Divisibilidad, MDC y Algoritmo de Euclides

Alan Reyes-Figueroa

Criptofrafía y Cifrado de Información (Aula 12) 21.septiembre.2021

Definición

Dados dos enteros $d, m \in \mathbb{Z}$ diremos que d ***divide*** *a m o que m es* ***divisible*** *entre m si existe $q \in \mathbb{Z}$ tal que $m = qd$, esto es $\frac{m}{d} \in \mathbb{Z}$ es un entero.*
En ese caso, escribimos $d \mid m$, y diremos que m es un ***múltiplo*** *de d, y que d es un* ***divisor*** *o* ***factor*** *de m.*
Si d no divide a m escribimos $d \nmid m$.

Ejemplos: $5 \mid 10$, pero $10 \nmid 5$.

Como $0 = 0 \cdot n$ se sigue que $n \mid 0$, $\forall n \in \mathbb{Z}$. Por otro lado, si $0 \mid n$, entonces existe $q \in \mathbb{Z}$ tal que $n = q \cdot 0 = 0$, de modo que $0 \nmid n$ para $n \neq 0$. Para un entero fijo n, los múltiplos de n son $0, \pm n, \pm 2n, \ldots$. Luego, no es difícil ver que entre n enteros consecutivos, siempre hay uno divisible entre n.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Propiedades *Para todo $x, y, z, w \in \mathbb{Z}$, valen*

a) $x \mid 0$, $1 \mid x$, $0 \nmid x$ *para* $x \neq 0$; $x \mid x$ *(reflexividad).*

b) $x \mid 1$, *si y sólo si,* $x = \pm 1$.

c) $x \mid y$, $y \mid z \;\Rightarrow\; x \mid z$ *(transitividad).*

d) $x \mid y$, $x \mid z \;\Rightarrow\; x \mid ay + bz$, *para todo* $a, b \in \mathbb{Z}$ *(linealidad).*

e) *Si* $x \mid y$, *entonces* $y = 0$ *ó* $|x| \leq |y|$ *(limitación).*

f) $x \mid y$, $x \mid y \pm z \;\Rightarrow\; x \mid z$.

g) $x \mid y$, $y \mid x \;\Rightarrow\; |x| = |y|$ *(antisimetría, a menos de signo).*

h) *Si* $x \mid y$ *y* $y \neq 0$, *entonces* $\frac{y}{x} \mid y$ *(divisores vienen en pares).*

i) $x \mid y$, $z \mid w \;\Rightarrow\; xz \mid yw$.

j) *Si* $z \neq 0$, *entonces* $x \mid y \;\Leftrightarrow\; xz \mid yz$.

<u>Prueba</u>: (a) Observe que $x = 1 \cdot x$, $0 = x \cdot 0$, $0 \mid x \Rightarrow x = q \cdot 0 = 0$; $x = x1$.
Para (b) $x \mid 1 \Leftrightarrow 1 = qx, \in \mathbb{Z} \Leftrightarrow q = \pm 1$, y portanto $x = \pm 1$.

En los ítems (c) a (h), la condición $x \mid y$ se da, de modo que $y = kx$, para algún $k \in \mathbb{Z}$.
En (c) $y \mid z \Rightarrow z = \ell y \Rightarrow z = \ell y = \ell(kx) = (k\ell)x$, con $k\ell \in \mathbb{Z} \Rightarrow x \mid z$.

En (d) $x \mid z \Rightarrow z = \ell x \Rightarrow ay + bz = a(kx) + b(\ell x) = (ak + b\ell)x \Rightarrow x \mid ay + bz$.

En (e), suponga $y \neq 0$. Entonces $k \neq 0 \Rightarrow |k| \geq 1 \Rightarrow |y| = |kx| = |k| \cdot |x| \geq |x|$.

En (f), por (c) tenemos que $x \mid y$, $x \mid y \pm z \Rightarrow x \mid y - (y \pm z) = \pm z$.

En (g), de (e) se tiene que $x \mid y$, $y \mid x \Rightarrow |y| \geq |x| \geq |y| \Rightarrow |y| = |x|$.

En (h), si $y \neq 0$, entonces $x \mid y \Rightarrow y = kx = (\frac{y}{x})x$. Como $\frac{y}{x} \in \mathbb{Z} \Rightarrow \frac{y}{x} \mid y$.

En (i), $y = kx$, $w = \ell z \Rightarrow yw = (kx)(\ell z) = (k\ell)xz \Rightarrow xz \mid yw$.

Finalmente (j), $(\Rightarrow)$ de (i) con $w = z$, se tiene que $x \mid y$, $z \mid z \Rightarrow xz \mid yz$. Para la recíproca $(\Leftarrow)$ $xz \mid yz$, $z \neq 0 \Rightarrow xz = k(yz) = kxz$, $k \in \mathbb{Z} \Rightarrow x = ky \Rightarrow x \mid y$. $\square$

Divisibilidad

Comentarios:

- Las propiedades (a), (c) y (g), corresponden a la reflexividad, transitividad y antisimetría (a menos de signo) de la relación $|$.
  Restricta a los naturales $\mathbb{N}$, la relación $|$ es un **orden parcial**.

- La propiedad (d) de linealidad sólo funciona para coeficientes en $\mathbb{Z}$.

- La propiedad (j) indica que en una relación de divisibilidad, podemos “cancelar” factores comunes (excepto 0).

- La (e), limitación, nos dice que el conjunto de divisores de un número entero n es finito. El número de divisores positivos de n es $\leq n$.

- La propiedad (h) nos indica que los divisores de n vienen en pares $(d, \frac{n}{d})$. **Obs!** No dice que los divisores d y $\frac{n}{d}$ son distintos.

Algoritmo de la División

El siguiente resultado juega un papel muy importante en la teoría de números.

Teorema (Algoritmo de la División)

Para cualesquiera enteros $a, b \in \mathbb{Z}$, $a > 0$, existe un único par (q, r) de enteros, tales que

$$b = qa + r, \quad y \quad 0 \leq r < a. \tag{1}$$

*En este caso, q es llamado **cociente** y r el **residuo** al dividir b entre a.*

Prueba: La prueba consiste de dos parte: la existencia y la unicidad.
Para la existencia, mostramos que el conjunto

$$S = \{b - xa : x \in \mathbb{Z},\ b - xa \geq 0\},$$

es no vacío. Para ello, mostramos un valor de x para el cual $b - xa \geq 0$.

Algoritmo de la División

Como $a \geq 1$, entonces $|b|a \geq |b| \;\Rightarrow\; b - (-|b|)a = b + |b|a \geq b + |b| \geq 0$. Así, para $x = -|b|$, el entero $b - xa \in S$.

Aplicando el Principio de buen orden, entonces S posee un elemento mínimo r. En particular, existe $q \in \mathbb{Z}$ tal que $r = b - qa \geq 0$.
Mostramos $r < a$. Si este no fuera el caso, entonces $r \geq a$ y $b - (q+1)a = (b - qa) - a = r - a \geq 0$ sería un elemento de S. Pero $b - (q+1)a < b - qa = r$, lo que contradice la minimalidad de r. Por lo tanto, $r < a$, y hemos probado que existen $q, r \in \mathbb{Z}$, con la propiedad (1).

Para mostrar la unicidad, suponga que existen dos representaciones en la forma deseada

$$b = qa + r = q'a + r', \quad \text{con} \quad 0 \leq r < a, \; 0 \leq r' < a.$$

Entonces, $r' - r = (q - q')a$. En particular, $|r' - r| = |q - q'|\, a$.

Algoritmo de la División

Por otro lado, como $0 \leq r < a$ entonces $-a < -r \leq 0$. Sumándola con la otra desigualdad $0 \leq r' < a$, obtenemos que la diferencia de residuos satisface $-a < r' - r < a \;\Rightarrow\; |r' - r| < a$. Entonces

$$0 \leq |q - q'|\, a = |r' - r| < a \text{ implica que } 0 \leq |q - q'| < 1.$$

Siendo q, q' ambos enteros, entonces $q - q'$ es también un entero. La desigualdad $0 \leq |q - q'| < 1$ implica que la única posibilidad es que $q - q' = 0 \;\Rightarrow\; q' = q$. De ahí que $r' - r = (q - q')a = 0 \cdot a = 0$ y $r' = r$. Esto muestra la unicidad de la representación. $\square$

Una versión más general del algoritmo es la siguiente:

Corolario (Algoritmo de la División)

Para cualesquiera enteros $a, b \in \mathbb{Z}$, $a \neq 0$, existe un único par (q, r) de enteros, tales que

$$b = qa + r, \quad y \quad 0 \leq r < |a|. \tag{2}$$

Prueba: Basta considerar el caso $a < 0$. Entonces $|a| > 0$ y el algoritmos de la división en (1) establece que existen únicos $q, r \in \mathbb{Z}$ tales que $b = q|a| + r$, con $0 \leq r < |a|$. Como $a < 0$, entonces $b = q|a| + r = (-q)a + r$, $0 \leq r < |a|$ satisface (2). $\square$

Ejemplo: Para ilustrar el algoritmo de la división, tome $a = 13$, $b = 61$.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Algoritmo de la División

Tenemos que

$$61 = 4 \cdot 13 + 9, \quad \text{con} \quad 0 \leq 9 < 13.$$

Observe que el algoritmo de la división equivale a hacer la "división tradicional" de $\frac{61}{13}$ a mano: $q = 4$ resulta el cociente, y 9 resulta ser el residual.

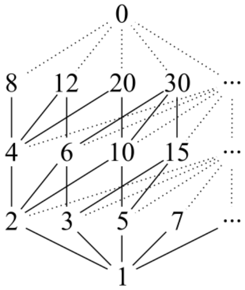
Esto también equivale a hacer $\frac{61}{13} = 4 + \frac{9}{13}$: pues

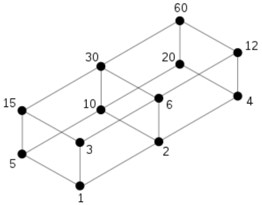
$$b = qa + r \;\Leftrightarrow\; \frac{b}{a} = q + \frac{r}{a}.$$

Ejemplo: Para ilustrar el algoritmo con $a < 0$, tomemos $a = -7$:

- Con $b = 1$: $1 = (0)(-7) + 1 \;\Rightarrow\; q = 0$, $r = 1$.
- Con $b = -2$: $-2 = 1(-7) + 5 \;\Rightarrow\; q = 1$, $r = 5$.
- Con $b = 60$: $60 = (-8)(-7) + 4 \;\Rightarrow\; q = -8$, $r = 4$.
- Con $b = -60$: $-60 = 9(-7) + 3 \;\Rightarrow\; q = 9$, $r = 3$.

MDC y MMC





Dados $a, b \in \mathbb{Z}$, a cada uno les podemos asociar su conjunto de divisores no-negativos D_a y D_b respectivamente.

Por la propiedad de limitación, estos conjuntos son finitos, y su intersección $D_a \cap D_b$ es finita. Luego, $D_a \cap D_b$ posee un elemento máximo, llamado el *máximo divisor común* (MDC) de a y b.

De forma similar, los conjuntos de los M_a y M_b de múltiplos no-negativos de a y de b, respectivamente. Ahora $M_a \cap M_b$ es no vacío y limitado inferiormente por 0. Este conjunto posee un elemento mínimo, llamado el *mínimo múltiplo común* (MMC) de a y b.

Definición

*Dados $a, b \in \mathbb{N}$, un **máximo divisor común (MDC)** de a y b es un entero positivo d que satisface*

1. $d \mid a$ *y* $d \mid b$,
2. $k \mid d$, *para todo* $k \in \mathbb{N}$ *tal que* $k \mid a$ *y* $k \mid b$.

*Similarmente, un **mínimo múltiplo común (MMC)** de a y b es un entero positivo m que satisface*

1. $a \mid m$ *y* $b \mid m$,
2. $m \mid k$, *para todo* $k \in \mathbb{N}$ *tal que* $a \mid k$ *y* $b \mid k$.

De las definiciones anteriores, se sigue que el MDC y el MMC son únicos:

MDC y MMC

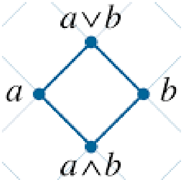
<u>Prueba</u>: Sean d_1 y d_2 dos MDC para a y b. Entonces $d_1 \mid a$, $d_1 \mid b$, $d_2 \mid a$, $2 \mid b$.
Como d_1 es MDC de a y b, y $d_2 \mid a$, $d_2 \mid b \;\Rightarrow\; d_1 \mid d_2$.
Como d_2 es MDC de a y b, y $d_1 \mid a$, $d_1 \mid b \;\Rightarrow\; d_2 \mid d_1$.
Entonces $|d_1| = |d_2|$, pero siendo d_1, d_2 no negativos, se concluye que $d_1 = d_2$.

La prueba es similar en el caso del MMC.

Notación. Como son únicos, denotamos por $d = (a, b)$ y por $m = [a, b]$ al MDC y MMC de a y b, respectivamente.

Otra forma de entender a $d = (a, b)$ y $m = [a, b]$ es que son el **ínfimo** y el **supremo**, respectivamente, de a y b, en la relación de divisibilidad $|$:

$$d = (a, b) = a \wedge b, \qquad m = [a, b] = a \vee b.$$



Ejemplo: Calcular el MDC y MMC de 360 y 84.
Solución: Factoramos los números 360 y 84 (en factores primos):

$$\begin{array}{r|l} 360 & 2 \\ 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad\qquad \begin{array}{r|l} 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \\ 1 & \\ & \\ & \end{array}$$

Los divisores coumnes para 360 y 84 son $2, 2, 3$. Entonces $(360, 84) = 2^2 \cdot 3 = 12$. Por otro lado, $[360, 84] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$.

Propiedades (Propiedades MDC y MMC)

Sean $a, b, c \in \mathbb{N}$. *Entonces*

1. $(a, b) = a \;\Leftrightarrow\; [a, b] = b \;\Leftrightarrow\; a \mid b$.
2. $(ca, cb) = c(a, b)$ *y* $[ca, cb] = c[a, b]$.
3. $(a, b) = (b, a)$ *y* $[a, b] = [b, a]$.
4. $((a, b), c) = (a, (b, c))$ *y* $[[a, b], c] = [a, [b, c]]$.
5. $[(a, c), (b, c)] = ([a, b], c)$.
6. $([a, c], [b, c]) = [(a, b), c]$.
7. $(a, b)[a, b] = ab$.

Prueba: Ejercicio!

Lema (Teorema de Bézout)

Para todo $a, b \in \mathbb{Z}$, existen $M, N \in \mathbb{Z}$ tales que $(a, b) = Ma + Nb$.

<u>Prueba</u>: Sea $S = \{xa + yb;\ x, y \in \mathbb{Z},\ xa + yb > 0\}$. Observe que $a = 1 \cdot a + 0 \cdot b, b = 0 \cdot a + 1 \cdot b \in S$, de forma que S es no vacío. Por el principio del buen orden, S posee un elemento mínimo $d > 0$. En particular, $d = Ma + Nb$ para algunos $M, N \in \mathbb{Z}$. Si aplicamos el algoritmo de la división, con d dividiendo a, existe $q \in Z$ tal que

$$a = qd + r, \quad 0 \leq r < d.$$

Si $r > 0$, entonces $r = a - qd = a - (Ma + Nb) = (1 - M)a - Nb$ sería elemento de S, lo que contradice la elección minimal de r en S. De ahí que $r = 0$. Portanto, $d \mid a$.

Repitiendo el argumento anterior del algoritmo de la división pero ahora con d dividiendo b, se concluye también que $d \mid b$.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Así, d es un divisor común de a y b.
Si c es otro divisor común de a y b, entonces $c \mid a$, $c \mid b$ $c \mid Ma + Nb = d$. Portanto $d = (a, b)$, y hemos establecido que existen $M, N \in \mathbb{Z}$ tales que

$$d = (a, b) = Ma + Nb. \ \square$$

Definición

Dos enteros a y b se llaman ***primos relativos*** *o* ***coprimos*** *si no tienen factores en común (aparte de 1). Esto es, si $(a, b) = 1$.*

Corolario

a y b son primos relativos. si y sólo si, existen $M, N \in \mathbb{Z}$ tales que $Ma + Nb = 1$.

Prueba: ($\Rightarrow$) a, b primos relativos, $\Rightarrow$ existen $M, N \in \mathbb{Z}$ con $1 = (a, b) = Ma + Nb$.
($\Leftarrow$) Si $d \mid a$ y $d \mid b$, entonces $d \mid Ma + Nb = 1$. Luego, $|d| = 1$. $\square$

Corolario

a) *Si* $a \mid c$, $b \mid c$ *y* $(a, b) = 1$, *entonces* $ab \mid c$.

b) *(Lema de* EUCLIDES*) Si* $a \mid bc$ *y* $(a, b) = 1$, *entonces* $a \mid c$.

Prueba: (a) Como $(a, b) = 1$, por el Teorema de Bézout, existen $x, y \in \mathbb{Z}$ tales que $xa + yb = 1$. Luego $xac + ybc = c$.
Ahora $b \mid c \;\Rightarrow\; ab \mid ac \mid xac$ y $a \mid c \;\Rightarrow\; ab \mid bc \mid ybc$. De ahí que $ab \mid xac + ybc = c$.

(b) Como $(a, b) = 1$, de nuevo por el Teorema de Bézout, existen $x, y \in \mathbb{Z}$ tales que $xa + yb = 1$. Luego $xac + ybc = c$.
Como $a \mid xab$ y $a \mid bc \mid ybc$, entonces $a \mid xab + ybc = c$. $\square$.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Corolario

Si $d = (a, b)$*, entonces* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Prueba: Sea $d = (a, b)$. Por el Teorema de Bézout, existen $x, y \in \mathbb{Z}$ tales que $xa + yb = d$. Dividiendo la ecuación anterior entre d, escribimos

$$x\left(\frac{a}{d}\right) + y\left(\frac{b}{d}\right) = 1.$$

Como $x, y \in \mathbb{Z}$, por el corolario al Teorema de Bézout a esta última ecuación, entonces $\frac{a}{d}$ y $\frac{b}{d}$ son primos relativos, y $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. $\square$.

Nota Aclaratoria! El Lema de Bézout **no es** un si y sólo si. De hecho más adelante vamos a probar que los enteros n que admiten representación en la forma $n = xa + yb$ son precisamente los múltiplos de $d = (a, b)$.
Sin embargo, vale un si y sólo sí, cuando se tiene $xa + yb = 1$. La única forma que 1 sea combinación lineal de a y b es cuando son coprimos.

Prop: $[a,b](a,b)=ab$, para $a,b\in\mathbb{N}$.

Prueba: Sea $d=(a,b)$. Por el Teorema de Bézout, existen $M,N\in\mathbb{Z}$ tales que $Ma+Nb=d$.
Por otro lado, $d\mid ab$. Sea entonces $m=\frac{ab}{d}\in\mathbb{N}$. Como $m=\left(\frac{a}{d}\right)b=a\left(\frac{b}{d}\right)$, sabemos que m es un múltiplo común de a y de b.

Suponga que n es otro múltiplo común de a y de b. Mostramos que $n\mid m$. En efecto,

$$\frac{n}{m}=\frac{n}{ab/d}=\frac{nd}{ab}=\frac{n(Ma+Nb)}{ab}=n\left(\frac{M}{b}+\frac{N}{a}\right)=\frac{n}{b}M+\frac{n}{a}N\in\mathbb{Z}.$$

Portanto, $m\mid n$, y entonces $m=[a,b]$ es el mínimo múltiplo común. Se concluye que $ab=md=[a,b](a,b)$. $\square$.

¿Cómo calcular (a, b)?

Lema

Para $a, b \in \mathbb{Z}$, $(a, b) = (a - b, b) = (a, b - a)$.

Prueba: Mostramos $(a, b) = (a - b, b)$. La otra igualdad es análoga.
Sean $d = (a, b)$, $c = (a - b, b)$. Entonces $d \mid a$, $d \mid b \;\Rightarrow\; d \mid a - b$. Luego, $d \mid c$.
Ahora, $c \mid a - b$, $c \mid b \;\Rightarrow\; c \mid (a - b) + b = a$. De ahí, $c \mid d$. Esto muestra que $d = c$. $\square$

Lema

Para todo $a \in \mathbb{Z}$, $(a, 0) = |a|$.

Prueba: $a \mid 0$ y $a \mid a \;\Rightarrow\; a \mid (a, 0)$. Por otro lado, $(a, 0) \mid a$. luego, por antisimetría, $(a, 0) = |a|$. $\square$

¿Cómo calcular (a, b)?

Esto ya nos da un primer algoritmo para calcular (a, b):

Algoritmo 1: (Cálculo del MDC por restas).

```
def mdc(a, b):
  if (b > a):
    return mdc(b,a)
  if (b == 0):
    return a
  else:
    return mdc(a-b,a)
```

Algoritmo de Euclides

Emplea el algoritmo de la división como base. Conocido por los griegos (publicado por EUCLIDES).

Lema (Euclides)

Si $a = qb + r$, entonces $(a, b) = (b, r)$.

Prueba: Sean $d = (a, b)$ y $f = (b, r)$.
Como $d \mid a$ y $d \mid b$, entonces $d \mid a - qb = r$. Luego $d \mid (b, r) = f$.
Como $f \mid b$ y $f \mid r$, entonces $f \mid qb - r = a$. Luego $f \mid (a, b) = d$.
Por antisimetría, $d \mid f$ y $f \mid d \;\Rightarrow (a, b) = d = f = (b, r)$. $\square$

El Algoritmo de Euclides se basa en el hecho que en la división $a = qb + r$, podemos descartar el dividendo y calcular (a, b) como (b, r).

Algoritmo de Euclides

El algoritmo euclidiano se puede describir de la siguiente manera: sean $a, b \in \mathbb{Z}$ cuyo máximo común (a, b) divisor se desea calcular. Como $(|a|, |b|) = (a, b)$, podemos suponer que $a > b > 0$. El primer paso es aplicar el Algoritmo de la División, para obtener

$$a = q_1 b + r_1, \qquad \text{con } 0 \leq r_1 < b.$$

Si $r_1 = 0$, entonces $b \mid a$ y $(a, b) = b$. Cuando $r_1 \neq 0$, dividimos b por r_1 para producir enteros q_2, r_2 tales que

$$b = q_2 r_1 + r_2, \qquad \text{con } 0 \leq r_2 < r_1.$$

Si $r_2 = 0$, entonces $r_1 \mid b$ y $(b, r_1) = r_1$, y nos detenemos. Caso contrario, $r_2 \neq 0$, continuamos este proceso y dividimos r_1 por r_2 para producir enteros q_3, r_3 tales que

$$r_1 = q_3 r_2 + r_3, \qquad \text{con } 0 \leq r_3 < r_2.$$

Algoritmo de Euclides

Este proceso de división continúa hasta que aparece un residuo cero, digamos, en el paso $n + l$, donde r_{n-1} se divide por r_n.

El resultado es el siguiente sistema de ecuaciones:

$$\begin{aligned} a &= q_1 b + r_1, \quad 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned} \tag{3}$$

Argumentamos que r_n, el último residuo distinto de cero que aparece de esta manera, es igual a (a, b).

Teorema (Algoritmo de Euclides)

En el sistema de ecuaciones (3), el máximo divisor común de a y b coincide con el último residuo diferente de cero. Esto es, $(a, b) = r_n$.

Prueba:
Por el Lema de Euclides, del sistema de ecuaciones (3), podemos concluir que

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Falta nada más garantizar un detalle. Que el sistema de ecuaciones (3) es posible. La construcción de las relaciones $r_{i-1} = q_{i+1}r_i + r_{i+1}$, $i = 0, 1, \ldots, n$, (aquí $r_{-1} = a, r_0 = b$) está garantizada por el Algoritmo de la División.

Ademas, de la relación de los residuos $0 \leq r_i < r_{i-1}$, $i = 1, 2, \ldots, n$,

Algoritmo de Euclides

se tiene que

$$0 = r_{n+1} < r_n < r_{n-1} < \ldots < r_1 < b.$$

Por lo tanto hay a lo sumo b ecuaciones en el sistema (3). Esto garantiza que el Algoritmo de Euclides consiste a lo sumo de b pasos. En particular, es finito y termina. $\square$

Algoritmo de Euclides

Ejemplo: Hallar $(12378, 3054)$.

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Luego, $(12378, 3054) = 6$.

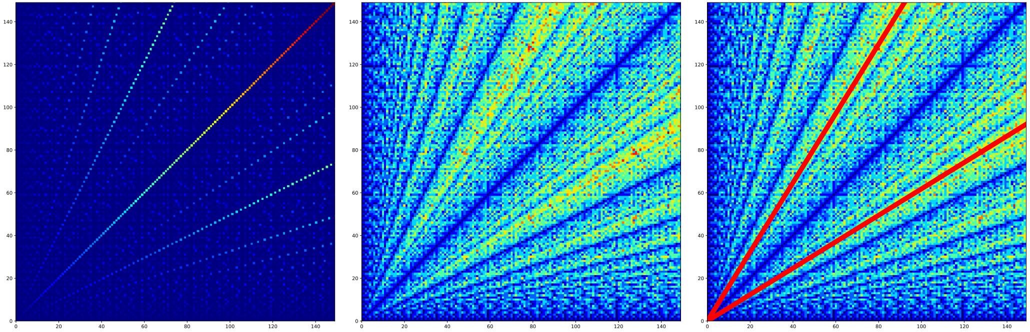
Algoritmo de Euclides

Consecuencias: A partir del algoritmo de Euclides, podemos calcular los coeficientes en el Teorema de Bézout.

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

$$\begin{aligned} (12378, 3054) = 6 &= 24 - 1(18) = 24 - 1(138 - 5 \cdot 24) = 6(24) - 1(138) \\ &= 6(162 - 138) - 1(138) = 6(162) - 7(138) \\ &= 6(162) - 7(3054 - 18 \cdot 162) = 132(162) - 7(3054) \\ &= 132(12378 - 4 \cdot 3054) - 7(3054) = \mathbf{132}(12378) + (-\mathbf{535})(3054). \end{aligned}$$

Algoritmo de Euclides



Comparación de valores en el algoritmo de Euclides. (a) $d = (a, b)$. (b) Número requerido de pasos. (c) Observe las diagonales que requieren más pasos coinciden con números a y b con una relación cercana al valor $\varphi = \frac{1+\sqrt{5}}{2}$, *e.g.* números de Fibonacci consecutivos.