradiciendo el hecho de q es el máximo de S.

Si $b < 0$, aplicamos el caso anterior a $-b$.
Para probar la unicidad supongamos que q_1, r_1 y q_2, r_2 verifican las condiciones del teorema, es decir,

$$a = bq_1 + r_1 \quad y \quad 0 \leq r_1 < |b|$$
$$a = bq_2 + r_2 \quad y \quad 0 \leq r_2 < |b|$$

y que $r_1 \leq r_2$. Restando, se tiene $b(q_1 - q_2) = r_2 - r_1$. Por lo tanto, $|b|$ divide a $r_2 - r_1$, pero también se tiene que $0 \leq r_2 - r_1 < |b|$. Esto sólo es posible si $r_2 - r_1 = 0$. Por lo tanto, $r_2 = r_1$ y, en consecuencia $q_2 = q_1$. ■

Ejemplo 1.12 *Cuatro ejemplos de división euclídea:*

i. $33 = 15.\ 2 + 3$, $q = 2$, $r = 3$
ii. $-33 = 15.\ (-2) - 3 = 15.\ (-2) -15 + 15 – 3 = 15(-3) + 12$, $q = -3$, $r = 12$
iii. $33 = (-15).(-2) + 3$, $q = -2$, $r = 3$
iv. $-33 = (-15).2 -3 = (-15).2 – 15 + 15 – 3 = (-15).3+12$, $q = 3$, $r = 12$ ■

1.3 Máximo común divisor y algoritmo de Euclides

1.3.1 Máximo común divisor

Definición 1.13 (Máximo común divisor) *Si $d \mid a$ y $d \mid b$ decimos que d es un **divisor común** (o factor común) de a y b.*
*Cualquier par de enteros a y b poseen divisores comunes positivos, por ejemplo 1. Por otra parte, si a y b no son los dos nulos, todos sus divisores comunes son menores o iguales que máx($|a|$, $|b|$). Si a y b son dos números enteros no los dos nulos, el conjunto de los divisores comunes positivos a a y b es no vacío y está acotado superiormente, por lo que podemos asegurar que de entre todos sus divisores comunes debe existir uno que es el mayor de ellos. Se le denomina **máximo común divisor** de a y b y se denota por mcd(a, b), siendo el único entero positivo d que satisface*

- *$d \mid a$ y $d \mid b$,*
- *Si $c \mid a$ y $c \mid b$, $c \mid d$.*

El caso a = b = 0 debe ser excluido, cualquier entero divide a 0 y es, por tanto, un divisor común de a y b, por lo que, en este caso, no existe un máximo común divisor. Esta definición puede extenderse al máximo común divisor de cualquier conjunto finito de enteros (no todos nulos).

Definición 1.14 *Dos números enteros se dicen **coprimos** o **primos entre sí**, si no poseen factores comunes no triviales, esto es, mcd(a,b) = 1.*

En la siguiente proposición se recogen propiedades básicas del máximo común divisor.

Proposición 1.15 *En las propiedades siguientes todos los números son enteros.*

1) $mcd(a, b) = mcd(b, a)$,
2) $mcd(a, b, c) = mcd(mcd(a, b), c) = mcd(a, mcd(b, c))$,
3) $mcd(a, 0) = mcd(a, a) = |a|$,
4) $mcd(a, b) = mcd(-a, b) = mcd(|a|, |b|)$
5) $mcd(ca, cb) = |c|\, mcd(a, b)$,
6) $mcd(a, b) = mcd(a, b + ac)$
7) $mcd\left(\frac{a}{mcd(a,b)}, \frac{b}{mcd(a,b)}\right) = 1$

La definición de máximo común divisor proporciona un algoritmo para calcular $mcd(a,b)$: construir la lista de divisores de a y b y tomar el mayor de los comunes. Sin embargo, para grandes números, este algoritmo es inaplicable.
En la próxima sección se va a construir un algoritmo eficiente para el cálculo del máximo común divisor.

1.3.2 Algoritmo de Euclides

Proposición 1.16 *Sean a y b dos números enteros y r el resto de la división euclídea de a por b , se verifica:*

$$d \mid a \text{ y } d \mid b \iff d \mid b \text{ y } d \mid r$$

La proposición anterior quiere decir los divisores comunes de a y b son los divisores comunes de b y de r, por lo que $mcd(a, b) = mcd(b, r)$.

Algoritmo 1.17 (Algoritmo de Euclides) El algoritmo de Euclides es un algoritmo eficiente que permite simplificar el cálculo del máximo común divisor reduciendo el tamaño de los enteros sin alterar su máximo común divisor. Eliminando casos triviales, podemos suponer que $a > b > 0$.
Sean $r_0 = a$, $r_1 = b$. Dividiendo, se tendrá que

$$r_0 = q_1 r_1 + r_2 \text{ con } 0 \le r_2 < r_1 = b$$

Si $r_2 = 0$, entonces $d \mid a$, por lo que $mcd(a, b) = b$ y hemos terminado.
Si $r_2 \neq 0$, dividimos r_1 entre r_2 y escribimos

$$r_1 = q_2 r_2 + r_3 \text{ con } 0 \le r_3 < r_2$$

el proceso se puede repetir si no se obtiene resto 0.
Dado que la sucesión de restos es decreciente y finita ($b = r_1 > r_2 > r_3 > \ldots \ge 0$), en algún momento habremos de encontrar un resto r_{n+1} igual a 0.
Los dos últimos pasos podemos escribirlos de la forma

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \text{ con } 0 < r_n < r_{n-1},$$
$$\text{y } r_{n-1} = q_n r_n + r_{n+1} \text{ con } r_{n+1} = 0.$$

■

Teorema 1.18 *En el proceso anterior, r_n es el máximo común divisor de a y b.*

Demostración.

$mcd(a, b) = mcd(r_0, r_1) = mcd(r_1, r_2) = \ldots = mcd(r_{n-2}, r_{n-1}) = mcd(r_{n-1}, r_n) = mcd(r_n, 0) = r_n$. ■

El algoritmo anterior puede extenderse al cálculo del máximo común divisor de más de dos enteros. Supongamos dados t enteros positivos $a_1,\ldots, a_t$ .Supongamos que i es el índice de la coordenada más pequeña de $(a_1,\ldots, a_t)$. En este caso se verifica que $mcd(a_1,\ldots, a_t) = mcd(rem(a_1, a_i), \ldots, rem(a_{i-1}, a_i), a_i, rem(a_{i+1}, a_i), \ldots, rem(a_t, a_i)$, donde $rem(a, b)$ representa al resto de dividir a entre b.

Ejemplo 1.19 *Calcular el mcd de* 120, 146 *y* 180.
En este caso, se tiene:
$mcd(120,146, 180) = mcd(120,26,60) = mcd(16,26,8) = mcd(0, 2, 8) = mcd(0, 2, 0) = 2$. ■

1.3.3. Teorema de Lamé

Denotemos por $E(a, b)$ el número de divisiones que realiza el algoritmo de Euclides si la entrada es (a, b). El objetivo es encontar una buena cota superior para $E(a, b)$.
Sea F_n el n-ésimo número de Fibonacci, recordemos que está definido por $F_0 = 0$, $F_1 = 1$ y $F_n = F_{n-1} + F_{n-2}$ si $n \geq 2$.

Lema 1.20 *Sean a y b enteros tales que $a > b > 0$ y supongamos que $E(a, b) = n$. Entonces, $a \geq F_{n+2}$ y $b \geq F_{n+1}$.*

Demostración. Utilizaremos la notación anterior y probaremos que $r_0 \geq F_{n+2}$ y $r_1 \geq F_{n+1}$ por inducción en n.
El enunciado es cierto para $n = 1$. En este caso, el algoritmo de Euclides consta de una única división, $r_0 = q_0 r_1$ y puesto que $r_0 > r_1$, los menores enteros positivos que lo verifican son $r_1 = 1 = F_2$ y $r_0 = 2 = F_3$.
Supongamos ahora que el enunciado es cierto para $i < n$; queremos probarlo para n.
El primer paso del algoritmo de Euclides es $r_0 = q_1 r_1 + r_2$, y sabemos que $E(r_1,r_2) = n - 1$.
Aplicando la hipótesis de inducción a $E(r_1, r_2) = n - 1$ se tendrá que $r_1 \geq F_{n+1}$ y $r_2 \geq F_n$.
Por lo tanto, $r_0 = q_1 r_1 + r_2 \geq r_1 + r_2 \geq F_{n+2}$. ■

Lema 1.21 *La sucesión de Fibonacci verifica que $\alpha^{n-1} < F_{n+1}$, para $n > 1$*, siendo $\alpha = \frac{1+\sqrt{5}}{2}$.

Demostración. Por inducción sobre n:
Veamos que es cierto para $n = 2$: $\alpha = \frac{1+\sqrt{5}}{2} < \frac{1+3}{2} = 2 = F_3$
Veamos que es cierto para $n = 3$: $\alpha^2 = \frac{3+\sqrt{5}}{2} < \frac{3+3}{2} = 3 = F_4$
(Por otra parte se verifica que $\alpha^2 = \alpha + 1$)
Supongamos que es cierto que se verifica para todo j con $2 < j < n$, esto es $\alpha^{j-1} < F_{j+1}$.
Veamos que es cierto para n:
$\alpha^{n-1} = \alpha^2 * \alpha^{n-3} = (\alpha + 1) * \alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3} < F_n + F_{n-1} = F_{n+1}$. ■

Teorema de Lamé 1.22 *Sean a y b dos enteros positivos con $a \geq b > 0$. Entonces, el número de divisiones realizadas en el algoritmo de Euclides para calcular E(a, b) es menor o igual que 5 veces el número de cifras decimales de b.*

Demostración. Aplicando los dos lemas anteriores te tiene: $\alpha^{n-1} < F_{n+1} \leq b$. Además $log_{10}\alpha \approx 0'208 > 0'2 = 1/5$
Por tanto $(n-1)\ log_{10}\alpha \leq log_{10}b$, esto es, $\frac{n-1}{5} < (n-1)\ log_{10}\alpha \leq log_{10}b$, en consecuencia, $n-1 < 5log_{10}b$.
Por otra parte si k es el número de cifras decimales de b se verifica que $b \leq 10^k$, por tanto, $log_{10}b \leq k$.
Se concluye $n-1 < 5\ log_{10}b \leq 5\ k$, esto es, $n < 5k+1$; al ser n entero se concluye que $n \leq 5k$. ■

El teorema anterior nos da una cota para el número de divisiones realizadas por el algoritmo de Euclides para el cálculo de *mcd*(*a*, *b*).

1.4 Algoritmo extendido de Euclides y resolución de ecuaciones diofánticas.

1.4.1. Algoritmo extendido de Euclides. Identidad de Bézout.

Definición 1.23 *Dados enteros a y b y su máximo común divisor d = mcd*(*a, b*)*, se denomina identidad de Bézout a la expresión de la forma*

$$ax + by = d \qquad x, y \in \mathbb{Z}$$

Ejemplo 1.24 El objetivo fundamental de esta sección es el demostrar que siempre existen tales enteros *x* e *y* y encontrar un algoritmo para su cálculo. Pero antes, veamos un ejemplo.
Aplicando el algoritmo de Euclides a $a = 180$ y $b = 146$, se tiene la siguiente sucesión de identidades:

$$180 = 1 * 146 + 34 \quad (1.1)$$
$$146 = 4 * 34 + 10 \quad (1.2)$$
$$34 = 3 * 10 + 4 \quad (1.3)$$
$$10 = 2 * 4 + 2 \quad (1.4)$$
$$4 = 2* 2 \quad (1.5)$$

Supongamos que queremos encontrar una identidad de Bézout, es decir, encontrar enteros *x* e *y* tales que $180 * x + 146 * y = 2$
Para ello, podemos volver hacia atrás en las identidades anteriores, es decir, de (1.5) se tiene

$$2 = 10 - 2 *4.$$

Ahora, de (1.4) podemos despejar 4 y llegar a

$$2 = 7 *10 - 2 * 34.$$

De nuevo, usando (1.3) llegamos a

$$2 = 7 * 146 - 30 * 34$$

Finalmente, usando (1.2) se tiene

$$2 = -30 *180 + 37 * 146$$

Esta forma de proceder implicará que para resolver una identidad de Bézout, tendremos que aplicar el algoritmo de Euclides (tomando nota de restos y cocientes) y después volver hacia atrás utilizando dichos restos y cocientes. En siguiente teorema veremos que se pueden organizar los cálculos de manera que no sea necesario.

Teorema 1.25 *Para todo par de enteros a y b no los dos nulos, existen enteros x e y tales que se verifica la identidad de Bézout:*

$$ax + by = mcd(a, b)$$

Demostración. Mediante un proceso inductivo sobe k vamos a demostrar que se existen x_k e y_k tales que:

$$ax_k + by_k = r_k \quad (0 \le k \le n),$$

siendo r_k los restos que se obtienen al aplicar el algoritmo de Euclides.
Para $k = 0$, basta tomar $x_0 = 1$ e $y_0 = 0$ y si $k = 1$, $x_1 = 0$ e $y_1 = 1$.
Ahora supongamos que hemos encontrado x_k e y_k para todo índice $0 \le k \le s$ y queremos calcular x_{s+1} e y_{s+1}. Se tendría:

$$r_{s+1} = r_{s-1} - r_s q_s = ax_{s-1} + by_{s-1} - q_s(ax_s + by_s) = a(x_{s-1} - q_s x_s) + b(y_{s-1} - q_s y_s)$$

Lo que hemos visto es que las sucesiones de enteros definidas por:

$$x_0 = 1, x_1 = 0, x_{k+1} = x_{k-1} - q_k x_k$$
$$y_0 = 0, y_1 = 1, y_{k+1} = y_{k-1} - q_k y_k$$

verifican

$$ax_k + by_k = r_k \ (0 \le k \le n).$$

Por tanto, particularizando en $k = n$ se obtiene que existen x_n e y_n tales que:

$$ax_n + by_n = r_n = mcd(a, b)$$

■

Ejercicio 1.26 Probar que a y b son coprimos si, y sólo si, existen enteros x e y tales que $ax+by = 1$.

Construcción 1.27: Interpretación matricial del algoritmo extendido de Euclides
Llamamos, al igual que antes, $r_0 = a$ y $r_1 = b$.
Consideremos las matrices

$$R_k = \begin{pmatrix} x_k & x_{k+1} \\ y_k & y_{k+1} \end{pmatrix}, S_k = \begin{pmatrix} r_k & r_{k+1} \\ x_k & x_{k+1} \\ y_k & y_{k+1} \end{pmatrix}, \text{ para } k \ge 0$$

$$Q_k = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}, \text{ para } k \ge 1$$

Recordemos que los coeficientes obtenidos en el teorema anterior verifican las ecuaciones:

$$x_0 = 1, x_1 = 0, x_{k+1} = x_{k-1} - q_k x_k$$
$$y_0 = 0, y_1 = 1, y_{k+1} = y_{k-1} - q_k y_k$$

Expresado en forma matricial:

$$R_0 = \begin{pmatrix} x_0 & x_1 \\ y_0 & y_1 \end{pmatrix} = I, \quad S_0 = \begin{pmatrix} r_0 & r_1 \\ x_0 & x_1 \\ y_0 & y_1 \end{pmatrix} = \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$R_k = \begin{pmatrix} x_k & x_{k+1} \\ y_k & y_{k+1} \end{pmatrix} = R_{k-1} Q_k$$

$$S_k = \begin{pmatrix} r_k & r_{k+1} \\ x_k & x_{k+1} \\ y_k & y_{k+1} \end{pmatrix} = S_{k-1} Q_k$$

(El producto de R_{k-1} por Q_k (es una matriz elemental) consiste en restar a la primera columna de R_{k-1} la segunda multiplicada por q_k e intercambiar las columnas de R_{k-1}).
Se verifica:

$$R_k = \begin{pmatrix} x_k & x_{k+1} \\ y_k & y_{k+1} \end{pmatrix} = R_{k-1}Q_k \;=\; R_0\, Q_1 \,\ldots Q_k\,,$$
$$S_k = \begin{pmatrix} r_k & r_{k+1} \\ x_k & x_{k+1} \\ y_k & y_{k+1} \end{pmatrix} = S_{k-1}Q_k \;=\; S_0\, Q_1 \,\ldots Q_k\,,$$

Por tanto $det(R_k) = (-1)^k$, esto es, $x_k\, y_{k+1} - x_{k+1} y_k = \pm 1$; lo que implica que $mcd(x_k, y_k) = 1$.

El algoritmo sigue hasta que en el lugar (1,2) de una de las matrices S_k aparezca un cero. De este modo, si en el algoritmo extendido de Euclides se realizan n divisiones, se tendrá

$$R_n = \begin{pmatrix} x_n & x_{n+1} \\ y_n & y_{n+1} \end{pmatrix} = R_{n-1}Q_n \quad \text{y } S_n = \begin{pmatrix} r_n & 0 \\ x_n & x_{n+1} \\ y_n & y_{n+1} \end{pmatrix} = S_{n-1}Q_n$$

con lo que se tiene:

$$ax_n + by_n = r_n = mcd(a, b),\ ax_{n+1} + by_{n+1} = r_{n+1} = 0,$$

Además $mcd(x_n, y_n) = mcd(x_{n+1}, y_{n+1}) = 1$.

En particular se tendrá, si $b \neq 0$, que la fracción $\frac{y_{n+1}}{x_{n+1}}$ es reducida e igual a $-\frac{a}{b}$. Dicho de otra manera

$$|x_{n+1}| = -\frac{b}{mcd(a,b)} \text{ e } |y_{n+1}| = \frac{a}{mcd(a,b)}$$

■

Ejemplo 1.28 *Veamos el ejemplo 1.23 con tratamiento matricial*

$$S_0 = \begin{pmatrix} 180 & 146 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Para la construcción de las natrices Q_k hay que tomar nota de los cocientes que se van obteniendo en el algoritmo de Euclides.

$$Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix},\ S_1 = S_0Q_1 = \begin{pmatrix} 180 & 146 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 146 & 34 \\ 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$Q_2 = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix},\ S_2 = S_1Q_2 = \begin{pmatrix} 146 & 34 \\ 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} = \begin{pmatrix} 34 & 10 \\ 1 & -41 \\ -1 & 5 \end{pmatrix}$$

$$Q_3 = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix},\ S_3 = S_2Q_3 = \begin{pmatrix} 34 & 10 \\ 1 & -41 \\ -1 & 5 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} 10 & 4 \\ -4 & 13 \\ 5 & -16 \end{pmatrix}$$

$$Q_4 = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix},\ S_4 = S_3Q_4 = \begin{pmatrix} 10 & 4 \\ -4 & 13 \\ 5 & -16 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 13 & -30 \\ -16 & 37 \end{pmatrix}$$

$$Q_5 = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix},\ S_5 = S_3Q_5 = \begin{pmatrix} 4 & 2 \\ 13 & -30 \\ -16 & 37 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -30 & 73 \\ 37 & -90 \end{pmatrix}$$

Hemos llegado a una matriz S cuyo término (1,2) es 0, $r_5 = 2$, $x_5 = -30$, $y_5 = 37$, con lo que se tiene (-30)*180 + 37*146 = 2. ■

Teorema 1.29 Si $a \mid bc$ y $mcd(a, b) = 1$, entonces $a \mid c$. En particular, si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.

Demostración. Gracias a la identidad de Bézout sabemos que existen enteros x e y tales que $ax + by = 1$. Multiplicando por c se tiene $c = cax + cby$, con lo que a divide a los dos sumandos a la derecha y, por lo tanto, divide a c.
■

1.4.2. Ecuaciones diofánticas.

Definición 1.30 *Se llaman **ecuaciones diofánticas** a aquéllas de las que nos interesan las soluciones enteras.*

Vamos a estudiar las ecuaciones diofánticas lineales en dos variables:

$$aX + bY = c \qquad a, b, c \in \mathbb{Z}$$

Puesto que el caso $a = b = 0$ no tiene ningún interés, supondremos que $(a, b) \neq (0; 0)$.

Proposición 1.31 *Dados enteros a, b, c la ecuación diofántica*

$$aX + bY = c$$

tiene solución si, y sólo si, mcd(a, b) divide a c. En caso de que tenga solución tiene infinitas, dadas por

$$\left\{\left(x_1 + t\frac{b}{mcd(a,b)}, y_1 - t\frac{a}{mcd(a,b)}\right), t \in \mathbb{Z}\right\},$$

donde (x_1,y_1) es una solución particular cualquiera.

Demostración.
Utilizando el Algoritmo de Euclides extendido, sabemos encontrar una solución si $c = mcd(a, b)$. Del mismo modo, es obvio encontrar una solución si $mcd(a, b)$ divide a c. Por tanto, la ecuación diofántica tiene solución si $mcd(a, b)$ divide a c.
Supongamos que tiene solución la ecuación diofántica $aX + bY = c$, existirán x e y tales que $ax + by = c$. Por tanto, todo factor común de a y de b también lo será de c. En particular, el máximo común divisor de a y de b dividirá a c.
Por tanto la ecuación diofántica $aX + bY = c$, $a, b, c \in \mathbb{Z}$ tiene solución si, y sólo si, $mcd(a, b)$ divide a c.

Sabemos cómo encontrar una solución: aplicamos el algoritmo extendido de Euclides a a y b, obteniendo x_0 e y_0 tales que $ax + by = mcd(a, b)$. Es claro que $\left(\frac{c}{mcd(a,b)}x_0, \frac{c}{mcd(a,b)}y_0\right)$ es solución de la ecuación diofántica dada.

Para encontrar más soluciones estudiaremos la ecuación diofántica $aX + bY = 0$ (la homogénea asociada)
Una solución obvia es de la homogénea es:

$$\left(\frac{b}{mcd(a,b)}, -\frac{a}{mcd(a,b)}\right),$$

pero también lo son todas las de la forma

$$\left(t\frac{b}{mcd(a,b)}, -t\frac{a}{mcd(a,b)}\right), \text{ con t} \in \mathbb{Z}.$$

Así pues, si (x_1, y_1) es solución cualesquiera de la ecuación diofántica dada, el conjunto

$$\left\{\left(x_1 + t\frac{b}{mcd(a,b)}, y_1 - t\frac{a}{mcd(a,b)}\right), \text{con t} \in \mathbb{Z}\right\}$$

es un conjunto de infinitas soluciones.

¿Hay más?. Para verlo, sea (x, y) una solución cualesquiera de la ecuación diofántica dada. Por tanto,

$$ax_1 + by_1 = c$$
$$ax + by = c$$

Restando se tiene $a(x-x_1) + b(y-y_1) = 0$ y, dividiendo por $mcd(a, b)$,

$$\frac{a}{mcd(a,b)}(x - x_1) + \frac{b}{mcd(a,b)}(y - y_1) = 0.$$

Ahora, supongamos que $b \neq 0$ (si $b = 0$ y $a \neq 0$, haríamos con a el mismo argumento que sigue). Como

$$mcd\left(\frac{a}{mcd(a,b)}, \frac{b}{mcd(a,b)}\right) = 1$$

y $\frac{b}{mcd(a,b)}$ divide a $\frac{a}{mcd(a,b)}(x - x_1)$, se tiene que $\frac{b}{mcd(a,b)}$ divide a $(x - x_1)$, es decir,

$$x - x_1 = t\frac{b}{mcd(a,b)}, \text{ para algún } t \in \mathbb{Z}$$

Sustituyendo se tiene $y_1 - y = t\frac{a}{mcd(a,b)}$

Por tanto el conjunto de soluciones de la ecuación diofántica dada siendo (x_1, y_1) es solución cualesquiera es

$$\left\{\left(x_1 + t\frac{b}{mcd(a,b)}, y_1 - t\frac{a}{mcd(a,b)}\right), \text{con } t \in \mathbb{Z}\right\}$$

■

Ejemplo 1.32 *Estudiar si existe o no solución para la ecuación diofántica*

$$15x + 40y = 1000$$

En caso afirmativo, encontrar todo el conjunto de soluciones.

$mcd(15, 40) = 5$ y 5 es divisor de 1000, por tanto la ecuación diofántica dada tiene solución.
En primer lugar procedemos a encontrar una solución de $15x + 40y = 5$,
$5 = 15*3 + 40*(-1)$, una solución sería (3,-1). A partir de ella se encuentra una solución de la dada.
$1000 = 5. 200$, por tanto (3.200,-1.200) = (600,-200) es una solución de la dada.

El conjunto de soluciones de la dada sería:
$x = 600 + t. 40/5 = 600 + 8t$, y = -200 - t 15/5 = -200 -3t, con $t \in \mathbb{Z}$

■

Ejemplo 1.33 *Estudiar si existe o no solución para la ecuación diofántica*

$$15x + 40y = 21$$

En caso afirmativo, encontrar todo el conjunto de soluciones.
$mcd(15, 40) = 5$ y 5 no es divisor de 21, por tanto la ecuación diofántica dada no tiene solución. ■

Ejemplo 1.34 *Dividir 1000 en dos sumandos positivos uno múltiplo de 15 y otro múltiplo de 40.*

Se trata de encontrar valores de $x, y \in \mathbb{Z}$ tales que $15x + 40y = 1000$.
En el ejemplo anterior se han encontrado el conjunto de soluciones. Ahora hay que imponer que esas soluciones sean positivas.

$x = 600 + 8t > 0 \Leftrightarrow 8t > -600 \Leftrightarrow t > -600/8 = -75$
$y = -200 - 3t > 0 \Leftrightarrow -200 > 3t \Leftrightarrow -200/3 > t \Leftrightarrow -67 \geq t$
Por tanto, interesan las soluciones $-67 \geq t > -75$. Basta dar a t uno de esos valores, por ejemplo, $t = -74$, $x = 600 + 8*(-74) = 8$, $y = -200 – 3*(-74) = 22$
Vemos que $1000 = 15*8 + 40*22$. ■

1.5 Números primos. Teorema fundamental de la aritmética.

1.5.1. Teorema fundamental de la aritmética

Definición 1.35 *Un entero $p > 1$ se dice **primo** si sus únicos divisores positivos son los triviales, es decir, 1 y p.*

Los primeros primos son:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Teorema 1.36 *Todo número entero mayor que 1 es producto de primos.*

Demostración. Por inducción sobre n

Para $n = 2$ es cierto

Supongamos que es cierto para $2 \leq i < k$, todo número entero i con $2 \leq i < k$ se puede poner como producto de primos.

Veamos que es cierto para k.

Si k es primo, ya es producto de primos.

Si k no es primo, es compuesto, por tanto existen dos enteros positivos a y b mayores que 1 tales que $k = ab$. Por tanto $a, b < ab = k$.

Aplicando la hipótesis de inducción a los números a y b, ambos se pueden poner como producto de primos. Por tanto $k = ab$ es producto de primos.

Se concluye que todos número entero mayor que 1 es producto de primos. ■

En particular, todo entero no nulo es producto de uno de los números naturales ±1 y de números primos. Veremos más adelante que esta expresión es única.

Teorema 1.37 *Existen infinitos números primos.*

Demostración. Esta demostración se hará por reducción al absurdo.
Supongamos que hay un número finito, digamos n, de números primos a los que denotaremos por $p_1, p_2, \ldots, p_n$. Consideremos el número

$$N = p_1 . p_2 \ldots . p_n + 1$$

Por el teorema anterior sabemos que N es producto de primos. Sea p un factor primo de N. Este primo es uno de los $p_1, p_2,\ldots, p_n$, digamos $p = p_i$. Entonces p_i divide a N y $p_1 p_2,\ldots p_n$. Por tanto p_i divide a $N - p_1 p_2 \ldots p_n$ que es igual a 1, con lo que hemos llegado a contradicción.
La hipótesis formulada no es cierta. Por tanto, no hay un número finito de primos. Esto es, existen infinitos números primos. ■

Proposición 1.38 *Si p es primo y* $p \mid a_1 a_2 \ldots a_n$, *entonces p divide a algún* a_i.

Demostración. Como consecuencia del teorema 1.26 se verifica que, en particular, si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.
Por un argumento inductivo se puede probar si p es primo y $p \mid a_1 a_2 \ldots a_n$, entonces p divide a algún a_i. ■

Teorema 1.39 (Teorema fundamental de la aritmética) *Todo entero positivo puede expresarse como producto de potencias no triviales de números primos*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

y, salvo, reordenación de los factores, esta factorización es única.

Demostración La existencia se sigue de un teorema anterior y, por lo tanto, sólo queda probar la unicidad.
Sea S el conjunto de enteros positivos que admiten dos factorizaciones distintas y, supongamos, por reducción al absurdo, que este conjunto es no vacío. Por la buena ordenación de $\mathbb{N}$, sabemos que, en ese caso, el conjunto S admite mínimo, digamos n. Se tendrán dos factorizaciones distintas de n:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$
$$n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$$

Es claro que p_1 divide a $q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$ y, por lo tanto, a alguno de los $q_i^{\beta_i}$. Aún más, se tendrá que p_1 divide a alguno de los q_i, que implica que es igual a él. Reordenando podemos suponer $p_1 = q_1$. En consecuencia se tendría

$$\frac{n}{p_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_1^{\beta_1 - 1} q_2^{\beta_2} \ldots q_s^{\beta_s}$$

Puesto que las factorizaciones de n consideradas eran distintas, tenemos dos factores distintos del entero positivo $\frac{n}{p_1} < n$, lo que contradice el hecho de que n sea el mínimo de S. ■

Teorema 1.40 *Si n es un número entero positivo compuesto, entonces tiene un divisor primo menor que* $\sqrt{n}$

Demostración. Si n es un número compuesto, tiene un factor positivo a. Por tanto, $n = ab$, con $1 < a, b$. Se verifica que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
En caso contrario, $a > \sqrt{n}$ y $b > \sqrt{n}$, y se tendría $n = ab > \sqrt{n}\sqrt{n} = n$, habríamos llegado a una contradicción. ■

1.5.2 Mínimo común múltiplo

Definición 1.41 *Si a y b son dos enteros, un* ***múltiplo común*** *de a y b es un entero c tal que* $a \mid c$, *y* $b \mid c$.
Si a y b son ambos no nulos, existen múltiplos comunes positivos, por ejemplo $|ab|$. *Al ser* $\mathbb{N}$ *un conjunto bien ordenado existe un menor múltiplo común positivo. Se le denomina* ***mínimo común múltiplo****, se denota por mcm(a, b), siendo el único entero positivo m que satisface:*

- $a \mid m$ *y* $b \mid m$,
- *Si* $a \mid c$ *y* $b \mid c$, $m \mid c$.

Teorema 1.42 *Sean a y b dos enteros. Se tiene*

$$|ab| = mcd(a,b).\ mcm(a,b)$$

Demostración. Se trata de probar que $m = \frac{|ab|}{mcd(a,b)}$ es el mínimo común múltiplo de *a* y *b*.

$m = \frac{|ab|}{mcd(a,b)} = |a|\frac{|b|}{mcd(a,b)}$, por tanto $a \mid m$

$m = \frac{|ab|}{mcd(a,b)} = |b|\frac{|a|}{mcd(a,b)}$, por tanto $b \mid m$

Por otro lado, supongamos que *c* es un entero que es múltiplo de *a* y *b*, es decir, $c = au$ para algún entero *u* y $c = bv$ para algún entero *v*.
Se tiene, entonces que

$$\frac{a}{mcd(a,b)}\,u = \frac{b}{mcd(a,b)}\,v$$

y como $\frac{a}{mcd(a,b)}$ y $\frac{b}{mcd(a,b)}$ son primos entre sí, aplicando el teorema 1.26 se obtiene que $\frac{a}{mcd(a,b)}$ divide *v*, es decir, $v = k\frac{a}{mcd(a,b)}$ para algún *k*.
Finalmente, se tendrá, $c = bv = k\frac{ab}{mcd(a,b)}$ para algún *k*.
Por tanto, c es múltiplo de $\frac{|ab|}{mcd(a,b)}$.
Como consecuencia $\frac{|ab|}{mcd(a,b)}$ es el mínimo común múltiplo de *a* y *b*. ■