

Números Enteros

Teresa Krick*

Departamento de Matemática, FCEyN, UBA e IMAS, CONICET

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 $a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c) (= a \cdot b \cdot c = a b c)$.

*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. Versión revisada en el año 2011, con el apoyo de los subsidios CONICET PIP 2008-2011 y FonCyT PICT 2010.

- *Existencia de Elemento Neutro* : Existe un elemento en \mathbb{Z} (único) que es el 1, que verifica que para todo $a \in \mathbb{Z}$, $1 \cdot a = a$.
- *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 $a, c \in \mathbb{Z}$ con $c \neq 0$. Se dice que *c divide a a* (o que *a es divisible por c*, o que *a es múltiplo de c*) si existe un elemento $k \in \mathbb{Z}$ tal que $a = k \cdot c$ (o sea si el cociente $\frac{a}{c}$ es un número entero).

Se nota $c | a$ (con una barrra vertical, no confundir con la barra del cociente /). O sea:

$$c | a \stackrel{\text{def}}{\iff} \exists k \in \mathbb{Z} : a = k \cdot c.$$

En caso contrario, se dice que *c no divide a a*, y se nota $c \nmid a$. Eso es cuando el cociente $\frac{a}{c} \notin \mathbb{Z}$, o sea no existe ningún entero $k \in \mathbb{Z}$ tal que $a = k \cdot c$.

El conjunto de los divisores positivos y negativos de un entero a se notará por $\text{Div}(a)$ y el de los divisores positivos por $\text{Div}_+(a)$.

(Nota : en algunos libros no se excluye el caso $c = 0$ pero se conviene que 0 divide únicamente al 0. Igualmente en este curso excluirémos el caso $c = 0$ para no “dividir por 0”.)

Ejemplos

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

- $7 \mid -56, -7 \mid 56, -7 \mid -56$.
- $7 \nmid 54$.
- $Div(-12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$ y $Div_+(-12) = \{1, 2, 3, 4, 6, 12\}$.
- $Div(1) = \{-1, 1\}$.

Ejemplos generales

- Todo número entero $c \neq 0$ satisface que $c \mid 0$ pues $0 = 0 \cdot b$ (aquí $k = 0$). Así el 0 tiene infinitos divisores : $Div(0) = \mathbb{Z} \setminus \{0\}$.
- $c \mid a \iff -c \mid a$ (pues $a = k \cdot c \iff a = (-k) \cdot (-c)$).
De la misma manera $c \mid a \iff c \mid -a \iff -c \mid -a$.
Se concluye que $c \mid a \iff |c| \mid |a|$ (donde $|x|$ denota el módulo o valor absoluto de x).
En particular a cada divisor negativo de a le corresponde un divisor positivo.
- Si $a \neq 0, c \mid a \implies |c| \leq |a|$ (pues $|a| = k|c|$ con $|a| \neq 0$ implica $k \neq 0$ también, y mas aún, $k \geq 1$; por lo tanto, $|a| = k|c| \geq |c|$).

En particular, todo número entero a no nulo tiene sólo un número finito de divisores, todos pertenecientes al conjunto

$$\{-|a|, \dots, -1, 1, \dots, |a|\}.$$

O sea $Div_+(a) \subset \{1, \dots, |a|\}$.

Además, por la observación del inciso anterior, el número total de divisores de a es el doble del número de divisores positivos.

- $c \mid a$ y $a \mid c \iff a = \pm c$ (pues $a = k \cdot c$ y $c = j \cdot a$ implica que $a = (k \cdot j) \cdot a$, por lo tanto k y j son dos números enteros que satisfacen $k \cdot j = 1$, o sea, $k = \pm 1$).
- 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* si a tiene únicamente 4 divisores (o 2 divisores positivos). Por ejemplo $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \dots$.

(En general los números primos se notan con las letras p, q, \dots)

- Se dice que a es *compuesto* si a tiene más que 4 divisores (o más que 2 divisores positivos). Por ejemplo $\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \dots$.

Se observa que a es compuesto si y sólo si tiene un divisor positivo b que satisface $2 \leq b \leq |a| - 1$ (pues ya vimos que $Div_+(a) \subset \{1, \dots, |a|\}$ 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 $a, b, c \in \mathbb{Z}$, $c \neq 0$.

- $c|a$ y $c|b \implies c|a+b$.
(Pues si $a = k \cdot c$ y $b = j \cdot c$ con $k, j \in \mathbb{Z}$, entonces $a + b = (k + j) \cdot c$, donde $k + j \in \mathbb{Z}$.)
- $c|a$ y $c|b \implies c|a-b$.
- $c|a+b$ no implica que $c|a$ y $c|b$: Por ejemplo, $6|4+8$ pero $6 \nmid 4$ y $6 \nmid 8$.
- Sin embargo si $c|a+b$ y se sabe que $c|a$, entonces $c|b$.
(Pues $c|(a+b) - a$.)
- $c|a \implies c|b \cdot a$, $\forall b \in \mathbb{Z}$.
- $c|a \implies c^2|a^2$ y $c^n|a^n$, $\forall n \in \mathbb{N}$.
(Pues si $a = k \cdot c$, entonces $a^2 = k^2 \cdot c^2$ y $a^n = k^n \cdot c^n$.)
- $c|a \cdot b$ no implica $c|a$ o $c|b$: Por ejemplo, $6|3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$.
Veremos más adelante que la propiedad $c|a \cdot b \implies c|a$ o $c|b$ se cumple cuando c es un número primo (es la propiedad más importante que cumplen los números primos). Si c no es primo, siempre se pueden encontrar a y b tales que $c|a \cdot b$ pero $c \nmid a$ y $c \nmid b$. ¿Quiénes?

Ejemplos

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

Para resolver esto, se trata de poner a la derecha del símbolo $|$ 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 $a-1|a-1$, por lo tanto $a-1|b(a-1)$ (para todo $b \in \mathbb{Z}$) y en particular $a-1|(a+1)(a-1)$. Así se tiene $a-1|a^2+5$ y $a-1|a^2-1$, por lo tanto $a-1$ divide a la diferencia, es decir $a-1|6$. 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 $a-1|a^2+5$, 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 $a-1|a^n-1$.

Esto ya se puede hacer a este nivel de distintas formas (después 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 $a-1|a^n-1$.

– Usando el Binomio de Newton :

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

Por lo tanto

$$a^n - 1 = (a-1) \left(n + \binom{n}{2} (a-1) + \dots + (a-1)^{n-1} \right) = k(a-1)$$

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

– Por inducción en n . La proposición es $p(n) : “a-1 \mid a^n - 1”$

$p(1)$ es Verdadera pues $a-1 \mid a-1$.

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

HI : $a-1 \mid a^h - 1$. Se quiere probar que $a-1 \mid a^{h+1} - 1$.

Pero $a^{h+1} - 1 = a(a^h - 1) + (a-1)$, y por HI, $a-1 \mid a^h - 1$, y por otro lado, $a-1 \mid a-1$, 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 $m \mid n$, entonces para todo $a \neq \pm 1$, $a^m - 1 \mid a^n - 1$.

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

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 $a, b, c \in \mathbb{Z}$ con $d \neq 0$. Se dice que a es congruente a b módulo c sii $d \mid a - b$.

Se nota $a \equiv b \pmod{c}$ o también $a \equiv b (c)$. O sea:

$$a \equiv b \pmod{c} \stackrel{\text{def}}{\iff} c \mid a - b.$$

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

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 $a, c \in \mathbb{Z}$ con $c \neq 0$. Entonces $a \equiv 0 \pmod{c} \iff c \mid a$.

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

Sea $c \in \mathbb{Z}$ con $c \neq 0$. Se verá ahora que la relación de congruencia módulo c 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 $c \in \mathbb{Z} \setminus \{0\}$. Sea \mathcal{R} la relación en \mathbb{Z} dada por

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

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

Prueba. –

- *Reflexividad* : Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{c}$ pues $c | a - a$.
- *Simetría* : Hay que probar que para todo $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod{c}$, entonces $b \equiv a \pmod{c}$. Pero $a \equiv b \pmod{c}$ significa que $c | a - b$, y por lo tanto $c | -(a - b) = b - a$, luego $b \equiv a \pmod{c}$.
- *Transitividad* : Hay que probar que para todo $a_1, a_2, a_3 \in \mathbb{Z}$ tales que $a_1 \equiv a_2 \pmod{c}$ y $a_2 \equiv a_3 \pmod{c}$ entonces $a_1 \equiv a_3 \pmod{c}$. Pero $a_1 \equiv a_2 \pmod{c}$ significa que $c | a_1 - a_2$, y $a_2 \equiv a_3 \pmod{c}$ significa que $c | a_2 - a_3$. Por lo tanto $c | (a_1 - a_2) + (a_2 - a_3)$, o sea $c | a_1 - a_3$, es decir $a_1 \equiv a_3 \pmod{c}$. ■

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 c clasifica (e identifica) los números enteros según su resto módulo c .

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

Propiedades 3.3 Sea $c \in \mathbb{Z} \setminus \{0\}$. Entonces :

- $a_1 \equiv b_1 \pmod{c}$ y $a_2 \equiv b_2 \pmod{c} \implies a_1 + a_2 \equiv b_1 + b_2 \pmod{c}$.
(Pues $c | a_1 - b_1$ y $c | a_2 - b_2 \implies c | (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$.)
- De la misma manera, se puede probar por inducción que para todo $n \in \mathbb{N}$:
 $a_1 \equiv b_1 \pmod{c}, \dots, a_n \equiv b_n \pmod{c} \implies a_1 + \dots + a_n \equiv b_1 + \dots + b_n \pmod{c}$.
- $a \equiv b \pmod{c}$ y $k \in \mathbb{Z} \implies ka \equiv kb \pmod{c}$.
- $a_1 \equiv b_1 \pmod{c}$ y $a_2 \equiv b_2 \pmod{c} \implies a_1 a_2 \equiv b_1 b_2 \pmod{c}$.
(Para probar esto se puede usar por ejemplo el item anterior y la transitividad : como $a_1 \equiv b_1 \pmod{c}$, entonces $a_1 a_2 \equiv b_1 a_2 \pmod{c}$ (multiplicando por a_2), y por otro lado, como $a_2 \equiv b_2 \pmod{c}$, se tiene $b_1 a_2 \equiv b_1 b_2 \pmod{c}$ (multiplicando por b_1), y finalmente por transitividad, se concluye que $a_1 a_2 \equiv b_1 b_2 \pmod{c}$.)

- Por inducción, se obtiene :

$$a_1 \equiv b_1 \pmod{c}, \dots, a_n \equiv b_n \pmod{c} \implies a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{c}.$$

- Tomando en los items anteriores a_1, \dots, a_n todos iguales a un mismo número a y b_1, \dots, b_n todos iguales a un mismo número b , se obtiene :

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

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

$$\begin{array}{l} a \equiv b \pmod{c} \text{ y } d|c \implies a \equiv b \pmod{d}, \\ a \equiv b \pmod{c} \text{ y } k \neq 0 \iff ka \equiv kb \pmod{kc}. \end{array}$$

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

La segunda afirmación es un si y solo si pues $c|a-b \iff kc|ka-kb$.

Resumimos las dos propiedades más importantes por ahora:

$$\boxed{\begin{array}{l} \left\{ \begin{array}{l} a_1 \equiv b_1 \pmod{c} \\ \vdots \\ a_n \equiv b_n \pmod{c} \end{array} \right. \implies \left\{ \begin{array}{l} a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{c} \\ a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{c} \end{array} \right. \end{array}}$$

Aplicaciones

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

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

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

Se probará por inducción en n , combinado con congruencia.

$$p(n) : "64 | 49^n + 16n - 1"$$

$p(0)$ es Verdadera como antes.

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

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

Se quiere probar que $64 | 49^{h+1} + 16(h+1) - 1$.

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

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

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

Se concluye que $64 | 49^n + 16n - 1$ 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 $a, c \in \mathbb{Z}$ con $c \neq 0$, existen $k, r \in \mathbb{Z}$ que satisfacen

$$a = kc + r \quad \text{con} \quad 0 \leq r < |c|.$$

Además, k y r son únicos en tales condiciones.

Se dice que k es el cociente y r es el resto de la división de a por c (a es el dividendo y c el divisor). Al resto r también lo notaremos $r_c(a)$ para distinguir que es el “resto de a al dividir por c ”.

Antes de pasar a la demostración, hagamos algunos ejemplos:

Ejemplos

- $a = 1038, c = 14$:

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

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

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

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

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

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 $0 \leq 12 < |c|$.

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

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

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 $0 \leq 12 < |c|$.

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 números y divisores positivos y luego corregir cociente y/o resto en cada caso.

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 c dados.

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

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

Aquí, $|c| = c$. La idea intuitiva es considerar los elementos $a, a - c, a - 2c, a - 3c, \dots$ hasta que caigamos en algún elemento menor que c 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 $a - jc$ para algún $j \in \mathbb{Z}$, es decir:

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

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

Luego, 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 satisface que $r = a - kc$, o sea $a = kc + r$.

Falta probar que $0 \leq r < c$ (ya que $|c| = c$ 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 c , entonces $r - c \geq 0$ aún. Luego se tendría que el elemento $r - c = a - kc - c = a - (k + 1)c$ está también en el conjunto A pero es menor que r ! Eso contradice que r sea el mínimo. Así, se concluye que no puede ocurrir que $r \geq c$, luego $r < c$.

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

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

- Caso $a < 0$:

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

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 $|c|$ a la expresión:

$$a = (-k')c - r' = ((-k')c - |c|) + (|c| - r').$$

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

$$0 < r' < |c| \implies -|c| < -r' < 0 \implies |c| - |c| < |c| - r' < |c| - 0 \implies 0 < r < |c|.$$

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 pérdida de generalidad, podemos suponer que $r \leq r'$, y luego:

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

Así, $(k - k')c = r' - r \implies c | r' - r \implies |c| | r' - r$. Como $r' - r \geq 0$ por ser $r' \geq r$, si $r' - r \neq 0$, se tiene, por lo que vimos en divisibilidad, que $|c| \leq r' - r$. Pero es fácil verificar que, dado que

$r' < |c|$, $r' - r < |c| - r < |c|$ (ya que $r \geq 0$). Luego no puede ser $r' - r \neq 0$, es decir tiene que ser $r' = r$.

Se concluye que $(k - k')c = 0$ y como $c \neq 0$, $k - k' = 0$, es decir $k = k'$ también. ■

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

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

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

$$r_c(a) = 0 \iff c|a \iff a \equiv 0 \pmod{c}.$$

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

Proposición 4.4 (Congruencia y restos)

Sean $a, b, c, r, r_1, r_2 \in \mathbb{Z}$ con $c \neq 0$. Entonces

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

Prueba. –

$$1. a = k \cdot c + r_c(a) \Rightarrow c|a - r_c(a) \Rightarrow a \equiv r_c(a) \pmod{c}.$$

(Se usa aquí que existen el cociente y el resto.)

$$2. a \equiv r \pmod{c} \Rightarrow c|a - r \Rightarrow a - r = k \cdot c \text{ para algún } k \in \mathbb{Z} \Rightarrow a = k \cdot c + r.$$

Pero la condición $0 \leq r < |c|$ implica entonces que $r = r_c(a)$.

(Se usa aquí la unicidad del resto.)

$$3. r_1 = 0 \cdot c + r_1 \text{ con } 0 \leq r_1 < |c| \Rightarrow r_1 = r_c(r_1).$$

Pero por otro lado, por (2), $r_1 \equiv r_2 \pmod{c}$ con $0 \leq r_2 < |c| \Rightarrow r_2 = r_c(r_1)$. Se concluye que $r_1 = r_2$ por la unicidad del resto.

4. (\implies): $a \equiv b \pmod{c}$ por hipótesis, y por (1), $a \equiv r_c(a) \pmod{c}$, $b \equiv r_c(b) \pmod{c}$. Por transitividad (y simetría), se concluye que $r_c(a) \equiv r_c(b) \pmod{c}$. Ahora por (3), $r_c(a) = r_c(b)$.

(\impliedby): $r_c(a) = r_c(b) \Rightarrow r_c(a) \equiv r_c(b) \pmod{c}$, y juntando por transitividad (y simetría) con $a \equiv r_c(a) \pmod{c}$, $b \equiv r_c(b) \pmod{c}$, resulta $a \equiv b \pmod{c}$. ■

Al dividir cualquier número entero por $c \in \mathbb{Z}, c \neq 0$, hay $|c|$ restos posibles: $0, 1, \dots, |c| - 1$. La conclusión es entonces que la congruencia módulo c clasifica los números enteros según su resto módulo c : dos números a y b están en la misma clase, o sea son “identificados”, si y sólo si tienen el mismo resto módulo c , y hay $|c|$ clases distintas, la clase del 0, o sea compuesta por los números divisibles por c , 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 c alcanza con poner a la derecha de la congruencia algo que cumple la condición de resto, es decir algún r con $0 \leq r < |c|$.

Como consecuencia de lo anterior se observa fácilmente lo siguiente

Consecuencia (Tablas de Restos)

Sea $a, b, c \in \mathbb{Z}$ con $c \neq 0$, y sea $n \in \mathbb{N}$. Entonces

- $r_c(a + b) = r_c(r_c(a) + r_c(b))$
- $r_c(a \cdot b) = r_c(r_c(a) \cdot r_c(b))$
- $r_c(a^n) = r_c(r_c(a)^n)$

La necesidad de tomar resto nuevamente (fuera de los paréntesis grandes) proviene del hecho que puede ocurrir que la suma o producto de los restos se pase de $|c|$, y entonces hay que volver a reducir... Es por eso que puede ser más sencillo trabajar directamente con las congruencias, siempre reduciendo de manera de obtener a la derecha del signo \equiv un número que cumple con la condición de resto, como se hace en las aplicaciones siguientes.

Aplicaciones

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

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

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

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 se puede usar que $6^2 = 36 \equiv 1 \pmod{35}$ y también que $34 \equiv -1 \pmod{35}$. Luego:

$$\begin{aligned} 34^{17771} - 6^{1001} &= 34^{17771} - 6^{2 \cdot 500 + 1} \\ &= 34^{17771} + (6^2)^{500} \cdot 6^1 \\ &\equiv (-1)^{17771} - 1^{500} \cdot 6 \pmod{35} \\ &\equiv -1 - 6 \pmod{35} \\ &\equiv -7 \pmod{35} \\ &\equiv 28 \pmod{35} \end{aligned}$$

Por lo tanto el resto es 28.

5 Desarrollos en base c

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

Consecuencia (Reglas de divisibilidad)

Sabiendo esto se explican muy fácilmente 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 $a = r_n r_{n-1} \dots r_1 r_0$,

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

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

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

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

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

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 ($0 \leq r_i < 10, 0 \leq i \leq n$): 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 $111 = 1 \cdot 10^2 + 1 \cdot 10 + 1$ 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 $c \geq 2$ 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 $c - 1$. Esto se justifica también en la vida real, por ejemplo las computadoras trabajan naturalmente en base 2, o sea con los “dígitos” o “bits” 0 y 1, ya que esto se corresponde con el paso o no de electricidad.

Teorema 5.1 (Desarrollo en base c)

Sea $c \in \mathbb{N}$ con $c \geq 2$. Todo número $a \in \mathbb{N}_0$ admite un desarrollo en base c de la forma

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

con $0 \leq r_i < c$ para $0 \leq i \leq n$ y $r_n \neq 0$ si $a \neq 0$.

Además dicho desarrollo, con las exigencias $0 \leq r_i < c$ impuestas para los dígitos, es único.

Se nota $a = (r_n \dots r_0)_c$.

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 c :

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

- Para $a = 0$, se tiene $0 = (0)_c$, 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 c . Queremos probar que entonces a admite también un desarrollo en base c .

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

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

Entonces

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

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 c .

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 c y por lo tanto es único, r_1 es el resto de la división de $(a - r_0)/c$ por c 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

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

con $0 \leq r_i, s_j < c$ 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 $r_c(a) = r_0 = s_0$, y además, el cociente de dividir a por c (que es único) es

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

Por hipótesis inductiva, el desarrollo en base c 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 c 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 al menos uno entre a y 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:

$$(a : b) \mid a, (a : b) \mid b \quad \text{y si } c \mid a \text{ y } c \mid b, \text{ entonces } c \leq (a : b).$$

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

$$\begin{aligned} \text{DivCom}(\{a, b\}) &:= \{c \in \mathbb{Z} : c \mid a \text{ y } c \mid b\} = \text{Div}(a) \cap \text{Div}(b) \\ \text{DivCom}_+(\{a, b\}) &:= \{c \in \mathbb{N} : c \mid a \text{ y } c \mid b\} = \text{Div}_+(a) \cap \text{Div}_+(b). \end{aligned}$$

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

Ejemplos

- $(12 : 18) = 6$, pues $\text{Div}_+(12) = \{1, 2, 3, 4, 6, 12\}$, $\text{Div}_+(18) = \{1, 2, 3, 6, 9, 18\}$
 $\Rightarrow \text{DivCom}_+(\{12, 18\}) = \{1, 2, 3, 6\}$.
- $(12 : -35) = 1$ ya que $\text{Div}_+(-35) = \{1, 5, 7, 35\} \Rightarrow \text{DivCom}_+(\{12, -35\}) = \{1\}$.
- $(a : b) = (b : a)$.
- $(a : b) = (-a : b) = (a : -b) = (-a : -b) = (|a| : |b|)$.
- 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:

$$\begin{cases} c|n^2+1 \\ c|n-1 \end{cases} \implies \begin{cases} c|n^2+1 \\ c|(n+1)(n-1) \end{cases} \implies \begin{cases} c|n^2+1 \\ c|n^2-1 \end{cases} \implies c|2.$$

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 $c|2$ 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 $(n^2 + 1 : n - 1) = 2$ (por ser el máximo).
 - 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 $n \in \mathbb{N}$:
 - $n = 1 \Rightarrow (0 : 4) = 4$, $n = 2 \Rightarrow (2 : 6) = 2$, $n = 3 \Rightarrow (6 : 8) = 2$, $n = 4 \Rightarrow (12 : 10) = 2$, $n = 5 \Rightarrow (20 : 12) = 4$, $n = 6 \Rightarrow (30 : 14) = 2$, ...
 - 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:

$$\begin{cases} c|n(n-1) \\ c|2(n+1) \end{cases} \implies \begin{cases} c|2n(n-1) \\ c|2n(n+1) \end{cases} \implies \begin{cases} c|2n^2-2n \\ c|2n^2+2n \end{cases} \implies c|4n.$$

Pero volviendo entonces al principio

$$\begin{cases} c|4n \\ c|2(n+1) \end{cases} \implies \begin{cases} c|4n \\ c|2 \cdot 2(n+1) \end{cases} \implies \begin{cases} c|4n \\ c|4n+4 \end{cases} \implies c|4.$$

Así, $DivCom_+(\{n(n-1), 2(n+1)\}) \subseteq \{1, 2, 4\}$, y luego por lo tanto ya podemos deducir que $(n(n - 1) : 2(n + 1)) \in \{1, 2, 4\}$.

- Investigamos ahora por separado los casos $n \equiv 0, 1, 2 \text{ ó } 3 \pmod{4}$.
 - Si $n \equiv 0 \pmod{4}$, entonces $2(n + 1) \equiv 2 \pmod{4}$ y por lo tanto 4 no puede ser un divisor común. Pero claramente tanto $n(n - 1)$ y $2(n + 1)$ son números pares, por lo tanto 2 sí es un divisor común. Luego en ese caso, $(n(n - 1) : 2(n + 1)) = 2$.

Si $n \equiv 1 \pmod{4}$:

$$\begin{cases} n(n-1) \equiv 1(1-1) \pmod{4} \\ 2(n+1) \equiv 2(1+1) \pmod{4} \end{cases} \implies \begin{cases} n(n-1) \equiv 0 \pmod{4} \\ 2(n+1) \equiv 0 \pmod{4} \end{cases} \implies \begin{cases} 4 \mid n(n-1) \\ 4 \mid 2(n+1) \end{cases}$$

Así, $4 \in \text{DivCom}_+(\{n(n-1), 2(n+1)\})$, luego, en este caso, $(n(n-1) : 2(n+1)) = 4$.

Si $n \not\equiv 2 \pmod{4}$, entonces $2(n+1) \equiv 2 \pmod{4}$ y estamos como en el primer caso: $(n(n-1) : 2(n+1)) = 2$.

Si $n \equiv 3 \pmod{4}$, entonces $n(n-1) \equiv 2 \pmod{4}$, y de nuevo, 4 no puede ser un divisor común. En este caso también $(n(n-1) : 2(n+1)) = 2$.

Se concluye que $(n(n-1) : 2(n+1)) = 4$ si $n \equiv 1 \pmod{4}$ y que $(n(n-1) : 2(n+1)) = 2$ si $n \not\equiv 1 \pmod{4}$ como se quería probar...

Observación 6.2 (Importante!)

Sean $a, b \in \mathbb{Z}$ no ambos nulos, y sea $j \in \mathbb{Z}$, entonces:

$$\text{DivCom}(\{a, b\}) = \text{DivCom}(\{b, a - jb\}) \quad \text{y} \quad \text{DivCom}_+(\{a, b\}) = \text{DivCom}_+(\{b, a - jb\}).$$

En particular, para todo $j \in \mathbb{Z}$, $(a : b) = (b : a - jb)$.

Aplicando esto a $r_b(a) = a - kb$, se obtiene $(a : b) = (b : r_b(a))$

Prueba. – Alcanza con probar la primer igualdad, la de los conjuntos DivCom :

Pero utilizando que $c \mid a, c \mid b \implies c \mid a - jb$ y $c \mid b, c \mid a - jb \implies c \mid a$, se tiene

$$c \in \text{DivCom}(\{a, b\}) \iff c \mid a \text{ y } c \mid b \iff c \mid a - jb \text{ y } c \mid b \iff c \mid \text{DivCom}(\{b, a - jb\}).$$

■

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 ($\sim 325 - \sim 265$ 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

$$\begin{aligned} 120 &= 1 \cdot 84 + 36 &\implies (120 : 84) &= (84 : 36) \\ 84 &= 2 \cdot 36 + 12 &\implies (84 : 36) &= (36 : 12) \\ 36 &= 3 \cdot 12 + 0 &\implies (36 : 12) &= (12 : 0). \end{aligned}$$

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:

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

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 la cantidad b) a un resto nulo ya que

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

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

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

■

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, $m = kn + r$ con $0 \leq r < n$, y entonces

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

dado que $n | kn \Rightarrow a^n - 1 | a^{kn} - 1$. Además, como $0 \leq a^r - 1 < a^n - 1$ por ser $0 \leq r < n$ 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

$$\begin{aligned} 84 &= 2 \cdot 36 + 12 &\implies 12 &= 84 - 2 \cdot 36 \\ 120 &= 1 \cdot 84 + 36 &\implies 12 &= 84 - 2 \cdot (120 - 1 \cdot 84) \\ &&&= 3 \cdot 84 - 2 \cdot 120. \end{aligned}$$

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.)

$$\begin{aligned} r_{\ell-2} &= k_{\ell-1}r_{\ell-1} + r_{\ell} &\implies r_{\ell} &= r_{\ell-2} - k_{\ell-1}r_{\ell-1} \\ r_{\ell-3} &= k_{\ell-2}r_{\ell-2} + r_{\ell-1} &\implies r_{\ell} &= r_{\ell-2} - k_{\ell-1}(r_{\ell-3} - k_{\ell-2}r_{\ell-2}) \\ &&&= (1 + k_{\ell-1}k_{\ell-2})r_{\ell-2} - k_{\ell-1}r_{\ell-3} \\ &\vdots && \\ r_1 &= k_2r_2 + r_3 &\implies r_{\ell} &= *r_1 + *'r_2 \\ b &= k_1r_1 + r_2 &\implies r_{\ell} &= *r_1 + *'(b - k_1r_1) \\ &&&= (* - k_1*')r_1 + *'b \\ a &= k_0b + r_1 &\implies r_{\ell} &= (* - k_1*')(a - k_0b) + *'b \\ &&&= sa + tb. \end{aligned}$$

Así, $(a : b) = r_{\ell} = sa + tb$ 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 y que 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 $c \in \mathbb{Z}$, con $c \neq 0$. Entonces:

$$\boxed{c | a \text{ y } c | b \iff c | (a : b)}$$

Prueba. –

(\Rightarrow): Esta es la implicación interesante y no trivial:

Recordemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = sa + tb$. Ahora, dado que por hipótesis, $c | a$ y $c | b$, se tiene que $c | sa + tb = (a : b)$.

(\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 $k \in \mathbb{Z}$ con $k \neq 0$. Entonces $(ka : kb) = |k| \cdot (a : b)$

Prueba. –

Sin pérdida de generalidad, podemos suponer $k > 0$.

Por un lado, aplicando la Proposición 6.5, se tiene

$$(a : b) | a \text{ y } (a : b) | b \implies k(a : b) | ka \text{ y } k(a : b) | kb \implies k(a : b) | (ka : kb).$$

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

$$(a : b) = sa + tb \implies k(a : b) = s(ka) + t(kb) \implies (ka : kb) | k(a : b).$$

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 $d \in \mathbb{N}$. Son equivalentes:

1. $d | a$, $d | b$ y si $c | a$ y $c | b$, entonces $c \leq d$.
2. $d | a$, $d | b$ y existen $s, t \in \mathbb{Z}$ tales que $d = sa + tb$.
3. $d | a$, $d | b$ y si $c | a$ y $c | b$, entonces $c | d$.

Si un número $d \in \mathbb{N}$ cumple cualquiera de esas 3 propiedades, entonces $d = (a : b)$. ■

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 Donald Knuth (quién de hecho es el creador del TeX (y LaTeX), editores con los que escribimos textos matemáticos que lucen tan bonitos, en particular este texto), y escribimos $a \perp b$. O sea:

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

Ejemplos

- $103 \perp 98$ pero $12202 \not\perp 43554$.
- $a \perp 0 \Leftrightarrow a = \pm 1$
- 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 c un divisor común entre $2a + b$ y $3a - 2b$,

$$\begin{cases} c \mid 2a + b \\ c \mid 3a - 2b \end{cases} \implies \begin{cases} c \mid 3(2a + b) \\ d \mid 2(3a - 2b) \end{cases} \implies \begin{cases} c \mid 6a + 3b \\ c \mid 6a - 4b \end{cases} \implies c \mid 7b.$$

De la misma manera:

$$\begin{cases} c \mid 2a + b \\ c \mid 3a - 2b \end{cases} \implies \begin{cases} c \mid 2(2a + b) \\ c \mid 3a - 2b \end{cases} \implies \begin{cases} c \mid 4a + 2b \\ c \mid 3a - 2b \end{cases} \implies c \mid 7a.$$

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

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

Se concluye que el máximo común divisor, que es el mayor de estos c 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!)

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

Prueba. –

(\Rightarrow) es el hecho que el mcd es combinación entera de los números.

(\Leftarrow) es por la Observación 6.4: $(a : b) \mid 1 \Rightarrow (a : b) = 1$. ■

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 (Propiedades esenciales de divisibilidad con coprimalidad)

Sean $a, b, c, d \in \mathbb{Z}$ con $c \neq 0$ y $d \neq 0$. Entonces

1. $c \mid a, d \mid a$ con $c \perp d \implies cd \mid a$.

2. $c|ab$ con $c \perp a \implies c|b$.

Observemos que estas afirmaciones no son ciertas si no se piden las propiedades de coprimidad. Por ejemplo $6|12$ y $4|12$ pero $24 \nmid 12$, y $6|2 \cdot 3 \nRightarrow 6|2$ o $6|3$. Por otro lado, las recíprocas siempre valen: $cd|a \Rightarrow c|a$ y $d|a$, y $c|b \Rightarrow cd|ab$. Luego podemos resumir la Proposición en:

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

Prueba de la Proposición 6.9.–

1. $c \perp d \Rightarrow 1 = sc + td \Rightarrow a = s(ca) + t(da)$, pero $d|a \Rightarrow cd|ca$ y $c|a \Rightarrow cd|da$, luego $cd|s(ca) + t(da) = a$.
2. $d \perp a \Rightarrow 1 = sd + ta$, luego $b = (sb)d + t(ab)$, pero $d|ab$, y $d|d$. Por lo tanto, $d|(sb)d + t(ab) = b$.

■

Ejemplo Cálculo de los $a, b \in \mathbb{Z}$ coprimos tales que $\frac{2}{a} + \frac{a}{b}$ 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, dado que $a|a^2$, $a|2b + a^2 \Leftrightarrow a|2b$, y, dado que $a \perp b$, $a|2b \Leftrightarrow a|2$. Es decir, $a \in \{\pm 1, \pm 2\}$.

De la misma forma, dado que $b|2b$, $b|2b + a^2 \Leftrightarrow b|a^2$, y, dado que $b \perp a^2$ (pues $a \perp b$), $b|a^2 \cdot 1 \Leftrightarrow b|1$, o sea $b \in \{\pm 1\}$.

Se obtienen luego los 8 pares $a = \pm 1, b = \pm 1$ y $a = \pm 2, b = \pm 1$.

Otra consecuencia muy útil 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 (“Coprimitizando”)

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

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

Prueba.–

Se sabe que $(a:b) = sa + tb$. Luego, dividiendo por $(a:b)$, se obtiene $1 = s\frac{a}{(a:b)} + t\frac{b}{(a:b)}$, es decir $\frac{a}{(a:b)}$ y $\frac{b}{(a:b)}$ son coprimos.

■

De hecho esta propiedad de cocientes coprimos permite presentar otra caracterización del máximo común divisor, como las propuestas en el Teorema 6.6:

Observación Sean $a, b \in \mathbb{Z}$, no ambos nulos. Sea $d \in \mathbb{N}$ un número que satisface que

$$d|a, d|b \quad \text{y} \quad \frac{a}{d} \perp \frac{b}{d}.$$

Entonces $d = (a : b)$.

(Esto vale por ejemplo porque $a/d \perp b/d \Leftrightarrow \exists s, t \in \mathbb{Z}$ con $1 = sa/d + tb/d$, lo que implica que $d = sa + tb$, la caracterización (2) del Teorema 6.6.)

Otras consecuencias son las siguientes:

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

1. $\boxed{a \perp b \text{ y } a \perp c \iff a \perp bc}$
2. $a \perp b \iff a^m \perp b^n$, para todo $m, n \in \mathbb{N}$.
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) $1 = sa + tb$ y $1 = s'a + t'c \implies$
 $1 = (sa + tb)(s'a + t'c) = s s' a^2 + s t' a c + t s' a b + t t' b c = (s s' a + s t' c + t s' b) a + t t' b c = s'' a + t'' b c,$
 con $s'' := s s' a + s t' c + t s' b$ y $t'' := t t'$ enteros.
 (\Leftarrow) $1 = sa + tbc \implies 1 = sa + (tc)b$ y $1 = sa + (tb)c$, es decir $a \perp b$ y $a \perp c$.
2. Se obtiene por inducción a partir de (1): intuitivamente $a \perp b \Rightarrow a \perp b^2 \Rightarrow a \perp b^3$ etc., y en forma simétrica $a \perp b^n \Rightarrow a^2 \perp b^n \Rightarrow a^3 \perp b^n$ etc.
3. Sea $d := (a : b)$. Por la Proposición 6.10, $a = da'$ y $b = db'$ con $a' \perp b'$. Luego $(a^n : b^n) = (d^n a'^n : d^n b'^n) = d^n (a'^n : b'^n) = d^n$, 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 c un posible divisor común:

$$\begin{cases} c \mid 2^n + 3^n \\ c \mid 2^n - 2 \cdot 3^n \end{cases} \implies c \mid 3^n + 2 \cdot 3^n \implies c \mid 3 \cdot 3^n.$$

De la misma manera:

$$\begin{cases} c \mid 2^n + 3^n \\ c \mid 2^n - 2 \cdot 3^n \end{cases} \implies \begin{cases} c \mid 2 \cdot 2^n + 2 \cdot 3^n \\ c \mid 2^n - 2 \cdot 3^n \end{cases} \implies c \mid 2 \cdot 2^n + 2^n \implies c \mid 3 \cdot 2^n.$$

Pero

$$c \mid 3 \cdot 3^n \text{ y } c \mid 3 \cdot 2^n \implies c \mid (3 \cdot 3^n : 3 \cdot 2^n) = 3(3^n : 2^n) = 3 \cdot 1 = 3.$$

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 $3 \mid 3^n$, que $3 \mid 2^n$, 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 $c|n, c|n+1 \Rightarrow c|1$), y aplicando la Consecuencia 2 de la Proposición 6.10.

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

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

Pues si $c|n$ y $c|n+2$, entonces $c|2$. Luego $(n : n+2) = 1$ si n es impar y $(n : n+2) = 2$ si n es par. Así, si $n \equiv 1 \pmod{2}$, es decir si n es impar, $(n^{100} : (n+2)^{150}) = 1$. Consideremos ahora el caso n par. Si n es par, mirandolo módulo 4, se tiene $n \equiv 0 \pmod{4}$ ó $n \equiv 2 \pmod{4}$:

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

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

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

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

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

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

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

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

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

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

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

Como siempre, sea c un posible divisor común:

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

De la misma manera:

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

Obtuvimos $c|a'^2$ y $c|b'^2$. Luego $c|(a'^2 : b'^2)$. Pero, como vimos arriba, $a' \perp b' \Rightarrow a'^2 \perp b'^2$, es decir $(a'^2 : b'^2) = 1$. O sea $c|1$. 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.

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

La condición $(a : 8) = 4$ implica que $a = 4a'$. Como $8 = 4 \cdot 2$, si se tuviera $2 | a'$ entonces se tendría $8 | (a : 8)$. Luego no puede ser $2 | a'$, o sea se tiene a' impar. Por lo tanto:

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

donde a' es impar. 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 $4a'^2 + 5a' + 8 \equiv 4a'^2 + 3 \pmod{5}$ y es fácil ver, según los posibles restos de a' módulo 5 , que ese número nunca es divisible por 5 .

Luego $(4a'^2 + 5a' + 8 : 20) = 1$ y por lo tanto $(a^2 + 5a + 32 : 80) = 4$.

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 $aX + bY = c$ 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

$$aX + bY = c,$$

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: $aX + 0Y = c$ 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

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

- $18X - 12Y = 60$ 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 $a, b, c \in \mathbb{Z}$ con a, b no nulos.

Entonces la ecuación diofántica $aX + bY = c$ admite soluciones enteras si y solo si $(a : b) | c$. Es decir:

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

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 $(a : b) | ax_0 + by_0 = c$, es decir, $(a : b) | c$.

(\Leftarrow): Sabemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = sa + tb$. Luego, dado que $(a : b) | c$, existe $k \in \mathbb{Z}$ tal que $c = k(a : b)$, y por lo tanto se tiene que $c = a(ks) + b(kt)$. Podemos tomar $x_0 := ks, y_0 := kt$. ■

Corolario 7.2 Sean $a, b, c \in \mathbb{Z}$ con a, b no nulos y **coprimsos**.

Entonces la ecuación diofántica $aX + bY = c$ tiene soluciones enteras.

La proposición da además una forma de conseguir una solución (x_0, y_0) particular (si existe), cuando no se consigue más fácilmente (por ejemplo a ojo) podemos aplicar el algoritmo de Euclides para escribir el mcd como combinación entera. Y luego de allí obtener la combinación entera que da c como en la demostración anterior. Pero siempre es más fácil trabajar directamente con la ecuación *coprimizada*:

Observación Sean $a, b, c \in \mathbb{Z}$ con a, b no nulos tales que $(a : b) | c$.

Entonces la ecuación diofántica $aX + bY = c$ es equivalente a (es decir tiene exactamente las mismas soluciones enteras que) la ecuación diofántica coprimizada:

$$a'X + b'Y = c', \text{ donde } a' := \frac{a}{(a : b)}, b' := \frac{b}{(a : b)} \text{ y } c' := \frac{c}{(a : b)}.$$

Adoptamos la notación \rightsquigarrow para ecuaciones diofánticas equivalentes, es decir con las mismas soluciones y resumimos lo anterior en

$$\boxed{\text{Si } (a : b) | c, \text{ entonces } aX + bY = c \rightsquigarrow \frac{a}{(a : b)}X + \frac{b}{(a : b)}Y = \frac{c}{(a : b)}}.$$

Siempre resulta más simple hacer este proceso de “coprimización” de entrada para encontrar una solución particular: se escribe el 1 como combinación entera de a' y b' : $1 = sa' + tb'$ y luego haciendo $c' = c'sa' + c'tb'$ se obtiene por ejemplo $x_0 = c's$ e $y_0 = c't$.

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

$$aX + bY = 0$$

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

Ejemplo Soluciones enteras de $18X + 27Y = 0$:

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 ecuación coprimizada:

$$18X + 27Y = 0 \iff 2X + 3Y = 0.$$

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

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

Volviendo al primer renglón, resulta:

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

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

Hemos probado: (x, y) solución entera \implies existe $k \in \mathbb{Z}$ tal que $x = 3k$ e $y = -2k$.

Verifiquemos la recíproca: Si $x = 3k$ e $y = -2k$ para el mismo $k \in \mathbb{Z}$, entonces (x, y) es solución de la ecuación. Efectivamente, se tiene $2x + 3y = 2(3k) + 3(-2k) = 0$.

Luego, hemos probado que el conjunto de soluciones enteras de esta ecuación es el conjunto:

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

(Observemos que si nos olvidamos de coprimizar la ecuación y nos quedamos, usando la misma estructura, con las soluciones de tipo $x = 27k, y = -18k, k \in \mathbb{Z}$, 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 7.3 Sean $a, b \in \mathbb{Z}$, no nulos.

El conjunto \mathcal{S}_0 de soluciones enteras de la ecuación diofántica $aX + bY = 0$ es

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

Prueba.-

Se tiene

$$aX + bY = 0 \iff a'X + b'Y = 0,$$

donde $a' = a/(a : b)$ y $b' = b/(a : b)$ son coprimos.

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

$$\begin{aligned} a'x + b'y = 0 &\iff a'x = -b'y \\ &\implies a' \mid b'y \text{ y } b' \mid a'x \\ &\stackrel{a' \perp b'}{\implies} a' \mid y \text{ y } b' \mid x \\ &\implies y = a'j \text{ y } x = b'k. \end{aligned}$$

Volviendo al primer renglón, resulta:

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

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

Hemos probado: (x, y) solución entera \implies existe $k \in \mathbb{Z}$ tal que $x = b'k$ e $y = -a'k$.

Verifiquemos la recíproca: Si $x = b'k$ e $y = -a'k$ para el mismo $k \in \mathbb{Z}$, entonces (x, y) es solución de la ecuación. Efectivamente, se tiene $a'x + b'y = a'(b'k) + b'(-a'k) = 0$. ■

Para resolver completamente una ecuación general $aX + bY = c$, que admite al menos una solución particular $(x_0, y_0) \in \mathbb{Z}^2$, nos podemos reducir al caso anterior observando que, dado que $ax_0 + by_0 = c$, se tiene que para $(x, y) \in \mathbb{Z}^2$,

$$ax + by = c \iff ax + by = ax_0 + by_0 \iff a(x - x_0) + b(y - y_0) = 0.$$

Es decir (x, y) es solución de $aX + bY = c$ si y solo si $(x - x_0, y - y_0)$ es solución de $aX + bY = 0$. Luego, aplicando la Proposición 7.3, obtenemos el Teorema siguiente:

Teorema 7.4 Sean $a, b, c \in \mathbb{Z}$, con a, b no nulos.

El conjunto \mathcal{S} de soluciones enteras de la ecuación diofántica $aX + bY = c$ 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, $a' := \frac{a}{(a : b)}$, $b' := \frac{b}{(a : b)}$, 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 $aX + bY = c$

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:

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

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 $18X + 27Y = -90$:

Hay soluciones pues $(18 : 27) = 9 \mid -90$.

Coprimizo: $2X + 3Y = 10$.

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 $175X + 275Y = 3000$:

Hay soluciones enteras pues $(125 : 50) = 25 \mid 3000$.

Coprimizo: $7X + 11Y = 120$.

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

Soluciones naturales:

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

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 análisis realizado para las ecuaciones diofánticas se aplica directamente a ciertas *ecuaciones lineales de congruencia*. Más específicamente a las ecuaciones de la forma

$$aX \equiv c \pmod{b},$$

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

Veremos ahora que la ecuación de congruencia $aX \equiv c \pmod{b}$ admite al menos una solución en \mathbb{Z} si y solo si la ecuación diofántica $aX - bY = c$ admite al menos una solución en \mathbb{Z}^2 , y por lo visto en el Teorema 7.4, esto es si y solo si $(a : -b) = (a : b) \mid c$.

Proposición 8.1 Sean $a, b, c \in \mathbb{Z}$, con a, b no nulos. Entonces:

La ecuación de congruencia $aX \equiv c \pmod{b}$ admite soluciones enteras si y solo si $(a : b) \mid c$. En ese caso la ecuación es equivalente a la ecuación de congruencia coprimizada

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

Para probar la segunda afirmación, es útil aislar la propiedad siguiente, que es inmediata:

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

$$ax \equiv c \pmod{b} \iff (ka)x \equiv kc \pmod{(kb)}.$$

Prueba. –

$$b \mid ax - c \iff k(ax - c) = kb \mid (ka)x - kc.$$

■

Prueba de la Proposición 8.1. –

Si $(a : b) \mid c$, entonces la ecuación diofántica $aX - bY = c$ admite al menos una solución particular $(x_0, y_0) \in \mathbb{Z}^2$. Es decir, $ax_0 - by_0 = c$, o equivalentemente $ax_0 - c = by_0$. Por lo tanto $b \mid ax_0 - c$, o lo que es lo mismo, $ax_0 \equiv c \pmod{b}$: $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación de congruencia $aX \equiv c \pmod{b}$.

Recíprocamente, si $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación de congruencia $aX \equiv c \pmod{b}$, entonces existe $y_0 \in \mathbb{Z}$ tal que $ax_0 - c = by_0$, por lo cual la ecuación diofántica $aX - bY = c$ admite la solución particular $(x_0, y_0) \in \mathbb{Z}^2$. Por lo visto en la sección anterior, esta ecuación diofántica tiene solución si y sólo si $(a : b) \mid c$.

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

■

Adoptamos la notación \iff para ecuaciones de congruencia equivalentes, o sea con las mismas soluciones, y resumimos lo anterior en

Si $(a : b) \mid c$, entonces $aX \equiv c \pmod{b} \iff \frac{a}{(a : b)}X \equiv \frac{c}{(a : b)} \pmod{\frac{b}{(a : b)}}.$
--

Corolario 8.3 Sean $a, b, c \in \mathbb{Z}$, con a, b no nulos y **coprimos**. Entonces, la ecuación de congruencia $aX \equiv c \pmod{b}$ tiene soluciones enteras.

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

La ecuación de congruencia $aX \equiv c \pmod{b}$

- no tiene soluciones cuando $(a : b) \nmid c$.

- tiene soluciones cuando $(a : b) \mid c$; en ese caso

$$aX \equiv c \pmod{b} \iff X \equiv x_0 \pmod{\frac{b}{(a : b)}}$$

donde $x_0 \in \mathbb{Z}$ es una solución particular.

Prueba. –

El primer inciso es la Proposición 8.1. Para probar la equivalencia del segundo inciso, tenemos que probar que las dos ecuaciones de congruencia tienen las mismas soluciones.

Si $x \in \mathbb{Z}$ es una solución cualquiera de la ecuación de congruencia original $ax \equiv c \pmod{b}$, entonces existe $y \in \mathbb{Z}$ tal que (x, y) es solución de la ecuación diofántica $aX - bY = c$. Por el Teorema 7.4, existe una solución particular (x_0, y_0) de la ecuación diofántica y $k \in \mathbb{Z}$ tales que $x = x_0 + (-b')k$ e $y = y_0 - a'k$. En particular $b' \mid x - x_0$, es decir $x \equiv x_0 \pmod{b'}$ como se quería probar.

Recíprocamente, si $x \equiv x_0 \pmod{b'}$ entonces $a'x \equiv a'x_0 \pmod{b'}$. Como $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación original, se tiene $a'x_0 \equiv c' \pmod{b'}$ (dada la equivalencia de la ecuación de congruencia original y la coprimizada) y por lo tanto, por transitividad, $a'x \equiv c' \pmod{b'}$ como se quería probar, ■

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

Ejemplos

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

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

(Aquí, $x_0 := 4$ es una solución particular.)

- La ecuación $3X \equiv 2 \pmod{4}$:

$$3X \equiv 2 \pmod{4} \iff X \equiv 2 \pmod{4}.$$

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

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

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

$$120X \equiv 60 \pmod{250} \iff 12X \equiv 6 \pmod{25} \iff 2X \equiv 1 \pmod{25} \iff X \equiv 13 \pmod{25} :$$

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

Observación 8.5 Sean $a, b, c, k \in \mathbb{Z}$ con a, b, k no nulos.

Si se cumple que b y k son coprimos, entonces se tiene la siguiente equivalencia de ecuaciones de congruencia

$$aX \equiv c \pmod{b} \iff (ka)X \equiv kc \pmod{b}.$$

Prueba. – Hay que probar que tienen las mismas soluciones x :

(\Rightarrow): Vale siempre.

(\Leftarrow): Esto es porque $b \mid k(ax - c)$ y $b \perp k$ implica $b \mid ax - c$. ■

Resolución completa de la ecuación de congruencia $aX \equiv c \pmod{b}$

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 $(a : b) \nmid c$.
 - (b) **sí** si $(a : b) \mid c$. En ese caso:
3. Coprimizo la ecuación:

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

4. Si puedo, ahora que $a' \perp b'$, simplifico todos los factores comunes entre a' y c' aplicando la Observación 8.5. Esto me simplifica la búsqueda de la solución particular.
5. Busco una solución particular $x_0 \in \mathbb{Z}$ que satisface que $a'x_0 \equiv c' \pmod{b'}$ (a ojo o encontrando una solución particular de la ecuación diofántica $a'X - b'Y = c'$ asociada).
6. Se concluye que

$$aX \equiv c \pmod{b} \iff X \equiv x_0 \pmod{b'}.$$

Es decir, todas las soluciones son los $x \in \mathbb{Z}$ que satisfacen la ecuación de congruencia

$$X \equiv x_0 \pmod{b'}.$$

9 Primos y Factorización

Recordemos que un número $p \in \mathbb{Z}$ es *primo* si y solo si es $\neq 0, \pm 1$ y tiene únicamente 4 divisores, o, lo que es lo mismo, si y solo si tiene únicamente 2 divisores positivos. También, que un número $a \in \mathbb{Z}$ es *compuesto* si y solo si es $\neq 0, \pm 1$ y existe $c \in \mathbb{Z}$ con $1 < c < |a|$ tal que $c \mid a$.

Los números primos juegan un papel fundamental en el conjunto de los números enteros, y su estudio es la base de la teoría de números o Aritmética.

Una de las propiedades esenciales que distingue a los números primos de los números compuestos es que “todo número es divisible por algún primo”:

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 : $p|a$ ”.

$a = 2$: $p(2)$ es verdadera pues $p := 2|2$.

$a > 2$:

- 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 $1 < c < a$ tal que $c|a$. Por hipótesis inductiva, como $1 < c < a$, existe un primo positivo p tal que $p|c$. Se concluye que $p|a$ por transitividad de la divisibilidad.

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. (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.) La demostración que damos a continuación fue hecha por Euclides alrededor el año 300 AC. Hay muchas otras demostraciones de este hecho (por ejemplo otra conocida se basa en que la serie armónica diverge).

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 $\mathcal{P} = \{p_1, \dots, p_N\}$. 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

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

contradicción que proviene de suponer que hay sólo finitos primos. ■

Otra consecuencia de este hecho es la famosa Criba de Eratóstenes de Cirene (~ 276 – ~ 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:
 $2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, 21, \cancel{22}, 23, \cancel{24}, 25, \cancel{26}, 27, \cancel{28}, 29, \cancel{30}, 31,$
 $\cancel{32}, \cancel{33}, \cancel{34}, \cancel{35}, \cancel{36}, \cancel{37}, \cancel{38}, \cancel{39}, \cancel{40}, \cancel{41}, \cancel{42}, , \cancel{43}, \cancel{44}, \cancel{45}, \cancel{46}, \cancel{47}, \cancel{48}, \cancel{49}, \cancel{50}, \cancel{51}, \cancel{52}, 53, \cancel{54}, 55, \cancel{56}, 57.$
 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:
 $2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, 25, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}, 31,$
 $\cancel{32}, \cancel{33}, \cancel{34}, \cancel{35}, \cancel{36}, \cancel{37}, \cancel{38}, \cancel{39}, \cancel{40}, \cancel{41}, \cancel{42}, , \cancel{43}, \cancel{44}, \cancel{45}, \cancel{46}, \cancel{47}, \cancel{48}, \cancel{49}, \cancel{50}, \cancel{51}, \cancel{52}, 53, \cancel{54}, 55, \cancel{56}, 57.$
 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:
 $2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}, 31,$
 $\cancel{32}, \cancel{33}, \cancel{34}, \cancel{35}, \cancel{36}, \cancel{37}, \cancel{38}, \cancel{39}, \cancel{40}, \cancel{41}, \cancel{42}, , \cancel{43}, \cancel{44}, \cancel{45}, \cancel{46}, \cancel{47}, \cancel{48}, \cancel{49}, \cancel{50}, \cancel{51}, \cancel{52}, 53, \cancel{54}, \cancel{55}, \cancel{56}, 57.$
- Se repite el procedimiento con el 7:
 $2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}, 31,$
 $\cancel{32}, \cancel{33}, \cancel{34}, \cancel{35}, \cancel{36}, \cancel{37}, \cancel{38}, \cancel{39}, \cancel{40}, \cancel{41}, \cancel{42}, , \cancel{43}, \cancel{44}, \cancel{45}, \cancel{46}, \cancel{47}, \cancel{48}, \cancel{49}, \cancel{50}, \cancel{51}, \cancel{52}, 53, \cancel{54}, \cancel{55}, \cancel{56}, 57.$
- 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:

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

■

Digresión sobre Complejidad (1) Dado un número a , hay un algoritmo muy natural para establecer si a es primo o no: simplemente se divide a a por todos los números c menores que él (o por todos los primos menores que él, produciéndolos por ejemplo con la criba, o en realidad alcanza con dividirlo por todos los primos menores que \sqrt{a} , ¿por qué?) y si nunca da resto 0, es que a es primo. Pero este algoritmo no es muy satisfactorio ya que la cantidad de candidatos a divisores c se asemeja a \sqrt{a} (más precisamente a $\sqrt{a/\ln(a)}$) como consecuencia del teorema de distribución de primos conjeturado por Adrien-Marie Legendre en 1798, refinado posteriormente por Carl-Friedrich Gauss, y demostrado independientemente por Jacques Hadamard y Charles-Jean de la Vallée Poussin en 1896): es comunmente aceptado que para que un algoritmo sea eficiente, el número de cuentas que realiza tiene que ser lineal en el tamaño de la entrada, en este caso $\log_2(a)$, o a lo sumo acotado por una potencia fija de ese tamaño (esto es lo que se llama un algoritmo polinomial, o que pertenece a la clase P).

Hasta muy recientemente, el mejor algoritmo para decidir si un número a es primo realizaba $\log_2(a)^{c \log \log \log(a)}$ para una constante fija c , o sea era “casi” polinomial.

En el año 2002, el informático indio, Manindra Agrawal, y dos de sus alumnos que estaban iniciando su tesis doctoral, Neeraj Kayal y Nitin Saxena, mostraron que “Primos está en P”, es decir que se puede establecer si un número entero a es primo (o no) haciendo una cantidad de cuentas acotada por una potencia fija de $\log_2(a)$.

Este test de primalidad (comunmente denominado test de primalidad AKS) no es en realidad

eficiente en la práctica: para ello se siguen usando tests “probabilistas” que dan una evidencia seria de primalidad cuando no pueden probar que un número es compuesto, y son suficientes a efectos prácticos. Sin embargo, el resultado de Agrawal, Kayal y Saxena es fantástico, no sólo por lograr finalmente un objetivo teórico de clasificación buscado por mucha gente durante mucho tiempo, sino por la simplicidad y elegancia de sus métodos. Así fue reconocido por la comunidad matemática: fue publicado en el año 2004 en la revista *Annals of Mathematics* (considerada la mejor revista matemática del mundo) y le valió a sus autores numerosos premios (y a los dos jóvenes excelentes trabajos).

Para terminar esta digresión, el número primo más grande conocido hoy (pero hoy 11 de Octubre de 2011, puede cambiar mañana!) es el “primo de Mersenne” $2^{43112609} - 1$, que tiene 12978189 dígitos según el sitio web <http://primes.utm.edu/largest.html>

Digresión sobre Complejidad (2) Un problema de otra índole, y cuya resolución haría muy famoso a cualquiera, es el problema de, dado un número a compuesto, encontrarle eficientemente un factor c no trivial. El mejor algoritmo a la fecha realiza una cantidad de cuentas lineal en $\sqrt[3]{a} \log_2(a)^{2/3}$, y el número más grande que se logró factorizar (anunciado en el 2010), usando cientos de computadoras que trabajaron durante más de 2 años, tiene 232 dígitos. Se sabe que este problema está en NP, lo que hablando sin precisión, significa que si un “oráculo” me provee de un candidato a factor c , se puede verificar haciendo una cantidad polinomial (en $\log(a)$) de cuentas, si c es efectivamente un factor o no de a . Se cree que este problema es difícil, o sea que no pertenece a la clase P. De hecho la mayoría de los protocolos criptográficos (para transmisión de datos en forma segura y secreta) que se utilizan hoy en día están basados en la dificultad de factorizar números compuestos grandes (o de problemas relacionados), así que mejor que así sea!

La propiedad esencial de los números primos Si p es un número primo (positivo), y $a \in \mathbb{Z}$ es cualquiera, entonces $Div_+(p) = \{1, p\}$ y por lo tanto $DivCom_+(\{p, a\}) \subset \{1, p\}$: es igual a $\{1, p\}$ si $p|a$ y es igual a $\{1\}$ si $p \nmid a$. Por lo tanto el máximo común divisor entre p y a , es igual a p cuando $p|a$ y es igual a 1 cuando $p \nmid a$:

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

En particular, observemos que si p y q son primos positivos distintos, entonces

$$p \perp q \quad \text{y} \quad p^m \perp q^n, \quad \forall m, n \in \mathbb{N}.$$

Volvamos a la Proposición 6.9 (2) para p y a . En este caso, ella dice: $p|ab$ y $p \nmid a \implies p|b$, o equivalentemente:

$$\boxed{p|ab \iff p|a \text{ o } p|b}$$

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, \dots, a_n números enteros, y p un primo. Entonces

$$p|a_1 \cdots a_n \iff p|a_i \text{ para algún } i, 1 \leq i \leq n, \quad \text{y} \quad p|a^n \iff p|a.$$

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 se escribe en forma única como producto de primos, (o se factoriza en forma única como producto de primos,) es decir

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

donde los p_k son primos positivos distintos, y $v_k \in \mathbb{N}$ para $1 \leq k \leq n$, y la 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 , $a \geq 2$:

$p(a)$: “ 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 $c = a/p$ satisface $2 \leq c \leq a - 1$. Por hipótesis 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 pérdida 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 $p_i | 1$ (lo que es absurdo) o $p_i | q_1^{w_1} \cdots q_m^{w_m}$, luego existe j tal que $p_i | q_j$ pero p_i y q_j son primos distintos. Contradicción, que proviene de suponer que sobró un primo de algún lado. ■

Remarquemos que un hecho fundamental que se desprende del teorema (y que de hecho apareció en la demostración de la unicidad) es que $p | a$ si y solo si p aparece en la factorización en primos

de a . Luego cualquiera sea $a \in \mathbb{Z}$, $a \neq 0$, a es divisible por sólo un número finito de primos distintos.

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

$$p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n} | a \iff \begin{cases} p_1^{v_1} | a \\ p_2^{v_2} | a \\ \vdots \\ p_n^{v_n} | a \end{cases}$$

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 excluimos 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 $\{-1, +1\}$:

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

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 $a \in \mathbb{Z}$, $a \neq 0$:

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

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).

Siguiendo esta notación, dado que $c = \pm \prod_{p \in \mathcal{P}} p^{v_p(c)}$, la propiedad en el recuadro anterior se reescribe entonces:

$$c | a \iff p^{v_p(c)} | a, \forall p \in \mathcal{P}$$

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. $v_p(a) \geq 1 \iff p | a$, y $v_p(a) \geq v \iff p^v | a$.
 Más aún, $v_p(a) = v \iff p^v | a$ y $p^{v+1} \nmid a$.

3. $v_p(ab) = v_p(a) + v_p(b)$ y $v_p(a^n) = n v_p(a)$ para todo $p \in \mathcal{P}$ y para todo $n \in \mathbb{N}$.
(Pues si $a = \text{sg}(a) \prod_{p \in \mathcal{P}} p^{v_p(a)}$ y $b = \text{sg}(b) \prod_{p \in \mathcal{P}} p^{v_p(b)}$, entonces

$$ab = \text{sg}(a)\text{sg}(b) \prod_{p \in \mathcal{P}} p^{v_p(a)+v_p(b)} = \text{sg}(a)\text{sg}(b) \prod_{p \in \mathcal{P}} p^{v_p(a)+v_p(b)}.$$

4. $c|a \Leftrightarrow v_p(c) \leq v_p(a)$ para todo $p \in \mathcal{P}$

(combinando la propiedad del recuadro y la propiedad del Inciso 2).

5. $c|a \Leftrightarrow c^n|a^n$
(pues $c|a \Leftrightarrow v_p(c) \leq v_p(a), \forall p \Leftrightarrow n v_p(c) \leq n v_p(a), \forall p \Leftrightarrow v_p(c^n) \leq v_p(a^n), \forall p \Leftrightarrow c^n|a^n$).

Ojo! Tiene que ser el mismo n de los dos lados, si no no vale: por ejemplo $c^2|a^3 \not\Leftrightarrow c|a$ como lo muestra $8^2|4^3$ pero $8 \nmid 4$.

6. $Div(a) = \{c \in \mathbb{Z} : v_p(c) \leq v_p(a), \forall p \in \mathcal{P}\}$ y $\#Div_+(a) = \prod_{p \in \mathcal{P}} (v_p(a) + 1)$,

donde este producto infinito está bien definido pues $v_p(a) + 1 \neq 1 \Leftrightarrow p|a$.

7. $(a : b) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a), v_p(b)\}}$. (1)

Esto es por lo siguiente: llamemos d al número de la derecha de la igualdad (1). Vamos a ver que $d|(a : b)$ y $(a : b)|d$.

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 $d|a$ y $d|b$. Luego $d|(a : b)$.

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, $(a : b)|d$.

8. $a \perp b$ si y solo si $v_p(a)$ y $v_p(b)$ no son simultáneamente positivos, cualquiera sea $p \in \mathcal{P}$.

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 muy 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, dada la disgresión sobre complejidad (2).

Ejemplos

- $Div(2^3 5^4) = \{\pm 2^i 5^j, 0 \leq i \leq 3, 0 \leq j \leq 4\}$, y por lo tanto, $2^3 5^4$ tiene $(3+1)(4+1) = 20$ divisores positivos distintos, y $2 \cdot 20 = 40$ divisores enteros, positivos y negativos.
- $Div(10^{10}) = \{\pm 2^i 5^j, 0 \leq i, j \leq 10\}$, 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.

- En general $p_1^{v_1} \cdots p_n^{v_n}$ tiene $(v_1 + 1) \cdots (v_n + 1)$ divisores positivos y el doble de positivos y negativos.
- Suma de los divisores positivos de 10^{10} :

$$\begin{aligned} \sum_{0 \leq i, j \leq 10} 2^i 5^j &= \sum_{i=0}^{10} \left(\sum_{j=0}^{10} 2^i 5^j \right) = \sum_{i=0}^{10} (2^i \sum_{j=0}^{10} 5^j) = \left(\sum_{j=0}^{10} 5^j \right) \left(\sum_{i=0}^{10} 2^i \right) \\ &= \frac{5^{11} - 1}{5 - 1} \cdot \frac{2^{11} - 1}{2 - 1} = (2^{11} - 1) \frac{5^{11} - 1}{4}. \end{aligned}$$

- 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 $n = 60$.
- $5 | a^2 \Rightarrow 5 | a$ porque 5 es primo. Más aún, se puede deducir que $25 | a^2 \Leftrightarrow 5 | a$:
 \Rightarrow : $25 | a^2$ implica en particular que $5 | a^2$ (por ser un factor de 25) y por lo tanto $5 | a$ por lo visto arriba.
 \Leftarrow : Está claro que si $5 | a$ entonces $25 | a^2$.
- $4 | a^2 \not\Rightarrow 4 | a$ pues por ejemplo $4 | 2^2$ pero $4 \nmid 2$.
- $10 | a^2 \Rightarrow 10 | a$ aunque 10 no es primo, pero por ser un producto de primos distintos:

$$10 | a^2 \xleftrightarrow[2 \cdot 5]{\Leftrightarrow} 2 | a^2 \text{ y } 5 | a^2 \xleftrightarrow[2, 5 \text{ primos}]{\Leftrightarrow} 2 | a \text{ y } 5 | a \xleftrightarrow[2 \cdot 5]{\Leftrightarrow} 10 = 2 \cdot 5 | a.$$

Pero más aún, $100 | a^2 \Leftrightarrow 10 | a$:
 \Rightarrow : $100 | a^2 \Rightarrow 10 | a^2$, y por lo visto arriba, se deduce que $10 | a$.
 \Leftarrow : Claramente $10 | a \Rightarrow 100 | a^2$.

- $32 | a^2 \Rightarrow 8 | a$, pues:
 $2^5 | a^2 \Rightarrow v_2(2^5) \leq v_2(a^2) \Rightarrow 5v_2(2) \leq 2v_2(a) \Rightarrow \frac{5}{2} \leq v_2(a) \xrightarrow{v_2(a) \in \mathbb{N}_0} 3 \leq v_2(a) \Rightarrow 2^3 | a.$

Más aún, lo que vale claramente es $8 | a \Leftrightarrow 64 | a^2$, ya que si el primo 2 aparece con exponente 3 en a , aparece con exponente 2.3 en a^2 , y recíprocamente si el primo 2 aparece con exponente 6 en a^2 , aparece con exponente $\frac{6}{2}$ en a .

- $2^4 \cdot 3^3 \cdot 5^7 | a^3 \Rightarrow 2^2 \cdot 3 \cdot 5^3 | a$, pues:

$$\begin{aligned} 2^4 \cdot 3^3 \cdot 5^7 | a^3 &\Leftrightarrow 2^4 | a^3 && \text{y } 3^3 | a^3 && \text{y } 5^7 | a^3 \\ &\Rightarrow v_2(2^4) \leq v_2(a^3) && \text{y } v_3(3^3) \leq v_3(a^3) && \text{y } v_5(5^7) \leq v_5(a^3) \\ &\Rightarrow 4 \leq 3v_2(a) && \text{y } 3 \leq 3v_3(a) && \text{y } 7 \leq 3v_5(a) \\ &\Rightarrow 2 \leq v_2(a) && \text{y } 1 \leq v_3(a) && \text{y } 3 \leq v_5(a) \\ &\Rightarrow 2^2 | a && \text{y } 3 | a && \text{y } 5^3 | a \\ \Rightarrow &2^2 \cdot 3 \cdot 5^3 | a \end{aligned}$$

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

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

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

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

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 $1200n$ 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 satisfacen 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 $(ab(a+b) : a^2 + b^2)$ para $a \perp b$:

Si aquí buscamos como siempre la forma de un divisor común d operando con las expresiones $ab(a+b)$ 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 $d := (ab(a+b) : a^2 + b^2)$, y sea p un primo. Se tiene

$$p|d \iff p|ab(a+b) \text{ y } p|a^2 + b^2.$$

Ahora bien:

$$p|ab(a+b) \iff p|a \text{ ó } p|b \text{ ó } p|a+b.$$

Miremos cada combinación de casos posibles por separado:

$$p|a \text{ y } p|a^2 + b^2 \underset{p \text{ primo}}{\iff} p|a^2 \text{ y } p|a^2 + b^2 \iff p|a^2 \text{ y } p|b^2 \underset{p \text{ primo}}{\iff} p|a \text{ y } p|b,$$

es una contradicción pues $a \perp b$ por hipótesis: no puede haber ningún primo que divida a ambos a la vez. De la misma forma:

$$p|b \text{ y } p|a^2 + b^2 \underset{p \text{ primo}}{\iff} p|b^2 \text{ y } p|a^2 + b^2 \iff p|b^2 \text{ y } p|a^2 \underset{p \text{ primo}}{\iff} p|b \text{ y } p|a,$$

contradicción. Finalmente:

$$p|a+b \text{ y } p|a^2 + b^2 \implies p|(a-b)(a+b) \text{ y } p|a^2 + b^2 \iff p|a^2 - b^2 \text{ y } p|a^2 + b^2 \implies p|2a^2 \text{ y } p|2b^2.$$

Luego $p|(2a^2 : 2b^2) = 2(a^2 : b^2) = 2$ por ser $a^2 \perp b^2$ al ser $a \perp b$ por hipótesis.

Se concluye que el único primo posible que puede dividir al mcd d es el primo 2. Luego $d = 2^k$ para algún $k \geq 0$.

Vamos a analizar ahora qué valores posibles puede tomar k . Dado que solo interviene el primo 2, que tiene que ver con la paridad, podemos por ejemplo distinguir 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, $2 \nmid d$ en este caso. Por lo tanto $d = 1$.
- $a \equiv 0 \pmod{2}$ y $b \equiv 1 \pmod{2}$ es igual al caso anterior: $d = 1$.
- $a \equiv b \equiv 1 \pmod{2} \Rightarrow a + b \equiv 0 \pmod{2}$ y $a^2 + b^2 \equiv 0 \pmod{2}$, luego $2 \mid ab(a + b)$ y $2 \mid a^2 + b^2$, es decir $2 \mid d$ y en este caso $d = 2^k$ con $k \geq 1$.
Pero al ser a y b impares, se tiene que $2^k \nmid a$ y $2^k \nmid b$, luego $2^k \mid ab(a + b)$ implica $2^k \mid a + b$. Junto con $2^k \mid a^2 + b^2$, el mismo análisis hecho arriba implica que $2^k \mid 2(a^2 + b^2) = 2$, es decir $k \leq 1$. Por lo tanto en este caso $d = 2$.

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 $|ab|$, y es único, por ser el menor.

El mínimo común múltiplo entre a y b se nota $\text{mcm}(a, b)$ o $[a : b]$ que es la notación que adoptamos aquí. Es entonces caracterizado por:

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

Ejemplos

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

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

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

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 $a \mid c$ y $b \mid c$. Luego $[a : b] \leq c$.

Pero por otro lado, $a \mid [a : b]$ y $b \mid [a : b]$ 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 $c \mid [a : b]$, y, al ser ambos positivos, $c \leq [a : b]$. ■

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

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

$$a \mid m \quad y \quad b \mid m \quad \implies \quad [a : b] \mid m.$$

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

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

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 para números grandes 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 para números grandes más veloz que factorizar.

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

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

Una forma: 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

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

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:

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

Otra forma: (tal vez más sencilla) es pensando en *coprimizar*: recordemos que $a = (a : b)a'$ y $b = (a : b)b'$ con $a \perp b$. Luego $(a : b)^2 a'b' = ab = (a : b)[a : b]$, es decir

$$a'b' = \frac{[a : b]}{(a : b)} = \frac{2^5 \cdot 3 \cdot 5^2 \cdot 17^2}{2^2 \cdot 3 \cdot 17} = 2^3 \cdot 5^2 \cdot 17, \text{ con } a' \perp b'.$$

Al ser $a' \perp b'$ no puede aparecer un mismo primo simultáneamente en a' y b' , y por lo tanto las posibilidades son (eligiendo cuáles son los primos que aparecen en a' y luego los restantes estarán en b'):

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

Multiplicando estos números por $(a : b) = 2^2 \cdot 3 \cdot 17$ se obtienen todos los pares (que obviamente coinciden con los que obtuvimos con la otra forma de resolver el problema).

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 “Último 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 seudoprimsos.
- 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:

$$\Phi : \begin{array}{ccc} \{1, 2, \dots, p-1\} & \longrightarrow & \{1, 2, \dots, p-1\} \\ k & \longmapsto & r_p(ka) \end{array}$$

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

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

- $\text{Im}(\Phi) \subseteq \{1, 2, \dots, p-1\}$:

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

$$\Phi(k) = 0 \iff r_p(ka) = 0 \iff p \mid ka \iff_{p \text{ primo}} p \mid k \text{ ó } p \mid a,$$

lo que es absurdo pues por hipótesis $p \nmid a$ y $p \nmid k$ por ser $k \in \{1, \dots, p-1\}$ más chico que p .

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

$$\Phi(k) = \Phi(j) \iff r_p(ka) = r_p(ja) \iff p \mid ka - ja = (k-j)a \iff_{p \text{ primo}} p \mid k-j \text{ ó } p \mid a,$$

lo que se cumple únicamente si $p \mid k-j$ pues $p \nmid a$. Ahora bien, como $1 \leq j \leq k \leq p-1$, se tiene que $k-j \in \{0, \dots, p-1\}$, luego

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

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

$$\begin{aligned} \text{Im}(\Phi) = \{1, 2, \dots, p-1\} &\implies \Phi(1) \cdot \Phi(2) \cdots \Phi(p-1) = 1 \cdot 2 \cdots (p-1) \implies \\ r_p(a) \cdot r_p(2a) \cdots r_p((p-1)a) &= 1 \cdot 2 \cdots (p-1) \implies \\ a \cdot 2a \cdots (p-1)a &\equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \implies \\ (p-1)! a^{p-1} &\equiv (p-1)! \pmod{p} \implies a^{p-1} \equiv 1 \pmod{p}, \end{aligned}$$

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 $1 \leq i \leq p-1$ 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:

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

Prueba. –

$$n = k(p-1) + r \implies a^n = a^{k(p-1)+r} = (a^{p-1})^k a^r \stackrel{\text{PTF}}{\equiv} 1^k a^r \equiv a^r \pmod{p}.$$

■

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

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

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

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 $0 \leq r < 6$:

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

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 $7 \nmid a$:

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

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

12 Teorema Chino del Resto (TCR)

Este teorema, sobre la resolución simultánea de varias congruencias, se encontraba ya en su forma original (sin demostración) en un libro de matemática chino en el Siglo III A.C. En el capítulo 8 aprendimos a resolver ecuaciones de congruencia: para cada ecuación de la forma $aX \equiv c \pmod{b}$ sabemos producir la ecuación equivalente (es decir con las mismas soluciones) más simple posible, que es de la forma $X \equiv x_0 \pmod{b'}$. Ahora se trata de resolver *sistemas* de ecuaciones de congruencia de la forma

$$\begin{cases} X \equiv c_1 \pmod{b_1} \\ X \equiv c_2 \pmod{b_2} \\ \vdots \\ X \equiv c_n \pmod{b_n} \end{cases} \quad (3)$$

donde $c_1, \dots, c_n \in \mathbb{Z}$ y $b_1, \dots, b_n \in \mathbb{Z}$ no nulos. Aquí resolver significa obtener una descripción equivalente via una ecuación de congruencia simple (que tenga las mismas soluciones) de la forma

$$X \equiv x_0 \pmod{b}.$$

Adoptamos como en el Capítulo 8 la notación \Leftrightarrow para sistemas de ecuaciones de congruencia equivalentes, o sea con las mismas soluciones.

Se utilizarán sistemáticamente las propiedades siguientes, que ya fueron mencionadas, además del hecho que ya sabemos resolver una ecuación de congruencia:

- Propiedades 3.3: Dados $x, c, b, d, k \in \mathbb{Z}$ con b, d, k no nulos, se tiene
 - $x \equiv c \pmod{b}$ y $d \mid b \implies x \equiv c \pmod{d}$,
 - $x \equiv c \pmod{b} \iff kx \equiv kc \pmod{kb}$.
 Lo que implica que $X \equiv c \pmod{b} \iff kX \equiv kc \pmod{kb}$.
- Como consecuencia de la Proposición 6.9 (1): Dados $c, b_1, b_2, \dots, b_n \in \mathbb{Z}$ con $b_i \perp b_j$ para $i \neq j$, se tiene

$$\begin{cases} X \equiv c \pmod{b_1} \\ X \equiv c \pmod{b_2} \\ \vdots \\ X \equiv c \pmod{b_n} \end{cases} \iff X \equiv c \pmod{b_1 \cdot b_2 \cdots b_n} \quad (4)$$

Ejemplos

-

$$\begin{cases} X \equiv 3 \pmod{22} \\ X \equiv 3 \pmod{5} \\ X \equiv 3 \pmod{21} \end{cases} \iff X \equiv 3 \pmod{22 \cdot 5 \cdot 21},$$

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

- De la misma forma:

$$X \equiv 50 \pmod{22 \cdot 5 \cdot 21} \iff \begin{cases} X \equiv 50 \pmod{22} \\ X \equiv 50 \pmod{5} \\ X \equiv 50 \pmod{21} \end{cases} \iff \begin{cases} X \equiv 6 \pmod{22} \\ X \equiv 0 \pmod{5} \\ X \equiv 8 \pmod{21} \end{cases} .$$

-

$$\begin{cases} X \equiv 3 \pmod{22} \\ X \equiv 4 \pmod{11} \end{cases} \iff \begin{cases} X \equiv 3 \pmod{2} \\ X \equiv 3 \pmod{11} \\ X \equiv 4 \pmod{11} \end{cases} \iff \begin{cases} X \equiv 1 \pmod{2} \\ X \equiv 3 \pmod{11} \\ X \equiv 4 \pmod{11} \end{cases} ,$$

y luego el sistema no tiene solución (es incompatible) pues la segunda y la tercer ecuación a la derecha no pueden satisfacerse simultáneamente.

-

$$\begin{cases} X \equiv 3 \pmod{22} \\ X \equiv 4 \pmod{8} \end{cases} \iff \begin{cases} X \equiv 1 \pmod{2} \\ X \equiv 3 \pmod{11} \\ X \equiv 4 \pmod{8} \end{cases}$$

y luego es incompatible pues la tercer ecuación a la derecha implica que si hubiera una solución x , entonces satisficiera también $x \equiv 4 \pmod{2}$ (aplicando una de las propiedades recordadas más arriba), es decir $x \equiv 0 \pmod{2}$, que es claramente incompatible con satisfacer la primer ecuación.

-

$$\begin{cases} X \equiv 1 \pmod{4} \\ X \equiv 5 \pmod{8} \end{cases} \iff X \equiv 5 \pmod{8}$$

pues si x cumple la segunda ecuación, cumple automáticamente la primera:
 $x \equiv 5 \pmod{8} \implies x \equiv 5 \pmod{4} \implies x \equiv 1 \pmod{4}$. La otra implicación es obvia.

-

$$\begin{cases} X \equiv 3 \pmod{22} \\ X \equiv 5 \pmod{8} \\ X \equiv 17 \pmod{20} \end{cases} \iff \begin{cases} X \equiv 1 \pmod{2} \\ X \equiv 3 \pmod{11} \\ X \equiv 5 \pmod{8} \\ X \equiv 1 \pmod{4} \\ X \equiv 2 \pmod{5} \end{cases} \iff \begin{cases} X \equiv 5 \pmod{8} \\ X \equiv 3 \pmod{11} \\ X \equiv 2 \pmod{5} \end{cases}$$

pues si $x \in \mathbb{Z}$ satisface $x \equiv 5 \pmod{8}$, entonces $x \equiv 5 \pmod{4}$ 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 tercer ecuación se cumplen automáticamente 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 b_i son coprimos dos a dos**. En esa situación vale el teorema siguiente:

Teorema 12.1 (Teorema Chino del Resto)

Sean $c_1, \dots, c_n \in \mathbb{Z}$ y $b_1, \dots, b_n \in \mathbb{Z}$ no nulos, con $b_i \perp b_j$ para $i \neq j$. Entonces el sistema de ecuaciones de congruencia

$$\begin{cases} X \equiv c_1 \pmod{b_1} \\ X \equiv c_2 \pmod{b_2} \\ \vdots \\ X \equiv c_n \pmod{b_n} \end{cases}$$

tiene soluciones.

Más aún,

$$\begin{cases} X \equiv c_1 \pmod{b_1} \\ X \equiv c_2 \pmod{b_2} \\ \vdots \\ X \equiv c_n \pmod{b_n} \end{cases} \rightsquigarrow X \equiv x_0 \pmod{b_1 \cdot b_2 \cdots b_n},$$

donde $x_0 \in \mathbb{Z}$ es una solución particular.

Finalmente, existe un único así con $0 \leq x_0 < b_1 \cdot b_2 \cdots b_n$.

Prueba. –

Supongamos que ya mostramos que el sistema tiene soluciones. Entonces, sea $x_0 \in \mathbb{Z}$ una solución particular, es decir $x_0 \in \mathbb{Z}$ satisface

$$\begin{cases} x_0 \equiv c_1 \pmod{b_1} \\ x_0 \equiv c_2 \pmod{b_2} \\ \vdots \\ x_0 \equiv c_n \pmod{b_n} \end{cases}.$$

En ese caso, por transitividad y aplicando la propiedad descrita en la Fórmula (4), tendremos para una solución cualquiera x :

$$\begin{cases} x \equiv c_1 \pmod{b_1} \\ x \equiv c_2 \pmod{b_2} \\ \vdots \\ x \equiv c_n \pmod{b_n} \end{cases} \iff \begin{cases} x \equiv x_0 \pmod{b_1} \\ x \equiv x_0 \pmod{b_2} \\ \vdots \\ x \equiv x_0 \pmod{b_n} \end{cases} \iff x \equiv x_0 \pmod{b_1 \cdot b_2 \cdots b_n},$$

O sea probamos la equivalencia enunciada en el Teorema.

El único x_0 que satisface $0 \leq x_0 < b_1 \cdots b_n$ se obtiene reemplazando la solución particular elegida por $r_{b_1 \cdots b_n}(x_0)$.

Para probar que existen soluciones (y hallar una solución particular x_0), vamos a subdividir el sistema (3) en n sistemas más simples y probar que cada uno de ellos tiene soluciones. Estos sistemas S_1, S_2, \dots, S_n son:

$$\begin{array}{ccc} \underline{S_1} : & \underline{S_2} : & \underline{S_n} : \\ \begin{cases} X \equiv c_1 \pmod{b_1} \\ X \equiv 0 \pmod{b_2} \\ X \equiv 0 \pmod{b_3} \\ \vdots \\ X \equiv 0 \pmod{b_n} \end{cases} & \text{y} \begin{cases} X \equiv 0 \pmod{b_1} \\ X \equiv c_2 \pmod{b_2} \\ X \equiv 0 \pmod{b_3} \\ \vdots \\ X \equiv 0 \pmod{b_n} \end{cases} & \text{y} \dots \text{y} \begin{cases} X \equiv 0 \pmod{b_1} \\ X \equiv 0 \pmod{b_2} \\ \vdots \\ X \equiv 0 \pmod{b_{n-1}} \\ X \equiv c_n \pmod{b_n} \end{cases} \end{array}$$

Supongamos que podemos probar que cada uno de estos sistemas S_ℓ , $1 \leq \ell \leq n$ tiene soluciones, y encontramos para cada uno una solución particular x_ℓ , es decir:

$$\begin{array}{ccc} \underline{S_1} : & \underline{S_2} : & \underline{S_n} : \\ \begin{cases} x_1 \equiv c_1 \pmod{b_1} \\ x_1 \equiv 0 \pmod{b_2} \\ x_1 \equiv 0 \pmod{b_3} \\ \vdots \\ x_1 \equiv 0 \pmod{b_n} \end{cases} & \text{y} \begin{cases} x_2 \equiv 0 \pmod{b_1} \\ x_2 \equiv c_2 \pmod{b_2} \\ x_2 \equiv 0 \pmod{b_3} \\ \vdots \\ x_2 \equiv 0 \pmod{b_n} \end{cases} & \text{y} \dots \text{y} \begin{cases} x_n \equiv 0 \pmod{b_1} \\ x_n \equiv 0 \pmod{b_2} \\ \vdots \\ x_n \equiv 0 \pmod{b_{n-1}} \\ x_n \equiv c_n \pmod{b_n} \end{cases} \end{array}$$

Entonces si definimos

$$x_0 := x_1 + x_2 + x_3 + \cdots + x_n,$$

se satisface que

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_n \equiv c_1 + 0 + 0 + \cdots + 0 \pmod{b_1} \\ x_1 + x_2 + x_3 + \cdots + x_n \equiv 0 + c_2 + 0 + \cdots + 0 \pmod{b_2} \\ \vdots \\ x_1 + x_2 + x_3 + \cdots + x_n \equiv 0 + 0 + \cdots + 0 + c_n \pmod{b_n} \end{cases} \implies \begin{cases} x_0 \equiv c_1 \pmod{b_1} \\ x_0 \equiv c_2 \pmod{b_2} \\ \vdots \\ x_0 \equiv c_n \pmod{b_n} \end{cases}$$

es decir, x_0 es una solución (particular) del sistema original, y en particular el sistema original tiene soluciones.

Aplicando lo que se hizo en el Capítulo 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 b_2, b_3, \dots, b_n son todos coprimos entre sí, si ponemos $B_1 := b_2 \cdot b_3 \cdots b_n$, se tiene la equivalencia descrita en la fórmula (4):

$$\begin{cases} X \equiv c_1 \pmod{b_1} \\ X \equiv 0 \pmod{b_2} \\ X \equiv 0 \pmod{b_3} \\ \vdots \\ X \equiv 0 \pmod{b_n} \end{cases} \iff \begin{cases} X \equiv c_1 \pmod{b_1} \\ X \equiv 0 \pmod{B_1} \end{cases}.$$

La segunda ecuación a la derecha indica que cualquier solución x tiene que satisfacer que $x = B_1 y$ para algún $y \in \mathbb{Z}$, y luego para cumplir con la primer ecuación, se tiene que satisfacer $B_1 y \equiv c_1 \pmod{b_1}$, o sea hay y es una solución de la ecuación

$$B_1 Y \equiv c_1 \pmod{b_1}. \quad (5)$$

Se observa que $B_1 \perp b_1$, por ser $B_1 = b_2 \cdots b_n$ y los b_i coprimos dos a dos. Por lo tanto, por el Corolario 8.3, la ecuación (5) tiene soluciones. Si y_1 es una solución particular, entonces claramente $x_1 := b_1 y_1$ es una solución particular del sistema S_1 .

Veamos de forma análoga que para todo ℓ , $1 \leq \ell \leq n$, el sistema

$$S_\ell : \begin{cases} X \equiv 0 \pmod{b_1} \\ \vdots \\ X \equiv 0 \pmod{b_{\ell-1}} \\ X \equiv c_\ell \pmod{b_\ell} \\ X \equiv 0 \pmod{b_{\ell+1}} \\ \vdots \\ X \equiv 0 \pmod{b_n} \end{cases}$$

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

Definamos $B_\ell := \prod_{j \neq \ell} b_j$ y repitamos lo que se hizo arriba para S_1 . Se tiene $B_\ell \perp b_\ell$ por ser todos los b_i coprimos dos a dos. Luego, por el Corolario 8.3, la ecuación de congruencia

$$B_\ell Y \equiv c_\ell \pmod{B_\ell}$$

tiene soluciones, y si y_ℓ es una solución particular, entonces, como arriba, $x_\ell := B_\ell y_\ell$ es una solución particular del sistema S_ℓ . ■

Ejemplos

$$\begin{cases} X \equiv 4 & (\text{mod } 8) \\ X \equiv 10 & (\text{mod } 35) \\ X \equiv 1 & (\text{mod } 3) \end{cases}$$

Como 8, 35 y 3 son coprimos 2 a 2, por el Teorema 12.1, el sistema tiene soluciones y es equivalente a $X \equiv x_0 \pmod{8 \cdot 35 \cdot 3}$, es decir $X \equiv x_0 \pmod{840}$, donde x_0 es una solución particular.

Para hallar una solución particular x_0 , se consideran los tres sistemas más simples:

$$\begin{array}{ccc} \underline{S_1} : & \underline{S_2} : & \underline{S_3} : \\ \begin{cases} X \equiv 4 & (\text{mod } 8) \\ X \equiv 0 & (\text{mod } 35) \\ X \equiv 0 & (\text{mod } 3) \end{cases}, & \begin{cases} X \equiv 0 & (\text{mod } 8) \\ X \equiv 10 & (\text{mod } 35) \\ X \equiv 0 & (\text{mod } 3) \end{cases}, & \begin{cases} X \equiv 0 & (\text{mod } 8) \\ X \equiv 0 & (\text{mod } 35) \\ X \equiv 1 & (\text{mod } 3) \end{cases}. \end{array}$$

Solución particular para S_1 :

$$\begin{cases} X \equiv 4 & (\text{mod } 8) \\ X \equiv 0 & (\text{mod } 35) \\ X \equiv 0 & (\text{mod } 3) \end{cases} \iff \begin{cases} X \equiv 4 & (\text{mod } 8) \\ X \equiv 0 & (\text{mod } 35 \cdot 3) \end{cases}$$

Es decir una solución x satisface $x = 105y$ donde y es solución de la ecuación $105Y \equiv 4 \pmod{8}$, o sea de la ecuación $Y \equiv 4 \pmod{8}$. Una solución particular es $y_1 = 4$, y por lo tanto $x_1 = 105y_1 = 420$ es una solución particular del sistema S_1 .

Solución particular para S_2 :

$$\begin{cases} X \equiv 0 & (\text{mod } 8) \\ X \equiv 10 & (\text{mod } 35) \\ X \equiv 0 & (\text{mod } 3) \end{cases} \iff \begin{cases} X \equiv 10 & (\text{mod } 35) \\ X \equiv 0 & (\text{mod } 8 \cdot 3) \end{cases}.$$

Es decir una solución x satisface $x = 24y$ donde y es solución de la ecuación $24Y \equiv 10 \pmod{35}$. 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 $x_2 = 24y_2 = 360$ es una solución particular del sistema S_2 .

Solución particular para S_3 :

$$\begin{cases} X \equiv 0 & (\text{mod } 8) \\ X \equiv 0 & (\text{mod } 35) \\ X \equiv 1 & (\text{mod } 3) \end{cases} \iff \begin{cases} X \equiv 1 & (\text{mod } 3) \\ X \equiv 0 & (\text{mod } 8 \cdot 35) \end{cases}.$$

Es decir una solución x satisface $x = 280y$ donde y es solución de la ecuación $280Y \equiv 1 \pmod{3}$, o sea de la ecuación $Y \equiv 1 \pmod{3}$. Una solución particular es $y_3 = 1$, por lo tanto $x_3 = 280y_3 = 280$ es una solución particular de S_3 .

Por lo tanto, aplicando la construcción del Teorema 12.1,

$$x_0 := x_1 + x_2 + x_3 = 240 + 360 + 280 = 1060$$

es una solución particular del sistema original, y éste es equivalente a $X \equiv 1060 \pmod{840}$. Claramente se puede achicar x_0 utilizando que $1060 \equiv 220 \pmod{840}$, y de esa manera se obtiene $0 \leq x_0 < 840$: se tiene entonces la equivalencia

$$\begin{cases} X \equiv 4 \pmod{8} \\ X \equiv 10 \pmod{35} \\ X \equiv 1 \pmod{3} \end{cases} \iff X \equiv 220 \pmod{840}.$$

(Y $x_0 = 220$ es la única solución particular del sistema que satisface $0 \leq x_0 < 840$.)

$$\begin{cases} X \equiv 3 \pmod{10} \\ X \equiv 1 \pmod{11} \\ X \equiv 3 \pmod{7} \end{cases}$$

Nuevamente, 10, 11 y 7 son coprimos 2 a 2, luego por el teorema el sistema tiene soluciones y es equivalente a $X \equiv x_0 \pmod{10 \cdot 11 \cdot 7}$, es decir $X \equiv x_0 \pmod{770}$, donde x_0 es una solución particular. Ahora bien, por el Corolario 8.3, la primer y tercer ecuación se pueden juntar en la ecuación $X \equiv 3 \pmod{70}$, al ser 10 y 7 coprimos. Por lo tanto para hallar una solución particular, es suficiente aquí considerar los dos sistemas:

$$\begin{array}{l} \underline{S_1}: \\ \begin{cases} X \equiv 3 \pmod{70} \\ X \equiv 0 \pmod{11} \end{cases}, \end{array} \quad \begin{array}{l} \underline{S_2}: \\ \begin{cases} X \equiv 0 \pmod{70} \\ X \equiv 1 \pmod{11} \end{cases}. \end{array}$$

Solución particular para S_1 :

Una solución particular x_1 satisface $x_1 = 11y_1$ donde y_1 es solución particular de la ecuación $11Y \equiv 3 \pmod{70}$. Por ejemplo $y_1 = 13$, y por lo tanto $x_1 = 11 \cdot 13 = 143$.

Solución particular para S_2 :

Una solución particular x_2 satisface $x_2 = 70y_2$ donde y_2 es solución particular de la ecuación $70Y \equiv 1 \pmod{11}$, o sea $4Y \equiv 1 \pmod{11}$. Por ejemplo $y_2 = 3$, y por lo tanto $x_2 = 70y_2 = 210$.

Así, $x_0 := x_1 + x_2 = 143 + 210 = 353$ es solución particular del sistema original, y se tiene la equivalencia

$$\begin{cases} X \equiv 3 \pmod{10} \\ X \equiv 1 \pmod{11} \\ X \equiv 3 \pmod{7} \end{cases} \iff X \equiv 353 \pmod{770}.$$

Ejemplos

- Retomemos el segundo ejemplo arriba:

$$\begin{cases} X \equiv 3 \pmod{70} \\ X \equiv 1 \pmod{11} \end{cases} .$$

Sabemos que el sistema tiene solución y es equivalente a $X \equiv x_0 \pmod{770}$ donde x_0 es la única solución particular del sistema con $0 \leq x_0 < 770$. Veamos si podemos encontrar ese x_0 “a ojo”. Para ello investiguemos los valores entre 0 y 770 que cumplen la primera ecuación. Estos son:

$$3, 73, 143, 213, 283, 353, 423, 493, \dots$$

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

$$3, 73, 143, 213, 283, \boxed{353}, \dots$$

¡Ya está! ¡encontramos uno, entonces ese es x_0 y el sistema es equivalente a la ecuación $X \equiv 353 \pmod{770}$!

- Volvamos al último ejemplo antes del enunciado del TCR:

$$\begin{cases} X \equiv 3 \pmod{22} \\ X \equiv 5 \pmod{8} \\ X \equiv 17 \pmod{20} \end{cases} \rightsquigarrow \begin{cases} X \equiv 5 \pmod{8} \\ X \equiv 3 \pmod{11} \\ X \equiv 2 \pmod{5} \end{cases}$$

Como 8, 11 y 5 son coprimos dos a dos, sabemos que el sistema es equivalente a

$$X \equiv x_0 \pmod{8 \cdot 11 \cdot 5 = 440}$$

donde x_0 , es la única solución del sistema con $0 \leq x_0 < 440$. 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:

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

¿Cuál cumple la condición con el módulo 8?

$$3, \cancel{14}, \cancel{25}, 36, \cancel{47}, 58, \boxed{69}, 80, \dots$$

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:

$$69, \boxed{157}, \dots$$

¡Ya está!

$$\begin{cases} X \equiv 3 \pmod{22} \\ X \equiv 5 \pmod{8} \\ X \equiv 17 \pmod{20} \end{cases} \rightsquigarrow X \equiv 157 \pmod{440}.$$

- Un ejemplo donde las ecuaciones iniciales no están en la forma $X \equiv c_\ell \pmod{b_\ell}$:

$$\begin{cases} 3X \equiv 2 \pmod{7} \\ 7X \equiv 5 \pmod{8} \\ 6X \equiv 8 \pmod{10} \end{cases} .$$

Primero se puede simplificar todo lo que se puede (por ejemplo un factor común en la tercer ecuación), y luego como los módulos resultan coprimos dos a dos, resolver cada ecuación en la forma $X \equiv c_\ell \pmod{b_\ell}$ para aplicar el TCR:

$$\begin{cases} 3X \equiv 2 \pmod{7} \\ 7X \equiv 5 \pmod{8} \\ 6X \equiv 8 \pmod{10} \end{cases} \iff \begin{cases} 3X \equiv 2 \pmod{7} \\ 7X \equiv 5 \pmod{8} \\ 3X \equiv 4 \pmod{5} \end{cases} \iff \begin{cases} X \equiv 3 \pmod{7} \\ X \equiv 3 \pmod{8} \\ X \equiv 3 \pmod{5} \end{cases} \iff X \equiv 3 \pmod{280},$$

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

- Sea $x \in \mathbb{Z}$ tal que $r_9(4x) = 2$, $r_{14}(3x) = 5$ y $r_{20}(3x) = 1$. Calcular los posibles restos de dividir a x por $9 \cdot 14 \cdot 20 = 2520$:

Se tiene que x es solución del sistema

$$\begin{cases} 4X \equiv 2 \pmod{9} \\ 3X \equiv 5 \pmod{14} \\ 3X \equiv 1 \pmod{20} \end{cases} \iff \begin{cases} 2X \equiv 1 \pmod{9} \\ 3X \equiv 5 \pmod{2} \\ 3X \equiv 5 \pmod{7} \\ 3X \equiv 1 \pmod{4} \\ 3X \equiv 1 \pmod{5} \end{cases} \iff \begin{cases} X \equiv 5 \pmod{9} \\ X \equiv 1 \pmod{2} \\ X \equiv 4 \pmod{7} \\ X \equiv 3 \pmod{4} \\ X \equiv 2 \pmod{5} \end{cases} \iff \begin{cases} X \equiv 5 \pmod{9} \\ X \equiv 4 \pmod{7} \\ X \equiv 3 \pmod{4} \\ X \equiv 2 \pmod{5} \end{cases}$$

pues si $x \equiv 3 \pmod{4}$, automáticamente se cumple que $x \equiv 1 \pmod{2}$. Al resolver este sistema con el método dado por el TCR, se obtiene que el sistema original es equivalente a

$$X \equiv 1607 \pmod{9 \cdot 7 \cdot 4 \cdot 5 = 1260} \iff X \equiv 347 \pmod{1260}$$

Luego el resto de dividir a x por 1260 es 347, pero si se quieren los posibles restos de dividir a x por $2520 = 2 \cdot 1260$, éstos son 347 y $347 + 1260 = 1607$, los dos números entre 0 y 2520 que son congruentes con 347 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 para 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.

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

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

$$\underline{r_5(n)}:$$

Por el PTF (Consecuencia 11.2), ya que 5 es primo,

$$3^{2^{25}} \underset{5 \nmid 3}{\equiv} 3^{r_4(2^{25})} \underset{4 \mid 2^{25}}{\equiv} 3^0 \equiv 1 \pmod{5}.$$

$r_{13}(n)$:

Como $13 \nmid 3$, para aplicar el PTF, necesitamos conocer $r_{12}(2^{25})$. Para ello alcanza con conocer $r_3(2^{25})$ y $r_4(2^{25})$ y luego aplicar el TCR.

$$2^{25} \underset{\text{PTF}, 3 \nmid 2}{\equiv} 2^{r_2(2^5)} \equiv 2^1 \equiv 2 \pmod{3} \quad \text{y} \quad 2^{25} \equiv 0 \pmod{4} \xrightarrow{\text{TCR}} 2^{25} \equiv 8 \pmod{12}.$$

Así,

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

$r_{390}(n)$:

$$\begin{cases} n \equiv 1 \pmod{2} \\ n \equiv 0 \pmod{3} \\ n \equiv 1 \pmod{5} \\ n \equiv 9 \pmod{13} \end{cases} \xleftrightarrow{\text{TCR}} n \equiv 321 \pmod{390}$$

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

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

Como $55 = 5 \cdot 11$, para $b \in \mathbb{Z}$ cualquiera, el valor de $(b : 55)$ puede ser en principio 1, 5, 11 o 55. Por lo tanto se observa que

$$(b : 55) = 11 \iff 11 \mid b \text{ y } 5 \nmid b.$$

Determinamos entonces para qué valores de $a \in \mathbb{Z}$, $11 \mid 12a^{41} - a^{31} - a$ y $5 \nmid 12a^{41} - a^{31} - a$:

Para el 11:

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

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

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

Por lo tanto

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

Para el 5:

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

Pero si $5 \nmid a$, entonces, por el PTF, $12a^{40} - a^{30} - 1 \equiv 2a^0 - a^2 - 1 \equiv 1 - a^2 \pmod{5}$. 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

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

Se concluye aplicando el TCR:

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

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

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

$$\begin{aligned} \begin{cases} c \mid 11a + 3 \cdot 2^{150} \\ c \mid 3a - 2^{151} \end{cases} &\implies \begin{cases} c \mid 33a + 9 \cdot 2^{150} \\ c \mid 33a - 11 \cdot 2^{151} \end{cases} \implies c \mid 31 \cdot 2^{150}. \\ \begin{cases} c \mid 11a + 3 \cdot 2^{150} \\ c \mid 3a - 2^{151} \end{cases} &\implies \begin{cases} c \mid 22a + 3 \cdot 2^{151} \\ c \mid 9a - 3 \cdot 2^{151} \end{cases} \implies c \mid 31 \cdot a. \end{aligned}$$

Ahora bien, $c \mid 31 \cdot 2^{150}$ y $c \mid 31 \cdot a \iff c \mid (31 \cdot 2^{150} : 31 \cdot a) = 31(2^{150} : a) = 31$ 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 $31 \mid 11a + 3 \cdot 2^{150}$ y que $31 \mid 3a - 2^{151}$. Pero por el PTF, al ser 31 primo que no divide a 2, se tiene:

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

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

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

Se concluye el ejercicio con el TCR:

$$\begin{cases} a \equiv 1 \pmod{4} \\ a \equiv 11 \pmod{31} \end{cases} \iff a \equiv 73 \pmod{124}.$$

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

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 $(5a : 7b) = 15$, se tiene

$$15 \mid 5a \iff 3 \mid a \quad \text{y} \quad 15 \mid 7b \xrightarrow{15 \perp 7} 15 \mid b.$$

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

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

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

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

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

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

Se concluye aplicando el TCR:

$$\begin{cases} 5a^{18} + 7b^{115} + 8^{40} \equiv 1 \pmod{9} \\ 5a^{18} + 7b^{115} + 8^{40} \equiv 1 \pmod{5} \\ 5a^{18} + 7b^{115} + 8^{40} \equiv 6 \pmod{7} \end{cases} \iff 5a^{18} + 7b^{115} + 8^{40} \equiv 181 \pmod{315}$$

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

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

Pongamos $b := 3a^{98} - 5a^{50} + 28$. 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

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

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

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

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:

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

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

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

Se concluye que

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

Para el 5:

$$3a^{98} - 5a^{50} + 28 \equiv_{\text{PTF}} 3a^{98} + 28 \equiv \begin{cases} 3 \pmod{5} & \text{si } 5|a \\ 3a^2 + 3 \pmod{5} & \text{si } 5 \nmid a. \end{cases}$$

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

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

Para el 7:

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

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

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

Se concluye entonces

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

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 en estas notas 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 funciona si la función Φ está definida en el conjunto de los números naturales $i \leq n$ coprimos con n (está claro que si p es primo, el conjunto $\{1, 2, \dots, p-1\}$ 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

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

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, $\mathcal{U}_p = \{1, 2, \dots, p-1\}$ y $\varphi(p) = p-1$.

La asignación $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ 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

$$a \perp n \implies a^{\varphi(n)} \equiv 1 \pmod{n}$$

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:

$$\begin{aligned} \Phi : \mathcal{U}_n &\longrightarrow \mathcal{U}_n \\ k &\longmapsto r_n(ka) \end{aligned}$$

(Observemos en particular que $\Phi(k) = r_n(ka) \equiv ka \pmod{n}$.)

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

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

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

$$\Phi(k) \perp n \iff r_n(ka) \perp n \stackrel{(*)}{\iff} ka \perp n \stackrel{a \perp n}{\iff} k \perp n,$$

donde (*) resulta de que $r \perp n \iff ka = jn + r \perp n$ (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 $k \geq j \in \mathcal{U}_n$, se tiene que $\Phi(k) = \Phi(j)$, queremos probar que entonces $k = j$. Pero de la misma forma que probamos esto en el PTF,

$$\Phi(k) = \Phi(j) \iff r_n(ka) = r_n(ja) \iff n \mid ka - ja = (k-j)a \stackrel{n \perp a}{\iff} n \mid k-j.$$

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

$$n \mid k-j \iff k-j = 0 \iff k = j.$$

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

$$\text{Im}(\Phi) = \mathcal{U}_n \implies \prod_{k \in \mathcal{U}_n} \Phi(k) = \prod_{k \in \mathcal{U}_n} k \implies \prod_{k \in \mathcal{U}_n} r_n(ka) = \prod_{k \in \mathcal{U}_n} k \implies$$

$$\prod_{k \in \mathcal{U}_n} (ka) \equiv \prod_{k \in \mathcal{U}_n} k \pmod{n} \implies \left(\prod_{k \in \mathcal{U}_n} k \right) a^{\varphi(n)} \equiv \prod_{k \in \mathcal{U}_n} k \pmod{n} \implies a^{\varphi(n)} \equiv 1 \pmod{n},$$

pues se puede simplificar $\prod_{k \in \mathcal{U}_n} k$ en el último renglón dado que n es coprimo con ese término (al ser 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:

$$n \perp a \implies a^m \equiv a^{r_{\varphi(n)}(m)} \pmod{n}$$

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 $\{1, 2, \dots, p^n\}$ 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: $p = 1p, 2p, 3p, \dots, p^{n-1}p = p^n$.

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

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

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

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

- 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 $a \in \mathbb{Z}, 0 \leq a \leq nm$ 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 $a \perp nm$ 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 $1 \leq a, a' \leq nm - 1$.

■

Consecuencia 14.5 Sean p_1, \dots, p_n primos distintos y $v_1, \dots, v_n \in \mathbb{N}$. 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 rápida 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 $n = pq$ producto de dos primos distintos. En ese caso, $\varphi(n) = \varphi(pq) = (p-1)(q-1)$ 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 teóricos matemáticos. Para más información se recomienda buscar en Internet.

¿Cuál es el objetivo de la criptografía? Mandar mensajes en forma secreta y segura... 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 interceptar el mensaje lo pueda entender. Convenimos que un mensaje es un número a , por ejemplo simplemente 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 bloquitos si hace falta.

¿Qué se entiende por clave pública-clave privada? Una persona, Bob, 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 una sola de ellas no puede hacer las dos cosas a la vez. Si Bob mantiene secreta su clave privada y le distribuye al resto del mundo su clave pública, el sistema RSA sirve para lo siguiente:

- Cualquier persona del resto del mundo, por ejemplo Alice, le puede mandar un mensaje encriptado a Bob usando la clave pública. Bob es el único que puede decodificar el mensaje, usando su clave privada. Ninguna otra persona del resto del mundo puede decodificar ese mensaje.
- Bob 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 Bob, puede decodificar y luego entender ese mensaje, y por lo tanto, como el mensaje tiene sentido, tiene garantía que el emisor (el firmante) del mensaje fue realmente Bob.

¿Cómo funciona?

Clave privada de Bob: (n, e) , clave pública de Bob: (n, d) , que satisfacen

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

$$de + t(p-1)(q-1) = 1$$

(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

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

(módulo un pequeño detalle para verificar...)

Mecanismo: Dado un mensaje a , $0 \leq a < n$, $C(a)$ denotará el mensaje encriptado.

Caso 1: Alice le manda un mensaje encriptado a Bob:

$$C(a) \equiv a^d \pmod{n} \text{ con } 0 \leq C(a) < n.$$

Para decodificarlo, Bob aplica la aplicación “inversa” que consiste en elevar a la e y tomar resto módulo n . Se tiene

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

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

Caso 2: Bob le quiere mandar un mensaje firmado por él al resto del mundo:

$$C(a) \equiv a^e \pmod{n} \text{ con } 0 \leq C(a) < n.$$

Para decodificarlo, el resto del mundo aplica la aplicación “inversa” que consiste en elevar a la d y tomar resto módulo n . Se tiene

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

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