Números Enteros

Teresa Krick*

1 Hechos generales

El conjunto de los números enteros es :

$$\mathbb{Z} \;=\; \{\dots,-3,-2,-1,0,1,2,3,\dots\} \;=\; -\mathbb{N}\cup\{0\}\cup\mathbb{N} \quad (\text{donde} -\mathbb{N} := \{-n; n\in\mathbb{N}\}).$$

Una de las razones de la necesidad de trabajar con estos números es que en $\mathbb{N}$ no se puede restar (en general), y así $\mathbb{Z}$ se obtiene a partir de $\mathbb{N}$ agregando los números negativos. Mencionemos que en $\mathbb{Z}$ la operación $+$ cumple las siguientes propiedades, que le dan una estructura de *Grupo Conmutativo* :

- Para todo $a,b\in\mathbb{Z}$, $a+b\in\mathbb{Z}$.
- *Conmutatividad :* Para todo $a,b\in\mathbb{Z}$, $a+b=b+a$.
- *Asociatividad :* Para todo $a,b,c\in\mathbb{Z}$, $(a+b)+c=a+(b+c)$ (y por lo tanto, se puede escribir $a+b+c$ sin aclarar qué se suma primero).
- *Existencia de Elemento Neutro :* Existe un elemento en $\mathbb{Z}$ (único) que es el 0, que verifica que para todo $a\in\mathbb{Z}$, $a+0=a$.
- *Existencia de Opuesto :* Para todo $a\in\mathbb{Z}$, existe un (único) elemento, que es $-a$, tal que $a+(-a)=0$.

La razón por la que se le da un nombre a los conjuntos con una operación que verifica las 5 propiedades mencionadas, es que se observó que hay muchísimos conjuntos que, junto con una operación, verifican esas propiedades (por ejemplo, con la suma, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^2$, $\mathbb{R}[X]$, ...) y entonces, a fin de estudiar las consecuencias de esas propiedades, conviene hacerlo de una vez por todos en el caso abstracto general y luego aplicarlo en cada caso en lugar de estudiarlas para cada conjunto en particular.

En $\mathbb{Z}$ también se puede multiplicar : la operación $\cdot$ cumple propiedades parecidas a $+$, aunque no todas :

- Para todo $a,b\in\mathbb{Z}$, $a\cdot b\in\mathbb{Z}$.
- *Conmutatividad :* Para todo $a,b\in\mathbb{Z}$, $a\cdot b=b\cdot a$.
- *Asociatividad :* Para todo $a,b,c\in\mathbb{Z}$, $(a\cdot b)\cdot c=a\cdot(b\cdot c)(=a\cdot b\cdot c=a\,b\,c)$.
- *Existencia de Elemento Neutro :* Existe un elemento en $\mathbb{Z}$ (único) que es el 1, que verifica que para todo $a\in\mathbb{Z}$, $1\cdot a=a$.

*Notas correspondientes a la parte de "Enteros" de la materia Algebra 1 de la Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, con el apoyo de los subsidios UBACyT X-198 y CONICET 2461/01.

- *No hay Existencia de Inverso multiplicativo :* Los únicos elementos inversibles a de $\mathbb{Z}$ para el producto, o sea que verifican que existe $a^{-1} \in \mathbb{Z}$ de manera que $a \cdot a^{-1} = 1$ son el 1 y el -1.

La propiedad siguiente relaciona el producto con la suma:

- *Distributividad del producto sobre la suma :* Para todo $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades de la suma y el producto en $\mathbb{Z}$ hacen que $\mathbb{Z}$ tenga una estructura de *Anillo Conmutativo* (estructura que conviene estudiar en general por las mismas razones que conviene estudiar la de Grupo).
Recordemos otras propiedades que ya conocemos de $\mathbb{Z}$ o también de subconjuntos de $\mathbb{Z}$:

- $\mathbb{Z}$ es un conjunto inductivo, que contiene estrictamente a $\mathbb{N}$ y para el cual no vale así nomás el principio de inducción ya que no tiene primer elemento por el cual empezar la inducción.
- Si fijamos $n_0 \in \mathbb{Z}$, en $\mathbb{Z}_{n_0} := \{m \in \mathbb{Z}; m \geq n_0\}$ vale el principio de inducción empezando en n_0. Por ejemplo en $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ vale el principio de inducción.
- Equivalentemente, $\mathbb{Z}_{n_0}$ y $\mathbb{N}_0$ son conjuntos bien ordenados, o sea, cualquier subconjunto no vacío de $\mathbb{Z}_{n_0}$ o $\mathbb{N}_0$ tiene primer elemento o mínimo (un elemento en el subconjunto menor o igual que todos los demás).

2 Divisibilidad

El hecho que los números enteros no son divisibles (con cociente entero) por cualquier otro número entero hace interesante estudiar la noción y consecuencias de la *divisibilidad*. (Este estudio no se justifica por ejemplo de la misma manera en $\mathbb{Q}$ o $\mathbb{R}$ donde todo número racional o real es divisible (con cociente racional o real) por cualquier otro número racional o real no nulo.)

Definición 2.1 (Divisibilidad)
Sean $a, d \in \mathbb{Z}$ con $d \neq 0$. Se dice que <u>d divide a a</u> (o que a es divisible por d, o que a es múltiplo de d) si existe un elemento $k \in \mathbb{Z}$ tal que $a = k \cdot d$ (o sea si el cociente $\frac{a}{d}$ es un número entero).
Se nota $d \,|\, a$ (con una barrra vertical, no confundir con la barra del cociente /). O sea:

$$d \,|\, a \underset{def}{\iff} \exists\, k \in \mathbb{Z} \,:\, a = k \cdot d.$$

En caso contrario, se dice que d no divide a a, y se nota $d \nmid a$. Eso es cuando el cociente $\frac{a}{d} \notin \mathbb{Z}$, o sea no existe ningún entero $k \in \mathbb{Z}$ tal que $a = k \cdot d$.
El conjunto de los divisores positivos y negativos de un entero a se notará por $Div\,(a)$ y el de los divisores positivos por $Div_+\,(a)$.
(Nota : en algunos libros no se excluye el caso $d = 0$ pero se conviene que 0 divide únicamente al 0. Igualmente en este curso excluiremos el caso $d = 0$ para no "dividir por 0".)

Ejemplos

- $7 \,|\, 56$ pues $56 = 8 \cdot 7$.
- $7 \,|\, -56$, $-7 \,|\, 56$, $-7 \,|\, -56$.

- $7 \nmid 54$.
- $Div(-12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$ y $Div_+(-12) = \{1, 2, 3, 4, 6, 12\}$.

Ejemplos generales

- Todo número entero $d \neq 0$ verifica que $d \mid 0$ pues $0 = 0 \cdot d$ (aquí $k = 0$). Así el 0 tiene infinitos divisores : $Div(0) = \mathbb{Z} \setminus \{0\}$.
- $d \mid a \iff -d \mid a$ (pues $a = k \cdot d \iff a = (-k) \cdot (-d)$).

  De la misma manera $d \mid a \iff d \mid -a \iff -d \mid -a$.

  Se concluye que $d \mid a \iff |d| \mid |a|$ (donde $|x|$ denota el módulo o valor absoluto de x).

  De esto se deduce que a cada divisor negativo le corresponde un divisor positivo, y que el número total de divisores (si es finito) de a es el doble del número de divisores positivos.
- $d \mid a$ y $a \mid d \iff a = \pm d$: Pues $a = k \cdot d$ y $d = \ell \cdot a$ implica que $a = (k \cdot \ell) \cdot a$, por lo tanto $k \cdot \ell = 1$, o sea, $k = \pm 1$.
- Si $a \neq 0$, entonces $Div_+(a) \subset \{1, \ldots, |a|\}$ y por lo tanto a tiene un número finito ($\leq |a|$) de divisores positivos, y un número finito ($\leq 2|a|$) de divisores positivos y negativos :

  Esto es pues $d \mid a \iff \exists\, k \in \mathbb{Z}$ tq $a = k \cdot d$; por lo tanto $|a| = |k| \cdot |d|$ y dado que $k \neq 0$ (pues $a \neq 0$), $|k| \geq 1$ y $|a| = |k| \cdot |d| \geq |d|$.
- Para todo $a \in \mathbb{Z}$, se tiene $1 \mid a$ y $-1 \mid a$, y también $a \mid a$ y $-a \mid a$.

  Así, si $a \neq \pm 1$, a tiene por lo menos 4 divisores distintos ($\pm 1, \pm a$), o 2 divisores positivos distintos (1, $|a|$).

  Hay números enteros que tienen únicamente esos 4 divisores, que son los asegurados, otros tienen más. Esto motiva la separación de los números enteros (distintos de 0, 1 y -1) en dos categorías, la de los números *primos* y la de los números *compuestos* :

Definición 2.2 (Números primos y compuestos)
Sea $a \in \mathbb{Z}$, $a \notin \{-1, 0, 1\}$.

- *Se dice que* a *es primo sii* a *tiene únicamente 4 divisores (o 2 divisores positivos). Por ejemplo* $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \ldots$.

  (En general los números primos se notan con las letras p, q, $\ldots$*)*
- *Se dice que* a *es compuesto sii* a *tiene más que 4 divisores (o más que 2 divisores positivos). Por ejemplo* $\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \ldots$.

  Se observa que a *es compuesto sii tiene un divisor positivo* d *con* $2 \leq d \leq |a| - 1$ *(pues ya vimos que* $Div_+(a) \subset \{1, \ldots, |a|\}$ *y si* a *tiene más que 2 divisores positivos, tiene que haber uno en "algún lugar en el medio").*

Más adelante, se trabajará mucho más con los números primos, que cumplen propiedades importantísimas, y constituyen los ladrillos de base para construir todos los números, en el sentido que cualquier número entero (distinto de 0 y ± 1) se escribe en forma única como producto de primos positivos (salvo el signo).

Se verán ahora algunas propiedades importantes de la divisibilidad :

Propiedades 2.3 *Sean* $a, b, d \in \mathbb{Z}$, $d \neq 0$.

- $d \mid a$ *y* $d \mid b \implies d \mid a+b$.
  (Pues si $a = k \cdot d$ *y* $b = \ell \cdot d$ *con* $k, \ell \in \mathbb{Z}$, *entonces* $a+b = (k+\ell) \cdot d$, *con* $k+\ell \in \mathbb{Z}$.*)*
- $d \mid a$ *y* $d \mid b \implies d \mid a-b$.
- $d \mid a+b$ *no implica que* $d \mid a$ *y* $d \mid b$ *: Por ejemplo,* $6 \mid 4+8$ *pero* $6 \nmid 4$ *y* $6 \nmid 8$.
- *Sin embargo si* $d \mid a+b$ *y* se sabe que $d \mid a$, *entonces* $d \mid b$.
  (Pues $d \mid (a+b)-a$.*)*
- $d \mid a \Longrightarrow d \mid a \cdot b \quad \forall\, b \in \mathbb{Z}$.
- $d \mid a \Longrightarrow d^2 \mid a^2$ *y* $d^n \mid a^n, \quad \forall\, n \in \mathbb{N}$.
  (Pues si $a = k \cdot d$, *entonces* $a^2 = k^2 \cdot d^2$ *y* $a^n = k^n \cdot d^n$.*)*
- $d \mid a \cdot b$ *no implica* $d \mid a$ *o* $d \mid b$ *: Por ejemplo,* $6 \mid 3 \cdot 4$ *pero* $6 \nmid 3$ *y* $6 \nmid 4$.

  La propiedad $d \mid a\,b \Rightarrow d \mid a$ *o* $d \mid b$ *se cumple siempre unicamente cuando* d *es un número primo. Es más, veremos que esta es la propiedad más importante que cumplen los números primos.*

Ejemplos

- Hallar todos los $a \in \mathbb{Z}, a \neq 1$, tales que $a-1 \mid a^2+5$.

  Para resolver esto, se trata de poner a la derecha del símbolo $\mid$ un número fijo, de manera de trabajar después con los divisores de ese número. Para ello se puede usar por ejemplo que se sabe que $a-1 \mid a-1$, por lo tanto $a-1 \mid b\,(a-1)$ (para todo $b \in \mathbb{Z}$) y en particular $a-1 \mid (a+1)(a-1)$. Así se tiene $a-1 \mid a^2+5$ y $a-1 \mid a^2-1$, por lo tanto $a-1$ divide a la diferencia, es decir $a-1 \mid 6$. Es decir $a-1 \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Por lo tanto $a \in \{-5, -2, -1, 0, 2, 3, 4, 7\}$, y se concluye verificando que para cada valor de ese conjunto es cierto que $a-1 \mid a^2+5$, o bien verificando y mostrando que en realidad todas las implicaciones usadas son equivalencias.

- Probar que para todo $a \in \mathbb{Z}, a \neq 1$, y para todo $n \in \mathbb{N}$ vale que $a-1 \mid a^n-1$.

  Esto ya se puede hacer a este nivel de distintas formas (despues veremos otra incluso) :

  - Usando la Serie Geométrica :
    $$\sum_{i=0}^{n-1} a^i = \frac{a^n-1}{a-1}$$
    Por lo tanto
    $$a^n - 1 = (a-1) \sum_{i=0}^{n-1} a^i$$
    y dado que la sumatoria da un número entero (pues es una suma de potencias de enteros) resulta que $a-1 \mid a^n-1$.

– Usando el Binomio de Newton :

$$a^n = ((a-1)+1)^n = \sum_{i=0}^{n} \binom{n}{i}(a-1)^i = 1 + n(a-1) + \binom{n}{2}(a-1)^2 + \cdots + (a-1)^n$$

Por lo tanto

$$a^n - 1 = (a-1)\big(n + \binom{n}{2}(a-1) + \cdots + (a-1)^{n-1}\big) = k\,(a-1)$$

donde $k \in \mathbb{Z}$ es la sumatoria que está dentro del paréntesis.

– Por inducción en n. La proposición es $p(n)$: "$a-1 \,|\, a^n - 1$"
$p(1)$ es Verdadera pues $a-1 \,|\, a-1$.
$p(k)$ Verdadera $\Longrightarrow p(k+1)$ Verdadera :
HI : $a-1 \,|\, a^k - 1$. Se quiere probar que $a-1 \,|\, a^{k+1} - 1$.
Pero $a^{k+1} - 1 = a(a^k - 1) + (a-1)$, y por HI, $a-1 \,|\, a^k - 1$, y por otro lado, $a-1 \,|\, a-1$, por lo tanto $a-1$ divide a la suma, como se quería probar.

(Las dos primeras tienen la ventaja sobre la última de dar también la expresión del cociente, y la primera es la más sencilla.)

- Sean $m, n \in \mathbb{N}$. Probar que si $m \,|\, n$, entonces para todo $a \neq \pm 1$, $a^m - 1 \,|\, a^n - 1$.

  Se tiene $n = k \cdot m$, luego $a^n = (a^m)^k$. Si ponemos $A := a^m$, por el inciso anterior se tiene que $A - 1 \,|\, A^k - 1$, es decir $a^m - 1 \,|\, a^n - 1$.

3 Congruencia

Se introduce ahora una notación debida a Carl Friedrich Gauss (1777–1855), conocido como el *Príncipe de los matemáticos*, y reconocido históricamente como uno de los dos o tres gigantes de la Matemática universal. La notación facilita mucho la forma de escribir y trabajar con los números enteros y la divisibilidad.

Definición 3.1 (Congruencia)
Sean $a, b, d \in \mathbb{Z}, d \neq 0$. *Se dice que* a es congruente a b módulo d *sii* $d \,|\, a - b$.
Se nota $a \equiv b \pmod{d}$ *o también* $a \equiv b\ (d)$. *O sea:*

$$a \equiv b \pmod{d} \underset{def}{\iff} d \,|\, a - b.$$

En caso contrario se nota $a \not\equiv b \pmod{d}$ *o* $a \not\equiv b\ (d)$.

Ejemplos

- $5 \equiv 3 \pmod 2$, $5 \equiv -1 \pmod 2$, $5 \equiv 1 \pmod 2$, $5 \not\equiv 2 \pmod 2$, $4 \equiv 0 \pmod 2$, $\forall\, k \in \mathbb{Z}$, $2k \equiv 0 \pmod 2$ y $2k + 1 \equiv 1 \pmod 2$.
- $13 \equiv 8 \pmod 5$ y $13 \equiv 3 \pmod 5$.
- Sean $a, d \in \mathbb{Z}$, $d \neq 0$, entonces $a \equiv 0 \pmod d \iff d \,|\, a$.

- Sean $k, r, d \in \mathbb{Z}$, $d \neq 0$, entonces $k \cdot d + 1 \equiv 1 \pmod{d}$ y $k \cdot d + r \equiv r \pmod{d}$.

Sea $d \in \mathbb{Z}$, $d \neq 0$, fijo. Se verá ahora que la relación de congruencia en $\mathbb{Z}$ es una relación de equivalencia en $\mathbb{Z}$, por lo tanto parte el conjunto de los números enteros en subconjuntos de elementos que son todos congruentes entre sí, y que son por lo tanto de alguna manera considerados "iguales" bajo ese concepto.

Proposición 3.2 *Sea $d \in \mathbb{Z} \setminus \{0\}$ fijo. Sea $\mathcal{R}$ la relación en $\mathbb{Z}$ dada por*

$$a \mathcal{R} b \iff a \equiv b \pmod{d}.$$

Entonces $\mathcal{R}$ es una relación de equivalencia.

Prueba.–

- *Reflexividad :* Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{d}$ pues $d \mid a - a$.
- *Simetría :* Hay que probar que para todo $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$, entonces $b \equiv a \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a - b$, y por lo tanto $d \mid -(a-b) = b - a$, por lo tanto $b \equiv a \pmod{d}$.
- *Transitividad :* Hay que probar que para todo $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$ y $b \equiv c \pmod{d}$ entonces $a \equiv c \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a - b$, y $b \equiv c \pmod{d}$ significa que $d \mid b - c$. Por lo tanto $d \mid (a-b) + (b-c)$, o sea $d \mid a - c$, es decir $a \equiv c \pmod{d}$.

■

La proposición anterior significa que se dividen los números enteros en subconjuntos de elementos congruentes entre sí, que se "identifican" de esa manera. Por ejemplo si se toma congruencia módulo 2, quedan por un lado los pares (que son todos congruentes entre sí y también congruentes a 0 módulo 2), y por otro lado los impares (que son congruentes entre sí y congruentes a 1 módulo 2). Cuando se toma congruencia módulo 3, $\mathbb{Z}$ queda subdividido en 3 subconjuntos : los que son de la forma $3k$, $k \in \mathbb{Z}$, por un lado, por otro lado los que son de la forma $3k + 1$ y por último los que se escriben como $3k + 2$. Más adelante se verá el Algoritmo de División, y se verá que la congruencia módulo d clasifica (e identifica) los números enteros según su resto módulo d.

A continuación, se enuncian propiedades de la congruencia, que son muy útiles para trabajar :

Propiedades 3.3 *Sea $d \in \mathbb{Z} \setminus \{0\}$ fijado. Entonces :*

- $a_1 \equiv b_1 \pmod{d}$ *y* $a_2 \equiv b_2 \pmod{d} \implies a_1 + a_2 \equiv b_1 + b_2 \pmod{d}$.
  (Pues $d \mid a_1 - b_1$ y $d \mid a_2 - b_2 \implies d \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$.)
- *De la misma manera, se puede probar por inducción que para todo $n \in \mathbb{N}$:*

  $$a_1 \equiv b_1 \pmod{d}, \ldots, a_n \equiv b_n \pmod{d} \implies a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{d}.$$

- $a \equiv b \pmod{d}$ *y* $c \in \mathbb{Z} \implies ca \equiv cb \pmod{d}$.
- $a_1 \equiv b_1 \pmod{d}$ *y* $a_2 \equiv b_2 \pmod{d} \implies a_1 a_2 \equiv b_1 b_2 \pmod{d}$.
  (Para probar esto se usa el item anterior y la transitividad : como $a_1 \equiv b_1 \pmod{d}$, entonces $a_1 a_2 \equiv b_1 a_2 \pmod{d}$ (multiplicando por a_2), y por otro lado, como $a_2 \equiv b_2 \pmod{d}$, se tiene $b_1 a_2 \equiv b_1 b_2 \pmod{d}$ (multiplicando por b_2), y finalmente por transitividad, se concluye que $a_1 a_2 \equiv b_1 b_2 \pmod{d}$.)

- *Por inducción, se tiene :*

$$a_1 \equiv b_1 \pmod{d}, \ldots, a_n \equiv b_n \pmod{d} \implies a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{d}.$$

- *Tomando en los items anteriores* $a_1 = \cdots = a_n = a$ *y* $b_1 = \cdots = b_n = b$*, se obtiene :*

$$a \equiv b \pmod{d} \implies a^2 \equiv b^2 \pmod{d} \quad y \quad a^n \equiv b^n \pmod{d}, \quad \forall\, n \in \mathbb{N}.$$

- *Las dos propiedades siguentes permiten reemplazar el módulo por un divisor o un múltiplo:*

$$\begin{array}{lllll} a \equiv b \pmod{d} & y & c \mid d & \implies & a \equiv b \pmod{c}, \\ a \equiv b \pmod{d} & y & c \neq 0 & \iff & c\,a \equiv c\,b \pmod{c\,d}. \end{array}$$

  La primera vale pues si $c \mid d$ *y* $d \mid a-b$*, entonces* $c \mid a-b$*. Pero observemos que la recíproca no es cierta en general, es decir* $a \equiv b \pmod{c}$ *y* $c \mid d$ *no implican que* $a \equiv b \pmod{d}$*. Por ejemplo* $10 \equiv 3 \pmod{7}$ *y* $7 \mid 14$ *pero* $10 \not\equiv 3 \pmod{14}$*.*

  La segunda afirmación es un si y solo si pues $d \mid a-b \iff c\,d \mid c\,a - c\,b$*.*

Resumimos las dos propiedades más importantes por ahora:

$$\left\{ \begin{array}{ll} a_1 \equiv b_1 & \pmod{d} \\ \vdots & \\ a_n \equiv b_n & \pmod{d} \end{array} \right. \implies \left\{ \begin{array}{ll} a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n & \pmod{d} \\ a_1 \cdots a_n \equiv b_1 \cdots b_n & \pmod{d} \end{array} \right.$$

Aplicaciones

- Retomamos el ejemplo anterior : $\forall\, n \in \mathbb{N},\ a \in \mathbb{Z} \setminus \{1\}$, vale $a-1 \mid a^n - 1$:

  Se tiene que $a \equiv 1 \pmod{a-1}$ pues $a-1 \mid a-1$, por lo tanto $a^n \equiv 1^n \pmod{a-1}$, es decir, $a-1 \mid a^n - 1$.

- Para todo $n \in \mathbb{N}_0$, $64 \mid 49^n + 16n - 1$:

  Se probará por inducción en n, combinado con congruencia.

$$p(n) : \text{“}64 \mid 49^n + 16n - 1\text{”}$$

  $p(0)$ es Verdadera como antes.

  $p(k)$ Verdadera $\implies p(k+1)$ Verdadera :

  HI : $64 \mid 49^k + 16k - 1$, o sea $49^k \equiv -16k + 1 \pmod{64}$.

  Se quiere probar que $64 \mid 49^{k+1} + 16(k+1) - 1$.

  Por HI, $49^{k+1} = 49 \cdot 49^k \equiv 49\,(-16k+1) \pmod{64}$.

  Por lo tanto, $49^{k+1} + 16(k+1) - 1 \equiv 49\,(-16k+1) + 16(k+1) - 1 \pmod{64}$.

  Distribuyendo y factorizando, resulta : $49^{k+1} + 16(k+1) - 1 \equiv -48 \cdot 16k + 64 \pmod{64}$. Pero $64 \equiv 0 \pmod{64}$ (pues $64 \mid 64$) y $-48 \cdot 16k \equiv 0 \pmod{64}$ (pues $64 \mid -48 \cdot 16k$), por lo tanto $-48 \cdot 16k + 64 \equiv 0 + 0 \pmod{64}$, y, de nuevo por transitividad, resulta $49^{k+1} + 16(k+1) - 1 \equiv 0 \pmod{64}$, o sea $64 \mid 49^{k+1} + 16(k+1) - 1$ como se quería probar.

  Se concluye que $64 \mid 49^n + 16n - 1$ para todo $n \in \mathbb{N}$.

4 Algoritmo de división

Vamos a enunciar y demostrar ahora el bien conocido algoritmo de división entera.

Teorema 4.1 (Algoritmo de división)
Dados $a, d \in \mathbb{Z}$ *con* $d \neq 0$, existen $k, r \in \mathbb{Z}$ *que verifican*

$$a = k\,d + r \quad \text{con} \quad 0 \leq r < |d|.$$

Además, k *y* r *son* únicos *en tales condiciones.*
Se dice que k *es el* <u>cociente</u> *y* r *es el* <u>resto</u> *de la división de* a *por* d *(*a *es el dividendo y* d *el divisor). Al resto* r *también lo notaremos* $r_d(a)$ *para distinguir que es el "resto de* a *módulo* d*".*

Antes de pasar a la demostración, hagamos algunos ejemplos:

Ejemplos

- $a = 1038, d = 14$:

  $$1038 = 74 \cdot 14 + 2 \implies k = 74, r = r_{14}(1038) = 12 \text{ ya que } 0 \leq 2 < |d|.$$

- $a = 1038, d = -14$:

  $1038 = 74 \cdot 14 + 2 = (-74) \cdot (-14) + 2 \implies k = -74, r = r_{-14}(1038) = 2$ ya que $0 \leq 2 < |d|$.

- $a = -1038, d = 14$:

  $$1038 = 74 \cdot 14 + 2 \implies -1038 = -74 \cdot 14 - 2 \text{ pero } -2 < 0.$$

  Hay que corregirlo, se hace restando y sumando el (módulo del) divisor 14:

  $$-1038 = (-74 \cdot 14 - 14) + (14 - 2) = -75 \cdot 14 + 12 \implies k = -75, r = r_{14}(-1038) = 12$$

  ya que $0 \leq 12 < |d|$.

- $a = -1038, d = -14$:

  $$1038 = 74 \cdot 14 + 2 \implies -1038 = 74 \cdot (-14) - 2 \text{ pero } -2 < 0.$$

  Se corrige nuevamente como arriba restando y sumando el módulo del divisor -14:

  $$-1038 = (74 \cdot (-14) - 14) + (14 - 2) = 75 \cdot (-14) + 12 \implies k = 75, r = r_{-14}(-1038) = 12$$

  ya que $0 \leq 12 < |d|$.

La conclusión —como veremos en la demostración del teorema— es que para saber dividir números positivos o negativos por divisores positivos o negativos, alcanza saber hacerlo para dividendos y divisores positivos y luego corregir cociente y/o resto en cada caso.

Observación 4.2 *Si* $0 \leq a < |d|$*, entonces* $a = 0 \cdot d + a$ *implica* $k = 0$ *y* $r = r_d(a) = a$ *pues* a *cumple la condición que tiene que cumplir el resto (se aplica la unicidad del cociente y el resto).*

Prueba del Teorema 4.1.–

El teorema consta de dos afirmaciones, la parte existencial, que requiere mostrar que existen k y r en las condiciones del teorema, y luego la unicidad: mostrar que no puede haber dos pares distintos de cociente y resto para a y d dados.

<u>*Existencia:*</u> Vamos a probar primero en detalle el caso $a \geq 0, d > 0$, ya que, como nos sugieren los ejemplos, los otros casos se reducen a ese.

- Caso $a \geq 0, d > 0$:

  Aquí, $|d| = d$. La idea intuitiva es considerar los elementos a, $a - d$, $a - 2d$, $a - 3d$, ... hasta que caigamos en algun elemento menor que d pero aún mayor o igual que cero. Este será el resto. Formalizamos esta idea de la manera siguiente:

  Sea A el subconjunto de $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ formado por los números de la forma $a - j\,d$ para algún $j \in \mathbb{Z}$, es decir:

  $$A = \{\, a - j\,d,\ j \in \mathbb{Z}\} \cap \mathbb{N}_0.$$

  Claramente A es un subconjunto de $\mathbb{N}_0$ que no es vacío ya que $a = a - 0 \cdot d$ pertenece a A (estamos considerando el caso $a \geq 0$).

  Luego, por el principio de buena ordenación, el conjunto A tiene un mínimo. Llamemos r a ese mínimo. Se tiene que $r \in A$ por un lado, y por otro lado r es menor que todos los demás elementos de A.

  Como $r \in A$, existe un elemento natural o cero, llamémoslo k, que verifica que $r = a - k\,d$, luego $a = k\,d + r$.

  Falta probar que $0 \leq r < d$ (ya que $|d| = d$ en el caso que estamos considerando):

  Claramente $r \geq 0$ ya que pertenece a A que es un subconjunto de $\mathbb{N}_0$.

  Si r fuese mayor o igual que d, entonces $r - d \geq 0$ aún. Luego se tendría que el elemento $r - d = a - k\,d - d = a - (k+1)\,d$ está también en el conjunto A pero es menor que r ! Eso contradice que r sea el mínimo. Así, se concluye $r < d$.

- Caso $a \geq 0, d < 0$:

  En este caso, $-d > 0$ (y por lo tanto $|d| = -d$) y se tiene que por el caso anterior, existen k', r' tal que $a = k'\,(-d) + r'$ con $0 \leq r' < |d|$. Se obtiene directamente $a = (-k')\,d + r'$, luego $k = -k', r = r'$.

- Caso $a < 0$:

  En este caso, tenemos $-a > 0$, y de los casos anteriores existen k', r' tal que $-a = k'\,d + r'$ con $0 \leq r' < |d|$. Luego $a = (-k')\,d - r'$.

  Si $r' = 0$, r' cumple la condición de resto y se obtiene $k = -k', r = r' = 0$.

  Pero si $r' \neq 0$, hay que corregirlo restando y sumando $|d|$ a la expresión:

  $$a = (-k')\,d - r' = ((-k')\,d - |d|) + (|d| - r').$$

  Así, si se define $k := -k' \pm 1$ según si $d < 0$ o $d > 0$, y $r := |d| - r'$, se tiene $a = k\,d + r$ con $0 < r < |d|$, ya que

  $$0 < r' < |d| \Longrightarrow -|d| < -r' < 0 \Longrightarrow |d| - |d| < |d| - r' < |d| - 0 \Longrightarrow 0 < r < |d|.$$

Unicidad: Supongamos que tenemos dos pares de cocientes y restos, k y r, y k' y r'. Vamos a probar que entonces $k = k'$ y $r = r'$.
Sin perdida de generalidad, podemos suponer que $r \leq r'$, y luego:

$$a = k\,d + r = k'\,d + r' \text{ con } 0 \leq r \leq r' < |d|.$$

Así, $(k - k')\,d = r' - r \Rightarrow d \,|\, r' - r \Rightarrow |d| \,|\, r' - r$. Como $r' - r \geq 0$ por ser $r' \geq r$, si $r' - r \neq 0$, se tiene, por lo que vimos en divisibilidad, que $|d| \leq r' - r$. Pero es facil verificar que, dado que $r' < |d|$, $r' - r < |d| - r < |d|$ (ya que $r \geq 0$). Luego no puede ser $r' - r \neq 0$, es decir tiene que ser $r' = r$.
Se concluye que $(k - k')\,d = 0$ y como $d \neq 0$, $k - k' = 0$, es decir $k = k'$ también.

■

La observación siguiente relaciona el algoritmo de división con la divisibilidad (y la congruencia). Es inmediata pero esencial:

Observación 4.3 *Sean $a, d \in \mathbb{Z}$, $c \neq 0$. Entonces*

$$r_d(a) = 0 \iff d \,|\, a \iff a \equiv 0 \pmod{d}.$$

Vamos a generalizar esa observación y clasificar los números según su resto:

Proposición 4.4 (Congruencia y restos)
Sean $a, b, d, r, r_1, r_2 \in \mathbb{Z}$, $d \neq 0$. Entonces

1. $a \equiv r_d(a) \pmod{d}$.
2. $a \equiv r \pmod{d}$ *con* $0 \leq r < |d| \implies r = r_d(a)$.
3. $r_1 \equiv r_2 \pmod{d}$ *con* $0 \leq r_1, r_2 < |d| \implies r_1 = r_2$.
4. $a \equiv b \pmod{d} \iff r_d(a) = r_d(b)$.

Prueba.–

1. $a = k \cdot d + r_d(a) \Rightarrow d \,|\, a - r_d(a) \Rightarrow a \equiv r_d(a) \pmod{d}$.
   (Se usa aquí que existen el cociente y el resto.)
2. $a \equiv r \pmod{d} \Rightarrow d \,|\, a - r \Rightarrow a - r = k \cdot d \Rightarrow a = k \cdot d + r$ para algún $k \in \mathbb{Z}$.
   Pero la condición $0 \leq r < |d|$ implica entonces que $r = r_d(a)$.
3. $r_1 = 0 \cdot d + r_1$ con $0 \leq r_1 < |d| \Rightarrow r_1 = r_d(r_1)$.
   Pero por otro lado, por (2), $r_1 \equiv r_2 \pmod{d}$ con $0 \leq r_2 < |d| \Rightarrow r_2 = r_d(r_1)$. Se concluye que $r_1 = r_2$ por la unicidad del resto.
4. $(\Rightarrow)$: $a \equiv b \pmod{d}$ por hipotesis, y por (1), $a \equiv r_d(a) \pmod{d}$, $b \equiv r_d(b) \pmod{d}$. Por transitividad (y simetría), se concluye que $r_d(a) \equiv r_d(b) \pmod{d}$. Ahora por (3), $r_d(a) = r_d(b)$.
   $(\Leftarrow)$: $r_d(a) = r_d(b) \Rightarrow r_d(a) \equiv r_d(b) \pmod{d}$, y juntando por transitividad (y simetría) con $a \equiv r_d(a) \pmod{d}$, $b \equiv r_d(b) \pmod{d}$, resulta $a \equiv b \pmod{d}$.

■

Al dividir cualquier número entero por $d \in \mathbb{Z}, d \neq 0$, hay $|d|$ posibles restos: $0, 1, \ldots, |d|-1$. La conclusión es entonces que la congruencia módulo d clasifica los números enteros según su resto módulo d: dos números a y b están en la misma clase, o sea son "identificados", ssi tienen el mismo resto módulo d, y hay $|d|$ clases distintas, la clase del 0, o sea compuesta por los números divisibles por d, la clase del 1, o sea compuesta por los números que tienen resto 1, etc... Además, la proposición anterior también nos dice que para calcular el resto de un número módulo d alcanza con poner a la derecha de la congruencia algo que cumple la condición de resto, es decir algún r con $0 \leq r < |d|$.

Aplicaciones

- Calcular el resto de dividir por 5 a $166^{1328} \cdot 4878 + 199999$:

  Cada número es congruente a su resto, luego $166 \equiv 1 \pmod 5 \Rightarrow 166^{1328} \equiv 1^{1328} \pmod 5$ y $4878 \equiv 3 \pmod 5$, $199999 \equiv 4 \pmod 5$ implican

  $$\begin{aligned} 166^{1328} \cdot 4878 + 199999 &\equiv 1 \cdot 3 + 4 \pmod 5 \\ &\equiv 7 \pmod 5 \\ &\equiv 2 \pmod 5 \end{aligned}$$

  Dado que 2 cumple la condición de ser resto módulo 5, se concluye que 2 es el resto.

- Calcular el resto de dividir por 35 a $34^{17771} - 6^{1001}$:

  A veces en lugar de reemplazar los números por su resto conviene reemplazarlos por -1 u observar algún comportamiento útil. Aquí por ejemplo:

  $34 \equiv -1 \pmod{35} \Rightarrow 34^{17771} \equiv (-1)^{17771} \pmod{35}$, es decir, $34^{17771} \equiv -1 \pmod{35}$, y $6^2 = 36 \equiv 1 \pmod{35} \Rightarrow 6^{1001} = 6^{2 \cdot 500 + 1} = (6^2)^{500} \cdot 6 \equiv 1^{500} \cdot 6 \pmod{35}$. Luego

  $$\begin{aligned} 34^{17771} - 6^{1001} &\equiv -1 - 6 \pmod{35} \\ &\equiv -7 \pmod{35} \\ &\equiv 28 \pmod{35} \end{aligned}$$

  Por lo tanto el resto es 28.

5 Desarrollos en base d

El sistema de numeración que utilizamos desde que —según parece— Fibonacci (1170-1250) lo introdujo en el mundo occidental, es el sistema decimal indo-arábigo, que es un sistema que funciona por posiciones de los dígitos (observar aquí otra aplicación del hecho que exista el número 0, para significar que hay una posición vacía). Así, cuando escribimos el número seis mil setescientos ochenta y nueve, 6789, nos referimos al número compuesto por 6 unidades de 1000 más 7 unidades de 100 más 8 unidades de 10 más 9 unidades (de 1), o sea al número

$$6789 = 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 9.$$

El número natural $a = r_n r_{n-1} \ldots r_1 r_0$ (donde $0 \leq r_i < 10$ para $0 \leq i \leq n$ y $r_n \neq 0$) simboliza entonces el número $r_n \cdot 10^n + \cdots + r_1 \cdot 10 + r_0$.

Consecuencia (Reglas de divisibilidad)

Con esto se explican muy facilmente las famosas reglas de divisibilidad. Por ejemplo todos saben que para ver si un número es divisible por 3, uno le suma los dígitos y se fija si esa suma es divisible por 3, o sea, si $a = r_n r_{n-1} \dots r_1 r_0$,

$$3 \mid a \iff 3 \mid r_n + r_{n-1} + \cdots + r_1 + r_0.$$

La explicación es muy sencilla: Dado que $10 \equiv 1 \pmod 3$, que implica que $10^i \equiv 1 \pmod 3$ para todo $i \in \mathbb{N}$, se tiene que

$$a = r_n \cdot 10^n + \cdots + r_1 \cdot 10 + r_0 \equiv r_n + \cdots + r_1 + r_0 \pmod 3.$$

Luego 3 divide el término de la izquierda si y solo si 3 divide el término de la derecha. Es más, para conocer el resto de un número módulo 3, alcanza con sumarle los dígitos y tomarle el resto módulo 3 a esa suma.
Como ejercicio queda verificar y/o enunciar las otras reglas de divisibilidad.

Retomando, el número natural $a = r_n \dots r_0$ corresponde al desarrollo decimal

$$a = r_n \cdot 10^n + \cdots + r_0 \cdot 10^0.$$

Las exigencias de un buen sistema de numeración es que cuando vemos un número queremos poder saber en forma bien determinada de qué número estamos hablando, además de requerir que todo número tenga un único desarrollo que le corresponda. Esto se logra con la condición impuesta sobre los dígitos ($0 \le r_i < 10, 0 \le i \le n$): para que un número esté bien determinado, los dígitos tienen que estar entre 0 y 9, ya que el lugar de un dígito en el número determina a qué potencia de 10 corresponde (si uno admitiera por ejemplo el 11 como un dígito, el número 111: ¿correspondería al número $111 = \cdot 10^2 + 1 \cdot 10 + 1$ o al $21 = 1 \cdot 10 + 11 \cdot 1$?, y si uno admitiera el 11 pero con otro símbolo para evitar confusiones como la de arriba, por ejemplo B, el número 11 tendría dos escrituras distintas, una como 11 y la otra como B).

Matemáticamente no hay nada que haga prevalecer el número 10 como elección para la base de numeración: uno puede fijar cualquier número natural $d \ge 2$ como base del sistema de numeración. Para la buena determinación y la unicidad, lo que se tiene que pedir ahora es que los dígitos estén entre 0 y $d-1$. Esto se justifica también en la vida real, por ejemplo las computadoras trabajan naturalmente en base 2, o sea con los "dígitos" 0 y 1, ya que esto se corresponde con el paso o no de la electricidad.

Teorema 5.1 (Desarrollo en base d)

Sea $d \in \mathbb{N}$, $d \ge 2$, fijado. Todo número $a \in \mathbb{N}_0$ admite *un desarrollo en base d de la forma*

$$a = r_n \cdot d^n + r_{n-1} \cdot d^{n-1} + \cdots + r_1 \cdot d + r_0,$$

con $0 \le r_i < d$ para $0 \le i \le n$ y $r_n \ne 0$ si $a \ne 0$.
Además dicho desarrollo, con las exigencias impuestas para los dígitos, es único.
Se nota $a = (r_n \dots r_0)_d$.

Observación 5.2 *En el caso de desarrollo en base 10, $(a)_{10}$ se nota simplemente a, en la forma que estamos acostumbrados.*

Ejemplo

$$6789 = (6789)_{10} = (1101010000101)_2 = (204124)_5 = (1A85)_{16}$$

(En base 16 los "dígitos" $10, 11, 12, 13, 14$ y 15 se reemplazan respectivamente por A, B, C, D, E y F para evitar confusiones.)

Prueba del Teorema 5.1.–

Existencia del desarrollo en base d:

La idea intuitiva es ir dividiendo iteradamente el número a y los sucesivos cocientes por d. Para formalizar la prueba se puede hacer por induccción en $a \in \mathbb{N}_0$:

- Para $a = 0$, se tiene $0 = (0)_d$, es decir estamos en el único caso en que todos los dígitos son cero.
- $a \geq 1$:

  La hipótesis inductiva es que todo número natural o cero menor que a admite un desarrollo en base d. Queremos probar que entonces a admite también un desarrollo en base d.

  Usando el algoritmo de división , dividimos a por d, y obtenemos un cociente k que verifica $0 \leq k < a$ y un resto r_0 que verifica $0 \leq r_0 < d$: Por hipótesis inductiva, al ser $0 \leq k < a$, k admite un desarrollo en base d que notamos por conveniencia en la forma:

  $$k = r_n \cdot d^{n-1} + \cdots + r_2 \cdot d + r_1 \quad \text{con } 0 \leq r_n, \ldots, r_1 < d.$$

  Entonces

  $$\begin{aligned} a &= k \cdot d + r_0 \\ &= (r_n \cdot d^{n-1} + \cdots + r_2 \cdot d + r_1) \cdot d + r_1 \\ &= r_n \cdot d^n + \cdots + r_1 \cdot d + r_0 \end{aligned}$$

  donde $0 \leq r_i < c$ para $0 \leq i \leq n$ como se quiere.

Así, todo $a \in \mathbb{N}$ admite un desarrollo en base d.

Unicidad: Es una consecuencia de la unicidad del resto y del cociente en el algoritmo de división: r_0 es el resto de la división de a por d y por lo tanto es único, r_1 es el resto de la división de $(a - r_0)/d$ por d y es único también, etc... Como antes, podemos formalizar esto por inducción en $a \in \mathbb{N}_0$.

- Para $a = 0$, el único desarrollo es claramente 0 para todos los dígitos.
- Para $a \geq 1$, supongamos que

  $$a = r_n \cdot d^n + \cdots + r_1 \cdot d + r_0 = s_m \cdot d + \cdots + s_1 \cdot d + s_0$$

  con $0 \leq r_i, s_j < d$ para $0 \leq i \leq n, 0 \leq j \leq m$ y $r_n \neq 0$, $s_m \neq 0$. Ahora bien, está claro que $r_d(a) = r_0 = s_0$, y además, el cociente de dividir a por d (que es único) es

  $$k = r_n \cdot d^{n-1} + \cdots + r_1 = s_m \cdot d^{m-1} + \cdots + s_1.$$

  Por hipótesis inductiva, el desarrollo en base d del cociente k es único, luego $n = m$ y $r_i = s_i$, $1 \leq i \leq n$.

Así concluimos que para todo $a \in \mathbb{N}_0$, el desarrollo en base d de a es único.

■

6 Máximo Común Divisor

Definición 6.1 (Máximo Común Divisor)
Sean $a, b \in \mathbb{Z}$ *, no ambos nulos. El* máximo común divisor *entre* a *y* b *es el mayor de los divisores comunes de* a *y* b *.*
Claramente ese número existe*, ya que la lista de divisores comunes es no vacía (*1 *es un divisor común) y finita (por ser* a *o* b *no nulo), y es único (por ser el mayor). Además es* positivo *por la misma razón.*
El máximo común divisor entre a *y* b *se nota* $\text{mcd}(a, b)$ *o* $(a : b)$ *que es la notación que adoptamos aquí. Es entonces caracterizado por:*

$$(a : b) \,|\, a,\ (a : b) \,|\, b \quad \textit{y si}\ \ d \,|\, a \ \textit{y}\ d \,|\, b,\ \textit{entonces}\ \ d \leq (a : b).$$

Notaremos en lo que sigue con $DivCom(\{a, b\})$ el conjunto de los divisores comunes de a y b y con $DivCom_+(\{a, b\})$ el conjunto de los divisores comunes positivos, es decir:

$$\begin{aligned} DivCom(\{a, b\}) &:= \{\, d \in \mathbb{Z} : d \,|\, a \text{ y } d \,|\, b \,\} = Div(a) \cap Div(b) \\ DivCom_+(\{a, b\}) &:= \{\, d \in \mathbb{N} : d \,|\, a \text{ y } d \,|\, b \,\} = Div_+(a) \cap Div_+(b). \end{aligned}$$

Luego, el máximo común divisor es el elemento más grande de cualquiera de esos dos conjuntos.

Ejemplos

- $(12 : 18) = 6$, pues $Div_+(12) = \{1, 2, 3, 4, 6, 12\}$, $Div_+(18) = \{1, 2, 3, 6, 9, 18\}$
  $\Rightarrow DivCom_+(\{12, 18\}) = \{1, 2, 3, 6\}$.
- $(12 : -35) = 1$ ya que $Div_+(-35) = \{1, 5, 7, 35\}$ $\Rightarrow DivCom_+(\{12, -35\}) = \{1\}$.
- $(a : b) = (b : a)$.
- $(a : b) = (-a : b) = (a : -b) = (-a : -b) = (|a| : |b|)$.
- Para todo $a \in \mathbb{Z}$, se tiene $(a : 1) = 1$
- Para todo $a \in \mathbb{Z}$, $a \neq 0$, se tiene $(a : 0) = |a|$.
- $b \,|\, a \iff (a : b) = |b|$.

Más ejemplos

- Cálculo de los valores de $(n^2 + 1 : n - 1)$ para $n \in \mathbb{N}$:
  - $n = 1 \Rightarrow (2 : 0) = 2$, $n = 2 \Rightarrow (5 : 1) = 1$, $n = 3 \Rightarrow (10 : 2) = 2$, $n = 4 \Rightarrow (17 : 3) = 1$, $n = 5 \Rightarrow (26 : 4) = 2$, $n = 6 \Rightarrow (37 : 5) = 1$, ...
    Pareciera que da 2 o 1 según si n es impar o par. Vamos a demostrar esto:
  - Vamos a investigar los posibles divisores comunes de n^2+1 y $n-1$ para luego determinar los posibles máximos:

$$\left\{ \begin{array}{l} d \,|\, n^2 + 1 \\ d \,|\, n - 1 \end{array} \right. \implies \left\{ \begin{array}{l} d \,|\, n^2 + 1 \\ d \,|\, (n + 1)(n - 1) \end{array} \right. \implies \left\{ \begin{array}{l} d \,|\, n^2 + 1 \\ d \,|\, n^2 - 1 \end{array} \right. \implies d \,|\, 2.$$

    Así, $DivCom_+(\{n^2 + 1, n - 1\}) \subseteq \{1, 2\}$, y luego $(n^2 + 1 : n - 1) \in \{1, 2\}$.
    (Notemos que como dedujimos que $c \,|\, 2$ por implicaciones, tiene que pasar que $d|2$ pero no es obligatorio que todo divisor de 2 sea un divisor común, o sea puede pasar que $DivCom_+(\{n^2 + 1, n - 1\})$ esté estrictamente contenido en el conjunto $\{1, 2\}$, como es el caso aquí para n par.)

– Investigamos ahora por separado los casos n impar, n par:
Si n es impar, n^2+1 y $n-1$ son pares, luego 2 es un divisor común, es decir $2 \in DivCom_+(\{n^2+1, n-1\})$. Por lo tanto, en este caso $(n^2+1 : n-1) = 2$.
Si n es par, n^2+1 y $n-1$ son impares, luego no son divisibles por 2:
$2 \notin DivCom_+(\{n^2+1, n-1\})$ y en este caso, $(n^2+1 : n-1) = 1$.

- Cálculo de los valores de $(n(n-1) : 2(n+1))$ para $n \in \mathbb{N}$:
  - $n = 1 \Rightarrow (0:4) = 4, n = 2 \Rightarrow (2:6) = 2, n = 3 \Rightarrow (6:8) = 2, n = 4 \Rightarrow (12:10) = 2, n = 5 \Rightarrow (20:12) = 4, n = 6 \Rightarrow (30:14) = 2, \ldots$
  Pareciera dar 4 o 2 según si $n \equiv 1 \pmod 4$ o no. Probemoslo:
  - Investiguemos los posibles divisores comunes de $n(n-1)$ y $2(n+1)$ para luego determinar los posibles máximos:

$$\left\{ \begin{array}{l} cd \,|\, n(n-1) \\ d \,|\, 2(n+1) \end{array} \right. \implies \left\{ \begin{array}{l} d \,|\, 2n(n-1) \\ d \,|\, 2n(n+1) \end{array} \right. \implies \left\{ \begin{array}{l} d \,|\, 2n^2-2n \\ d \,|\, 2n^2+2n \end{array} \right. \implies d \,|\, 4n.$$

  Pero volviendo entonces al principio

$$\left\{ \begin{array}{l} d \,|\, 4n \\ d \,|\, 2(n+1) \end{array} \right. \implies \left\{ \begin{array}{l} d \,|\, 4n \\ d \,|\, 2 \cdot 2(n+1) \end{array} \right. \implies \left\{ \begin{array}{l} d \,|\, 4n \\ d \,|\, 4n+4 \end{array} \right. \implies d \,|\, 4.$$

  Así, $DivCom_+(\{n^2-n, 2(n+1)\}) \subseteq \{1,2,4\}$, y luego $(n^2-n : 2(n+1)) \in \{1,2,4\}$.
  - Investigamos ahora por separado los casos $n \equiv 1 \pmod 4$ y $n \not\equiv 1 \pmod 4$:
  Si $n \equiv 1 \pmod 4$:

$$\left\{ \begin{array}{ll} n(n-1) \equiv 1(1-1) & (\text{mod } 4) \\ 2(n+1) \equiv 2(1+1) & (\text{mod } 4) \end{array} \right. \implies \left\{ \begin{array}{ll} n(n-1) \equiv 0 & (\text{mod } 4) \\ 2(n+1) \equiv 0 & (\text{mod } 4) \end{array} \right. \implies \left\{ \begin{array}{l} 4 \,|\, n(n-1) \\ 4 \,|\, 2(n+1) \end{array} \right.$$

  Así, $4 \in DivCom_+(\{n(n-1), 2(n+1)\})$, luego, en este caso, $(n(n-1) : 2(n+1)) = 4$.
  Si $n \not\equiv 1 \pmod 4$, $n+1 \not\equiv 2 \pmod 4$ e investigando los casos, se observa que $2(n+1) \not\equiv 0 \pmod 4$, luego $4 \notin DivCom_+(\{n^2-n, 2(n+1)\})$. Pero por otro lado $n(n-1)$ y $2(n+1)$ siempre son pares, luego $2 \in DivCom_+(\{n(n-1), 2(n+1)\})$. Se concluye que en este caso $(n(n-1) : 2(n+1)) = 2$.

Observación 6.2 (Importante!)
Sean $a, b \in \mathbb{Z}$ no ambos nulos, y sea $j \in \mathbb{Z}$, entonces:

$$DivCom(\{a,b\}) = DivCom(\{b, a - j\,b\}) \quad y \quad DivCom_+(\{a,b\}) = DivCom_+(\{b, a - j\,b\}).$$

En particular, para todo $j \in \mathbb{Z}$, $(a:b) = (b : a - j\,b)$.
Aplicando esto a $r_b(a) = a - k\,b$, se obtiene $\boxed{(a:b) = (b : r_b(a))}$

Prueba.– Alcanza con probar la primer igualdad, la de los conjuntos $DivCom$:
Pero utilizando que $d \,|\, a, d \,|\, b \Rightarrow d \,|\, a - j\,b$ y $d \,|\, b, d \,|\, a - j\,b \Rightarrow d \,|\, a$, se tiene

$$d \in DivCom(\{a,b\}) \iff d \,|\, a \text{ y } d \,|\, b \iff d \,|\, a - j\,b \text{ y } d \,|\, b \iff d \,|\, DivCom(\{b, a - j\,b\}).$$

■

La observación anterior provee directamente de un algoritmo para calcular el máximo común divisor entre dos números, que no depende de calcular sus divisores. Este algoritmo fue introducido o recopilado por Euclides (~ 325–~ 265 AC) en "Los Elementos", y se lo llama directamente *Algoritmo de Euclides*. Es el algoritmo más eficiente posible para calcular el máximo común divisor (al menos para números grandes), mucho más eficiente que encontrar los divisores comunes, por ejemplo mediante factorización. Lo vamos a ejemplificar primero en un caso particular.

Ejemplo Cálculo de $(120 : -84)$:

Como $(120 : -84) = (120 : 84)$, calculamos este último para simplificar las divisiones (esto no es esencial para el algoritmo). Se tiene

$$\begin{array}{rcl@{\quad}c@{\quad}rcl} 120 &=& 1 \cdot 84 + 36 & \Longrightarrow & (120 : 84) &=& (84 : 36) \\ 84 &=& 2 \cdot 36 + 12 & \Longrightarrow & (84 : 36) &=& (36 : 12) \\ 36 &=& 3 \cdot 12 + 0 & \Longrightarrow & (36 : 12) &=& (12 : 0). \end{array}$$

Pero $(12 : 0) = 12$, luego $(120 : -84) = 12$ ya que

$$(120 : -84) = (120 : 84) = (84 : 36) = (36 : 12) = (12 : 0) = 12.$$

Algoritmo de Euclides

Entrada: $a, b \in \mathbb{Z}$, no ambos nulos.
Salida: $(a : b)$.

Como $(a : b) = (|a| : |b|)$, sin pérdida de generalidad podemos suponer $a, b \geq 0$, más aún $a \geq b > 0$ ya que $(a : b) = (b : a)$ y si $b = 0$, entonces $(a : b) = a$. Se divide a por b y luego los sucesivos divisores por los sucesivos restos, hasta llegar a un resto nulo:

$$\begin{array}{lcll@{\quad}ccccc} a &=& k_0 \cdot b + r_1 & \text{con} & 0 & \leq & r_1 & < & b \\ b &=& k_1 \cdot r_1 + r_2 & \text{con} & 0 & \leq & r_2 & < & r_1 \\ r_1 &=& k_2 \cdot r_2 + r_3 & \text{con} & 0 & \leq & r_3 & < & r_2 \\ \vdots & & & & & & & & \\ r_{\ell-2} &=& k_{\ell-1} \cdot r_{\ell-1} + r_\ell & \text{con} & 0 & \leq & r_\ell & < & r_{\ell-1} \\ r_{\ell-1} &=& k_\ell \cdot r_\ell + r_{\ell+1} & \text{con} & & r_{\ell+1} & = & 0. & \end{array}$$

Entonces $(a : b) = r_\ell$, el último resto no nulo.

Justificación.–

Siempre se llega en un número finito de pasos (acotado a simple vista por b) a un resto nulo ya que

$$b > r_1 > r_2 > r_3 > \cdots \geq 0,$$

y esta sucesión estrictamente decreciente de restos ≥ 0 no puede ser infinita.
Cuando en el procedimiento se llega a un resto nulo, $r_{\ell+1} = 0$, se tiene

$$(a : b) = (b : r_1) = (r_1 : r_2) = \cdots = (r_{\ell-1} : r_\ell) = (r_\ell : 0) = r_\ell.$$

■

Aplicación $(a^m - 1 : a^n - 1) = a^{(m:n)} - 1$ para $a \in \mathbb{N}$, $a \neq 1$, y $m, n \in \mathbb{N}$:

Vamos a probar que en efecto este es el último resto no nulo al realizar el algoritmo de Euclides para encontrar el mcd.

Recordemos que vimos en los primeros ejemplos de divisibilidad que: $n \,|\, m \;\Rightarrow\; a^n - 1 \,|\, a^m - 1$. En el caso general, $m = k\,n + r$ con $0 \le r < n$, y entonces

$$a^m - 1 = a^{k\,n+r} - 1 = a^r(a^{k\,n} - 1) + (a^r - 1) = k'(a^n - 1) + a^r - 1,$$

dado que $n \,|\, k\,n \;\Rightarrow a^n - 1 \,|\, a^{k\,n} - 1$. Además, como $0 \le a^r - 1 < a^n - 1$ por ser $0 \le r < n$ y $a \in \mathbb{N}$, $a \neq 0$, se tiene que $a^r - 1$ es el resto de dividir a $a^m - 1$ por $a^n - 1$. Por lo tanto, aplicando la Observación 6.2, se obtiene

$$(a^m - 1 : a^n - 1) = (a^n - 1 : a^{r_n(m)} - 1).$$

La conclusión se obtiene de la misma manera que se probó el algoritmo de Euclides.

Una consecuencia inmediata del algoritmo de Euclides es el importantísimo resultado siguiente: El máximo común divisor entre dos números se puede escribir como combinación entera de esos números, y de hecho es el número natural más chico con esa propiedad.

Teorema 6.3 (mcd y combinación entera)

Sean $a, b \in \mathbb{Z}$, no ambos nulos. Entonces: $\boxed{\exists\; s, t \in \mathbb{Z} \,:\, (a : b) = sa + tb}$

Antes de demostrar este teorema, miremos cómo se pueden obtener en forma sistemática coeficientes enteros s y t, en el caso particular del ejemplo que calculamos antes:

Ejemplo (continuación) $(120 : -84) = 12$:

Mirando las dos divisiones que permitieron obtener a 12 como último resto no nulo, pero al revés, se tiene

$$\begin{array}{rcl@{\quad\Longrightarrow\quad}rcl} 84 &=& 2\cdot 36 + 12 & 12 &=& 84 - 2\cdot 36 \\ 120 &=& 1\cdot 84 + 36 & 12 &=& 84 - 2\cdot(120 - 1\cdot 84) \\ & & & & =& 3\cdot 84 - 2\cdot 120. \end{array}$$

Por lo tanto, $12 = -2\cdot 120 + 3\cdot 84 = -2\cdot 120 + (-3)\cdot(-84)$. Aquí, $s = -2$ y $t = -3$ sirven.

Prueba del Teorema 6.3.–

Se miran al revés las sucesivas divisiones hasta la que da al máximo común divisor como último resto no nulo, y, tratando los sucesivos divisores y restos como si fueran variables y reagrupando, se obtiene una escritura entera de $(a : b)$ como combinación entera de a y b. (Luego, si habíamos —para simplificar las divisiones— cambiado los signos de los a y b originales, se modifican los signos para escribir $(a : b)$ como combinación entera de los a y b originales.)

$$\begin{array}{rcl@{\quad\Longrightarrow\quad}rcl} r_{\ell-2} &=& k_{\ell-1}r_{\ell-1} + r_\ell & r_\ell &=& r_{\ell-2} - k_{\ell-1}r_{\ell-1} \\ r_{\ell-3} &=& k_{\ell-2}r_{\ell-2} + r_{\ell-1} & r_\ell &=& r_{\ell-2} - k_{\ell-1}(r_{\ell-3} - k_{\ell-2}r_{\ell-2}) \\ & & & & =& (1 + k_{\ell-1}k_{\ell-2})r_{\ell-2} - k_{\ell-1}r_{\ell-3} \\ \vdots & & & & & \\ r_1 &=& k_2 r_2 + r_3 & r_\ell &=& *r_1 + *'r_2 \\ b &=& k_1 r_1 + r_2 & r_\ell &=& *r_1 + *'(b - k_1 r_1) \\ & & & & =& (* - k_1 *')r_1 + *'b \\ a &=& k_0 b + r_1 & r_\ell &=& (* - k_1 *')(a - k_0 b) + *'b \\ & & & & =& s\,a + t\,b. \end{array}$$

Así, $(a : b) = r_\ell = s\,a + t\,b$ donde claramente $s, t \in \mathbb{Z}$ ya que son obtenidos sumando y multiplicando enteros.

■

Observación 6.4 *Sean $a, b \in \mathbb{Z}$, no ambos nulos.*
Si $c \in \mathbb{Z}$ es tal que $c = s'a + t'b$ con $s', t' \in \mathbb{Z}$, entonces $(a : b) \,|\, c$. En particular si $c \in \mathbb{N}$, $(a : b) \leq c$.

Prueba.– Dado que $(a : b) \,|\, a$ y $(a : b) \,|\, b$, se tiene $(a : b) \,|\, s'a + t'b$, luego $(a : b) \,|\, c$.

■

La observación anterior nos dice que el máximo común divisor $(a : b)$ es el número *natural* más chico que se puede escribir como combinación entera de a y b. Todas las demás combinaciones enteras de a y b son divisibles por él.

El Teorema 6.3 tiene otra consecuencia importantísima que no es obvia a primer vista: el máximo común divisor no solo es el más grande de los divisores comunes sino que también es divisible por ellos.

Proposición 6.5 (mcd y divisibilidad)

Sean $a, b \in \mathbb{Z}$, no ambos nulos y sea $d \in \mathbb{Z}$, $d \neq 0$. Entonces: $\boxed{d \,|\, a \;\; y \;\; d \,|\, b \iff d \,|\, (a : b)}$

Prueba.–

$(\Rightarrow)$: Esta es la implicación interesante y no trivial:
Recordemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s\,a + t\,b$. Ahora, dado que por hipotesis, $d \,|\, a$ y $d \,|\, b$, se tiene que $d \,|\, sa + tb = (a : b)$.

$(\Leftarrow)$: Esta implicación es obvia por la transitividad de la divisibilidad.

■

Otra consecuencia útil del Teorema 6.3, de la Observación 6.4 y de la Proposición 6.5 es la siguiente:

Consecuencia

Sean $a, b \in \mathbb{Z}$, no ambos nulos, y sea $c \in \mathbb{Z}$, $c \neq 0$. Entonces $\boxed{(c\,a : c\,b) = |c| \cdot (a : b)}$

Prueba.–

Sin pérdida de generalidad, podemos suponer $c > 0$.
Por un lado, aplicando la Proposición 6.5, se tiene

$$(a : b) \,|\, a \text{ y } (a : b) \,|\, b \implies c\,(a : b) \,|\, c\,a \text{ y } c\,(a : b) \,|\, c\,b \implies c\,(a : b) \,|\, (c\,a : c\,b).$$

Por otro lado, por el Teorema 6.3 y la Observación 6.4, se tiene

$$(a : b) = s\,a + t\,b \implies c\,(a : b) = s\,(c\,a) + t\,(c\,b) \implies (c\,a : c\,b) \,|\, c\,(a : b).$$

Como ambos términos son positivos, se concluye que son iguales.

■

En realidad, los resultados que se obtuvieron permiten tres caracterizaciones equivalentes del máximo común divisor, que se enuncian a continuación. La primera corresponde a la Definición 6.1 del mcd y es la caracterización intuitiva, la segunda corresponde principalmente al Teorema 6.3 y la tercera a la Proposición 6.5, y son las operativas. Se deja la prueba a cargo del lector, mencionando simplemente que alcanza con probar (*1* $\Rightarrow$ *2*), (*2* $\Rightarrow$ *3*) y (*3* $\Rightarrow$ *1*), ya que por ejemplo para probar que (*2* $\Rightarrow$ *1*) se usa (*2* $\Rightarrow$ *3* $\Rightarrow$ *1*).

Teorema 6.6 *Sean $a, b \in \mathbb{Z}$, no ambos nulos, y sea $c \in \mathbb{Z}$, $c \neq 0$. Son equivalentes:*

1. *$c = (a : b)$.*
2. *$c \in \mathbb{N}$, $c \mid a$, $c \mid b$ y existen $s, t \in \mathbb{Z}$ tales que $c = sa + tb$.*
3. *$c \in \mathbb{N}$, $c \mid a$, $c \mid b$ y si $d \mid a$ y $d \mid b$, entonces $d \mid c$.*

■

Una atención especial merecen los pares de números cuyo máximo común divisor es igual a 1. Juegan un papel central en lo que sigue.

Definición 6.7 (Números coprimos)
Sean $a, b \in \mathbb{Z}$, no ambos nulos. Se dice que $a, b \in \mathbb{Z}$, no ambos nulos, son coprimos si y solo si $(a : b) = 1$, es decir si y solo si los únicos divisores comunes de a y b son ± 1. En ese caso, seguimos la notación introducida por el matemático e informático actual D. Knuth, y escribimos $a \perp b$. O sea:

$$a \perp b \underset{def}{\iff} (a : b) = 1$$

Ejemplos

- $103 \perp 98$ pero $12202 \not\perp 43554$.
- $a \perp 0 \iff a = \pm 1$
- Para todo $b \in \mathbb{Z}$, $\pm 1 \perp b$.
- Para $a, b \in \mathbb{Z}$ coprimos, los distintos valores que puede tomar $(2a + b : 3a - 2b)$ son exactamente el 1 y el 7:
  - Investiguemos algunos valores de $(2a + b : 3a - 2b)$ con $a \perp b$:
    $a = 1, b = 0 : (2 : 3) = 1$; $a = 1, b = 1 : (3 : 1) = 1$; $a = 3, b = 1 : (7 : 7) = 7$.
    Luego, efectivamente los dos valores, 1 y 7, se obtienen. Hay que probar que son los únicos dos posibles.
  - Como en los primeros ejemplos generales de cálculo de mcd, investigamos los posibles divisores comunes. Sea d un divisor común entre $2a + b$ y $3a - 2b$,

$$\left\{ \begin{array}{l} d \mid 2a + b \\ d \mid 3a - 2b \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 3(2a + b) \\ d \mid 2(3a - 2b) \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 6a + 3b \\ d \mid 6a - 4b \end{array} \right. \implies d \mid 7b.$$

    De la misma manera:

$$\left\{ \begin{array}{l} d \mid 2a + b \\ d \mid 3a - 2b \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 2(2a + b) \\ d \mid 3a - 2b \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 4a + 2b \\ d \mid 3a - 2b \end{array} \right. \implies d \mid 7a.$$

    Luego $d \mid 7a$ y $d \mid 7b$. Aplicando la Proposición 6.5, la Consecuencia vista arriba y el hecho que $a \perp b$, se tiene

$$d \mid (7a : 7b) = 7(a : b) = 7 \implies d \mid 7.$$

    Se concluye que el máximo común divisor, que es el mayor de estos d posibles, es o bien 1 o 7 como se quería probar (además efectivamente ya mostramos que había casos en que es 1 y casos en que es 7).

Observación 6.8 (Fundamental!)

$$\boxed{a \perp b \iff \exists\, s,t \in \mathbb{Z} \;:\; 1 = s\,a + t\,b}$$

Prueba.–
$(\Rightarrow)$ es el hecho que el mcd es combinación entera de los números.
$(\Leftarrow)$ es por la Observación 6.4: $(a:b)\,|\,1 \;\Rightarrow\; (a:b) = 1$.

■

La proposición que sigue trata de propiedades esenciales de divisibilidad cuando hay números coprimos de por medio. No se podrían demostrar estas propiedades si no se tuviera la Observación 6.8.

Proposición 6.9 *Sean* $a,b,c,d \in \mathbb{Z}$, $c \neq 0$, $d \neq 0$. *Entonces*

1. $c\,|\,a,\; d\,|\,a$ *con* $c \perp d \implies c\,d\,|\,a$.
2. $d\,|\,a\,b$ *con* $d \perp a \implies d\,|\,b$.

Observemos que estas afirmaciones no son ciertas si no se piden las propiedades de coprimalidad. Por ejemplo $6\,|\,12$ y $4\,|\,12$ pero $24 \nmid 12$, y $6\,|\,2\cdot 3 \not\Rightarrow 6\,|\,2$ o $6\,|\,3$. Por otro lado, las recíprocas siempre valen: $c\,d\,|\,a \Rightarrow c\,|\,a$ y $d\,|\,a$, y $d\,|\,b \Rightarrow d\,|\,a\,b$. Luego podemos resumir la Proposición en:

$$\boxed{\text{Si } c \perp d\text{, entonces: } c\,|\,a,\, d\,|\,a \iff c\,d\,|\,a \quad , \quad \text{y si } d \perp a\text{, entonces: } d\,|\,a\,b \iff d\,|\,b}$$

Prueba de la Proposición 6.9.–

1. $c \perp d \;\Rightarrow\; 1 = s\,c + t\,d \;\Rightarrow\; a = s\,(c\,a) + t\,(d\,a)$, pero $d\,|\,a \;\Rightarrow\; c\,d\,|\,c\,a$ y $c\,|\,a \;\Rightarrow\; c\,d\,|\,d\,a$, luego $c\,d\,|\,s\,(c\,a) + t\,(d\,a) = a$.
2. $d \perp a \;\Rightarrow\; 1 = s\,d + t\,a$, luego $b = (s\,b)\,d + t\,(a\,b)$, pero $d\,|\,a\,b$, y $d\,|\,d$. Por lo tanto, $d\,|\,(s\,b)\,d + t\,(a\,b) = b$.

■

Ejemplo Cálculo de los $a,b \in \mathbb{Z}$ coprimos tales que $\dfrac{2}{a} + \dfrac{a}{b}$ es entero.

$$\frac{2}{a} + \frac{a}{b} = \frac{2b + a^2}{ab} \in \mathbb{Z} \iff ab\,|\,2b + a^2.$$

Pero al ser $a \perp b$, $ab\,|\,2b + a^2 \Leftrightarrow a\,|\,2b + a^2$ y $b\,|\,2b + a^2$.
Pero $a\,|\,2b + a^2$ y $a\,|\,a^2 \;\Rightarrow\; a\,|\,2b$, y $a \perp b \;\Rightarrow\; a\,|\,2 \;\Rightarrow\; a \in \{\pm 1, \pm 2\}$.
De la misma forma, $b\,|\,2b + a^2$ y $b\,|\,2b \;\Rightarrow\; b\,|\,a^2 = a \cdot a$, pero $b \perp a \;\Rightarrow\; b\,|\,a$, y nuevamente $b \perp a \;\Rightarrow\; b\,|\,1$, o sea $b \in \{\pm 1\}$.
Finalmente se verifica que los 8 pares $a = \pm 1, b = \pm 1$ y $a = \pm 2, b = \pm 1$ sirven.

Otra consecuencia muy util de la Proposición 6.8, ya que se trata siempre de reducirse a pares coprimos para poder aplicar proposiciones como la anterior, es la siguiente:

Proposición 6.10 ("Coprimizando")

Sean $a,b \in \mathbb{Z}$, *no ambos nulos. Entonces* $\dfrac{a}{(a:b)} \perp \dfrac{b}{(a:b)}$.

Por lo tanto: $\boxed{a = (a:b)\,a' \;\; y \;\; b = (a:b)\,b' \;\; con \;\; a', b' \in \mathbb{Z} \;\; coprimos}$

Prueba.–

Se sabe que $(a:b) = s\,a + t\,b$. Luego, dividiendo por $(a:b)$, se obtiene $1 = s\dfrac{a}{(a:b)} + t\dfrac{b}{(a:b)}$. ■

Otras consecuencias son las siguientes:

Consecuencias Sean $a, b, c \in \mathbb{Z}$, no nulos.

1. $\boxed{a \perp b \text{ y } a \perp c \iff a \perp b\,c}$
2. $a \perp b \iff a^m \perp b^n$, para todo $m, n \in \mathbb{N}_0$.
3. $(a^n : b^n) = (a:b)^n$. (Ojo! el mismo exponente para a y b. Si no, no es cierto: dar un ejemplo.)

Prueba.–

1. $(\Rightarrow)$ $1 = s\,a + t\,b$ y $1 = s'a + t'c \implies$

   $1 = (s\,a+t\,b)(s'a+t'c) = s\,s'a^2+s\,t'a\,c+t\,s'a\,b+t\,t'b\,c = (s\,s'a+s\,t'c+t\,s'b)\,a+t\,t'b\,c = s''a+t''b\,c,$

   con $s'' := s\,s'a + s\,t'c + t\,s'b$ y $t'' := t\,t'$ enteros.

   $(\Leftarrow)$ $1 = s\,a + t\,b\,c \Longrightarrow 1 = s\,a + (t\,c)\,b$ y $1 = s\,a + (t\,b)\,c$, es decir $a \perp b$ y $a \perp c$.
2. Es una consecuencia directa de (1.). ¿ Por qué ?
3. Sea $c := (a:b)$. Por la Proposición 6.10, $a = c\,a'$ y $b = c\,b'$ con $a' \perp b'$. Luego $(a^n : b^n) = (c^n a'^n : c^n b'^n) = c^n(a'^n : b'^n) = c^n$, por el inciso anterior.

■

Ejemplos

- Para todo $n \in \mathbb{N}$, $(2^n + 3^n : 2^n - 2\cdot 3^n) = 1$:

  Como siempre, sea d un posible divisor común:

  $$\left\{\begin{array}{l} d \,|\, 2^n + 3^n \\ d \,|\, 2^n - 2\cdot 3^n \end{array}\right. \implies d \,|\, 3^n + 2\cdot 3^n \implies d \,|\, 3\cdot 3^n.$$

  De la misma manera:

  $$\left\{\begin{array}{l} d \,|\, 2^n + 3^n \\ d \,|\, 2^n - 2\cdot 3^n \end{array}\right. \implies \left\{\begin{array}{l} d \,|\, 2\cdot 2^n + 2\cdot 3^n \\ d \,|\, 2^n - 2\cdot 3^n \end{array}\right. \implies d \,|\, 2\cdot 2^n + 2^n \implies d \,|\, 3\cdot 2^n.$$

  Pero

  $$d \,|\, 3\cdot 3^n \text{ y } d \,|\, 3\,2^n \implies d \,|\, (3\cdot 3^n : 3\cdot 2^n) = 3\,(3^n : 2^n) = 3\cdot 1 = 3.$$

  Por lo tanto, $(2^n + 3^n : 2^n - 2\cdot 3^n) = 1$ o 3. Falta descartar que sea 3. Pero claramente 3 no puede ser un divisor común ya que $3 \nmid 2^n + 3^n$ (pues si lo dividiera, se tendría, como $3 \,|\, 3^n$, que $3 \,|\, 2^n$, pero $2^n \equiv (-1)^n \pmod 3$, es decir $2^n \equiv \pm 1 \pmod 3$).

- Para todo $n \in \mathbb{N}$, $(n^{100} : (n+1)^{150}) = 1$:

  Eso es porque $n \perp n+1$ (pues $d \mid n, d \mid n+1 \Rightarrow d \mid 1$), y aplicando la Consecuencia 2 de la Proposición 6.10.

- Para todo $n \in \mathbb{N}$, se tiene:

$$(n^{100} : (n+2)^{150}) = \begin{cases} 1 & \text{si} \quad n \equiv 1 \pmod 2 \\ 2^{150} & \text{si} \quad n \equiv 0 \pmod 4 \\ 2^{100} & \text{si} \quad n \equiv 2 \pmod 4 \end{cases}$$

  Pues si $d \mid n$ y $d \mid n+2$, entonces $d \mid 2$. Luego $(n : n+2) = 1$ si n es impar y $(n : n+2) = 2$ si n es par. Así, si $n \equiv 1 \pmod 2$, $(n^{100} : (n+2)^{150}) = 1$. Consideremos ahora el caso $n \equiv 0 \pmod 2$, que se descompone en los casos $n \equiv 0 \pmod 4$ y $n \equiv 2 \pmod 4$:

  - Caso $n \equiv 0 \pmod 4$: $n = 4\,k = 2^2 k$, luego $n+2 = 2\,(2\,k+1)$ y

$$(n^{100} : (n+2)^{150}) = ((2^2 k)^{100} : (2(2\,k+1))^{150})$$

$$= (2^{200} k^{100} : 2^{150} (2\,k+1)^{150}) = 2^{150} (2^{50} k^{100} : (2\,k+1)^{150}).$$

    Ahora bien, $2 \perp 2\,k+1 \Rightarrow 2^{50} \perp (2\,k+1)^{150}$, y $k \perp 2\,k+1$ (probarlo!) $\Rightarrow k^{100} \perp (2\,k+1)^{150}$. Se concluye aplicando la Consecuencia 1 de la Proposición 6.10.

  - Caso $n \equiv 2 \pmod 4$: $n = 4\,k+2 = 2\,(2\,k+1)$, luego $n+2 = 2^2(k+1)$ y

$$(n^{100} : (n+2)^{150}) = (2^{100}(2\,k+1)^{100} : 2^{300}(k+1)^{150}) = 2^{100}((2\,k+1)^{100} : 2^{200}(k+1)^{150}).$$

    Ahora bien, $2 \perp 2\,k+1 \Rightarrow 2^{200} \perp (2\,k+1)^{100}$, y $k+1 \perp 2\,k+1$ (probarlo!) $\Rightarrow (k+1)^{150} \perp (2\,k+1)^{100}$. Se concluye aplicando la Consecuencia 1 de la Proposición 6.10.

- $(a : b) = 6 \implies (a\,b : 6\,a - 6\,b) = 36$:

  Coprimizando, se tiene $a = 6\,a'$, $b = 6\,b'$ con $a' \perp b'$, luego

$$(a\,b : 6\,a - 6\,b) = (36\,a'b' : 36a' - 36b') = (36\,a'b' : 36(a' - b')) = 36(a'b' : a' - b').$$

  Para concluir falta probar entonces que $a' \perp b' \Rightarrow a'b' \perp a' - b'$:

  Como siempre, sea d un posible divisor común:

$$\begin{cases} d \mid a'b' \\ d \mid a' - b' \end{cases} \implies \begin{cases} d \mid a'b' \\ d \mid a'(a' - b') \end{cases} \implies \begin{cases} d \mid a'b' \\ d \mid {a'}^2 - a'b' \end{cases} \implies d \mid {a'}^2$$

  De la misma manera:

$$\begin{cases} d \mid a'b' \\ d \mid a' - b' \end{cases} \implies \begin{cases} d \mid a'b' \\ d \mid b'(a' - b') \end{cases} \implies \begin{cases} d \mid a'b' \\ d \mid a'b' - {b'}^2 \end{cases} \implies d \mid {b'}^2$$

  Obtuvimos $d \mid {a'}^2$ y $d \mid {b'}^2$. Luego $d \mid ({a'}^2 : {b'}^2)$. Pero, como vimos arriba, $a' \perp b' \Rightarrow {a'}^2 \perp {b'}^2$, es decir $({a'}^2 : {b'}^2) = 1$. O sea $d \mid 1$. Así se prueba que los únicos divisores comunes de $a'b'$ y $a' - b'$ son ± 1, luego $a'b' \perp a' - b'$ como queríamos probar.

- $(a:8)=4 \implies (a^2+5\,a+32:80) = ?:$

  $(a:8)=4$ significa que $a=4\,a', 8=4\cdot 2$ con $a'\perp 2$, es decir, a' impar y se tiene:

  $$(a^2+5\,a+32:80) = (16\,a'^2+20\,a'+32:80) = (4\,(4\,a'^2+5a'+8):4\,20) = 4\,(4a'^2+5a'+8:20).$$

  Ahora bien, $(4a'^2+5a'+8:20) \in \{1,2,4,5,10,20\}$, y como claramente $2 \nmid 4a'^2+5a'+8$ pues a' es impar, 2 no es un divisor común (no divide al mcd). Luego $(4a'^2+5a'+8:20) \in \{1,5\}$.

  Falta averiguar si puede ser 5: pero $4\,a'^2+5\,a'+8 \equiv 4\,a'^2+3 \pmod 5$ y es facil ver, según los posibles restos de a' módulo 5, que ese número nunca es divisible por 5.

  Luego $(a^2+5\,a+32:80)=4$.

7 Ecuaciones Diofánticas

Vamos a aplicar ahora lo visto a la resolución de ciertas ecuaciones en enteros, que se llaman *Ecuaciones Diofánticas*. Se llaman así las ecuaciones con coeficientes enteros de las cuales se buscan las soluciones enteras. El nombre se puso por Diofanto de Alejandría ($\sim$200–$\sim$284) quien fue quien desarrolló ese tipo de ecuaciones en su obra "La Aritmética". Las ecuaciones diofánticas más sencillas son las ecuaciones de la forma $a\,X+b\,Y=c$ con $a,b,c\in\mathbb{Z}$, donde a y b no son ambos nulos, de las cuales se buscan los pares de soluciones *enteras*. Observemos que una ecuación de este tipo es la ecuación de una recta en $\mathbb{R}^2$, que sabemos resolver en $\mathbb{R}^2$, y que nos estamos preguntando por qué puntos de coordenadas ambas enteras pasa esa recta.

El problema es entonces el siguiente: encontrar todos los pares $(x,y)\in\mathbb{Z}^2$ que son solución de la ecuación

$$a\,X+b\,Y=c,$$

donde a,b,c son enteros dados, a,b no ambos nulos.

Como primer paso queremos decidir si existe al menos una solución entera (x_0,y_0).

Observación Si $a=0$ o $b=0$ (pongamos $b=0$), el problema se vuelve un problema de divisibilidad: $a\,X+0\,Y=c$ tiene solución entera si y solo si $a\,|\,c$, y en ese caso las soluciones son todos los pares $(c/a,j)$, $j\in\mathbb{Z}$. Luego en lo que sigue podemos suponer a y b no nulos.

Ejemplos

- $5\,X+9\,Y=1$ tiene por ejemplo como solución entera $x_0=2$, $y_0=-1$.
- $5\,X+9\,Y=10$ tiene como solución entera $x_0=10\cdot 2=20$, $y_0=-1\cdot 10=-10$.
- $4\,X+6\,Y=7$ no tiene solución entera porque el resultado de lo de la izquierda es claramente siempre. De hecho recordamos que si un número se escribe como combinación entera de a y b, entonces tiene que ser un múltiplo de $(a:b)$.
- $4\,X+6\,Y=2$ tiene solución ya que $2=(4:6)$ y sabemos que el mcd es combinación entera de los números. Se puede elegir aquí $x_0=-1$, $y_0=1$.
- $18\,X-12\,Y=2$ no tiene solución entera pues $(18:12)=6$ y $6\nmid 2$.
- $18\,X-12\,Y=60$ tiene solución pues $(18:12)\,|\,60$: por ejemplo escribimos $6=18\cdot 1-12\cdot 1$ y así obtenemos $60=10\cdot 6=18\cdot 10-12\cdot 10$, es decir $x_0=10$, $y_0=10$.

Concluimos la siguiente proposición:

Proposición 7.1 *Sean* $a, b, c \in \mathbb{Z}$, a, b *no nulos.*
Entonces la ecuación diofántica $a\,X + b\,Y = c$ *admite soluciones enteras si y solo si* $(a : b) \,|\, c$. *Es decir:*

$$\boxed{\exists\ (x, y) \in \mathbb{Z}^2 :\ a\,x + b\,y = c \iff (a : b) \,|\, c}$$

Prueba.–

($\Rightarrow$): Sea $(x_0, y_0) \in \mathbb{Z}^2$ una solución entera, entonces, como siempre, dado que $(a : b) \,|\, a$ y $(a : b) \,|\, b$, se concluye que $(a : b) \,|\, a\,x_0 + b\,y_0 = c$, es decir, $(a : b) \,|\, c$.

($\Leftarrow$): Sabemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s\,a + t\,b$. Luego, si $c = k\,(a : b)$, se tiene que $c = a\,(k\,s) + b\,(k\,t)$, y podemos tomar $x_0 := k\,s$, $y_0 := k\,t$.

■

La proposición da además una forma de conseguir una solución (x_0, y_0) particular (si existe), cuando no se consigue más facilmente, aplicando el algoritmo de Euclides para escribir el mcd como combinación entera. Es más, dado que la ecuación diofántica $a\,X + b\,Y = c$ es claramente equivalente a (es decir tiene exactamente las mismas soluciones que) la ecuación *coprimizada*:

$$a' \cdot X + b' \cdot Y = c', \quad \text{con } a' := \frac{a}{(a : b)},\ b' := \frac{b}{(a : b)} \ \text{ y } \ c' := \frac{c}{(a : b)},$$

y que esta última resulta diofántica también si la original admite una solución entera (pues $(a : b) \,|\, c$), siempre resulta más simple hacer este proceso de entrada para encontrar una solución particular: se escribe el 1 como combinación entera de a' y b' y luego se multiplican los coeficientes s y t obtenidos por c'.

El paso siguiente es, dada una ecuación diofántica que admite al menos una solución entera, encontrarlas todas.

Vamos a tratar primero en detalle un caso particular, el caso $c = 0$, es decir el caso de una ecuación diofántica de tipo

$$a\,X + b\,Y = 0$$

que siempre tiene solución pues $(a : b) \,|\, 0$. Miramos primero un ejemplo.

Ejemplo Soluciones enteras de $18\,X + 27\,Y = 0$:
La solución más simple es $x_0 = 0$, $y_0 = 0$. O también se tiene $x_1 = 27$, $y_1 = -18$. Así que la solución no es única. También por ejemplo $x_2 = -27$, $y_2 = 18$ o $x_3 = 3$, $y_3 = -2$ sirven. Vamos a probar que son infinitas. ¿ Cómo se consiguen todas ?
Por lo mencionado arriba, la ecuación original es equivalente a la euación coprimizada:

$$2\,X + 3\,Y = 0.$$

Ahora bien, sea $(x, y) \in \mathbb{Z}^2$ solución:

$$\begin{aligned} 2\,x + 3\,y = 0 \quad &\iff \quad 2\,x = -3\,y \\ &\implies \quad 2 \,|\, 3\,y \ \text{ y } \ 3 \,|\, 2\,x \\ &\implies \quad 2 \,|\, y \ \ (\text{pues } 2 \perp 3) \ \text{ y } \ 3 \,|\, x \ (\text{pues } 3 \perp 2) \\ &\implies \quad y = 2\,j \ \text{ y } \ x = 3\,k. \end{aligned}$$

Volviendo al primer renglón, resulta:

$$2\,(3\,k) = -3\,(2\,j) \implies j = -k.$$

Es decir: $x = 3\,k$ e $y = -2\,k$ para algún $k \in \mathbb{Z}$.

Hemos probado: (x, y) solución entera $\implies$ existe $k \in \mathbb{Z}$ tal que $x = 3\,k$ e $y = -2\,k$.
Verifiquemos la recíproca: Si $x = 3\,k$ e $y = -2\,k$ para el mismo $k \in \mathbb{Z}$, entonces (x, y) es solución de la ecuación. Efectivamente, se tiene $2\,x + 3\,y = 2\,(3\,k) + 3\,(-2\,k) = 0$.
Luego, hemos probado que el conjunto de soluciones enteras de esta ecuación es el conjunto:

$$\mathcal{S}_0 \;=\; \{\; (x, y) : x = 3\,k,\, y = -2\,k;\; k \in \mathbb{Z} \;\}.$$

(Observemos que si nos olvidamos de coprimizar la ecuación y nos quedamos, usando la misma estructura, con las soluciones de tipo $x = 27\,k$, $y = -18\,k$, $k \in \mathbb{Z}$, perdemos soluciones ya que se nos escapa por ejemplo la solución de antes $x_3 = 3$, $y_3 = -2$.)

Este procedimiento se puede generalizar sin problemas:

Proposición 7.2 *Sean $a, b \in \mathbb{Z}$, no nulos.*
El conjunto $\mathcal{S}_0$ de soluciones enteras de la ecuación diofántica $a\,X + b\,Y = 0$ es

$$\mathcal{S}_0 \;=\; \{\; (x, y) : x = b'k,\, y = -a'k;\; k \in \mathbb{Z} \;\}, \quad \textit{donde}\;\; a' := \frac{a}{(a : b)} \;\;\text{y}\;\; b' := \frac{b'}{(a : b)}.$$

Prueba.–
La ecuación original $a\,X + b\,Y = 0$ es equivalente a la ecuación coprimizada $a'X + b'Y = 0$. Esta sigue siendo una ecuación diofántica, y se tiene $a' \perp b'$.
Claramente, todo par (x, y) de la forma $x = b'k$ e $y = -a'k$ para el mismo $k \in \mathbb{Z}$ es solución de la ecuación coprimizada, y por lo tanto de la original. En efecto se tiene $a'x + b'y = a'(b'k) + b'(-a'k) = 0$.
Reciprocamente, vamos a probar que toda solución $(x, y) \in \mathbb{Z}^2$ es de esa forma:

$$\begin{aligned} a'x + b'y = 0 \;&\iff\; a'x = -b'y \\ &\implies\; a' \,|\, b'y \;\text{ y }\; b' \,|\, a'x \\ &\implies\; a' \,|\, y \;\text{ (pues } a' \perp b') \;\text{ y }\; b' \,|\, x \;\text{ (pues } b' \perp a') \\ &\implies\; y = a'\,j \;\text{ y }\; x = b'\,k. \end{aligned}$$

Volviendo al primer renglón, $a'x = -b'y$, resulta:

$$a'(b'k) = -b'(a'j) \implies j = -k.$$

Es decir, $x = b'k$ e $y = -a'k$ para algún $k \in \mathbb{Z}$.

■

Para resolver completamente una ecuación general $a\,X + b\,Y = c$, que admite al menos una solución entera (x_0, y_0), nos podemos reducir al caso anterior observando que, dado que $a\,x_0 + b\,y_0 = c$, se tiene que para $(x, y) \in \mathbb{Z}^2$,

$$a\,x + b\,y = c \iff a\,x + b\,y = a\,x_0 + b\,y_0 \iff a\,(x - x_0) + b\,(y - y_0) = 0.$$

Es decir (x, y) es solución de $a\,X + b\,Y = c$ si y solo si $(x - x_0, y - y_0)$ es solución de $a\,X + b\,Y = 0$.
Luego, aplicando la Proposición 7.2, obtenemos el Teorema siguiente:

Teorema 7.3 *Sean* $a, b, c \in \mathbb{Z}$, a, b *no nulos.*
El conjunto $\mathcal{S}$ *de soluciones enteras de la ecuación diofántica* $a\,X + b\,Y = c$ *es:*

- $\mathcal{S} = \emptyset$, *si* $(a : b) \nmid c$.
- $\mathcal{S} = \{\ (x, y) : x = x_0 + b'k,\ y = y_0 - a'k;\ k \in \mathbb{Z}\ \}$, *donde* (x_0, y_0) *es una solución particular,* $a' := \dfrac{a}{(a : b)}$, $b' := \dfrac{b}{(a : b)}$, *si* $(a : b) \mid c$.

Resumimos el algoritmo que se obtiene a partir del Teorema en el cuadro siguiente:

Resolución completa de la ecuación diofántica $a\,X + b\,Y = c$

1. ¿ Tiene solución la ecuación ?
   (a) **no** si $(a : b) \nmid c$. En ese caso $\mathcal{S} = \emptyset$.
   (b) **sí** si $(a : b) \mid c$. En ese caso:
2. Coprimizo la ecuación:
$$a'\,X + b'\,Y = c', \quad \text{con } a' := \frac{a}{(a : b)},\ b' := \frac{b}{(a : b)} \ \text{ y } \ c' := \frac{c}{(a : b)}.$$
3. Busco una solución particular $(x_0, y_0) \in \mathbb{Z}^2$ (a ojo o aplicando el algoritmo de Euclides).
4. Todas las soluciones son:
$$\mathcal{S} = \{\ (x, y) : x = x_0 + b'k,\ y = y_0 - a'k;\ k \in \mathbb{Z}\ \}.$$

Ejemplos

- Soluciones enteras de $18\,X + 27\,Y = -90$:
  Hay soluciones pues $(18 : 27) = 9 \mid -90$.
  Coprimizo: $2\,X + 3\,Y = 10$.
  Solución particular: $(x_0, y_0) := (5, 0)$.
  Entonces $\mathcal{S} = \{\,(x, y) :\ x = 5 + 3k,\ y = -2k,\ k \in \mathbb{Z}\,\}$.
- Soluciones *naturales* de $175\,X + 275\,Y = 3000$:
  Hay soluciones enteras pues $(125 : 50) = 25 \mid 3000$.
  Coprimizo: $7\,X + 11\,Y = 120$.
  Solución particular?
$$\begin{aligned} & 11 = 1 \cdot 7 + 4,\ 7 := 1 \cdot 4 + 3,\ 4 = 1 \cdot 3 + 1 \\ \Rightarrow\ & 1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7 \\ \Rightarrow\ & 120 = 7 \cdot (-360) + 11 \cdot 240 \\ \Rightarrow\ & (x_0, y_0) = (-360, 240). \end{aligned}$$

Soluciones enteras: $x = -360 + 11\,k,\ y = 240 - 7\,k,\ k \in \mathbb{Z}$.

Soluciones naturales:

$$\begin{array}{ccccc} x > 0 & \text{e} & y > 0 & \Longrightarrow \\ -360 + 11\,k > 0 & \text{y} & 240 - 7\,k > 0 & \Longrightarrow \\ 11\,k > 360 & \text{y} & 240 > 7\,k & \Longrightarrow \\ k > (360/11) = 32,7... & \text{y} & k < (240/7) = 34,2... & \end{array}$$

Por lo tanto $k \in \{33, 34\}$: hay dos pares de soluciones naturales, $x_1 := -360 + 11 \cdot 33 = 3,\ y_1 := 240 - 7 \cdot 33 = 9$ y $x_2 := -360 + 11 \cdot 34 = 14,\ y_2 := 240 - 7 \cdot 34 = 2$.

Entonces $\mathcal{S}_{\mathbb{N}} = \{\,(3, 9),\ (14, 2)\,\}$.

8 Ecuaciones de Congruencia

El analisis realizado para las ecuaciones diofánticas se aplica directamente a ciertas *ecuaciones lineales de congruencia*. Más especificamente a las ecuaciones de la forma

$$a\,X \equiv c \pmod{b},$$

donde $a, b, c \in \mathbb{Z}$, con a y b no nulos, de las cuales se buscan las soluciones *enteras*.

Ahora bien, si $\mathcal{S}$ denota el conjunto de soluciones enteras de esa ecuación , es decir

$$\mathcal{S} := \{\ x \in \mathbb{Z} : a\,x \equiv c \pmod{b}\,\},$$

entonces se tiene:

$$\begin{array}{rcl} x \in \mathcal{S} & \Longleftrightarrow & a\,x \equiv c \pmod{b} \\ & \Longleftrightarrow & b \,|\, a\,x - c \\ & \Longleftrightarrow & \exists\ y \in \mathbb{Z} : a\,x - c = b\,y \\ & \Longleftrightarrow & \exists\ y \in \mathbb{Z} : a\,x - b\,y = c \\ & \Longleftrightarrow & \exists\ y \in \mathbb{Z} : (x, y) \text{ es solución de la ecuación diofántica } a\,X - b\,Y = c. \end{array}$$

En particular, la ecuación de congruencia $a\,X \equiv c \pmod{b}$ admite al menos una solución en $\mathbb{Z}$ si y solo si la ecuación diofántica $a\,X - b\,Y = c$ admite al menos una solución en $\mathbb{Z}^2$. Por lo visto en el Teorema 7.3, esto es si y solo si $(a : -b) = (a : b) \,|\, c$. Hemos probado la primer parte de la proposición siguiente:

Proposición 8.1 *Sean $a, b, c \in \mathbb{Z}$, a, b no nulos. Entonces:*
La ecuación de congruencia $a\,X \equiv c \pmod{b}$ admite soluciones enteras si y solo si $(a : b) \,|\, c$.
En ese caso la ecuación es equivalente a la ecuación de congruencia coprimizada

$$a'X \equiv c' \pmod{b'} \quad \textit{donde}\ \ a' := \frac{a}{(a : b)},\ b' := \frac{b}{(a : b)}\ \ y\ \ c' := \frac{c}{(a : b)}.$$

La segunda afirmación se puede probar via las ecuaciones diofánticas como antes, pero también podemos aislar la propiedad siguiente que es inmediata pero muy útil:

Proposición 8.2 *Sean $a', b', c', d \in \mathbb{Z}$, con $a', b', d \neq 0$. Entonces, para $x \in \mathbb{Z}$, se tiene:*

$$(d\,a')\,x \equiv d\,c' \pmod{(d\,b')} \iff a'x \equiv c' \pmod{b'}.$$

Prueba.–

$$d\,b' \mid d\,a'x - d\,c' = d\,(a'x - c') \iff b' \mid a'x - c'.$$

■

Prueba de la Proposición 8.1.–

Si $(a : b) \mid c$, la ecuación $a'X \equiv c' \pmod{b'}$ sigue teniendo todos sus coeficientes enteros, y se aplica la proposición anterior para $d := (a : b)$, $a := d\,a'$, $b := d\,b'$ y $c := d\,c'$.

■

El paso siguiente es (como en el caso de las ecuaciones diofánticas) dada una ecuación de congruencia que admite al menos una solución entera, encontrarlas todas:

Teorema 8.3 *Sean $a, b, c \in \mathbb{Z}$, a, b no nulos.*
El conjunto $\mathcal{S}$ de soluciones enteras de la ecuación de congruencia $a\,X \equiv c \pmod{b}$ es:

- $\mathcal{S} = \emptyset$, *si* $(a : b) \nmid c$.
- $\mathcal{S} = \{x \in \mathbb{Z} : x \equiv x_0 \pmod{b'}\}$, *donde x_0 es una solución particular y* $b' := \dfrac{b}{(a : b)}$, *si* $(a : b) \mid c$.

Prueba.–

El primer inciso es la Proposición 8.1. Para el segundo:

$(\supseteq)$: x_0 solución particular significa $a'\,x_0 \equiv c' \pmod{b'}$. Luego,

$$x \equiv x_0 \pmod{b'} \implies a'\,x \equiv a'\,x_0 \pmod{b'} \implies a'\,x \equiv c' \pmod{b'}$$

como se quería probar, dada la equivalencia de la ecuación de congruencia original y la coprimizada.

$(\subseteq)$: Por la relación observada entre soluciones de la ecuación de congruencia y soluciones de la diofántica correspondiente, $x \in \mathcal{S}$ si y solo si existe $y \in \mathbb{Z}$ tal que (x, y) es solución de la ecuación diofántica $a\,X - b\,Y = c$. Por el Teorema 7.3, esto es si y solo si existe una solución particular (x_0, y_0) de la ecuación diofántica, y $k \in \mathbb{Z}$ tal que $x = x_0 + b'k$, $y = y_0 + a'k$. Luego $x = x_0 + b'k$ para algún $k \in \mathbb{Z}$, es decir $x \equiv x_0 \pmod{b'}$.

■

Antes de resumir el algoritmo que se obtiene a partir del Teorema, hagamos algunos ejemplos.

Ejemplos

- La ecuación $9\,X \equiv 2 \pmod{15}$ no tiene solución pues $(9 : 15) \nmid 2$.
- La ecuación $9\,X \equiv 6 \pmod{15}$:

  $$9\,x \equiv 6 \pmod{15} \iff 3\,x \equiv 2 \pmod{5} \iff x \equiv 4 \pmod{5}.$$

  (Aquí, $x_0 := 4$ es una solución particular.)
- La ecuación $3\,X \equiv 2 \pmod{4}$:

  $$3\,x \equiv 2 \pmod{4} \iff x \equiv 2 \pmod{4}.$$

- La ecuación $12\,X \equiv 6 \pmod{10}$ tiene solución pues $(12:10) = 2 \,|\, 6$. Pero es aún más facil simplificar todo lo que se puede en la ecuación antes, como $12 \equiv 2 \pmod{10}$, se tiene:

$$12\,x \equiv 6 \pmod{10} \iff 2\,x \equiv 6 \pmod{10} \iff x \equiv 3 \pmod{5}.$$

- La ecuación $120\,X \equiv 60 \pmod{250}$ tiene solución pues $(120:250) = 10 \,|\, 60$.

  $120\,x \equiv 60 \pmod{250} \Leftrightarrow 12\,x \equiv 6 \pmod{25} \Leftrightarrow 2\,x \equiv 1 \pmod{25} \Leftrightarrow x \equiv 13 \pmod{25}$:

  Aquí la observación crucial fue: $6\,(2\,x) \equiv 6 \cdot 1 \pmod{25}$ y $6 \perp 25$ implica que se puede simplificar el 6, es decir implica $2\,x \equiv 1 \pmod{25}$. Esto se generaliza en la siguiente observación:

Observación 8.4 *Sean $a, b, c, d \in \mathbb{Z}$, a, b, d no nulos. Entonces, si b y d son coprimos, para $x \in \mathbb{Z}$ se tiene:*

$$(d\,a)\,x \equiv d\,c \pmod{b} \iff a\,x \equiv c \pmod{b}.$$

Prueba.–

($\Leftarrow$): Vale siempre.
($\Rightarrow$): Esto es porque $b \,|\, d\,(a\,x - c)$ y $b \perp d$ implica $b \,|\, a\,x - c$.

■

Resolución completa de la ecuación de congruencia $a\,X \equiv c \pmod{b}$

1. Antes que nada reemplazo a por $r_b(a)$ y c por $r_b(c)$ sin cambiar las soluciones, ya que $a \equiv r_b(a) \pmod{b}$ y $c \equiv r_b(c) \pmod{b}$, o por algún otro número conveniente que sea congruente, por ejemplo -1. Así, de entrada se tiene que los coeficientes de la ecuación de congruencia son los más simples posibles.

2. ¿ Tiene solución la ecuación ?

   (a) **no** si $(a:b) \nmid c$. En ese caso $\mathcal{S} = \emptyset$.

   (b) **sí** si $(a:b) \,|\, c$. En ese caso:

3. Coprimizo la ecuación:

$$a'\,X \equiv c' \pmod{b'}, \quad \text{con } a' := \frac{a}{(a:b)},\ b' := \frac{b}{(a:b)} \ \text{ y } \ c' := \frac{c}{(a:b)}.$$

4. Si puedo, ahora que $a' \perp b'$, simplifico todos los factores comunes entre a' y c' aplicando la proposición anterior. Esto me simplifica la búsqueda de la solución particular.

5. Busco una solución particular $x_0 \in \mathbb{Z}$ que verifica que $a'x_0 \equiv c' \pmod{b'}$.

6. Todas las soluciones son:

$$\mathcal{S} = \{\ x \in \mathbb{Z} : x \equiv x_0 \pmod{b'}\ \}.$$

---

9 Primos y Factorización

Recordemos que un número $p \in \mathbb{Z}$, distinto de $0, 1$ y -1 es primo si y solo si tiene únicamente 4 divisores, o equivalentemente 2 divisores positivos. Los números primos juegan un papel fundamental en el conjunto de los números enteros, empezando porque cumplen la proposición siguiente.

Proposición 9.1 *Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces existe un primo (positivo) p tal que $p \,|\, a$.*

Prueba.–
La demostración intuitiva de "si a es primo, ya está pues es divisible por él mismo, y si no, es compuesto, entonces es divisible por algún b más chico, si ese b es primo, ya está, si no es divisible por algún c más chico, etc..." se formaliza por inducción en a:
Claramente alcanza probar la proposición para a positivo, es decir para $a \geq 2$ (pues $a \neq 0, \pm 1$).
La proposición es entonces: $p(a)$: "$\exists\, p$ primo positivo : $p \,|\, a$".
$\underline{a = 2}$: $p(2)$ es verdadera pues $p := 2 \,|\, 2$.
$\underline{a > 2}$:

- Si a es primo, $p(a)$ es verdadera pues $p := a \,|\, a$.
- Si a no es primo, entonces es compuesto, y por lo tanto existe c con $2 \leq c \leq a - 1$ tal que $c \,|\, a$. Por hipotesis inductiva, existe un primo positivo p tal que $p \,|\, c$. Se concluye que $p \,|\, a$ por transitividad.

Así, todo número distinto de $0, \pm 1$ es divisible por algún primo positivo.

■

Una consecuencia de este hecho es que hay infinitos primos distintos, demostración hecha por Euclides. (El hecho que haya infinitos números naturales no garantiza de por sí que haya infinitos primos ya que los infinitos números podrían obtenerse multiplicando de distintas formas y a distintas potencias finitos primos.)

Consecuencia Existen infinitos primos positivos distintos.

Prueba.– Supongamos que no es así y que hay sólo un número finito N de primos positivos. O sea que el conjunto $\mathcal{P}$ de primos positivos es $\mathcal{P} = \{ p_1, \ldots, p_N \}$. Consideremos el siguiente número natural M:

$$M := p_1 p_2 \cdots p_N + 1.$$

Dado que $M \geq 2$ pues $2 \in \mathcal{P}$, existe por la proposición anterior un primo positivo $p_i \in \mathcal{P}$ que divide a M. Pero

$$p_i \,|\, M \quad \text{y} \quad p_i \,|\, p_1 p_2 \cdots p_N \quad \Longrightarrow \quad p_i \,|\, 1,$$

contradicción que proviene de suponer que hay sólo finitos primos.

■

Otra consecuencia de este hecho es la famosa Criba de Eratóstenes de Cirene ($\sim$276–$\sim$194 AC), que construye recursivamente la lista de todos los primos hasta un número dado. Por ejemplo aquí la lista de primos hasta 57:

Criba de Eratóstenes (hasta 57)

- Se escribe la lista de todos los números del 2 al 57:

  $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31,$
  $32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, , 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57.$

- Se tachan los múltiplos estrictos del primero de la lista:

  $2, 3, \not4, 5, \not6, 7, \not8, 9, \not{10}, 11, \not{12}, 13, \not{14}, 15, \not{16}, 17, \not{18}, 19, \not{20}, 21, \not{22}, 23, \not{24}, 25, \not{26}, 27, \not{28}, 29, \not{30}, 31,$
  $\not{32}, 33, \not{34}, 35, \not{36}, 37, \not{38}, 39, \not{40}, 41, \not{42}, , 43, \not{44}, 45, \not{46}, 47, \not{48}, 49, \not{50}, 51, \not{52}, 53, \not{54}, 55, \not{56}, 57.$

  El primero que sobrevivió, en este caso el 3, es claramente primo, ya que sino tendría que ser divisible por un primo más chico que él.

- Se tachan los múltiplos estrictos (no tachados en la lista) del 3:

  $2, 3, \not4, 5, \not6, 7, \not8, \not9, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, 25, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31,$
  $\not{32}, \not{33}, \not{34}, 35, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, , 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, 55, \not{56}, \not{57}.$

  El primero que sobrevivió, en este caso el 5, es claramente primo, ya que sino tendría que ser divisible por un primo más chico que él.

- Se repite el procedimiento con el 5:

  $2, 3, \not4, 5, \not6, 7, \not8, \not9, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31,$
  $\not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, , 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56}, \not{57}.$

- Se repite el procedimiento con el 7:

  $2, 3, \not4, 5, \not6, 7, \not8, \not9, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31,$
  $\not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, , 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, \not{49}, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56}, \not{57}.$

- Se puede probar que alcanza hacer esto hasta que se alcanzó el último primo $p \leq \sqrt{57}$, es decir hasta el primo $p = 7$, pues todo número compuesto n es divisible por algún primo menor o igual que su raíz cuadrada (probarlo). Luego la lista que quedó de números no tachados son todos los primos menores o iguales que 57, es decir:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.$$

■

Ahora bien, si p es un número primo (positivo), y $a \in \mathbb{Z}$ es cualquiera, entonces el máximo común divisor entre p y a, al ser un divisor de p primo, puede ser únicamente p o 1, en función de si p divide a a o no:

$$(p : a) = \begin{cases} p & \text{si} \quad p \mid a \\ 1 & \text{si} \quad p \nmid a \end{cases} \qquad \text{y} \qquad p \perp a \iff p \nmid a.$$

Luego, la Proposición 6.9 (2) dice: $p \mid a\, b$ y $p \nmid a \implies p \mid b$, o equivalentemente:

$$\boxed{p \mid a\, b \iff p \mid a \quad \text{o} \quad p \mid b}$$

Esta es la propiedad más importante que cumplen los números primos (comparar con el último inciso de las Propiedades 2.3). Más aún, esta propiedad caracteriza los números primos: p es primo si y solo si cada vez que p divide a un producto divide a alguno de los factores. Y la propiedad se generaliza inmediatamente a

Proposición 9.2 *Sean* $a, a_1, \ldots, a_n$ *números enteros, y* p *un primo. Entonces*

$$p \mid a_1 \cdots a_n \iff p \mid a_i \text{ para algún } i,\ 1 \le i \le n, \qquad y \qquad p \mid a^n \iff p \mid a.$$

Estamos ahora en condiciones de demostrar completamente el famoso *Teorema Fundamental de la Aritmética*, piedra angular de toda la teoría de números, acerca de la factorización única de los números como producto de primos. Este teorema era ya conocido por los griegos de la época de Pitágoras (S. VI ac), y es el que justifica el interés de los matemáticos por conocer mejor el comportamiento de los primos: cómo se distribuyen, cómo conseguirlos, etc.

Teorema 9.3 (Teorema Fundamental de la Aritmética)
Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. *Entonces* a *admite una factorización como producto de primos, en la forma*

$$a = \pm p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n}$$

donde los p_k *son primos positivos* distintos, *y* $v_k \in \mathbb{N}$ *para* $1 \le k \le n$.
Más aún, esta escritura es única salvo permutación de los primos.

Prueba.–

Existencia: Nuevamente, alcanza con probar el teorema para a positivo, y se formaliza por inducción en a, $a \ge 2$:

$p(a)$: "a admite una factorización como producto de primos".

$a = 2$: $p(2)$ es verdadera pues $2 = +2^1$.

$a > 2$:

- Si a es un primo p, $p(a)$ es verdadera pues $a = p = +p^1$.
- Si a no es primo, entonces es divisible por algún primo positivo p más chico que él, y por lo tanto el cociente $c = a/p$ verifica $2 \le c \le a - 1$. Por hipotesis inductiva, c admite una factorización como producto de primos, en la forma $c = p_1^{v_1} \cdots p_n^{v_n}$. Por lo tanto a admite la factorización
$$a = +pp_1^{v_1} \cdots p_n^{v_n}.$$

Así, todo número distinto de $0, \pm 1$ admite una factorización como producto de primos.

Unicidad: Supongamos que $a = \pm p_1^{v_1} \cdots p_n^{v_n} = \pm q_1^{w_1} \cdots q_m^{w_m}$ en las condiciones del enunciado. Queremos probar que entonces los signos, los primos y los exponentes coinciden.
Claramente los signos coinciden, así que podemos suponer a positivo.

En la expresión $p_1^{v_1} \cdots p_n^{v_n} = q_1^{w_1} \cdots q_m^{w_m}$, simplifiquemos todos los primos comunes que aparecen a la menor potencia a la que aparecen.
Si al hacer eso no sobra nada, o sea obtenemos $1 = 1$, es que todos los primos y las potencias coincidían.
Si no pasa eso y sobra algo de algún lado al menos, obtenemos una expresión igual pero donde $p_i \neq q_j$ para todos los que sobraron. Podemos suponer sin perdida de generalidad que del lado izquierdo sobró un p_i. Entonces tenemos que p_i divide a lo que sobró del lado derecho o al 1 si no sobró nada. O sea $p_i \mid 1$ (lo que es absurdo) o $p_i \mid q_1^{w_1} \cdots q_m^{w_m}$, luego existe j tal que $p_i \mid q_j$ pero p_i y q_j son primos distintos. Contradicción, que proviene de suponer que sobró un primo de algún lado.

■

Observemos ahora que primos distintos son coprimos entre sí, y más aún, aplicando las consecuencias de la Proposición 6.9, potencias de primos distintos son coprimas entre sí también. Luego, aplicando recursivamente la Proposición 6.9 (1), se obtiene lo siguiente para $p_1, \ldots, p_n$ primos distintos dos a dos , $v_1, \ldots, v_n \in \mathbb{N}$ y $a \in \mathbb{Z}$ arbitrario:

$$\boxed{p_1^{v_1} \mid a \quad \text{y} \quad p_2^{v_2} \mid a \quad \text{y} \quad \ldots \quad \text{y} \quad p_n^{v_n} \mid a \iff p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n} \mid a}$$

Introducimos ahora una notación para simplificar la escritura en el Teorema Fundamental de la Aritmética y poder enunciar claramente muchas propiedades que son consecuencia de ese teorema.

Notación Dado $a \in \mathbb{Z}$, $a \neq 0$, y p primo positivo, vamos a notar con $v_p(a)$ el exponente exacto de p que aparece en la factorización de a como producto de primos. Por ejemplo $v_2(24) = 3$, $v_3(24) = 1$ y $v_p(24) = 0$ para todo $p \neq 2, 3$ pues $24 = 2^3 \cdot 3$. Se observa que entonces $24 = 2^{v_2(24)} \cdot 3^{v_3(24)}$. No excluímos acá los casos $a = \pm 1$, pues $v_p(\pm 1) = 0$ para todo primo p.
También vamos a utilizar la función signo, de $\mathbb{Z} \setminus \{0\}$ en $\{-1, +1\}$:

$$\operatorname{sg}(a) := \begin{cases} -1 & \text{si} \quad a < 0 \\ +1 & \text{si} \quad a > 0 \end{cases}$$

y finalmente notar por $\mathcal{P}$ el conjunto de los primos positivos, es decir,

$$\mathcal{P} := \{\, p \in \mathbb{Z} : p \text{ primo positivo} \,\}.$$

Con estas convenciones podemos escribir para $a \in \mathbb{Z}$, $a \neq 0$:

$$a = \operatorname{sg}(a) \prod_{p \in \mathcal{P}} p^{v_p(a)},$$

donde este producto infinito está bien definido ya que hay sólo un número finito de factores a la derecha que son distintos de 1 (pues un número $a \neq 0$ es divisible por sólo un número finito de primos distintos).

Consecuencias Sean $a, b, c \in \mathbb{Z}$, no nulos. Entonces

1. $v_p(a) \geq 0$ (y es entero) para todo $p \in \mathcal{P}$.
2. $v_p(a\,b) = v_p(a) + v_p(b) \quad$ y $\quad v_p(a^n) = n\, v_p(a)$ para todo $p \in \mathcal{P}$ y para todo $n \in \mathbb{N}$.
3. $p \mid a \iff v_p(a) \geq 1$, $\quad$ y $\quad p^v \mid a \iff v_p(a) \geq v$.
4. $\boxed{d \mid a \iff v_p(d) \leq v_p(a) \text{ para todo } p \in \mathcal{P}}$
5. $$Div(a) = \{d \in \mathbb{Z} : v_p(d) \leq v_p(a)\ \forall p \in \mathcal{P}\ \} \quad \text{y} \quad \#Div_+(a) = \prod_{p \in \mathcal{P}} (v_p(a) + 1),$$
   donde este producto infinito está bien definido pues $v_p(a) + 1 \neq 1 \Leftrightarrow p \mid a$.
6. $$(a : b) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a), v_p(b)\}}. \tag{1}$$
   Esto es por lo siguiente: llamemos c al número de la derecha de la igualdad (1). Vamos a ver que $c \mid (a : b)$ y $(a : b) \mid c$.

Por un lado, como para todo $p \in \mathcal{P}$, $\min\{v_p(a), v_p(b)\} \leq v_p(a)$ y $\min\{v_p(a), v_p(b)\} \leq v_p(b)$, se tiene, aplicando el inciso 4, que $c \,|\, a$ y $c \,|\, b$. Luego $c \,|\, (a : b)$.

Pero por otro lado, $(a : b) \,|\, a$ y $(a : b) \,|\, b$ implica, aplicando la otra implicación del inciso 4, que para todo $p \in \mathcal{P}$, $v_p((a : b)) \leq v_p(a)$ y $v_p((a : b)) \leq v_p(b)$, luego $v_p((a : b)) \leq \min\{v_p(a), v_p(b)\}$. Así, nuevamente, $(a : b) \,|\, c$.

7. $a \perp b \iff v_p(a) \cdot v_p(b) = 0$ para todo $p \in \mathcal{P}$.

   Esto es porque $a \perp b \Leftrightarrow (a : b) = 1$, es decir no hay ningún primo $p \in \mathcal{P}$ que divide simultaneamente a a y a b, luego si $v_p(a) > 0$ tiene que ser $v_p(b) = 0$ y vice-versa.

Un comentario sobre el cálculo del máximo común divisor entre dos números via la fórmula (1): puede parecer más simple a primera vista factorizar los números y aplicar esta fórmula antes que aplicar el Algoritmo de Euclides. Sin embargo en el caso general, para números arbitrariamente grandes, es más veloz el cálculo mediante el algoritmo de Euclides (la cantidad de cuentas a realizar depende polinomialmente del logaritmo en base 2 de los números considerados) que pasando por la factorización (hasta ahora no se conoce ningún algoritmo para factorizar un número cuya cantidad de cuentas no dependa esencialmente del número considerado en lugar de su logaritmo en base 2).

Ejemplos

- $Div(10^{10}) = \{\pm 2^i 5^j,\ 0 \leq i, j \leq 10\}$, y por lo tanto, 10^{10} tiene $(10+1)(10+1) = 11^2$ divisores positivos distintos, y $2 \cdot 11^2$ divisores enteros, positivos y negativos.

- Suma de los divisores positivos de 10^{10}:

$$\sum_{0 \leq i,j \leq 10} 2^i 5^j = \sum_{i=0}^{10} (\sum_{j=0}^{10} 2^i 5^j) = \sum_{i=0}^{10} (2^i \sum_{j=0}^{10} 5^j) = (\sum_{j=0}^{10} 5^j)(\sum_{i=0}^{10} 2^i)$$

$$= \frac{5^{11}-1}{5-1} \cdot \frac{2^{11}-1}{2-1} = (2^{11}-1)\frac{5^{11}-1}{4}.$$

- $p_1^{v_1} \cdots p_n^{v_n}$ tiene $(v_1+1) \cdots (v_n+1)$ divisores positivos y el doble de positivos y negativos.

- El menor número natural n con 12 divisores positivos es el 60:

  Por (5) arriba, $\prod_p (v_p(n)+1) = 12 = 6 \cdot 2 = 4 \cdot 3 = 3 \cdot 2 \cdot 2$ implica que n es de alguna de las formas siguientes: $n = p^{11}$ o $n = p^5 \cdot q$ o $n = p^3 \cdot q^2$ o $n = p^2 \cdot q \cdot r$. Ahora, en cada una de estas formas el número más chico es $2^{11} = 2048$, $2^5 \cdot 3 = 96$, $2^3 \cdot 3^2 = 72$ y $2^2 \cdot 3 \cdot 5 = 60$. Por lo tanto el menor es $n = 60$.

- $5 \,|\, a^2 \implies 5 \,|\, a$ porque 5 es primo.

- $10 \,|\, a^2 \implies 10 \,|\, a$ aunque 10 no es primo, pero por ser un producto de primos distintos:

$$10 \,|\, a^2 \implies 2 \,|\, a^2 \text{ y } 5 \,|\, a^2 \implies 2 \,|\, a \text{ y } 5 \,|\, a \underset{2 \perp 5}{\implies} 10 = 2 \cdot 5 \,|\, a.$$

- $4 \,|\, a^2 \not\Longrightarrow 4 \,|\, a$ pues por ejemplo $4 \,|\, 2^2$ pero $4 \nmid 2$.

  Sin embargo $4 \,|\, a^2 \Rightarrow 2 \,|\, a^2 \Rightarrow 2 \,|\, a$, por ser 2 primo.

- $8 \,|\, a^2 \implies 4 \,|\, a$, pues:

$$2^3 \,|\, a^2 \implies v_2(2^3) \leq v_2(a^2) \implies 3 \leq 2\, v_2(a) \implies 2 \leq v_2(a) \Longrightarrow 2^2 \,|\, a.$$

- $2^4 \cdot 3^3 \cdot 5^7 \mid a^3 \implies 2^2 \cdot 3 \cdot 5^3 \mid a$, pues:

$$\begin{array}{lllllll} 2^4 \cdot 3^3 \cdot 5^7 \mid a^3 & \implies & 2^4 \mid a^3 & \text{y} & 3^3 \mid a^3 & \text{y} & 5^7 \mid a^3 \\ & \implies & v_2(2^4) \leq v_2(a^3) & \text{y} & v_3(3^3) \leq v_3(a^3) & \text{y} & v_5(5^7) \leq v_5(a^3) \\ & \implies & 4 \leq 3\, v_2(a) & \text{y} & 3 \leq 3\, v_3(a) & \text{y} & 7 \leq 3\, v_5(a) \\ & \implies & 2 \leq v_2(a) & \text{y} & 1 \leq v_3(a) & \text{y} & 3 \leq v_5(a) \\ & \implies & 2^2 \mid a & \text{y} & 3 \mid a & \text{y} & 5^3 \mid a \\ & \implies & 2^2 \cdot 3 \cdot 5^3 \mid a & & & & \end{array}$$

- $d^n \mid a^n \implies d \mid a$:

$$d^n \mid a^n \implies \forall\, p,\ v_p(d^n) \leq v_p(a^n) \implies \forall\, p,\ n\, v_p(d) \leq n\, v_p(a) \implies \forall\, p,\ v_p(d) \leq v_p(a) \implies d \mid a.$$

- Ojo: $d^2 \mid a^3 \not\Longrightarrow d \mid a$. Por ejemplo $8^2 \mid 4^3$.

- $\sqrt{2} \notin \mathbb{Q}$:

  Supongamos $\sqrt{2} \in \mathbb{Q}$: $\sqrt{2} = \frac{a}{b}$, con $a, b \in \mathbb{N}$. Luego $\sqrt{2}\, b = a \implies 2\, b^2 = a^2$. Entonces, $v_2(2\, b^2) = v_2(a^2)$, es decir, $1 + 2\, v_2(b) = 2\, v_2(a)$. Absurdo comparando la paridad de ambos números.

- ¿ Existen $a, b \in \mathbb{Z}$ tales que $12\, a^2 = b^4$?

  En tal caso se tiene $v_2(12\, a^2) = v_2(b^4)$ y $v_3(12\, a^2) = v_3(b^4)$, es decir $2 + 2\, v_2(a) = 4\, v_2(b)$ y $1 + 2\, v_3(a) = 4\, v_3(b)$.

  La primer afirmación no presenta contradicción pero la segunda sí, por comparación de paridades. Luego no existen.

- ¿Cuál es el mínimo $n \in \mathbb{N}$ tal que $1200\, n$ es un cubo?

  $2^4 \cdot 3 \cdot 5^2 \cdot n = a^3$ implica que los exponentes del término de la izquierda tienen que ser múltiplos de 3. La forma más económica de lograrlo es tomando $n = 2^2 \cdot 3^2 \cdot 5 = 180$.

- Divisores positivos n de 1260 que verifican que $(n : 150) = 10$:

  Por la forma de los divisores positivos de $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$, se tiene que $n = 2^i \cdot 3^j \cdot 5^k \cdot 7^\ell$ con $0 \leq i, j \leq 2$ y $0 \leq k, \ell \leq 1$. Por otro lado $(n : 2 \cdot 3 \cdot 5^2) = 10 = 2 \cdot 5$ implica que:

$$\min\{i, 1\} = 1,\ \min\{j, 1\} = 0,\ \min\{k, 2\} = 1,\ \min\{\ell, 0\} = 0,$$

  es decir, $i = 1$ o 2, $j = 0$, $k = 1$ y $\ell = 0$ o 1. Los posibles valores de n son entonces: $2 \cdot 5 = 10$, $2^2 \cdot 5 = 20$, $2 \cdot 5 \cdot 7 = 70$ y $2^2 \cdot 5 \cdot 7 = 140$.

- Posibles valores de $(a\, b\, (a + b) : a^2 + b^2)$ para $a \perp b$:

  Si aquí buscamos como siempre la forma de un divisor común d operando con las expresiones $a\, b\, (a + b)$ y $a^2 + b^2$, no podemos nunca independizarnos de a o de b. Pero podemos aprovechar la propiedad de caracterización de los primos para trabajar de la forma siguiente:

  Sea $c := (a\, b\, (a + b) : a^2 + b^2)$.

  Si $c \neq 1$, entonces existe un primo p (positivo) tal que $p \mid c$. Luego $p \mid a\, b\, (a+b)$ y $p \mid a^2 + b^2$. Ahora bien:

$$\left\{\begin{array}{c} p\,|\,a\,b\,(a+b) \\ \text{y} \\ p\,|\,a^2+b^2 \end{array}\right. \Rightarrow \left\{\begin{array}{ccccccc} p\,|\,a & \Rightarrow & p\,|\,b^2 & \Rightarrow & p\,|\,a \text{ y } p\,|\,b & \Rightarrow & \text{Contradiccón} \\ \text{ó} & & & & & & \\ p\,|\,b & \Rightarrow & p\,|\,a^2 & \Rightarrow & p\,|\,a \text{ y } p\,|\,b & \Rightarrow & \text{Contradicción} \\ \text{ó} & & & & & & \\ p\,|\,a+b & \Rightarrow & p\,|\,a^2-b^2 & \Rightarrow & p\,|\,2\,a^2 \text{ y } p\,|\,2\,b^2 & \Rightarrow & p|(2a^2:2b^2)=2 \end{array}\right.$$

Se concluye que el único primo posible divisor del mcd c es el primo 2. Luego $c = 2^k$ para algún $k \geq 0$. Vamos a analizar ahora qué valores posibles puede tomar k. Distinguemos los casos a par, b impar; a impar, b par; y a y b impares, es decir $a \equiv b \equiv 1 \pmod 2$ (dado que el caso a y b pares no se puede dar por ser $a \perp b$).

- $a \equiv 1 \pmod 2$ y $b \equiv 0 \pmod 2 \Rightarrow a^2 + b^2 \equiv 1 \pmod 2$, luego 2 no es un divisor común, es decir, $2 \nmid c$ en este caso. Por lo tanto $c = 1$.
- $a \equiv 0 \pmod 2$ y $b \equiv 1 \pmod 2$ es igual al caso anterior: $c = 1$.
- $a \equiv b \equiv 1 \pmod 2$: $2\,|\,a+b$ y $2\,|\,a^2+b^2 \Rightarrow 2\,|\,c \Rightarrow k \geq 1$.
  Además $c\,|\,a\,b\,(a+b)$ y $c = 2^k \perp a$, $c = 2^k \perp b$ implican $c = 2^k\,|\,a+b$. Junto con $c = 2^k\,|\,a^2+b^2$, el mismo análisis hecho arriba implica que $2^k\,|\,2\,(a^2 : b^2) = 2$, es decir $k \leq 1$. Por lo tanto en este caso $c = 2$

10 Mínimo Común Múltiplo

Definición 10.1 (Mínimo Común Múltiplo)

Sean $a, b \in \mathbb{Z}$, no nulos. El mínimo común múltiplo entre a y b es el menor de los múltiplos comunes positivos de a y b.
Claramente ese número existe*, ya que hay que buscarlo entre los múltiplos comunes positivos menores o iguales que $|a\,b|$, y es único, por ser el menor.*
El mínimo común múltiplo entre a y b se nota $\operatorname{mcm}(a,b)$ *o $[a : b]$ que es la notación que adoptamos aquí. Es entonces caracterizado por:*

$$[a:b] \in \mathbb{N}, \quad a\,|\,[a:b],\ b\,|\,[a:b] \quad \textit{y si } m \in \mathbb{N} \textit{ es tal que } a\,|\,m \textit{ y } b\,|\,m, \textit{ entonces } [a:b] \leq m.$$

Ejemplos

- $[a : b] = [-a : b] = [a : -b] = [-a : -b] = [|a| : |b|]$.
- Para todo $a \in \mathbb{Z}$, se tiene $[a : 1] = |a|$
- $b\,|\,a \iff [a : b] = |a|$.

Pero el mínimo común múltiplo también tiene una caracterización conocida en términos de los factores primos de los números a y b:

Observación 10.2

$$[a:b] = \prod_{p \in \mathcal{P}} p^{\max\{v_p(a), v_p(b)\}}. \tag{2}$$

Prueba.– Llamemos c al número de la derecha de la igualdad (2). Vamos a ver que $[a:b] \leq c$ y $c \leq [a:b]$.
Por un lado, como para todo $p \in \mathcal{P}$, $v_p(a) \leq \max\{v_p(a), v_p(b)\}$ y $v_p(b) \leq \max\{v_p(a), v_p(b)\}$, se tiene que $a \,|\, c$ y $b \,|\, c$. Luego $[a:b] \leq c$.
Pero por otro lado, $a \,|\, [a:b]$ y $b \,|\, [a:b]$ implica que para todo $p \in \mathcal{P}$, $v_p(a) \leq v_p([a:b])$ y $v_p(b) \leq v_p([a:b])$, luego $\max\{v_p(a), v_p(b)\} \leq v_p([a:b])$. Así $c \,|\, [a:b]$, y, al ser ambos positivos, $c \leq [a:b]$.

■

De la misma forma que se probó que si $a \,|\, [a:b]$ y $b \,|\, [a:b]$, entonces $c \,|\, [a:b]$ en la demostración anterior, se prueba que si $m \in \mathbb{Z}$ no nulo es tal $a \,|\, m$ y $b \,|\, m$, entonces $c \,|\, m$, pero c es el mínimo común múltiplo! Luego:

Consecuencia 10.3 *Sean $a, b, m \in \mathbb{Z}$ no nulos. Entonces:*

$$a \,|\, m \quad y \quad b \,|\, m \quad \Longrightarrow \quad [a:b] \,|\, m.$$

Ejemplo Sean $a = 2^7 \cdot 5^2 \cdot 7^6 \cdot 13$ y $b = -2^5 \cdot 3^4 \cdot 7^6 \cdot 13^2 \cdot 19$. Entonces

$$(a:b) = 2^5 \cdot 7^6 \cdot 13 \quad \text{y} \quad [a:b] = 2^7 \cdot 3^4 \cdot 5^2 \cdot 7^6 \cdot 13^2 \cdot 19.$$

Observemos que

$$|a \cdot b| = 2^{7+5} \cdot 3^{0+4} \cdot 5^{2+0} \cdot 7^{6+6} \cdot 13^{1+2} \cdot 19^{0+1} = 2^{5+7} \cdot 3^{0+4} \cdot 5^{0+2} \cdot 7^{6+6} \cdot 13^{1+2} \cdot 19^{0+1} = (a:b) \cdot [a:b].$$

Este hecho se generaliza ya que para todo $p \in \mathcal{P}$, se tiene que $v_p(a) + v_p(b) = \min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\}$:

Proposición 10.4 *Sean $a, b \in \mathbb{Z}$, no nulos, entonces*

$$|a \cdot b| = (a:b) \cdot [a:b].$$

En particular, si $a \perp b$, entonces $[a:b] = |a \cdot b|$.

■

Esto da una alternativa para calcular el mínimo común múltiplo cuando uno no conoce la factorización de los números. De hecho esta forma de calcular el mínimo común múltiplo es en el caso general mas veloz que factorizar los números para luego aplicar la fórmula (2), ya que calcular el máximo común divisor por el algoritmo de Euclides es en general más veloz que factorizar.

Ejemplo Determinación de todos los pares de números $a, b \in \mathbb{N}$ que verifican que

$$(a:b) = 2^2 \cdot 3 \cdot 17 \quad \text{y} \quad [a:b] = 2^5 \cdot 3 \cdot 5^2 \cdot 17^2 :$$

Se tiene que $a \cdot b = (a:b)[a:b] = 2^7 \cdot 3^2 \cdot 5^2 \cdot 17^3$, es decir $a = 2^i \cdot 3^j \cdot 5^k \cdot 17^\ell$ y $b = 2^{i'} \cdot 3^{j'} \cdot 5^{k'} \cdot 17^{\ell'}$, con

$$\begin{array}{lll} i + i' = 7, & \min\{i, i'\} = 2, & \max\{i, i'\} = 5 \\ j + j' = 2, & \min\{j, j'\} = 1, & \max\{j, j'\} = 1 \\ k + k' = 2, & \min\{k, k'\} = 0, & \max\{k, k'\} = 2 \\ \ell + \ell' = 3, & \min\{\ell, \ell'\} = 1, & \max\{\ell, \ell'\} = 2 \end{array}$$

Se deduce que $i = 2, i' = 5$ o $i = 5, i' = 2$, $j = j' = 1$, $k = 0, k' = 2$ o $k = 2, k' = 0$ y $\ell = 1, \ell' = 2$ o $\ell = 2, \ell' = 1$. Todos los pares posibles $a, b \in \mathbb{N}$ son entonces:

$$\begin{aligned}
a &= 2^2 \cdot 3^1 \cdot 5^0 \cdot 17^1 \quad , \quad b = 2^5 \cdot 3^1 \cdot 5^2 \cdot 17^2 \\
a &= 2^5 \cdot 3^1 \cdot 5^0 \cdot 17^1 \quad , \quad b = 2^2 \cdot 3^1 \cdot 5^2 \cdot 17^2 \\
a &= 2^2 \cdot 3^1 \cdot 5^2 \cdot 17^1 \quad , \quad b = 2^5 \cdot 3^1 \cdot 5^0 \cdot 17^2 \\
a &= 2^5 \cdot 3^1 \cdot 5^2 \cdot 17^1 \quad , \quad b = 2^2 \cdot 3^1 \cdot 5^0 \cdot 17^2 \\
a &= 2^2 \cdot 3^1 \cdot 5^0 \cdot 17^2 \quad , \quad b = 2^5 \cdot 3^1 \cdot 5^2 \cdot 17^1 \\
a &= 2^5 \cdot 3^1 \cdot 5^0 \cdot 17^2 \quad , \quad b = 2^2 \cdot 3^1 \cdot 5^2 \cdot 17^1 \\
a &= 2^2 \cdot 3^1 \cdot 5^2 \cdot 17^2 \quad , \quad b = 2^5 \cdot 3^1 \cdot 5^0 \cdot 17^1 \\
a &= 2^5 \cdot 3^1 \cdot 5^2 \cdot 17^2 \quad , \quad b = 2^2 \cdot 3^1 \cdot 5^0 \cdot 17^1
\end{aligned}$$

11 El Pequeño Teorema de Fermat (PTF)

Este teorema es uno de los tantos que debemos al abogado y matemático francés Pierre de Fermat (1601–1665). Fermat, el mayor *matemático amateur* de todos los tiempos, dejó una obra importantísima en Teoría de Números, además de ser un pionero en Teoría de Probabilidades, Cálculo Variacional y Geometría Analítica. Poseía la traducción latina de la Aritmética de Diofanto, realizada por Bachet a fines del Siglo XVI, y tenía la particularidad de escribir en los márgenes de ese libro enunciados matemáticos y comentarios, la mayoría de las veces sin demostraciones. El Pequeño Teorema fue luego demostrado y generalizado por el matemático suizo Leonhard Euler (1707–1783). Euler demostró la casi totalidad de los resultados enunciados por Fermat, con la excepción de la afirmación —inspirada en el teorema de Pitágoras— conocida como el "Ultimo Teorema de Fermat":

Cualquiera sea $n > 2$*, no existen* $a, b, c \in \mathbb{N}$ *tales que* $a^n + b^n = c^n$.

Este fue probado recién en los años 1993–1994 por el matemático inglés Andrew Wiles, con la ayuda parcial de su discípulo R. Taylor.

Teorema 11.1 (Pequeño Teorema de Fermat)
Sean $a \in \mathbb{Z}$ *y* p *un primo positivo. Entonces*

1. $a^p \equiv a \pmod{p}$
2. $\boxed{p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}}$

Observaciones

- El teorema es falso en general si p no es primo: por ejemplo $3^4 = 81 \not\equiv 3 \pmod{4}$.
- Sin embargo existen números n no primos para los cuales vale el enunciado del pequeño teorema: $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$. Esos números se suelen llamar "seudoprimos" o "primos de Carmichael" (por más que no sean primos) según el matemático que descubrió en 1909 el más chico de ellos, el número $n := 561 = 3 \cdot 11 \cdot 17$. En 1995 se probó que existen infinitos seudoprimos.
- Las dos afirmaciones del teorema son equivalentes:

  (*1* $\Rightarrow$ *2*): Por hipótesis, $a^p \equiv a \pmod{p}$. Si $p \nmid a$, es decir $a \perp p$, se puede simplificar un a de los dos lados (justificar!) y queda $a^{p-1} \equiv 1 \pmod{p}$.

(*2* $\Rightarrow$ *1*): Hay que probar que para $a \in \mathbb{Z}$ cualquiera, $a^p \equiv a \pmod p$. Si $p \nmid a$, por (*2*) vale que $a^{p-1} \equiv 1 \pmod p$, luego multiplicando por a se obtiene $a^p \equiv a \pmod p$. Mientras que si $p \mid a$, entonces tanto a como a^p son congruentes con 0 módulo p (pues p los divide, así, $a^p \equiv 0 \equiv a \pmod p$ también.

Prueba del Teorema 11.1.–

Por la observación anterior, para probar el Teorema alcanza con probar el caso (*2*) en que $p \nmid a$, es decir $a \perp p$, que es el caso interesante y no trivial.

Fijamos $a \in \mathbb{Z}$ tal que $p \nmid a$ y definimos la siguiente función:

$$\begin{array}{rccc} \Phi: & \{1,2,\ldots,p-1\} & \longrightarrow & \{1,2,\ldots,p-1\} \\ & i & \longmapsto & r_p(i\,a) \end{array}$$

Por ejemplo, $\Phi(1) = r_p(a)$, $\Phi(2) = r_p(2\,a)$, $\Phi(3) = r_p(3\,a)$, etc. (Observemos en particular que $\Phi(i) = r_p(i\,a) \equiv i\,a \pmod p$.)

Veamos primero que esta función está bien definida (es decir que la imagen $\mathrm{Im}(\Phi)$ de la función Φ realmente está incluída en el codominio) y luego que es biyectiva.

- $\mathrm{Im}(\Phi) \subseteq \{1,2,\ldots,p-1\}$:

  Por definición de resto módulo p, está claro que $\mathrm{Im}(\Phi) \subseteq \{0,1,2,\ldots,p-1\}$. Hay que probar que nunca se obtiene el 0, es decir que no existe $i \in \{1,\ldots,p-1\}$ tal que $\Phi(i) = 0$. Pero

  $$\Phi(i) = 0 \iff r_p(i\,a) = 0 \iff p \mid i\,a \underset{p \text{ primo}}{\iff} p \mid i \;\text{ ó }\; p \mid a,$$

  lo que es absurdo pues por hipótesis $p \nmid a$ y $p \nmid i$ por ser $i \in \{1,\ldots,p-1\}$.

- Para probar que Φ es biyectiva, dado que es una función de un conjunto finito en sí mismo, alcanza con probar que es inyectiva:

  Supongamos que para $1 \le j \le i \le p-1$, se tiene que $\Phi(i) = \Phi(j)$, queremos probar que entonces $i = j$. Pero de la misma forma que probamos la buena definición,

  $$\Phi(i) = \Phi(j) \iff r_p(i\,a) = r_p(j\,a) \iff p \mid i\,a - j\,a = (i-j)\,a \underset{p \text{ primo}}{\iff} p \mid i-j \;\text{ ó }\; p \mid a,$$

  lo que se cumple unicamente si $p \mid i-j$ pues $p \nmid a$. Ahora bien, como $1 \le j \le i \le p-1$, se tiene que $i-j \in \{0,\ldots,p-1\}$, luego

  $$p \mid i-j \iff i-j = 0 \iff i = j.$$

- Por lo tanto Φ es biyectiva, es decir suryectiva también. Así

  $$\begin{gathered} \mathrm{Im}(\Phi) = \{1,2,\ldots,p-1\} \implies \Phi(1)\cdot\Phi(2)\cdots\Phi(p-1) = 1\cdot 2\cdots(p-1) \implies \\ r_p(a)\cdot r_p(2\,a)\cdots r_p((p-1)\,a) = 1\cdot 2\cdots(p-1) \implies \\ a\cdot 2\,a\cdots(p-1)\,a \equiv 1\cdot 2\cdots(p-1) \pmod p \implies \\ (p-1)!\,a^{p-1} \equiv (p-1)! \pmod p \implies a^{p-1} \equiv 1 \pmod p, \end{gathered}$$

  pues se puede simplificar $(p-1)!$ en el último renglón dado que $p \nmid (p-1)!$ (ya que $p \mid (p-1)!$ si y solo si existe i con $1 \le i \le p-1$ tal que $p \mid i$).

■

Consecuencia 11.2 *Sean* $a \in \mathbb{Z}, n \in \mathbb{N}$ *y* p *primo positivo. Si* $p \nmid a$, *entonces* $n \equiv r \pmod{(p-1)} \implies a^n \equiv a^r \pmod{p}$. *En particular:*

$$\boxed{p \nmid a \quad \Longrightarrow \quad a^n \equiv a^{r_{p-1}(n)} \pmod{p}}$$

Prueba.–

$$n = k\,(p-1) + r \implies a^n = a^{k(p-1)+r} = (a^{(p-1)})^k\, a^r \underset{p \nmid a}{\equiv} 1^k\, a^r \equiv a^r \pmod{p}.$$

■

Ejemplos

- $r_{11}(27^{2154})$:

  Como $27 \equiv 5 \pmod{11}$, $27^{2154} \equiv 5^{2154} \pmod{11}$, y como $11 \nmid 5$, se tiene que

  $$2154 \equiv 4 \pmod{10} \implies 5^{2154} \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9 \pmod{11}.$$

  Por lo tanto $r_{11}(27^{2154}) = 9$.

- $r_{11}(24^{13^{1521}})$:

  $$\begin{array}{l} 24^{13^{1521}} \equiv 2^{13^{1521}} \pmod{11} \quad \text{y} \quad 11 \nmid 2 \implies \quad 13^{1521} \equiv ? \pmod{10} \\ 13^{1521} \equiv 3^{1521} \equiv (3^2)^{760}\, 3 \equiv (-1)^{760}\, 3 \equiv 3 \pmod{10} \implies \\ 2^{13^{1521}} \equiv 2^3 \equiv 8 \pmod{11}. \end{array}$$

  Por lo tanto $r_{11}(24^{13^{1521}}) = 8$.

- Determinación de los $n \in \mathbb{N}$ tales que $4^n \equiv 1 \pmod{7}$:

  $4^n \equiv 4^r \pmod{7}$ si $n \equiv r \pmod{6}$, por el PTF ya que $7 \nmid 4$. Luego alcanza con investigar los valores de 4^r con $0 \le r < 6$:

  $$\begin{array}{lll} n \equiv 0 \pmod{6} & \implies & 4^n \equiv 4^0 \equiv 1 \pmod{7} \\ n \equiv 1 \pmod{6} & \implies & 4^n \equiv 4^1 \equiv 4 \pmod{7} \\ n \equiv 2 \pmod{6} & \implies & 4^n \equiv 4^2 \equiv 2 \pmod{7} \\ n \equiv 3 \pmod{6} & \implies & 4^n \equiv 4^3 \equiv 4^2 \cdot 4 \equiv 2 \cdot 4 \equiv 1 \pmod{7} \\ n \equiv 4 \pmod{6} & \implies & 4^n \equiv 4^4 \equiv 4^3 \cdot 4 \equiv 1 \cdot 4 \equiv 4 \pmod{7} \\ n \equiv 5 \pmod{6} & \implies & 4^n \equiv 4^5 \equiv 4^3 \cdot 4^2 \equiv 1 \cdot 2 \equiv 2 \pmod{7} \end{array}$$

  Se concluye que $4^n \equiv 1 \pmod{7} \iff n \equiv 1 \pmod{6}$ ó $n \equiv 3 \pmod{6}$, es decir:

  $$4^n \equiv 1 \pmod{7} \iff n \equiv 0 \pmod{3}.$$

- $\forall\, n \in \mathbb{N},\ 7 \mid a^{360} - a^{60}$:

  Aquí para usar la versión más rápida del PTF, hay que separar los casos en que $7 \mid a$ y $7 \nmid a$:

  $$\begin{array}{lllllllll} 7 \mid a & \implies & a^{360} \equiv 0 \pmod{7} & \text{y} & a^{60} \equiv 0 \pmod{7} & \implies & a^{360} \equiv a^{60} \pmod{7} \\ 7 \nmid a & \implies & a^{360} \equiv 1 \pmod{7} & \text{y} & a^{60} \equiv 1 \pmod{7} & \implies & a^{360} \equiv a^{60} \pmod{7} \end{array}$$

  Por lo tanto, en ambos casos, $a^{360} \equiv a^{60} \pmod{7}$.

12 Teorema Chino del Resto (TCR)

Se trata ahora de resolver sistemas de ecuaciones de congruencia de la forma

$$\left\{\begin{array}{rcll} x & \equiv & a_1 & (\mathrm{mod}\ m_1) \\ x & \equiv & a_2 & (\mathrm{mod}\ m_2) \\ & \vdots & & \\ x & \equiv & a_n & (\mathrm{mod}\ m_n) \end{array}\right. \tag{3}$$

donde $a_1, \ldots, a_n \in \mathbb{Z}$ y $m_1, \ldots, m_n \in \mathbb{N}$.

Se utilizarán sistematicamente las propiedades siguientes que ya mencionamos antes, además del hecho que ya sabemos resolver una ecuación de congruencia (Sección 8):

- Propiedades 3.3: $x \equiv a \pmod{m}$ y $n \,|\, m \implies x \equiv a \pmod{n}$ y para $c \neq 0$: $x \equiv a \pmod{m} \iff c\,x \equiv c\,a \pmod{(c\,m)}$.
- Proposición 6.9 (1): Sean $m_1, m_2, \ldots, m_n \in \mathbb{N}$ con $\underline{m_i \perp m_j \text{ para } i \neq j}$. Luego

$$\left\{\begin{array}{rcll} x & \equiv & a & (\mathrm{mod}\ m_1) \\ x & \equiv & a & (\mathrm{mod}\ m_2) \\ & \vdots & & \\ x & \equiv & a & (\mathrm{mod}\ m_n) \end{array}\right. \iff \quad x \equiv a \pmod{m_1 \cdot m_2 \cdots m_n} \tag{4}$$

Ejemplos

- $$\left\{\begin{array}{rcll} x & \equiv & 3 & (\mathrm{mod}\ 22) \\ x & \equiv & 3 & (\mathrm{mod}\ 5) \\ x & \equiv & 3 & (\mathrm{mod}\ 21) \end{array}\right. \iff x \equiv 3 \pmod{22 \cdot 5 \cdot 21},$$

  por la Propiedad (4), pues $22 = 2 \cdot 11$, 5 y $21 = 3 \cdot 7$ son coprimos dos a dos.

- De la misma forma:

$$x \equiv 50 \pmod{22 \cdot 5 \cdot 21} \iff \left\{\begin{array}{rcll} x & \equiv & 50 & (\mathrm{mod}\ 22) \\ x & \equiv & 50 & (\mathrm{mod}\ 5) \\ x & \equiv & 50 & (\mathrm{mod}\ 21) \end{array}\right. \iff \left\{\begin{array}{rcll} x & \equiv & 6 & (\mathrm{mod}\ 22) \\ x & \equiv & 0 & (\mathrm{mod}\ 5) \\ x & \equiv & 8 & (\mathrm{mod}\ 21) \end{array}\right.$$

- $$\left\{\begin{array}{rcll} x & \equiv & 3 & (\mathrm{mod}\ 22) \\ x & \equiv & 4 & (\mathrm{mod}\ 11) \end{array}\right. \iff \left\{\begin{array}{rcll} x & \equiv & 3 & (\mathrm{mod}\ 2) \\ x & \equiv & 3 & (\mathrm{mod}\ 11) \\ x & \equiv & 4 & (\mathrm{mod}\ 11) \end{array}\right. \iff \left\{\begin{array}{rcll} x & \equiv & 1 & (\mathrm{mod}\ 2) \\ x & \equiv & 3 & (\mathrm{mod}\ 11) \\ x & \equiv & 4 & (\mathrm{mod}\ 11) \end{array}\right.$$

  y luego el sistema no tiene solución (es <u>incompatible</u>) pues la segunda y la tercer ecuación a la derecha no pueden verificarse al mismo tiempo.

- $$\left\{\begin{array}{rcll} x & \equiv & 3 & (\mathrm{mod}\ 22) \\ x & \equiv & 4 & (\mathrm{mod}\ 8) \end{array}\right. \iff \left\{\begin{array}{rcll} x & \equiv & 1 & (\mathrm{mod}\ 2) \\ x & \equiv & 3 & (\mathrm{mod}\ 11) \\ x & \equiv & 4 & (\mathrm{mod}\ 8) \end{array}\right.$$

  y luego es incompatible pues la tercer ecuación a la derecha implica en particular que $x \equiv 4 \pmod{2}$, es decir $x \equiv 0 \pmod{2}$, que es claramente incompatible con la primer ecuación.

- $$\left\{\begin{array}{rcll} x & \equiv & 1 & (\mathrm{mod}\ 4) \\ x & \equiv & 5 & (\mathrm{mod}\ 8) \end{array}\right. \iff x \equiv 5 \pmod 8$$

  pues si se cumple la segunda ecuación, se cumple automaticamente la primera: $x \equiv 5 \pmod 8 \Longrightarrow x \equiv 5 \pmod 4 \Longrightarrow x \equiv 1 \pmod 4$.

- $$\left\{\begin{array}{rcll} x & \equiv & 3 & (\mathrm{mod}\ 22) \\ x & \equiv & 5 & (\mathrm{mod}\ 8) \\ x & \equiv & 17 & (\mathrm{mod}\ 20) \end{array}\right. \iff \left\{\begin{array}{rcll} x & \equiv & 1 & (\mathrm{mod}\ 2) \\ x & \equiv & 3 & (\mathrm{mod}\ 11) \\ x & \equiv & 5 & (\mathrm{mod}\ 8) \\ x & \equiv & 1 & (\mathrm{mod}\ 4) \\ x & \equiv & 2 & (\mathrm{mod}\ 5) \end{array}\right. \iff \left\{\begin{array}{rcll} x & \equiv & 5 & (\mathrm{mod}\ 8) \\ x & \equiv & 3 & (\mathrm{mod}\ 11) \\ x & \equiv & 2 & (\mathrm{mod}\ 5) \end{array}\right.$$

  pues la ecuación $x \equiv 5 \pmod 8$ implica que $x \equiv 5 \pmod 4$ y $x \equiv 5 \pmod 2$, es decir $x \equiv 1 \pmod 2$ y $x \equiv 1 \pmod 4$ (si en el medio se cumple la tercera se cumplen automaticamente la primera y la última).

En estos ejemplos se ve que cuando el sistema no es incompatible, se reduce a resolver un sistema (3) **pero con la condición de que los m_i son coprimos dos a dos**. En esa situación vale el teorema siguiente:

Teorema 12.1 (Teorema Chino del Resto)
Sean $a_1, \ldots, a_n \in \mathbb{Z}$ y sean $m_1, \ldots, m_n \in \mathbb{N}$ con $m_i \perp m_j$ para $i \neq j$. Entonces existe $a \in \mathbb{Z}$ tal que

$$\left\{\begin{array}{rcll} x & \equiv & a_1 & (\mathrm{mod}\ m_1) \\ x & \equiv & a_2 & (\mathrm{mod}\ m_2) \\ & \vdots & & \\ x & \equiv & a_n & (\mathrm{mod}\ m_n) \end{array}\right. \iff \quad x \equiv a \pmod{m_1 \cdot m_2 \cdots m_n}$$

Prueba.–
Se trata de encontrar una solución particular $a \in \mathbb{Z}$ del sistema, es decir un número $a \in \mathbb{Z}$ tal que

$$\left\{\begin{array}{rcll} a & \equiv & a_1 & (\mathrm{mod}\ m_1) \\ a & \equiv & a_2 & (\mathrm{mod}\ m_2) \\ & \vdots & & \\ a & \equiv & a_n & (\mathrm{mod}\ m_n) \end{array}\right. .$$

Pues en ese caso, por transitividad y aplicando la Propiedad (4), tendremos:

$$\left\{\begin{array}{rcll} x & \equiv & a_1 & (\mathrm{mod}\ m_1) \\ x & \equiv & a_2 & (\mathrm{mod}\ m_2) \\ & \vdots & & \\ x & \equiv & a_n & (\mathrm{mod}\ m_n) \end{array}\right. \iff \left\{\begin{array}{rcll} x & \equiv & a & (\mathrm{mod}\ m_1) \\ x & \equiv & a & (\mathrm{mod}\ m_2) \\ & \vdots & & \\ x & \equiv & a & (\mathrm{mod}\ m_n) \end{array}\right. \iff x \equiv a \pmod{m_1 \cdot m_2 \cdots m_n}.$$

Para hallar una solución particular a vamos a subdividir el sistema (3) en n sistemas más simples y buscar una solución particular para cada uno de ellos. Estos sistemas S_1, S_2, $\ldots$, S_n son:

$$\underline{S_1}: \qquad \underline{S_2}: \qquad \underline{S_n}:$$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ x \equiv 0 \pmod{m_3} \\ \vdots \\ x \equiv 0 \pmod{m_n} \end{cases} \text{ y } \begin{cases} x \equiv 0 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv 0 \pmod{m_3} \\ \vdots \\ x \equiv 0 \pmod{m_n} \end{cases} \text{ y } \cdots \text{ y } \begin{cases} x \equiv 0 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \vdots \\ x \equiv 0 \pmod{m_{n-1}} \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Supongamos que para cada uno de estos sistemas S_ℓ, $1 \leq \ell \leq n$, encontramos una solución particular x_ℓ. Entonces si definimos

$$a := x_1 + x_2 + x_3 + \cdots + x_n,$$

se verifica que

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_n \equiv a_1 + 0 + 0 + \cdots + 0 \pmod{m_1} \\ x_1 + x_2 + x_3 + \cdots + x_n \equiv 0 + a_2 + 0 + \cdots + 0 \pmod{m_2} \\ \vdots \\ x_1 + x_2 + x_3 + \cdots + x_n \equiv 0 + 0 + \cdots + 0 + a_n \pmod{m_n} \end{cases} \Longrightarrow \begin{cases} a \equiv a_1 \pmod{m_1} \\ a \equiv a_2 \pmod{m_2} \\ \vdots \\ a \equiv a_n \pmod{m_n} \end{cases}$$

es decir, a es una solución particular, como se buscaba.

Aplicando lo que se hizo en la Sección 8, vamos a ver que todos los sistemas S_ℓ, $1 \leq \ell \leq n$, admiten soluciones y vamos a elegir para cada uno de ellos una solución particular x_ℓ.

Miremos el sistema S_1:
Como $m_2, m_3, \ldots, m_n$ son todos coprimos entre sí, si ponemos $M_1 := m_2 \cdot m_3 \cdots m_n$, se tienen las equivalencias

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ x \equiv 0 \pmod{m_3} \\ \vdots \\ x \equiv 0 \pmod{m_n} \end{cases} \Longleftrightarrow \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv 0 \pmod{M_1} \end{cases} \Longleftrightarrow \begin{cases} x = M_1\, y \\ \text{con} \\ M_1\, y \equiv a_1 \pmod{m_1} \end{cases}$$

(Verificar la equivalencia de la derecha). Pero la ecuación de congruencia

$$M_1\, y \equiv a_1 \pmod{m_1} \tag{5}$$

admite soluciones pues $M_1 \perp m_1$ (por ser $M_1 = m_2 \cdots m_n$ y los m_i coprimos dos a dos). Sea y_1 una solución particular de (5). Luego $x_1 := m_1\, y_1$ es una solución particular del sistema S_1.

De la misma forma, probemos que para todo ℓ, $1 \leq \ell \leq n$, el sistema

$$S_\ell: \quad \begin{cases} x \equiv 0 \pmod{m_1} \\ \vdots \\ x \equiv 0 \pmod{m_{\ell-1}} \\ x \equiv a_\ell \pmod{m_\ell} \\ x \equiv 0 \pmod{m_{\ell+1}} \\ \vdots \\ x \equiv 0 \pmod{m_n} \end{cases}$$

admite soluciones y por lo tanto se puede elegir para él una solución particular x_ℓ.

Definamos $M_\ell := \prod_{j\neq\ell} m_j$. Se tiene $M_\ell \perp m_\ell$ por ser todos los m_i coprimos dos a dos. Luego la ecuación de congruencia

$$M_\ell\, y \equiv a_\ell \pmod{m_\ell}$$

admite soluciones, y si y_ℓ es una solución particular de esa ecuación, entonces, como arriba, $x_\ell := M_\ell\, y_\ell$ es una solución particular del sistema S_ℓ.

■

Ejemplos

- $$\begin{cases} x \equiv 4 \pmod 8 \\ x \equiv 10 \pmod{35} \\ x \equiv 1 \pmod 3 \end{cases}$$

  Como 8, 35 y 3 son coprimos 2 a 2, por el Teorema 12.1, existe $a \in \mathbb{Z}$ tal que el sistema es equivalente a $x \equiv a \pmod{8\cdot 35\cdot 3}$, es decir $x \equiv a \pmod{840}$.

  Se consideran los tres sistemas:

  $\underline{S_1}$:
  $$\begin{cases} x \equiv 4 \pmod 8 \\ x \equiv 0 \pmod{35} \\ x \equiv 0 \pmod 3 \end{cases}$$

  $\underline{S_2}$:
  $$\begin{cases} x \equiv 0 \pmod 8 \\ x \equiv 10 \pmod{35} \\ x \equiv 0 \pmod 3 \end{cases}$$

  $\underline{S_3}$:
  $$\begin{cases} x \equiv 0 \pmod 8 \\ x \equiv 0 \pmod{35} \\ x \equiv 1 \pmod 3 \end{cases}$$

  Solución particular para S_1:

  $$\begin{cases} x \equiv 4 \pmod 8 \\ x \equiv 0 \pmod{35} \\ x \equiv 0 \pmod 3 \end{cases} \iff \begin{cases} x = 35\cdot 3\cdot y \\ \text{con} \\ 35\cdot 3\cdot y \equiv 4 \pmod 8 \end{cases} \iff \begin{cases} x = 105\, y \\ \text{con} \\ y \equiv 4 \pmod 8 \end{cases}$$

  Luego, una solución particular es $y_1 = 4$, por lo tanto $x_1 = 105\, y_1 = 420$.

  Solución particular para S_2:

  $$\begin{cases} x \equiv 0 \pmod 8 \\ x \equiv 10 \pmod{35} \\ x \equiv 0 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} x = 8\cdot 3\cdot y \\ \text{con} \\ 8\cdot 3\cdot y \equiv 10 \pmod{35} \end{cases} \Leftrightarrow \begin{cases} x = 24\, y \\ \text{con} \\ 24\, y \equiv 10 \pmod{35} \end{cases}$$

  Aplicando el algoritmo de Euclides se obtiene que

  $$\begin{aligned} 1 = 11\cdot 35 - 16\cdot 24 &\implies 24\cdot(-16) \equiv 1 \pmod{35} \\ &\implies 24\cdot(-160) \equiv 10 \pmod{35} \implies 24\cdot 15 \equiv 10 \pmod{35}. \end{aligned}$$

  Luego, una solución particular es $y_2 = 15$, y por lo tanto $x_2 = 24\, y_2 = 360$.

  Solución particular para S_3:

  $$\begin{cases} x \equiv 0 \pmod 8 \\ x \equiv 0 \pmod{35} \\ x \equiv 1 \pmod 3 \end{cases} \iff \begin{cases} x = 8\cdot 35\cdot y \\ \text{con} \\ 8\cdot 35\cdot y \equiv 1 \pmod 3 \end{cases} \iff \begin{cases} x = 280\, y \\ \text{con} \\ y \equiv 1 \pmod 3 \end{cases}$$

  Luego, una solución particular es $y_3 = 1$, por lo tanto $x_3 = 280\, y_3 = 280$.

Por lo tanto, aplicando la construcción del Teorema 12.1, $a := x_1+x_2+x_3 = 240+360+280 = 1060$ verifica que el sistema original es equivalente a $x \equiv 1060 \pmod{840}$. Claramente se puede achicar a utilizando que $1060 \equiv 220 \pmod{840}$, y de esa manera se obtiene $0 \leq a < 840$:

$$\left\{ \begin{array}{rcll} x & \equiv & 4 & (\text{mod } 8) \\ x & \equiv & 10 & (\text{mod } 35) \\ x & \equiv & 1 & (\text{mod } 3) \end{array} \right. \iff x \equiv 220 \pmod{840}.$$

- $$\left\{ \begin{array}{rcll} x & \equiv & 3 & (\text{mod } 10) \\ x & \equiv & 1 & (\text{mod } 11) \\ x & \equiv & 3 & (\text{mod } 7) \end{array} \right.$$

  Nuevamente, $10, 11$ y 7 son coprimos 2 a 2, luego por el teorema existe a tal que el sistema es equivalente a $x \equiv a \pmod{10 \cdot 11 \cdot 7}$, es decir $x \equiv a \pmod{770}$. Ahora bien, la primera y la tercer ecuación se pueden juntar claramente en la ecuación $x \equiv 3 \pmod{70}$, luego es suficiente aquí considerar los dos sistemas:

  $$\underline{S_1}: \quad \left\{ \begin{array}{rcll} x & \equiv & 3 & (\text{mod } 70) \\ x & \equiv & 0 & (\text{mod } 11) \end{array} \right. \qquad \underline{S_2}: \quad \left\{ \begin{array}{rcll} x & \equiv & 0 & (\text{mod } 70) \\ x & \equiv & 1 & (\text{mod } 11) \end{array} \right.$$

  Solución particular para S_1:

  $$\left\{ \begin{array}{rcll} x & \equiv & 3 & (\text{mod } 70) \\ x & \equiv & 0 & (\text{mod } 11) \end{array} \right. \iff \left\{ \begin{array}{rcll} x & = & 11\,y & \\ & \text{con} & & \\ 11\,y & \equiv & 3 & (\text{mod } 70) \end{array} \right. \iff \left\{ \begin{array}{rcll} x & = & 11\,y & \\ & \text{con} & & \\ y & \equiv & 13 & (\text{mod } 70) \end{array} \right.$$

  Luego, una solución particular es $y_1 = 13$, por lo tanto $x_1 = 11\,y_1 = 143$.

  Solución particular para S_2:

  $$\left\{ \begin{array}{rcll} x & \equiv & 0 & (\text{mod } 70) \\ x & \equiv & 1 & (\text{mod } 11) \end{array} \right. \iff \left\{ \begin{array}{rcll} x & = & 70\,y & \\ & \text{con} & & \\ 70\,y & \equiv & 1 & (\text{mod } 11) \end{array} \right. \iff \left\{ \begin{array}{rcll} x & = & 70\,y & \\ & \text{con} & & \\ 4\,y & \equiv & 1 & (\text{mod } 11) \end{array} \right.$$

  La ecuación $4\,y \equiv 1 \pmod{11}$ admite a 3 como solución particular. Tomamos $y_2 = 3$, por lo tanto $x_2 = 70\,y_2 = 210$.

  Así, $a := x_1 + x_2 = 143 + 210 = 353$. Se tiene:

  $$\left\{ \begin{array}{rcll} x & \equiv & 3 & (\text{mod } 10) \\ x & \equiv & 1 & (\text{mod } 11) \\ x & \equiv & 3 & (\text{mod } 7) \end{array} \right. \iff x \equiv 353 \pmod{770}.$$

Observación 12.2 *Una consecuencia inmediata del TCR es que existe un único a, con $0 \leq a < m_1 \cdot m_2 \cdots m_n$, tal que el sistema original es equivalente a $x \equiv a \pmod{m_1 m_2 \cdots m_n}$.*
Así, si se conoce los restos de x al dividirlo por m_1, m_2,..., y m_n, entonces se conoce el resto de x al dividirlo por $m_1 \cdot m_2 \cdots m_n$.

Ejemplos

- Retomemos el segundo ejemplo arriba: $x \equiv 3 \pmod{70}$ y $x \equiv 1 \pmod{11}$: Sabemos que existe a con $0 \leq a < 770$ que verifica el sistema y que es único en esas condiciones. Investiguemos los valores entre 0 y 770 que cumplen la primer ecuación. Estos son:

$$3, 73, 143, 213, 283, 353, 423, 493, ...$$

Entre ellos, ¿cuál es el que cumple también la segunda ecuación?

$$\not{3},\ \not{7}3,\ 1\not{4}3,\ 2\not{1}3,\ 2\not{8}3,\ \boxed{353}, \ldots$$

Ya está! encontramos uno, entonces es ese!

- Volvamos al último ejemplo antes del enunciado del TCR:

$$\begin{cases} x \equiv 3 & (\text{mod } 22) \\ x \equiv 5 & (\text{mod } 8) \\ x \equiv 17 & (\text{mod } 20) \end{cases} \iff \begin{cases} x \equiv 5 & (\text{mod } 8) \\ x \equiv 3 & (\text{mod } 11) \\ x \equiv 2 & (\text{mod } 5) \end{cases}$$

Como 8, 11 y 5 son coprimos dos a dos, sabemos que existe un único a con $0 \leq a < 8 \cdot 11 \cdot 5 = 440$ que verifica el sistema. Empecemos por investigar los que cumplen las dos ecuaciones con el módulo más grande. Para ello escribimos primero los los números entre 0 y $11 \cdot 8 = 88$ que cumplen la ecuación con el módulo 11:

$$3, 14, 25, 36, 47, 58, 69, \ldots$$

¿Cuál cumple la condición con el módulo 8?

$$\not{3},\ 1\not{4},\ 2\not{5},\ 3\not{6},\ 4\not{7},\ 5\not{8}, \boxed{69},\ 80, \ldots$$

Luego los que resuelven esas dos ecuaciones son $x \equiv 69 \pmod{88}$. Ahora, escribimos los números entre 0 y 440 que cumplen esa condición e investigamos cuál es el que cumple la ecuación con el módulo 5:

$$6\not{9},\ \boxed{157}, \ldots$$

Ya está!

$$\begin{cases} x \equiv 3 & (\text{mod } 22) \\ x \equiv 5 & (\text{mod } 8) \\ x \equiv 17 & (\text{mod } 20) \end{cases} \iff x \equiv 157 \pmod{440}.$$

- $$\begin{cases} 3\,x \equiv 2 & (\text{mod } 7) \\ 7\,x \equiv 5 & (\text{mod } 8) \\ 6\,x \equiv 8 & (\text{mod } 10) \end{cases}$$

Primero hay que resolver cada ecuación y dejarla en la forma $x \equiv \ldots$ Entonces:

$$\begin{cases} 3\,x \equiv 2\ (7) \\ 7\,x \equiv 5\ (8) \\ 6\,x \equiv 8\ (10) \end{cases} \iff \begin{cases} x \equiv 3\ (7) \\ x \equiv 3\ (8) \\ 3\,x \equiv 4\ (5) \end{cases} \iff \begin{cases} x \equiv 3\ (7) \\ x \equiv 3\ (8) \\ x \equiv 3\ (5) \end{cases} \iff x \equiv 3\ (280)$$

pues 7, 8 y 5 son coprimos dos a dos.

- Si $r_9(4\,x)=2$, $r_{14}(3\,x)=5$ y $r_{20}(3\,x)=1$, cálculo de los posibles restos de dividir a x por $9\cdot 14\cdot 20=2520$:

$$\left\{\begin{array}{lcl} 4\,x & \equiv & 2\ (9)\\ 3\,x & \equiv & 5\ (14)\\ 3\,x & \equiv & 1\ (20)\end{array}\right. \iff \left\{\begin{array}{lcl} 2\,x & \equiv & 1\ (9)\\ 3\,x & \equiv & 5\ (2)\\ 3\,x & \equiv & 5\ (7)\\ 3\,x & \equiv & 1\ (4)\\ 3\,x & \equiv & 1\ (5)\end{array}\right. \iff \left\{\begin{array}{lcl} x & \equiv & 5\ (9)\\ x & \equiv & 1\ (2)\\ x & \equiv & 4\ (7)\\ x & \equiv & 3\ (4)\\ x & \equiv & 2\ (5)\end{array}\right. \iff \left\{\begin{array}{lcl} x & \equiv & 5\ (9)\\ x & \equiv & 4\ (7)\\ x & \equiv & 3\ (4)\\ x & \equiv & 2\ (5)\end{array}\right.$$

pues la ecuación $x\equiv 3\ (4)$ implica $x\equiv 1\ (2)$. Al resolver este sistema se obtiene

$$x\equiv 1607\ (9\cdot 7\cdot 4\cdot 5).$$

Luego los posibles restos de dividir a x por 2520 son 1607 y $1607+1260=2867$, los dos números entre 0 y 2520 que son congruentes con 1607 módulo 1260.

13 Miscelánea

En esta sección se dan ejemplos que conectan varios de los resultados vistos. En la medida de lo posible se enuncia en cada paso el resultado que se aplica y se justifica que se está en las condiciones de aplicarlo. Se recomienda controlar en detalle cada uno de esos pasos y efectuar las cuentas que faltan.

- Resto de dividir $n:=3^{2^{25}}$ por 390:

  Como $390=2\cdot 3\cdot 5\cdot 13$ es un producto de primos distintos, se puede averiguar el resto de dividir n por cada uno de esos primos (aplicando si necesario el PTF) y luego combinar los resultados por medio del TCR.

  $\underline{r_2(n)}$:
  $$3^{2^{25}}\equiv 1^{2^{25}}\equiv 1 \pmod 2.$$

  $\underline{r_3(n)}$:
  $$3^{2^{25}}\equiv 0^{2^{25}}\equiv 0 \pmod 3.$$

  $\underline{r_5(n)}$:
  Por el PTF (Consecuencia 11.2),
  $$3^{2^{25}}\underset{5\nmid 3}{\equiv} 3^{r_4(2^{25})}\underset{4\,|\,2^{25}}{\equiv} 3^0\equiv 1 \pmod 5.$$

  $\underline{r_{13}(n)}$:
  Como $13\nmid 3$, para aplicar el PTF, necesitamos conocer $r_{12}(2^{25})$:
  $$2^{25}\underset{3\nmid 2}{\equiv} 2^{r_2(25)}\equiv 2^1\equiv 2 \pmod 3 \quad\text{y}\quad 2^{25}\equiv 0 \pmod 4 \underset{\text{TCR}}{\implies} 2^{25}\equiv 8 \pmod{12}.$$

  Así,
  $$3^{2^{25}}\equiv 3^{r_{12}(2^{25})}\equiv 3^8\equiv (3^3)^2\cdot 3^2\equiv 9 \pmod{13}$$

$\underline{r_{390}(n)}$:

$$\left\{\begin{array}{ll} n\equiv 1 & (\mathrm{mod}\ \ 2)\\ n\equiv 0 & (\mathrm{mod}\ \ 3)\\ n\equiv 1 & (\mathrm{mod}\ \ 5)\\ n\equiv 9 & (\mathrm{mod}\ 13)\end{array}\right. \underset{\text{TCR}}{\iff} \quad n\equiv 321 \pmod{390}$$

Se concluye que $r_{390}(3^{2^{25}}) = 321$.

- Determinación de todos los $a\in\mathbb{Z}$ tales que $(12\,a^{41}-a^{31}-a : 55) = 11$:

  Como $55 = 5\cdot 11$, para $b\in\mathbb{Z}$ cualquiera el valor de $(b:55)$ puede ser 1, 5, 11 o 55. Luego, se verifica que $(b:55)=11 \iff 11\,|\,b$ y $5\nmid b$. Determinamos entonces para qué valores de $a\in\mathbb{Z}$, $11\,|\,12\,a^{41}-a^{31}-a$ y $5\nmid 12\,a^{41}-a^{31}-a$:

  $\underline{\text{Para el } 11}$:

  $$11\,|\,12\,a^{41}-a^{31}-a = a\,(12\,a^{40}-a^{30}-1) \underset{11 \text{ primo}}{\iff} 11\,|\,a \ \text{ ó } \ 11\,|\,12\,a^{40}-a^{30}-1.$$

  Pero si $11\nmid a$, por el PTF, $a^n\equiv a^{r_{10}(n)} \pmod{11}$. Luego en ese caso,

  $$12\,a^{40}-a^{30}-1\equiv 1\,a^0-a^0-1\equiv 1 \pmod{11} \implies 11\nmid a^{40}-a^{30}-1.$$

  Por lo tanto

  $$11\,|\,12\,a^{41}-a^{31}-a \iff 11\,|\,a.$$

  $\underline{\text{Para el } 5}$:

  $$5\,|\,12\,a^{41}-a^{31}-a = a\,(12\,a^{40}-a^{30}-1) \underset{5 \text{ primo}}{\iff} 5\,|\,a \ \text{ ó } \ 5\,|\,12\,a^{40}-a^{30}-1.$$

  Pero si $5\nmid a$, entonces, por el PTF, $12\,a^{40}-a^{30}-1\equiv 2\,a^0-a^2-1\equiv 1-a^2 \pmod{5}$. Mirando las posibles congruencias de $a^2 \pmod 5$, se tiene

  $$1-a^2\equiv 0 \pmod 5 \iff a^2\equiv 1 \pmod 5 \iff a\equiv 1 \text{ ó } 4 \pmod 5.$$

  Por lo tanto

  $$\begin{aligned} 5\,|\,12\,a^{41}-a^{31}-a &\iff a\equiv 0 \text{ ó } 1 \text{ ó } 4 \pmod 5,\\ 5\nmid 12\,a^{41}-a^{31}-a &\iff a\equiv 2 \text{ ó } 3 \pmod 5.\end{aligned}$$

  Se concluye aplicando el TCR:

  $$\begin{aligned}(12\,a^{41}-a^{31}-a : 55) = 11 &\iff \left\{\begin{array}{l} a\equiv 0 \pmod{11}\\ a\equiv 2 \text{ ó } 3 \pmod 5\end{array}\right.\\ &\iff a\equiv 22 \text{ ó } 33 \pmod{55}.\end{aligned}$$

- Determinación de todos los $a\in\mathbb{Z}$ tal que $a\equiv 1 \pmod 4$ y $(11\,a+3\cdot 2^{150} : 3\,a-2^{151}) = 31$:

  Veamos primero cuáles son los posibles valores del mcd para ver las condiciones que necesitamos. Sea d un divisor común. Entonces:

  $$\left\{\begin{array}{l} d\,|\,11\,a+3\cdot 2^{150}\\ d\,|\,3\,a-2^{151}\end{array}\right. \implies \left\{\begin{array}{l} d\,|\,33\,a+9\cdot 2^{150}\\ d\,|\,33\,a-11\cdot 2^{151}\end{array}\right. \implies d\,|\,31\cdot 2^{150}.$$

$$\left\{\begin{array}{l} d \,|\, 11\,a + 3\cdot 2^{150} \\ d \,|\, 3\,a - 2^{151} \end{array}\right. \implies \left\{\begin{array}{l} d \,|\, 22\,a + 3\cdot 2^{151} \\ d \,|\, 9\,a - 3\cdot 2^{151} \end{array}\right. \implies d \,|\, 31\cdot a.$$

Así, $d \,|\, 31\cdot 2^{150}$ y $d \,|\, 31\cdot a \implies d \,|\, (31\cdot 2^{150} : 31\cdot a) = 31\,(2^{150} : a) = 31$ pues $a \equiv 1 \pmod 4$ implica que a es impar, por lo tanto coprimo con 2^{150}.

Por lo tanto, el mcd puede ser 1 o 31. Para que sea 31 nos tenemos que asegurar que $31 \,|\, 11\,a + 3\cdot 2^{150}$ y que $31 \,|\, 3\,a - 2^{151}$. Pero por el PTF, al ser 31 primo que no divide a 2, se tiene:

$$\begin{aligned} 31 \,|\, 11\,a + 3\cdot 2^{150} &\iff 11\,a + 3\cdot 2^{150} \equiv 0 \pmod{31} \\ &\iff 11\,a + 3 \equiv 0 \pmod{31} \iff a \equiv 11 \pmod{31}. \end{aligned}$$

Hay que verificar entonces que si $a \equiv 11 \pmod{31}$, se tiene que $3\,a - 2^{151} \equiv 0 \pmod{31}$:

$$a \equiv 11 \pmod{31} \underset{\text{PTF}}{\implies} 3\,a - 2^{151} \equiv 3\cdot 11 - 2^{r_{30}(151)} \equiv 33 - 2 \equiv 0 \pmod{31}.$$

Se concluye el ejercicio con el TCR:

$$\left\{\begin{array}{ll} a \equiv 1 & \pmod 4 \\ a \equiv 11 & \pmod{31} \end{array}\right. \iff a \equiv 73 \pmod{124}.$$

- Determinación de $r_{315}(5\,a^{18} + 7\,b^{115} + 8^{40})$ sabiendo que $(5\,a : 7\,b) = 15$.

  Como $315 = 3^2\cdot 5\cdot 7$, conviene encontrar los restos módulo 3^2, 5 y 7 para luego aplicar el TCR.

  Para el 3^2: Como $(5\,a : 7\,b) = 15$, se tiene

  $$15 \,|\, 5\,a \Leftrightarrow 3 \,|\, a \quad \text{y} \quad 15 \,|\, 7\,b \underset{15\perp 7}{\Leftrightarrow} 15 \,|\, b.$$

  En particular, $3 \,|\, b$, y por lo tanto $3^2 \,|\, a^{18}$ y $3^2 \,|\, b^{115}$:

  $$5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 8^{40} \equiv (-1)^{40} \equiv 1 \pmod 9.$$

  Para el 5: Por lo visto arriba, $5 \,|\, b$, y así:

  $$5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 3^{40} \underset{\text{PTF}}{\equiv} 1 \pmod 5.$$

  Para el 7: La condición $(5\,a : 7\,b) = 15$ dice en particular que $7 \nmid a$ (pues sino, como $7 \,|\, 7\,b$, se tendría que 7 divide al mcd). Por lo tanto

  $$5\,a^{18} + 7\,b^{115} + 8^{40} \underset{\text{PTF}}{\equiv} 5\cdot 1 + 1^{40} \equiv 6 \pmod 7.$$

  Se concluye aplicando el TCR:

  $$\left\{\begin{array}{ll} 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 1 & \pmod 9 \\ 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 1 & \pmod 5 \\ 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 6 & \pmod 7 \end{array}\right. \iff 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 181 \pmod{315}$$

  Por lo tanto $r_{315}(5\,a^{18} + 7\,b^{115} + 8^{40}) = 181$.

- Valores de $a \in \mathbb{Z}$ para los cuales $(3\,a^{98} - 5\,a^{50} + 28 : 140\,a) = 14$.

  Pongamos $b := 3\,a^{98} - 5\,a^{50} + 28$. Se tiene que $140 = 2^2 5^2 7$ y $14 = 2 \cdot 7$. Luego, por definición del mcd, se tiene que cumplir que para todo p primo positivo,

$$v_p(2 \cdot 7) = \min\{v_p(b), v_p(2^2 5^2 7\,a)\}.$$

  Es decir

$$\begin{array}{lll}
1 = \min\{v_2(b), v_2(2^2 5^2 7\,a)\} = \min\{v_2(b), 2 + v_2(a)\} & \iff & v_2(b) = 1; \\
1 = \min\{v_7(b), v_7(2^2 5^2 7\,a)\} = \min\{v_7(b), 1 + v_7(a)\} & \iff & v_7(b) \geq 1, \\
 & & \text{y si } v_7(a) \geq 1 \text{ entonces } v_7(b) = 1; \\
0 = \min\{v_5(b), v_5(2^2 5^2 7\,a)\} = \min\{v_5(b), 2 + v_5(a)\} & \iff & v_5(b) = 0; \\
0 = \min\{v_p(b), v_p(2^2 5^2 7\,a)\} = \min\{v_p(b), v_p(a)\} & \iff & v_p(b) \cdot v_p(a) = 0 \quad \forall p \neq 2, 5, 7.
\end{array}$$

  Miremos la última condición: ¿quiénes son los primos que pueden dividir a la vez a b y a a?

$$p \,|\, a \text{ y } p \,|\, 3\,a^{98} - 5\,a^{50} + 28 \implies p \,|\, 28 \implies p = 2 \text{ ó } 7.$$

  Por lo tanto ningún primo distinto de 2 y 7 divide a la vez a b y a a: la última condición se cumple siempre. Reescribiendo las otras condiciones, se tiene entonces:

$$(3\,a^{98} - 5\,a^{50} + 28 : 140\,a) = 14 \iff \left\{ \begin{array}{l}
2 \,|\, 3\,a^{98} - 5\,a^{50} + 28, \\
\text{pero } 2^2 \nmid 3\,a^{98} - 5\,a^{50} + 28; \\
7 \,|\, 3\,a^{98} - 5\,a^{50} + 28, \\
\text{pero si } 7 \,|\, a \text{ entonces } 7^2 \nmid 3\,a^{98} - 5\,a^{50} + 28; \\
5 \nmid 3\,a^{98} - 5\,a^{50} + 28.
\end{array} \right.$$

  Para el 2: $3\,a^{98} - 5\,a^{50} + 28 \equiv a^{98} - a^{50} \equiv 0 \pmod 2$ independientemente de a ya que a^{98} y a^{50} tienen la misma paridad.

  Para el 4: $a \equiv 0 \pmod 2 \Rightarrow 3\,a^{98} - 5\,a^{50} + 28 \equiv 0 \pmod 4$ (pues $2 \,|\, a \Rightarrow 4 \,|\, a^2$), y $a \equiv 1 \pmod 2 \Rightarrow a^2 \equiv 1 \pmod 4$ (hacerlo!) $\Rightarrow 3\,a^{98} - 5\,a^{50} + 28 \equiv 3 \cdot 1^{49} - 1^{25} \equiv 2 \pmod 4$.

  Se concluye que

$$2 \,|\, 3\,a^{98} - 5\,a^{50} + 28 \quad \text{y} \quad 4 \nmid 3\,a^{98} - 5\,a^{50} + 28 \iff a \equiv 1 \pmod 2.$$

  Para el 5:

$$3\,a^{98} - 5\,a^{50} + 28 \equiv 3\,a^{98} + 28 \underset{\text{PTF}}{\equiv} \left\{ \begin{array}{lll}
3 \pmod 5 & \text{si} & 5 \,|\, a \\
3\,a^2 + 3 \pmod 5 & \text{si} & 5 \nmid a.
\end{array} \right.$$

  Ahora bien, por tabla, $3\,a^2 + 3 \equiv 0 \pmod 5 \Leftrightarrow a^2 + 1 \equiv 0 \pmod 5 \Leftrightarrow a \equiv 2 \text{ ó } 3 \pmod 5$. Se concluye

$$5 \nmid 3\,a^{98} - 5\,a^{50} + 28 \iff a \equiv 0 \text{ ó } 1 \text{ ó } 4 \pmod 5.$$

  Para el 7:

$$3\,a^{98} - 5\,a^{50} + 28 \equiv 3\,a^{98} - 5\,a^{50} \equiv \left\{ \begin{array}{lll}
0 \pmod 7 & \text{si} & 7 \,|\, a \\
3\,a^2 - 5\,a^2 \equiv -2\,a^2 \not\equiv 0 \pmod 7 & \text{si} & 7 \nmid a.
\end{array} \right.$$

  Se concluye que $7 \,|\, a$ y por lo tanto, hay que averiguar si puede pasar que $7^2 \,|\, 3\,a^{98} - 5\,a^{50} + 28$. Pero

$$7 \,|\, a \implies 7^2 \,|\, a^2 \implies 3\,a^{98} - 5\,a^{50} + 28 \equiv 28 \not\equiv 0 \pmod{7^2}.$$

Se concluye entonces

$$7 \,|\, 3\,a^{98} - 5\,a^{50} + 287 \Longleftrightarrow a \equiv 0 \pmod 7, \text{ y en ese caso } 7^2 \nmid 3\,a^{98} - 5\,a^{50} + 287.$$

Se concluye aplicando el TCR:

$$\begin{cases} a \equiv 1 \pmod 2 \\ a \equiv 0 \pmod 7 \\ a \equiv 0 \text{ ó } 1 \text{ ó } 4 \pmod 5 \end{cases} \iff a \equiv 35 \text{ ó } 21 \text{ ó } 49 \pmod{70}.$$

14 Apéndice: El Teorema de Euler

La demostración del Pequeño Teorema de Fermat presentada fue dada por Euler, quien en forma natural la generalizó para números $n \in \mathbb{N}$, $n \geq 2$, cualesquiera. Se dio cuenta que la misma demostración funcionaba si la función Φ estaba definida en el conjunto de los números naturales $i \leq n$ coprimos con n (está claro que si p es primo, el conjunto $\{1, 2, \ldots, p-1\}$ coincide con el conjunto de los números menores o iguales que p coprimos con p, y que $p-1$ es el cardinal de ese conjunto). Así, para $n \in \mathbb{N}$ dado, se definen dos objetos, el conjunto $\mathcal{U}_n$ de los números naturales menores o iguales que n coprimos con él, y la cantidad $\varphi(n)$, que es el cardinal de ese conjunto, es decir $\varphi(n)$ cuenta la cantidad de números naturales menores o iguales que n que son coprimos con él:

Definición 14.1 *Sea $n \in \mathbb{N}$ dado, se define*

$$\mathcal{U}_n := \{\, i \in \mathbb{N},\ 1 \leq i \leq n :\ i \perp n \,\} \qquad y \qquad \varphi(n) := \#\mathcal{U}_n.$$

Por ejemplo, $\mathcal{U}_1 = \{1\}$ y $\varphi(1) = 1$, $\mathcal{U}_6 = \{\,1, 5\,\}$ y $\varphi(6) = 2$, $\mathcal{U}_8 = \{\,1, 3, 5, 7\,\}$ y $\varphi(8) = 4$, $\mathcal{U}_{15} = \{\,1, 2, 4, 7, 8, 11, 13, 14\,\}$ y $\varphi(15) = 8$. Además si p es primo, $\mathcal{U}_p = \{\,1, 2, \ldots, p-1\,\}$ y $\varphi(p) = p - 1$.

La asignación $\varphi : \mathbb{N} \to \mathbb{N}$ define una función, la *función φ de Euler*, que tiene una gran importancia en Teoría de Números, no sólo desde el punta de vista teórico sino también desde el punto de vista de la dificultad de su cálculo. Nos referimos a ella con más detalle después.

Teorema 14.2 (Teorema de Euler)
Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}$, $n \geq 2$. Entonces

$$\boxed{a \perp n \quad \Longrightarrow \quad a^{\varphi(n)} \equiv 1 \pmod n}$$

Prueba.–

Vamos a imitar paso por paso la demostración hecha del pequeño teorema de Fermat.

Sea $a \in \mathbb{Z}$ tal que $a \perp n$. Definimos la función:

$$\begin{array}{rccc} \Phi : & \mathcal{U}_n & \longrightarrow & \mathcal{U}_n \\ & i & \longmapsto & r_n(i\,a) \end{array}$$

(Observemos en particular que $\Phi(i) = r_n(i\,a) \equiv i\,a \pmod n$.)

Veamos primero que esta función está bien definida (es decir que la imagen $\mathrm{Im}(\Phi)$ de la función Φ realmente está incluída en el codominio) y luego que es biyectiva.

- $\mathrm{Im}(\Phi) \subseteq \mathcal{U}_n$:

  Por definición de resto módulo n, está claro que $\mathrm{Im}(\Phi) \subseteq \{0, 1, 2, \ldots, n-1\}$. Falta probar entonces que para todo $i \in \mathcal{U}_n$, es decir $i \perp n$, se tiene que $\Phi(i) \perp n$ para garantizar que $\Phi(i) \in \mathcal{U}_n$. Pero

  $$\Phi(i) \perp n \iff r_n(i\,a) \perp n \underset{(*)}{\iff} i\,a \perp n \underset{a \perp n}{\iff} i \perp n,$$

  donde $(*)$ resulta de que $n \perp r \Leftrightarrow n \perp r + k\,n$ (considerando posibles divisores comunes).

- Para probar que Φ es biyectiva, dado que es una función de un conjunto finito en sí mismo, alcanza con probar que es inyectiva:

  Supongamos que para $i \geq j \in \mathcal{U}_n$, se tiene que $\Phi(i) = \Phi(j)$, queremos probar que entonces $i = j$. Pero de la misma forma que probamos esto en el PTF,

  $$\Phi(i) = \Phi(j) \iff r_n(i\,a) = r_n(j\,a) \iff n \,|\, i\,a - j\,a = (i-j)\,a \underset{n \perp a}{\iff} n \,|\, i - j.$$

  Ahora bien, como $1 \leq j \leq i \leq n-1$, se tiene que $i - j \in \{0, \ldots, n-1\}$, luego

  $$n \,|\, i - j \iff i - j = 0 \iff i = j.$$

- Por lo tanto Φ es biyectiva, es decir suryectiva también. Así

  $$\mathrm{Im}(\Phi) = \mathcal{U}_n \implies \prod_{i \in \mathcal{U}_n} \Phi(i) = \prod_{i \in \mathcal{U}_n} i \implies \prod_{i \in \mathcal{U}_n} r_n(i\,a) = \prod_{i \in \mathcal{U}_n} i \implies$$

  $$\prod_{i \in \mathcal{U}_n} (i\,a) \equiv \prod_{i \in \mathcal{U}_n} i \pmod{n} \implies (\prod_{i \in \mathcal{U}_n} i)\, a^{\varphi(n)} \equiv \prod_{i \in \mathcal{U}_n} i \pmod{n} \Longrightarrow a^{\varphi(n)} \equiv 1 \pmod{n},$$

  pues se puede simplificar $\prod_{i \in \mathcal{U}_n} i$ en el último renglón dado que n es coprimo con ese término (ya que es coprimo con cada uno de sus factores).

■

Se obtiene la consecuencia correspondiente, como en el caso del PTF. Se recomienda demostrarla.

Consecuencia 14.3 *Sean* $a \in \mathbb{Z}, n, m \in \mathbb{N}$. *Si* $n \perp a$, *entonces* $m \equiv r \pmod{\varphi(n)} \implies a^m \equiv a^r \pmod{n}$. *En particular:*

$$\boxed{n \perp a \quad \Longrightarrow \quad a^m \equiv a^{r_{\varphi(n)}(m)} \pmod{n}}$$

Para aplicar este resultado, es importante poder calcular el valor de $\varphi(n)$ para $n \in \mathbb{N}$, además en lo posible sin tener que listar todos los elementos de $\mathcal{U}_n$.

Ejemplos

- Sea $p \in \mathbb{N}$ *primo*, entonces $\varphi(p) = p - 1$.
- Sea $p \in \mathbb{N}$ primo y $n \in \mathbb{N}$, entonces $\varphi(p^n) = p^n - p^{n-1} = (p-1)\,p^{n-1}$.

  Pues en este caso el conjunto $\mathcal{U}_{p^n}$ se obtiene del conjunto $\{1, 2, \ldots, p^n\}$ quitando todos los elementos no coprimos con p^n, es decir divisibles por p. Pero en ese conjunto hay exactamente p^{n-1} elementos divisibles por p, estos son: $p = 1p$, $2p$, $3p$, $\ldots$, $p^{n-1}p = p^n$.

Vamos a probar ahora un resultado importante que permite calcular el valor de $\varphi(n)$ conociendo la factorización de n.

Proposición 14.4 *Sean* $n, m \in \mathbb{N}$ coprimos. *Entonces* $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

Prueba.–

Esto es una consecuencia del Teorema Chino del Resto! Vamos a definir una biyección Ψ entre $\mathcal{U}_{nm}$ y $\mathcal{U}_n \times \mathcal{U}_m$. Por lo tanto los dos conjuntos tienen el mismo cardinal, es decir $\varphi(nm) = \varphi(n)\varphi(m)$. Definimos

$$\begin{array}{rcl} \Psi : \mathcal{U}_{nm} & \longrightarrow & \mathcal{U}_n \times \mathcal{U}_m \\ a & \longmapsto & (r_n(a), r_m(a)) \end{array}$$

- La función Ψ está bien definida, es decir su imagen está efectivamente contenida en el codominio, pues

$$a \perp n\,m \iff a \perp n \text{ y } a \perp m \iff r_n(a) \perp n \text{ y } r_m(a) \perp m.$$

- Ψ es suryectiva: Para todo para $(a_1, a_2) \in \mathcal{U}_n \times \mathcal{U}_m$, por el Teorema Chino del Resto, dado que $n \perp m$, existe $a \in \mathbb{Z}, 0 \leq a \leq n\,m$ tal que $a \equiv a_1 \pmod{n}$, $a \equiv a_2 \pmod{m}$, es decir $a_1 = r_n(a)$, $a_2 = r_m(a)$. Falta verificar que $a \perp n\,m$ pero eso es por el mismo argumento que usamos para probar la buena definición.

- Ψ es inyectiva ya que si $a, a' \in \mathcal{U}_{nm}$ son tales que $\Psi(a) = \Psi(a')$, es decir, $r_n(a) = r_n(a')$ y $r_m(a) = r_m(a')$, entonces $a \equiv a' \pmod{n}$ y $a \equiv a' \pmod{m}$ y por lo tanto, al ser $n \perp m$, $a \equiv a' \pmod{nm}$, luego $a = a'$ pues $1 \leq a, a' \leq n\,m - 1$.

■

Consecuencia 14.5 *Sean* $p_1, \ldots, p_n$ *primos distintos y* $v_1, \ldots, v_n \in \mathbb{N}$. *Entonces*

$$\varphi(p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n}) = \varphi(p_1^{v_1})\,\varphi(p_2^{v_2}) \cdots \varphi(p_n^{v_n}) = (p_1 - 1)\,p_1^{v_1 - 1}(p_2 - 1)\,p_2^{v_2 - 1} \cdots (p_n - 1)\,p_n^{v_n - 1}.$$

Esta fórmula permite calcular el valor de $\varphi(n)$ para cualquier $n \in \mathbb{N}$, via su factorización. Por ejemplo $\varphi(400) = \varphi(2^4 \cdot 5^2) = (2-1)\,2^3(5-1)\,5 = 160$. Hasta la fecha no se conoce ninguna otra forma de calcular en general $\varphi(n)$, que sea esencialmente más rapida que esta, que pasa por la factorización. Este hecho fundamenta el interés y la importancia hoy en día de la aplicación a la criptografía siguiente:

Aplicación (El sistema RSA de Criptografía)

Este sistema criptográfico, que fue introducido en 1978 por R.L. Rivest, A. Shamir y L. Adleman, es un sistema de clave pública-clave privada y de firma digital, que se basa en el teorema de Euler para el caso de $n = p\,q$ producto de dos primos distintos. En ese caso, $\varphi(n) = \varphi(p\,q) = (p-1)(q-1)$ y el Teorema afirma:

$$a \perp n \implies a^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

La aplicación va a ser descrita en forma muy resumida aquí, y no va a contemplar los aspectos de implementación sino simplemente tener en cuenta los aspectos matemáticos y teóricos. Para más información se recomienda buscar por Internet.

'? Cuál es el objetivo de la criptografía ? Codificar información (un mensaje) de manera que solo el receptor al cual va dirigido el mensaje lo pueda decodificar (entender) y ninguna otra persona que

llegue a interceptae el mensaje lo puede entender. Convenimos que un mensaje es un número a, por ejemplo simplement asignándole a cada letra del alfabeto un valor numérico y yuxtaponiendo esos valores. También podemos convenir en que ese número a es menor o igual que cierto número n, recortando el mensaje a original en bloquecitos si hace falta.

'? Qué se entiende por clave pública-clave privada ? Una persona N va a poseer una clave privada, conocida solamente por ella, y va a hacer pública la clave pública asociada a su clave privada. Tanto la clave pública como la privada sirven para codificar o decodificar mensajes, pero ninguna sola puede hacer las dos cosas a la vez. Si N tiene su clave privada y el resto del mundo la clave pública de N, el sistema RSA sirve para lo siguiente:

- Cualquiera del resto del mundo le puede mandar un mensaje encriptado a N usando la clave pública. N es el único que puede decodificar el mensaje, usando su clave privada. Ninguna otra persona del resto del mundo puede decodificar ese mensaje.
- N le puede mandar al resto del mundo un mensaje encriptado usando su clave privada. Cualquiera del resto del mundo, al usar la clave pública de N, puede decodificar y luego entender ese mensaje, y por lo tanto tiene garantía que el emisor (el firmante) del mensaje fue realmente N.

¿ Cómo funciona ?
Clave privada de N: (n, e), clave pública de N: (n, d), donde

- $n = p\,q$ es el producto de dos primos distintos p y q grandes, sólo conocidos por N.
- e coprimo con $(p-1)(q-1)$ es elegido por N.
- d, calculado por N mediante el algoritmo de Euclides, cumple la condición

$$d\,e + t\,(p-1)(q-1) = 1$$

(existen d y t en esas condiciones pues $e \perp (p-1)((q-1)$).
Dado que $a^{(p-1)(q-1)} \equiv 1 \pmod{n}$, esta elección de e y d implica que

$$a^{de} \equiv a^{de} a^{t\,(p-1)(q-1)} \equiv a^1 \equiv a \pmod{n}.$$

Mecanismo: Dado un mensaje a, $0 \le a < n$, $C(a)$ denotará el mensaje encriptado.
Caso 1: Alguien del resto del mundo le manda un mensaje encriptado a N: $C(a) \equiv a^d \pmod{n}$, $0 \le C(a) < n$. Para decodificarlo, N aplica la aplicación "inversa" que consiste en elevar a la e y tomar resto módulo n. Se tiene

$$C(a)^e \equiv (a^d)^e \equiv a^{de} \equiv a^1 \equiv a \pmod{n},$$

luego el resto módulo n de $C(a)^c$ coincide con n.
Caso 2: N le quiere mandar un mensaje firmado a alguien del resto del mundo: $C(a) \equiv a^e \pmod{n}$, $0 \le C(a) < n$. Para decodificarlo, el resto del mundo aplica la aplicación "inversa" que consiste en elevar a la d y tomar resto módulo n. Se tiene

$$C(a)^d \equiv (a^e)^d \equiv a^{de} \equiv a^1 \equiv a \pmod{n},$$

luego el resto módulo n de $C(a)^d$ coincide con n.