Números enteros

1. Divisibilidad.

El conjunto de los números enteros

$$\mathbb{Z} = \{n \in \mathbb{R} \,/\, n \in \mathbb{N} \vee n = 0 \vee -n \in \mathbb{N}\}$$

es cerrado para la suma, la resta y el producto, es decir, se verifica: si $a, b \in \mathbb{Z}$ entonces $a + b, a - b, a.b \in \mathbb{Z}$. Pero $\mathbb{Z}$ no es cerrado para la división: $\frac{15}{8} \notin \mathbb{Z}$. Sin embargo, para algunos valores de $a, b \in \mathbb{Z}$ vale que $\frac{b}{a} \in \mathbb{Z}$, por ejemplo, para $b = 36$ y $a = 12$.

Dados $a, b \in \mathbb{Z}$ diremos que a *divide a* b (o que a *es un divisor de* b o también que b *es múltiplo de* a) si $\exists\, k \in \mathbb{Z}$ tal que $b = a.k$ y en tal caso escribiremos $a \mid b$.
Notar que cuando $a \neq 0$ decir que a divide a b es lo mismo que decir que el cociente $\frac{b}{a}$ es entero.

Ejemplos.

i) $3 \mid 0$ pues $\exists\, k \in \mathbb{Z}$ tal que $0 = 3.k$. En efecto, basta tomar $k = 0$.
ii) $15 \mid -90$ pues $-90 = 15.(-6)$
iii) $14 \not| 21$
iv) $0 \mid 0$
v) Los divisores de 11 son 1, -1, 11 y -11
vi) Los divisores de 12 son ± 1, ± 2, ± 3, ± 4, ± 6 y ± 12

Propiedades de la divisibilidad.

i) $a \mid 0$ para todo $a \in \mathbb{Z}$
ii) $0 \mid a$ si y sólo si $a = 0$
iii) $1 \mid a$ y $-1 \mid a$ para todo $a \in \mathbb{Z}$
iv) $a \mid 1$ o $a \mid -1$ si y sólo si $a = 1$ o $a = -1$
v) $a \mid a$ para todo $a \in \mathbb{Z}$
vi) $a \mid b$ y $b \mid a$ si y sólo si $a = b$ o $a = -b$
vii) $a \mid b \wedge b \mid c \implies a \mid c$
viii) $a \mid b \iff a \mid -b \iff -a \mid b \iff -a \mid -b$
ix) Si $a, b \in \mathbb{N}$ y $a \mid b$ entonces $a \leq b$
x) $a \mid b \wedge a \mid c \implies a \mid b + c$
xi) Si $a \mid b$ entonces $a \mid b.c$ para todo $c \in \mathbb{Z}$
xii) $a \mid b + c \wedge a \mid b \implies a \mid c$
xiii) $a \mid b \wedge a \mid c \implies a \mid b - c$

Demostración: Demostraremos iv), vi), ix), x) y xi). Dejamos como ejercicio la demostración de las restantes propiedades.

iv) ($\Longrightarrow$) Si $a \mid 1$ entonces existe $k \in \mathbb{Z}$ tal que $1 = a.k$. Luego, tomando valor absoluto en ambos miembros se tiene que $1 = |a|.|k|$. Notar que $|a|$ y $|k|$ son números naturales. Si fuese $|a| > 1$ entonces resultaría que $1 = |a|.|k| > 1$. Por lo tanto debe ser $|a| = 1$ de donde se deduce que $a = 1$ o $a = -1$. De la misma manera se ve que si $a \mid -1$ entonces $a = 1$ o $a = -1$.
($\Longleftarrow$) Es trivial.

vi) ($\Longrightarrow$) Si $a \mid b$ y $b \mid a$ entonces existen enteros k y h tales que $b = a.k$ y $a = b.h$. Luego, $b = (b.h).k = b.(h.k)$, de donde resulta que $b = 0$ o $h.k = 1$.
Si $b = 0$ entonces, como $b \mid a$, por ii) debe ser $a = 0$ y por lo tanto $a = b$. Y si $h.k = 1$, entonces $h \mid 1$ y por lo tanto de iv) resulta que $h = 1$ o $h = -1$. Luego, como $a = b.h$ se tiene que $a = b$ o $a = -b$.
($\Longleftarrow$) Es trivial.

ix) Sean $a, b \in \mathbb{N}$. Si $a \mid b$ entonces existe $k \in \mathbb{Z}$ tal que $b = a.k$ y como $a, b \in \mathbb{N}$ entonces $k \in \mathbb{N}$. Luego $k \geq 1$ y por lo tanto $b = a.k \geq a$.

x) Si $a \mid b$ y $a \mid c$ entonces existen $k, h \in \mathbb{Z}$ tales que $b = a, k$ y $c = a.h$. Luego $b + c = a.k + a.h = a(k + h)$ y como $k + h \in \mathbb{Z}$ pues $k, h \in \mathbb{Z}$ resulta que $a \mid b + c$.

xi) Si $a \mid b$ entonces existe $k \in \mathbb{Z}$ tal que $b = a.k$. Luego, para todo $c \in \mathbb{Z}$ se tiene que $b.c = a.k.c$ y como $k.c \in \mathbb{Z}$ esto significa que $a \mid b.c$ □

Notar que si $\mathcal{R}$ es la relación en $\mathbb{Z}$ definida por $a\mathcal{R}b \Longleftrightarrow a \mid b$ entonces las propiedades v) y vii) dicen que $\mathcal{R}$ es reflexiva y transitiva. Sin embargo, esta relación no es simétrica ni antisimétrica. Pero si la restringimos al conjunto $\mathbb{N}$ de los números naturales entonces resulta antisimétrica por vi), es decir, la relación en $\mathbb{N}$ definida por $a\mathcal{R}b \Longleftrightarrow a \mid b$ es una relación de orden.

Ejemplo. Determinemos todos los $a \in \mathbb{Z}$ tales que $a + 1 \mid 2a^2 + 9$.

Sea $a \in \mathbb{Z}$ tal que $a + 1 \mid 2a^2 + 9$. Como $a + 1 \mid a + 1$ por v) entonces $a + 1 \mid (a + 1).c$ para cualquier $c \in \mathbb{Z}$ por xi). En particular, $a+1 \mid (a+1)(2a-2) = 2a^2-2$. Luego, $a+1 \mid 2a^2+9$ y $a + 1 \mid 2a^2 - 2$ y entonces, por xiii) resulta que $a + 1 \mid (2a^2 + 9) - (2a^2 - 2) = 11$ de donde se deduce que $a + 1 = \pm 1, \pm 11$. Por lo tanto $a = 0$ o $a = -2$ o $a = 10$ o $a = -12$.
Notar que hemos probado que si $a + 1 \mid 2a^2 + 9$ entonces $a = 0$ o $a = -2$ o $a = 10$ o $a = -12$, lo que no significa que todos esos valores de a satisfagan lo pedido sino que las soluciones se encuentran entre estos valores de a. Es decir, hasta ahora hemos probado que $\{a \in \mathbb{Z} \,/\, a + 1 \mid 2a^2 + 9\} \subseteq \{0, -2, 10, -12\}$
Para ver cuáles de estos valores de a satisfacen $a + 1 \mid 2a^2 + 9$ debemos chequear cada uno de ellos:
Si $a = 0$ entonces $a + 1 = 1$ y $2a^2 + 9 = 9$. Como $1 \mid 9$ entonces $a = 0$ satisface lo pedido.

Si $a = -2$ entonces $a + 1 = -1$ y $2a^2 + 9 = 17$. Como $-1 \mid 17$ entonces $a = -2$ satisface lo pedido.
Si $a = 10$ entonces $a + 1 = 11$ y $2a^2 + 9 = 209$. Como $11 \mid 209$ entonces $a = 10$ satisface lo pedido.
Si $a = -12$ entonces $a + 1 = -11$ y $2a^2 + 9 = 297$. Como $-11 \mid 297$ entonces $a = -12$ satisface lo pedido.

Por lo tanto $\{a \in \mathbb{Z} \,/\, a + 1 \mid 2a^2 + 9\} = \{0, -2, 10, -12\}$

2. Números primos.

Observemos que 1, -1, a y $-a$ son siempre divisores de a. Si $a = 1$ o $a = -1$ entonces, por iv), 1 y -1 son los únicos divisores de a. En cualquier otro caso, a tiene por lo menos 4 divisores.

Diremos que $p \in \mathbb{Z}$ es *primo* si p posee exactamente 4 divisores. Diremos que $a \in \mathbb{Z}$ es *compuesto* si $a \neq 1, -1$ y a no es primo.

Ejemplos.

i) 2, -2, 7 y -3 son primos.
ii) 0 no es primo pues tiene infinitos divisores.
iii) 4 no es primo pues tiene 6 divisores. Luego, 4 es compuesto.
iv) -21 no es primo pues tiene 8 divisores. Luego, -21 es compuesto.
v) 1 y -1 no son primos pues tienen 2 divisores y tampoco son compuestos.

Notar que $p \in \mathbb{Z}$ es primo si y sólo si $-p$ es primo ya que p y $-p$ tienen los mismos divisores.

Proposición. Sea $a \in \mathbb{Z}$, $a \neq 1, -1$. Entonces existe un primo positivo p tal que $p \mid a$.

Demostración: Sea $a \in \mathbb{Z}$ tal que $a \neq 1, -1$ y consideremos el conjunto

$$S = \{n \in \mathbb{N} \,/\, n \geq 2 \text{ y } n \mid a\}$$

S es un subconjunto no vacío de $\mathbb{N}$: en efecto, si $a = 0$ entonces $2 \in S$, si $a > 0$ entonces $a \in S$ y si $a < 0$ entonces $-a \in S$. Luego, por el principio de buena ordenación, S posee un primer elemento p. Entonces $p \in \mathbb{N}$, $p \geq 2$, $p \mid a$ y $p \leq n$ para todo $n \in S$. Veamos que p es primo:

Para ello, basta ver que los únicos divisores positivos de p son 1 y p. Sea b un divisor positivo de p tal que $b \neq 1$. Probaremos que $b = p$.
Como $b \in \mathbb{N}$ y $b \neq 1$ entonces $b \geq 2$. Además, como $b \mid p$ y $p \mid a$ entonces $b \mid a$. Luego, $b \in S$. Por lo tanto, como p es el primer elemento de S, resulta que $p \leq b$. Pero por otra parte, como $b, p \in \mathbb{N}$ y $b \mid p$, entonces $b \leq p$. Luego, $b = p$ como queríamos probar.
Luego, p es un primo positivo y $p \mid a$. □

Teorema. Existen infinitos primos.

Demostración: Supongamos que sólo existe un número finito de primos, $p_1, p_2, \ldots, p_n$. Sea

$$a = 1 + \prod_{i=1}^{n} p_i = 1 + p_1.p_2.\ldots.p_n$$

Notemos que $p_1.p_2.\ldots.p_n \neq 0$ pues 0 no es primo y, como 3 es primo, entonces $p_1.p_2.\ldots.p_n$ debe ser divisible por 3. Luego $a \neq 1, -1$ y por lo tanto, por la proposición anterior, a debe ser divisible por algún primo. Luego, existe j, $1 \leq j \leq n$ tal que $p_j \mid a$.
Como $p_j \mid a$ y $p_j \mid p_1.p_2.\ldots.p_n = a - 1$ entonces $p_j \mid a - (a-1)$ de donde $p_j \mid 1$. Luego, $p_j = 1$ o $p_j = -1$, pero esto no puede ocurrir porque p_j es primo. Luego no puede ser que existan finitos primos. □

Veamos ahora un método para encontrar primos.

Criba de Eratóstenes. Sea $a \in \mathbb{N}$, $a \neq 1$. Por la proposición anterior, existe un primo positivo p tal que $p \mid a$ y como $p, a \in \mathbb{N}$ y $p \mid a$, debe ser $p \leq a$. Luego,

$$\text{si } a \text{ no es primo, existe un primo positivo } p < a \text{ tal que } p \mid a \qquad (*)$$

Supongamos ahora que queremos hallar todos los primos positivos menores o iguales que 38. Entonces procedemos de la siguiente manera:
Consideremos la lista de todos los números naturales menores o iguales que 38. Iremos tachando todos aquellos números que no sean primos y, al terminar, los números no tachados serán los primos buscados. En primer lugar, tachamos el 1 ya que no es primo:

~~1~~	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							

Si 2 no fuese primo, por $(*)$, existiría un primo positivo $p < 2$ tal que $p \mid 2$. Luego, 2 es primo. Además, ningún otro múltiplo de 2 puede ser primo ya que es divisible por 2. Luego, marcamos el 2 para indicar que ya probamos que es primo y tachamos todos los otros múltiplos de 2 ya que sabemos que no son primos

~~1~~	2̌	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~~							

Ahora, el primer número que no está marcado ni tachado, en este caso el 3, debe ser primo. En efecto, si 3 no fuese primo, por $(*)$, sería divisible por un primo positivo estrictamente

menor que 3. Pero el único posible es 2 y sabemos que 3 no es divisible por 2 porque si lo fuera estaría tachado. Por lo tanto, 3 es primo y ningún otro múltiplo de 3 puede ser primo ya que es divisible por 3. Luego, marcamos el 3 para indicar que ya probamos que es primo y tachamos todos los otros múltiplos de 3 ya que sabemos que no son primos

$$\begin{array}{cccccccccccccc} \not{1} & \check{2} & \check{3} & \not{4} & 5 & \not{6} & 7 & \not{8} & \not{9} & \not{10} & 11 & \not{12} & 13 & \not{14} & \not{15} \\ \not{16} & 17 & \not{18} & 19 & \not{20} & \not{21} & \not{22} & 23 & \not{24} & 25 & \not{26} & \not{27} & \not{28} & 29 & \not{30} \\ 31 & \not{32} & \not{33} & \not{34} & 35 & \not{36} & 37 & \not{38} \end{array}$$

Ahora, el primer número que no está marcado ni tachado, en este caso el 5, debe ser primo. En efecto, si 5 no fuese primo, por $(*)$, sería divisible por un primo positivo estrictamente menor que 5. Pero los únicos posibles son 2 y 3 y sabemos que 5 no es divisible por 2 ni por 3 porque si lo fuera estaría tachado. Por lo tanto, 5 es primo y ningún otro múltiplo de 5 puede ser primo ya que es divisible por 5. Luego, marcamos el 5 para indicar que ya probamos que es primo y tachamos todos los otros múltiplos de 5 ya que sabemos que no son primos

$$\begin{array}{cccccccccccccc} \not{1} & \check{2} & \check{3} & \not{4} & \check{5} & \not{6} & 7 & \not{8} & \not{9} & \not{10} & 11 & \not{12} & 13 & \not{14} & \not{15} \\ \not{16} & 17 & \not{18} & 19 & \not{20} & \not{21} & \not{22} & 23 & \not{24} & \not{25} & \not{26} & \not{27} & \not{28} & 29 & \not{30} \\ 31 & \not{32} & \not{33} & \not{34} & \not{35} & \not{36} & 37 & \not{38} \end{array}$$

Continuamos de esta manera hasta que no quede ningún número que no esté marcado o tachado

$$\begin{array}{cccccccccccccc} \not{1} & \check{2} & \check{3} & \not{4} & \check{5} & \not{6} & \check{7} & \not{8} & \not{9} & \not{10} & \check{11} & \not{12} & \check{13} & \not{14} & \not{15} \\ \not{16} & \check{17} & \not{18} & \check{19} & \not{20} & \not{21} & \not{22} & \check{23} & \not{24} & \not{25} & \not{26} & \not{27} & \not{28} & \check{29} & \not{30} \\ \check{31} & \not{32} & \not{33} & \not{34} & \not{35} & \not{36} & \check{37} & \not{38} \end{array}$$

Luego, los primos positivos menores que 38 son los que están marcados, es decir, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 y 37.

Proposición. Sea $a \in \mathbb{N}$, $a \neq 1$. Si a no es primo entonces existe un primo p tal que $1 < p \leq \sqrt{a}$ y $p \mid a$.

Demostración: El conjunto de primos positivos que dividen a a es un subconjunto no vacío de $\mathbb{N}$. Luego, por el principio de buena ordenación posee un primer elemento p, es decir, p es el menor primo positivo que divide a a.
Como $p \mid a$ entonces existe $b \in \mathbb{Z}$ tal que $a = p.b$, y como $a, p \in \mathbb{N}$ entonces $b \in \mathbb{N}$. Además, $b \neq 1$ pues a no es primo. Luego, existe un primo positivo q tal que $q \mid b$.

Como $q \mid b$ y $b \mid a$ entonces $q \mid a$ y por lo tanto debe ser $p \leq q$ ya que p es el menor primo positivo que divide a a. Además, $q \leq b$ ya que $q \mid b$. Luego, $p \leq b$ de donde $p^2 \leq p.b = a$, es decir, $p \leq \sqrt{a}$. □

Ejemplo. Probemos que 1009 es primo.

Si 1009 no fuese primo entonces sería divisible por un primo positivo $p \leq \sqrt{1009} < 32$. Los primos menores que 32 son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 y 31 (los calculamos antes usando la Criba de Eratóstenes). Pero ninguno de ellos divide a 1009 (ejercicio) de manera que 1009 debe ser primo.

3. Algoritmo de división.

Si repartimos 15 caramelos entre 5 chicos, a cada chico le tocarán 3 caramelos y no sobrará ninguno. La razón de que no sobre ninguno es que $5 \mid 15$. Pero si repartimos 17 caramelos entre 5 chicos entonces a cada chico le tocarán 3 caramelos y sobrarán 2 pues $17 = 5.3 + 2$. Probaremos que dados $a, b \in \mathbb{Z}$, $b \neq 0$, existen únicos $q, r \in \mathbb{Z}$ tales que $a = b.q + r$ y $0 \leq r < |b|$. Pero antes veamos cuál es la idea de la demostración:

Supongamos que $a = 32$ y $b = 6$. Queremos hallar $q, r \in \mathbb{Z}$ tales que $32 = 6.q + r$ y $0 \leq r < 6$. Observemos que entonces debe ser $r = 32 - 6.q$. De todos los números de la forma $32 - 6.q$ el valor de r buscado será aquél que satisfaga $0 \leq r < 6$.
Veamos cómo son los valores que toma $32 - 6.q$ para algunos $q \in \mathbb{Z}$:

q	$32 - 6.q$
0	32
1	26
2	20
3	14
4	8
5	2
6	-4
7	-10

El valor de r buscado es $r = 2$ que es el correspondiente a $q = 5$. Como vemos, incrementar q en 1 equivale a restarle 6 a $32 - 6.q$ pues $32 - 6.(q + 1) = 32 - 6.q - 6$. Luego, los valores de $32 - 6.q$ que vamos obteniendo son cada vez más chicos y difieren en 6. Por lo tanto, partiendo de $32 = 32 - 6.0$ ($q = 0$) y restando 6 varias veces (es decir, incrementando q) es claro que en algún momento vamos a obtener un número r de la forma $32 - 6.q$ tal que $0 \leq r < 6$ y que si seguimos restando 6 (incrementando q) no vamos a volver a obtener un número en ese rango. Notemos que el r buscado es el menor entero no negativo de la forma $32 - 6.q$, con $q \geq 0$.

En general, dados $a, b > 0$, partiendo de $a = a - b.0$ $(q = 0)$ y restando b sucesivas veces (incrementando q) obtendremos un único r de la forma $a - b.q$ que verifique $0 \leq r < b$. Además,

$$r = \min \{a - b.q \,/\, q \in \mathbb{N}_0\} \cap \mathbb{N}_0$$

donde $\mathbb{N}_0$ es el conjunto de enteros no negativos, es decir, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Teorema. (Algoritmo de división) Sean $a, b \in \mathbb{Z}$, $b \neq 0$. Entonces $\exists!\ q, r \in \mathbb{Z} \,/\, a = b.q + r$ y $0 \leq r < |b|$.

Demostración: Existencia: supongamos primero que $a \geq 0$ y $b > 0$. En este caso $|b| = b$. Sea

$$S = \{a - b.q \,/\, q \in \mathbb{N}_0\} \cap \mathbb{N}_0$$

Como $S \neq \emptyset$ pues $a \in S$ (tomando $q = 0$) entonces, por el principio de buena ordenación, S posee un primer elemento r. Es decir, $r \in S$ y $r \leq x$ para todo $x \in S$.
Como $r \in S$ entonces $r \in \mathbb{N}_0$ y $r = a - b.q$ para algún $q \in \mathbb{N}_0$. Luego $q, r \in \mathbb{Z}$, $r \geq 0$ y $a = b.q + r$.
Falta ver que $r < b$. Supongamos que no, es decir, que $r \geq b$. Entonces $r - b \geq 0$ de donde $r - b \in \mathbb{N}_0$ y

$$r - b = a - b.q - b = a - b(q + 1)$$

donde $q + 1 \in \mathbb{N}_0$. Luego, $r - b \in S$. Pero esto no puede ocurrir pues r es el primer elemento de S y $r - b < r$. Luego debe ser $r < b$.

Supongamos ahora que $a \geq 0$ y $b < 0$. En este caso $|b| = -b$.
Como $a \geq 0$ y $-b > 0$ entonces, por lo que probamos antes, existen $q', r' \in \mathbb{Z}$ tales que $a = (-b).q' + r'$ y $0 \leq r' < -b$. Luego, tomando $q = -q' \in \mathbb{Z}$ y $r = r'$ y teniendo en cuenta que $|b| = -b$, resulta que $a = b.q + r$ y $0 \leq r < |b|$.
Ahora consideremos el caso en que $a < 0$ y $b > 0$. En este caso $|b| = b$.
Como $-a > 0$ y $b > 0$ entonces, por lo que probamos antes, existen $q', r' \in \mathbb{Z}$ tales que $-a = b.q' + r'$ y $0 \leq r' < b$. Luego $a = b.(-q') - r'$. Si fuese $r' = 0$ entonces basta tomar $q = -q' \in \mathbb{Z}$ y $r = 0$.
Supongamos entonces que $r' > 0$. Luego, $a = b.(-q') - r' = b(-q' - 1) + b - r'$ y tomando $q = -q' - 1 \in \mathbb{Z}$ y $r = b - r' \in \mathbb{Z}$ y teniendo en cuenta que $0 < r' < b$ y $|b| = b$, resulta que $a = b.q + r$ y $0 \leq r < |b|$.

Finalmente veamos el caso en que $a < 0$ y $b < 0$. Ahora $|b| = -b$.
Como $-a > 0$ y $-b > 0$ entonces, por lo que probamos antes, existen $q', r' \in \mathbb{Z}$ tales que $-a = (-b).q' + r'$ y $0 \leq r' < -b$. Si fuese $r' = 0$ entonces basta tomar $q = q'$ y $r = 0$.
Supongamos entonces que $r' > 0$. Luego, $a = b.q' - r' = b(q' + 1) - b - r'$ y tomando $q = q' + 1 \in \mathbb{Z}$ y $r = -b - r' \in \mathbb{Z}$ y teniendo en cuenta que $0 < r' < -b$ y $|b| = -b$, resulta que $a = b.q + r$ y $0 \leq r < |b|$.

Unicidad: Supongamos que $a = b.q_1 + r_1$ con $q_1 \in \mathbb{Z}$ y $0 \leq r_1 < |b|$ y que $a = b.q_2 + r_2$ con $q_2 \in \mathbb{Z}$ y $0 \leq r_2 < |b|$. Probaremos que entonces $q_1 = q_2$ y $r_1 = r_2$.

Como $b.q_1 + r_1 = b.q_2 + r_2$ entonces $r_1 - r_2 = b.(q_2 - q_1)$.
Supongamos primero que $r_1 \neq r_2$. Entonces, tomando valor absoluto, $|r_1 - r_2| = |b|.|q_2 - q_1|$ de donde $|b|$ divide a $|r_1 - r_2|$. Luego, como $|r_1 - r_2| \in \mathbb{N}$ y $|b| \in \mathbb{N}$ resulta que $|b| \leq |r_1 - r_2|$. Pero esto no puede ocurrir, pues $0 \leq r_1 < |b|$ y $0 \leq r_2 < |b|$ (si $r_1 < r_2$ entonces $|r_1 - r_2| = r_2 - r_1 \leq r_2 < |b|$ y si $r_2 < r_1$ entonces $|r_1 - r_2| = r_1 - r_2 \leq r_1 < |b|$). Luego debe ser $r_1 = r_2$ y por lo tanto $b.(q_2 - q_1) = r_1 - r_2 = 0$ de donde $q_2 = q_1$ ya que $b \neq 0$. □

Dados $a, b \in \mathbb{Z}$, $b \neq 0$, sean $q, r \in \mathbb{Z}$ los únicos que satisfacen $a = b.q + r$ y $0 \leq r < |b|$. Entonces diremos que q es el *cociente* y r es el *resto* de la división de a por b. Observemos que la unicidad del cociente y el resto nos dicen que si $a = b.k + s$, con $k, s \in \mathbb{Z}$ y $0 \leq s < |b|$ entonces k es el cociente y s es el resto de la división de a por b.

Ejemplos. i) Hallemos el cociente q y el resto r de la división de -132 por 17.
Primero hallamos el cociente y el resto de división de 132 por 17: $132 = 17.7 + 13$. Luego,

$$-132 = 17(-7) - 13 = 17(-8) + 17 - 13 = 17(-8) + 4$$

Como $0 \leq 4 < 17$ entonces $q = -8$ y $r = 4$.

ii) Hallemos el cociente q y el resto r de la división de 18 por 25.
Como $18 = 25.0 + 18$ y $0 \leq 18 < 25$ entonces $q = 0$ y $r = 18$.

iii) El cociente y el resto de la división de 360 por -9 son $q = -40$ y $r = 0$.

Notación: Dados $a, b \in \mathbb{Z}$, $b \neq 0$, denotaremos por $r_b(a)$ al resto de la división de a por b

Ejemplo. Sea $a \in \mathbb{Z}$ tal que $r_5(a) = 2$. Calculemos $r_5(3a - 7)$ y $r_{10}(2a^2 + 9)$.
Como $r_5(a) = 2$ entonces existe $q \in \mathbb{Z}$ tal que $a = 5q + 2$. Luego

$$3a - 7 = 3(5q + 2) - 7 = 5(3q) + 6 - 7 = 5(3q) - 1 = 5(3q - 1) + 5 - 1 = 5(3q - 1) + 4$$

y

$$\begin{aligned} 2a^2 + 9 &= 2(5q + 2)^2 + 9 = 2(25q^2 + 20q + 4) + 9 = 10(5q^2 + 4q) + 8 + 9 = \\ &= 10(5q^2 + 4q) + 17 = 10(5q^2 + 4q + 1) + 7 \end{aligned}$$

Como $3q - 1 \in \mathbb{Z}$ y $0 \leq 4 < 5$ entonces $r_5(3a - 7) = 4$ y como $5q^2 + 4q + 1 \in \mathbb{Z}$ y $0 \leq 7 < 10$ entonces $r_{10}(2a^2 + 9) = 7$.

Sistemas de numeración. Una aplicación importante del algoritmo de división es la siguiente: todo número natural n admite un desarrollo en base s ($s > 1$), es decir, dado $s \in \mathbb{N}$, $s > 1$ entonces, para todo $n \in \mathbb{N}$, existen únicos $a_0, a_1, \ldots, a_k \in \mathbb{Z}$ tales que $0 \leq a_i < s$ para $i = 1, 2, \ldots, k$ y

$$n = \sum_{i=0}^{k} a_i s^i$$

Utilizaremos la notación $(a_k\ a_{k-1}\ \ldots\ a_1\ a_0)_s$ para indicar el desarrollo en base s de n. Veamos en un ejemplo cómo calcular los a_i utilizando el algoritmo de división: calculemos el desarrollo en base $s = 3$ de $n = 38$.
Dividimos $n = 38$ por $s = 3$ obteniendo el cociente $q_0 = 12$ y el resto $a_0 = 2$. Ahora dividimos $q_0 = 12$ por $s = 3$ obteniendo un cociente $q_1 = 4$ y un resto $a_1 = 0$. Ahora dividimos $q_1 = 4$ por $s = 3$ obteniendo un cociente $q_2 = 1$ y $a_2 = 1$. Como $0 \leq q_2 < 3$, tomando $a_3 = q_2 = 1$ resulta que $n = (a_3\ a_2\ a_1\ a_0)_s$ pues

$$n = 3.q_0 + a_0 = 3(3.q_1 + a_1) + a_0 = 3^2.q_1 + 3.a_1 + a_0 = 3^2(3.q_2 + a_2) + 3.a_1 + a_0 =$$

$$= 3^3.q_2 + 3^2.a_2 + 3.a_1 + a_0 = 3^3.a_3 + 3^2.a_2 + 3.a_1 + a_0 = \sum_{i=0}^{3} a_i.3^i = (a_3\ a_2\ a_1\ a_0)_s$$

es decir, $38 = 3^3.1 + 3^2.1 + 3.0 + 2 = (1\ 1\ 0\ 2)_3$

Cuando la base s es mayor que 10 se utilizan letras para indicar los a_i mayores que 9: A en lugar de 10, B en lugar de 11, etc. Por ejemplo, dejamos como ejercicio al lector verificar que $1838 = (A\ B\ 5)_{13}$, es decir, $1838 = 10.13^2 + 11.13 + 5$.

Ejercicio. Calcular el desarrollo en base 2 de 36 y el desarrollo en base 15 de 873.

Los granjeros rusos multiplicaban dos números sin necesidad de conocer las tablas de multiplicar. Veamos cómo hacían en un ejemplo. Supongamos que queremos multiplicar 37 por 29. Entonces colocamos cualquiera de ellos, por ejemplo el 37 a la izquierda, debajo de él la parte entera de su mitad que es 18, debajo de éste la parte entera de su mitad que es 9, etc, hasta llegar a 1. Ahora construímos una columna derecha colocando primero el 29, debajo de éste el doble que es 58, debajo de él el doble que es 116, etc, hasta que la columna derecha contenga la misma cantidad de números que la columna izquierda:

37	29
18	58
9	116
4	232
2	464
1	928

Ahora, para cada número de la izquierda que sea par, eliminamos el correspondiente número de la derecha y sumamos los números que quedaron a la derecha:

37	29
18	
9	116
4	
2	
1	928
	1073

El resultado obtenido es 1073, que es el producto de 37 por 29.

Ejercicio. Justifique el método usado por los granjeros rusos.

Propiedades del resto.

1) $r_b(a) = 0$ si y sólo si $b \mid a$
2) $r_b(a + c) = r_b(r_b(a) + r_b(c))$
3) $r_b(a.c) = r_b(r_b(a).r_b(c))$
4) $r_b(a^n) = r_b([r_b(a)]^n)$

Demostración: Dejamos como ejercicio las demostraciones de 1), 2) y 4)
3) Sean $q, q' \in \mathbb{Z}$ los cocientes de la división de a y c por b. Entonces $a = b.q + r_b(a)$ y $c = b.q' + r_b(c)$. Luego

$$a.c = [b.q + r_b(a)].[b.q' + r_b(c)] = b[q.b.q' + q.r_b(c) + q'.r_b(a)] + r_b(a).r_b(c)$$

Si fuese $0 \leq r_b(a).r_b(c) < |b|$ entonces ese sería el resto, pero podría ocurrir que no fuese así. Sin embargo, si dividimos $r_b(a).r_b(c)$ por b obtenemos un cociente $q'' \in \mathbb{Z}$ y el resto $r_b(r_b(a).r_b(c))$ de esta división es mayor o igual que 0 y menor que $|b|$. Luego, $r_b(a).r_b(c) = b.q'' + r_b(r_b(a).r_b(c))$ donde $0 \leq r_b(r_b(a).r_b(c)) < |b|$ y, por lo tanto,

$$\begin{aligned} a.c &= b[q.b.q' + q.r_b(c) + q'.r_b(a)] + r_b(a).r_b(c) = \\ &= b[q.b.q' + q.r_b(c) + q'.r_b(a)] + b.q'' + r_b(r_b(a).r_b(c)) = \\ &= b[q.b.q' + q.r_b(c) + q'.r_b(a) + q''] + r_b(r_b(a).r_b(c)) \end{aligned}$$

donde $0 \leq r_b(r_b(a).r_b(c)) < |b|$. Luego, $r_b(a.c) = r_b(r_b(a).r_b(c))$. □

Ejemplos. i) $r_{15}(17.44) = r_{15}(r_{15}(17).r_{15}(44)) = r_{15}(2.14) = r_{15}(28) = 13$.

ii) $r_{15}(42^2 + 37) = r_{15}(r_{15}(42^2) + r_{15}(37)) = r_{15}[r_{15}[r_{15}(42)]^2) + r_{15}(37)] = r_{15}[r_{15}(12^2) + r_{15}(37)] = r_{15}[r_{15}(144) + r_{15}(37)] = r_{15}(9 + 7) = r_{15}(16) = 1$.

Como se observa, esta manera de calcular los restos nos obliga a poner r_{15} muchas veces. Veamos otra manera menos engorrosa.

4. Congruencias.

Sean $a, b \in \mathbb{Z}$ y sea $m \in \mathbb{N}$. Diremos que a es *congruente* a b *módulo* m si $m \mid b - a$. En tal caso escribiremos $a \equiv b\ (m)$.

Ejemplos. i) $14 \equiv -8\ (11)$ pues $-8 - 14 = -22$ es divisible por 11.

ii) $26 \equiv 196\ (17)$ pues $17 \mid 196 - 26 = 170$ es divisible por 17.

iii) $783 \equiv 13\ (110)$ pues $13 - 783 = -770$ es divisible por 110.

iv) $151 \equiv 1851\ (100)$ pues $1851 - 151 = 1700$ es divisible por 100

v) $-722 \equiv 7$ (9 pues $7-(-722) = 729$ es divisible por 9.

Propiedades de la congruencia.

1) $a \equiv a\ (m)$ para todo $a \in \mathbb{Z}$, $m \in \mathbb{N}$
2) $a \equiv b\ (m) \Longrightarrow b \equiv a\ (m)$
3) $a \equiv b\ (m)$ y $b \equiv c\ (m) \Longrightarrow a \equiv c\ (m)$
4) $a \equiv b\ (m) \Longrightarrow a+c \equiv b+c\ (m)$ para todo $c \in \mathbb{Z}$
5) $a \equiv b\ (m) \Longrightarrow a.c \equiv b.c\ (m)$ para todo $c \in \mathbb{Z}$
6) $a \equiv b\ (m)$ y $c \equiv d\ (m) \Longrightarrow a+c \equiv b+d\ (m)$ y $a.c \equiv b.d\ (m)$
7) $a \equiv b\ (m) \Longrightarrow a^n \equiv b^n\ (m)$ para todo $n \in \mathbb{N}$
8) $a \equiv r_m(a)\ (m)$ para todo $a \in \mathbb{Z}$, $m \in \mathbb{N}$
9) Si $a \equiv r\ (m)$ y $0 \leq r < m$ entonces $r = r_m(a)$
10) $a \equiv 0\ (m) \Longleftrightarrow m \mid a$
11) $a \equiv a+mq\ (m)$ para todo $q \in \mathbb{Z}$
12) Sea $c \in \mathbb{N}$. Entonces $a \equiv b\ (m) \Longleftrightarrow a.c \equiv b.c\ (m.c)$

Demostración: Sólo probaremos 6), 9) y 12), el resto queda como ejercicio para el lector.
6) Si $a \equiv b\ (m)$ y $c \equiv d\ (m)$ entonces, por 4), $a+c \equiv b+c\ (m)$ y $c+b \equiv d+b\ (m)$. Luego, por 3) $a+c \equiv d+b\ (m)$.
De manera análoga, si $a \equiv b\ (m)$ y $c \equiv d\ (m)$ entonces, por 5), $a.c \equiv b.c\ (m)$ y $c.b \equiv d.b\ (m)$. Luego, por 3) $a.c \equiv d.b\ (m)$.

9) Si $a \equiv r\ (m)$ y $0 \leq r < m$ entonces $m \mid r-a$ y $0 \leq r < m$. Luego, $r-a = m.q$ para algún $q \in \mathbb{Z}$ de donde $a = m(-q)+r$ y $0 \leq r < m$. Por lo tanto, por la unicidad del cociente y el resto, $-q$ debe ser el cociente y r debe ser el resto de la división de a por m.

12) $a \equiv b\ (m) \Longleftrightarrow m \mid b-a \Longleftrightarrow \exists\, q \in \mathbb{Z} \,/\, b-a = m.q \Longleftrightarrow \exists\, q \in \mathbb{Z} \,/\, (b-a).c = m.c.q \Longleftrightarrow \exists\, q \in \mathbb{Z} \,/\, b.c-a.c = m.c.q \Longleftrightarrow m.c \mid b.c-a.c \Longleftrightarrow a.c \equiv b.c\ (m.c)$ □

Sea $m \in \mathbb{N}$. Si consideramos la relación $\mathcal{R}$ en $\mathbb{Z}$ definida por $a\mathcal{R}b \Longleftrightarrow a \equiv b\ (m)$ entonces las propiedades 1), 2) y 3) dicen que $\mathcal{R}$ es reflexiva, simétrica y transitiva, es decir, es una relación de equivalencia.

Ejemplos. i) Hallemos el resto de la división de -132 por 17. Por la propiedad 11), $-132 \equiv -132+17.10\ (17)$. Luego $-132 \equiv 38\ (17)$ y como $38 \equiv 4\ (17)$ entonces, por 3), $-132 \equiv 4\ (17)$. Por lo tanto, usando ahora la propiedad 9) resulta que $r_{17}(-132) = 4$.

ii) Sea $a \in \mathbb{Z}$ tal que $r_5(a) = 2$. Calculemos $r_5(3a-7)$ y $r_{10}(2a^2+9)$. Por 8), $a \equiv 2\ (5)$. Luego, usando 4), 5) y 3), $3a-7 \equiv 3.2-7 = -1 \equiv 4\ (5)$.
Como $a \equiv 2\ (5)$ entonces por 7), $a^2 \equiv 4\ (5)$ y ahora, por 12), $2a^2 \equiv 8\ (10)$. Y como $9 \equiv -1\ (10)$, por 6), $2a^2+9 \equiv 8-1 = 7\ (10)$.

iii) Hallemos $r_{15}(17.44)$.
$17 \equiv 2\ (15)$ y $44 \equiv -1\ (15)$. Luego, por 6), $17.44 \equiv 2(-1) = -2 \equiv -2+15 = 13\ (15)$. Luego, $r_{15}(17.44) = 13$ por 9).

iv) Hallemos $r_{15}(42^2+37)$.
$42 \equiv -3\ (15)$. Luego, por 7), $42^2 \equiv 9\ (15)$. Por otro lado, $37 \equiv 7 \equiv -8\ (15)$. Luego, por 6) $42^2+37 \equiv 9-8=1\ (15)$ y, de 9) se tiene que $r_{15}(42^2+37)=1$.

v) Hallar $r_{53}(54^{1000})$, $r_{38}(75^{513})$ y $r_8(5^n)$ para cada $n \in \mathbb{N}$.
Por 7),

$$54 \equiv 1\ (53) \Longrightarrow 54^{1000} \equiv 1^{1000} = 1\ (53)$$
$$75 \equiv -1\ (38) \Longrightarrow 75^{513} \equiv (-1)^{513} = -1 \equiv 37\ (38)$$

y luego, por 9), se tiene que $r_{53}(54^{1000})=1$ y $r_{38}(75^{513})=37$

Veamos como calcular $r_8(5^n)$:
Notemos que $5^2 \equiv 25 \equiv 1\ (8)$. Luego, por 7),

$$5^{2k} = (5^2)^k \equiv 1^k = 1\ (8) \text{ y } 5^{2k+1} = 5^{2k}.5 \equiv 1.5 = 5\ (8)$$

Por lo tanto, usando 9),

$$r_8(5^n) = \begin{cases} 1 & \text{si } n \text{ es par} \\ 5 & \text{si } n \text{ es impar} \end{cases}$$

vi) Probemos que $7 \mid 2^{43}+6.3^{815}-25$

$$2^1 \equiv 2\ (7),\ 2^2 \equiv 4\ (7),\ 2^3 \equiv 1\ (7)$$

Luego, $2^{3k} = (2^3)^k \equiv 1^k = 1\ (7)$ para todo $k \in \mathbb{N}$. Por lo tanto,

$$2^{43} = 2.2^{42} = 2.2^{3.14} \equiv 2.1 = 2\ (7)$$

$$3^1 \equiv 3\ (7),\ 3^2 \equiv 2\ (7),\ 3^3 \equiv -1\ (7)$$

Luego, $3^{3k} = (3^3)^k \equiv (-1)^k\ (7)$ para todo $k \in \mathbb{N}$. Por lo tanto,

$$3^{815} = 9.3^{813} = 9.3^{3.271} \equiv 9.(-1)^{271} = -9 \equiv 5\ (7)$$

Por lo tanto, $2^{43}+6.3^{815}-25 \equiv 2+6.5-25 = 7 \equiv 0\ (7)$ de donde $7 \mid 2^{43}+6.3^{815}-25$.

vii) Probemos que $5 \mid a^5-a$ para todo $a \in \mathbb{Z}$.
Como los posibles restos de la división de a por 5 son 0, 1, 2, 3 y 4 entonces $a \equiv 0\ (5)$ o $a \equiv 1\ (5)$ o $a \equiv 2\ (5)$ o $a \equiv 3\ (5)$ o $a \equiv 4\ (5)$. Consideremos la tabla de restos módulo 5:

a	0	1	2	3	4
a^2	0	1	4	4	1
$a^4=(a^2)^2$	0	1	1	1	1
$a^5=a.a^4$	0	1	2	3	4

Como se ve en la tabla de restos, $a^5 \equiv a\ (5)$ de donde $5 \mid a^5 - a$

viii) Sabiendo que $r_7(a^5) = 3$ hallar $r_7(a)$.
Haciendo la tabla de restos módulo 7

a	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1
$a^4 = (a^2)^2$	0	1	2	4	4	2	1
$a^5 = a.a^4$	0	1	4	5	2	3	6

se ve que $r_7(a) = 5$.

Ejercicio. Probar que $11 \mid 131^{2n} - 1$ para todo $n \in \mathbb{N}$. Sugerencia: $131 \equiv -1\ (11)$

5. Máximo común divisor.

Recordemos que la relación en $\mathbb{N}$ definida por $a \mathcal{R} b \iff a \mid b$ es una relación de orden. Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, diremos que d es el *máximo común divisor* entre a y b si es el mayor, respecto del orden $\mathcal{R}$, de los divisores positivos comunes de a y b. Es decir, d es el único número entero que satisface las condiciones:

i) $d \in \mathbb{N}$ (d es positivo)
ii) $d \mid a$ y $d \mid b$ (d es un divisor de a y de b)
iii) Dado $c \in \mathbb{N}$, si $c \mid a$ y $c \mid b$ entonces $c \mid d$ (Si c es un divisor positivo de a y de b entonces $c \mathcal{R} d$, es decir, c es menor o igual que d respecto de la relación de orden $\mathcal{R}$).
Notemos que d es también el mayor, respecto del orden usual, de los divisores positivos de a y b. En efecto si c es un divisor positivo de a y de b entonces por iii) se tiene que $c \mid d$ de donde $c \leq d$.
Notemos además que la condición iii) es equivalente a la condición: "dado $c \in \mathbb{Z}$, si $c \mid a$ y $c \mid b$ entonces $c \mid d$".

El siguiente teorema garantiza que un tal d existe y es único.

Teorema. Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$. Entonces $\exists!\, d \in \mathbb{Z}$ que satisface:

i) $d \in \mathbb{N}$
ii) $d \mid a$ y $d \mid b$
iii) Dado $c \in \mathbb{Z}$, si $c \mid a$ y $c \mid b$ entonces $c \mid d$

Demostración: Existencia: Sea $H = \{at + bs \,/\, t, s \in \mathbb{Z}\} \cap \mathbb{N}$. Veamos que $H \neq \emptyset$:
Si $a > 0$ entonces $a \in H$ pues $a = a.1 + b.0$, si $a < 0$ entonces $-a \in H$ pues $-a = a.(-1) + b.0$ y si $a = 0$ entonces $b \neq 0$ en cuyo caso b o $-b$ pertenecen a H según sea $b > 0$ o $b < 0$.
Luego, H es un subconjunto no vacío de $\mathbb{N}$. Sea d el primer elemento de H (existe por el principio de buena ordenación). Luego $h \in H$ y $d \leq h$ para todo $h \in H$.
Probemos que d satisface i), ii) y iii):

i) $d \in \mathbb{N}$ pues $d \in H$ y $H \subseteq \mathbb{N}$.

ii) Veamos que $d \mid a$. Sean $q, r \in \mathbb{Z}$ el cociente y el resto de la división de a por d. Luego, $a = d.q + r$ y $0 \leq r < d$. Queremos probar que $r = 0$.
Supongamos que no, es decir, que $r > 0$. Entonces $r \in \mathbb{N}$. Además, como $d \in H$ entonces $d = at + bs$ con $t, s \in \mathbb{Z}$. Luego,

$$r = a - d.q = a - (at + bs)q = a(1 - tq) + b(-sq)$$

y como $1 - tq, -sq \in \mathbb{Z}$ y $r \in \mathbb{N}$ entonces $r \in H$. Pero esto no puede ocurrir pues $r < d$ y d es el primer elemento de H.
Por lo tanto debe ser $r = 0$. Luego, $d \mid a$.

Análogamente se ve que $d \mid b$. Luego, $d \mid a$ y $d \mid b$.

iii) Sea $c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$.
Como $d \in H$ entonces $d = at + bs$, con $t, s \in \mathbb{Z}$. Veamos que $c \mid d$:
Como $c \mid a$ entonces $c \mid at$ y como $c \mid b$ entonces $c \mid bs$. Luego $c \mid at + bs = d$.

Unicidad: Supongamos que d_1 y d_2 son enteros que satisfacen i), ii) y iii).
Veamos que $d_1 = d_2$:

Como d_1 satisface ii) entonces $d_1 \mid a$ y $d_1 \mid b$. Pero como d_2 satisface iii) esto implica que $d_1 \mid d_2$. Y como d_1 y d_2 satisfacen i) entonces $d_1 \leq d_2$.
Como d_2 satisface ii) entonces $d_2 \mid a$ y $d_2 \mid b$. Pero como d_1 satisface iii) esto implica que $d_2 \mid d_1$. Y como d_1 y d_2 satisfacen i) entonces $d_2 \leq d_1$.
Luego, $d_1 = d_2$. □

Notación. Denotaremos por $(a : b)$ al máximo común divisor entre a y b, es decir, al único $d \in \mathbb{Z}$ que satisface las condiciones i), ii) y iii) del teorema.

Corolario. Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$. Entonces $\exists\, t, s \in \mathbb{Z}$ tales que $(a : b) = at + bs$.

Demostración: Sea $H = \{at + bs \,/\, t, s \in \mathbb{Z}\} \cap \mathbb{N}$. En la demostración del teorema vimos que existe $d \in H$ que satisface i), ii) y iii) (el primer elemento de H). Luego, por la unicidad del máximo común divisor, debe ser $(a : b) = d$. Por lo tanto $(a : b) \in H$ lo que muestra que $\exists\, t, s \in \mathbb{Z}$ tales que $(a : b) = at + bs$ □

Observación. Los enteros t y s del corolario no son únicos. Por ejemplo, si $a = 24$ y $b = 15$ entonces $(a : b) = 3 = 2a - 3b = -3a + 5b$

Ejemplos. 1) Veamos que efectivamente $(24 : 15) = 3$.
Sea $d = (24 : 15)$. Como $3 \mid 24$, $3 \mid 15$ y d satisface iii) del teorema entonces $3 \mid d$. Luego, $3 \leq d$ pues $d \in \mathbb{N}$
Por otra parte, como d satisface ii) del teorema entonces $d \mid 24$ y $d \mid 15$, de donde resulta que $d \mid 24 - 15 = 9$. Luego, $d \mid 15$ y $d \mid 9$ por lo tanto $d \mid 15 - 9 = 6$. Pero entonces $d \mid 9$ y $d \mid 6$, luego $d \mid 9 - 6 = 3$ y, como $d \in \mathbb{N}$ entonces $d \leq 3$.

2) Veamos que, dado $a \in \mathbb{Z}$, si $d = (7a-2 : 4a+1)$ entonces $d = 1, 3, 5$ o 15. Por ejemplo, si $a = 1$ entonces $d = (5 : 5) = 5$, si $a = 2$ entonces $d = (12 : 9) = 3$, si $a = 0$ entonces $d = (-2 : 1) = 1$ y si $a = -4$ entonces $d = (-30 : -15) = 15$.

Como $d \mid 7a-2$ y $d \mid 4a+1$ entonces $d \mid 4(7a-2)$ y $d \mid 7(4a+1)$, es decir $d \mid 28a-8$ y $d \mid 28a+7$. Luego, $d \mid (28a+7)-(28a-8) = 15$. Luego, como $d \in \mathbb{N}$ y $d \mid 15$ entonces $d = 1, 3, 5$ o 15.

Diremos que a y b son *coprimos* si $(a : b) = 1$. Notar que a y b no son coprimos si y sólo si existe un primo positivo p tal que $p \mid a$ y $p \mid b$.
En efecto, sea $d = (a : b)$. Si existe un primo positivo p tal que $p \mid a$ y $p \mid b$ entonces $p \mid d$ de donde $d \neq 1$.
Recíprocamente, si $d \neq 1$ entonces $d > 1$. Luego, existe un primo positivo p tal que $p \mid d$ y como $d \mid a$ y $d \mid b$ entonces $p \mid a$ y $p \mid b$.

Propiedades del máximo común divisor. Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$. Entonces valen

1) $(a : b) = (b : a)$

2) $(a : b) = (-a : b) = (a : -b) = (-a : -b)$

3) Si p es un primo positivo entonces

$$(a : p) = \begin{cases} p & \text{si } p \mid a \\ 1 & \text{en otro caso} \end{cases}$$

4) Si $a \mid b$ entonces $(a : b) = |a|$. En particular, si $a \neq 0$ entonces $(a : 0) = |a|$

5) a y b son coprimos si y sólo si $\exists\, r, s \in \mathbb{Z}$ tales que $1 = ra + sb$ (1 es *combinación lineal entera* de a y b).

Notemos que si 1 es combinación lineal entera de a y b entonces cualquier entero es combinación lineal entera de a y b: si $1 = ra + sb$ y $c \in \mathbb{Z}$ entonces $c = c.1 = (cr)a + (cs)b$.

6) Si $d = (a : b)$ entonces $\frac{a}{d}$ y $\frac{b}{d}$ son enteros y $\left(\frac{a}{d} : \frac{b}{d}\right) = 1$

Demostración: Probaremos 5) y 6), el resto queda como ejercicio.

5) ($\Longrightarrow$) Vale por el corolario.
($\Longleftarrow$) Sea $d = (a : b)$, queremos ver que $d = 1$. Si $1 = ra + sb$, como $d \mid a$ y $d \mid b$ entonces $d \mid ra$ y $d \mid sb$. Luego $d \mid ra + sb = 1$ y como $d \in \mathbb{N}$ entonces $d = 1$.

6) Como $d \mid a$ y $d \mid b$ entonces $\frac{a}{d}$ y $\frac{b}{d}$ son enteros. Veamos que son coprimos. Para ello, por 5) basta ver que 1 es combinación lineal entera de $\frac{a}{d}$ y $\frac{b}{d}$.
Por el corolario, como $d = (a : b)$ entonces $\exists\, r, s \in \mathbb{Z}$ tales que $d = ra + sb$. Luego, $1 = r\,\dfrac{a}{d} + s\,\dfrac{b}{d}$ □

Proposición. Sean $a, b \in \mathbb{Z}$, $b \neq 0$. Si $a = bq + r$, con $q, r \in \mathbb{Z}$, entonces $(a : b) = (b : r)$.

Demostración: Sea $d = (a : b)$. Probaremos que $(b : r) = d$, para lo cual debemos ver que d satisface:

i) $d \in \mathbb{N}$
ii) $d \mid b$ y $d \mid r$
iii) Dado $c \in \mathbb{Z}$, si $c \mid b$ y $c \mid r$ entonces $c \mid d$

Sabemos que $d \in \mathbb{N}$ ya que $d = (a : b)$. Además, por la misma razón vale que $d \mid b$. Veamos que $d \mid r$. Como $d \mid a$ y $d \mid b$ entonces $d \mid a$ y $d \mid bq$ de donde $d \mid a - bq = r$.
Sea ahora $c \in \mathbb{Z}$ tal que $c \mid b$ y $c \mid r$. Entonces $c \mid bq$ y $c \mid r$, de donde $c \mid a = bq + r$. Luego $c \mid a$ y $c \mid b$ lo que implica que $c \mid d$ pues $d = (a : b)$.
Hemos probado entonces que d satisface i), ii) y iii). Luego, por la unicidad del máximo común divisor, $(b : r) = d$. □

Algoritmo de Euclides. La proposición anterior nos da un algoritmo con el que podemos calcular $d = (a : b)$ y escribir a d como combinación lineal de a y b, es decir, hallar $r, s \in \mathbb{Z}$ tales que $d = ra + sb$. Veremos cómo en un ejemplo:
Calcularemos $d = (990 : 187)$ y lo escribiremos como combinación lineal de 990 y 187. Para ello usaremos el algoritmo de división y la proposición sucesivas veces.

Primero dividimos 990 por 187: $990 = 187.5 + 55$. Entonces$(990 : 187) = (187 : 55)$.
Ahora dividimos 187 por 55: $187 = 55.3 + 22$. Entonces $(187 : 55) = (55 : 22)$.
Luego dividimos 55 por 22: $55 = 22.2 + 11$. Entonces $(55 : 22) = (22 : 11)$.
Finalmente dividimos 22 por 11: $22 = 11.2 + 0$. Entonces $(22 : 11) = (11 : 0) = 11$.
Por lo tanto $(990 : 187) = 11$. En general, el resto de cada división es mayor o igual que cero y estrictamente menor que el resto de la división anterior y por lo tanto en algún momento debemos obtener un resto igual a cero. El máximo común divisor buscado es el último resto no nulo.

Veamos ahora cómo escribir a 11 como combinación lineal de 990 y 187:

$$\begin{aligned} 990 = 187.5 + 55 \quad &\Longrightarrow \quad 55 = 990 - 5.187 \qquad (1) \\ 187 = 55.3 + 22 \quad &\Longrightarrow \quad 22 = 187 - 3.55 \qquad (2) \\ 55 = 22.2 + 11 \quad &\Longrightarrow \quad 11 = 55 - 2.22 \qquad (3) \end{aligned}$$

Luego, usando primero (3), luego (2) y finalmente (1) se tiene que

$$\begin{aligned} 11 &= 55 - 2.22 = 55 - 2(187 - 3.55) = 55 - 2.187 + 6.55 = 7.55 - 2.187 = \\ &= 7.(990 - 5.187) - 2.187 = 7.990 - 35.187 - 2.187 = 7.990 - 37.187 = \\ &= 7.990 + (-37).187 \end{aligned}$$

Proposición. Sean $a, b, c \in \mathbb{Z}$. Si $a \mid b.c$ y $(a : b) = 1$ entonces $a \mid c$.

Demostración: Como $(a : b) = 1$ entonces existen $r, s \in \mathbb{Z}$ tales que $1 = ra + sb$. Luego, $c = rac + sbc$. Como $a \mid rac$ y $a \mid sbc$ pues $a \mid bc$ entonces $a \mid rac + sbc = c$ □

Corolario 1. Sean $a, b \in \mathbb{Z}$ y sea p un primo. Si $p \mid a.b$ entonces $p \mid a$ o $p \mid b$.

Demostración: Basta usar la proposición anterior y que si $p \not| a$ entonces $(p : a) = 1$. □

Ejercicio. Hallar $a, b, c \in \mathbb{Z}$ tales que $c \mid a.b$, $c \not| a$ y $c \not| b$.

Corolario 2. Sean $a, b, c \in \mathbb{Z}$ y sea $m \in \mathbb{N}$ tal que $(c : m) = 1$. Entonces

$$ac \equiv bc\ (m) \Longleftrightarrow a \equiv b\ (m)$$

Demostración: Ejercicio.

Proposición. Sean $a, b, c \in \mathbb{Z}$ tales que $(a : b) = 1$. Si $a \mid c$ y $b \mid c$ entonces $a.b \mid c$.

Demostración: Como $(a : b) = 1$ entonces existen $r, s \in \mathbb{Z}$ tales que $1 = ra + sb$. Luego, $c = rac + sbc$. Como $a \mid c$ entonces $c = a.k$ para algún $k \in \mathbb{Z}$ y como $b \mid c$ entonces $c = b.h$ para algún $h \in \mathbb{Z}$. Luego $c = rac + sbc = rabh + sbak = ab(rh + sk)$ y como $rh + sk \in \mathbb{Z}$ entonces $ab \mid c$. □

Corolario. Sean $a, b \in \mathbb{Z}$ y sean $m_1, m_2 \in \mathbb{N}$ tales que $(m_1 : m_2) = 1$. Entonces

$$a \equiv b\ (m_1) \text{ y } a \equiv b\ (m_2) \Longleftrightarrow a \equiv b\ (m_1.m_2)$$

Demostración: Ejercicio.

Ejercicio. Sean $a, b \in \mathbb{Z}$ y $m_1, m_2, \ldots, m_k \in \mathbb{N}$ tales que $(m_i : m_j) = 1$ para todo $i \neq j$. Probar que $a \equiv b\ (m_i)\ \forall\, i \Longleftrightarrow a \equiv b\ (m_1.m_2 \ldots m_k)$

Ejemplos.

1) Hallar todos los $a \in \mathbb{Z}$ tales que $7a \equiv 1\ (30)$.
$7a \equiv 1\ (30) \Longleftrightarrow 7a \equiv 91\ (30) \Longleftrightarrow 7a \equiv 7.13\ (30)$. Como $(7 : 30) = 1$, usando el corolario 2, esto último es equivalente a $a \equiv 13\ (30)$. Luego, los $a \in \mathbb{Z}$ que satisfacen lo pedido son los de la forma $a = 30q + 13$ con $q \in \mathbb{Z}$.

2) Sea a un entero impar no divisible por 3. Probar que $24 \mid a^2 - 1$.
Como $24 = 3.8$ y $(3 : 8) = 1$ entonces basta probar que $3 \mid a^2 - 1$ y $8 \mid a^2 - 1$.
Veamos primero que $3 \mid a^2 - 1$: como $3 \not| a$ entonces los posibles restos de la división de a por 3 son 1 y 2. Luego, $a \equiv 1\ (3)$ o $a \equiv 2 \equiv -1\ (3)$. Luego, $a^2 \equiv 1\ (3)$ y por lo tanto $3 \mid a^2 - 1$.
Ahora veamos que $8 \mid a^2 - 1$. Como a es impar entonces $a = 2k + 1$ para algún $k \in \mathbb{Z}$. Luego,

$$a^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k = 4k(k + 1)$$

y como k es par o $k + 1$ es par entonces $k(k + 1)$ siempre es par, de donde $k(k + 1) = 2q$ para algún $q \in \mathbb{Z}$. Por lo tanto $a^2 - 1 = 4k(k + 1) = 8q$. Luego $8 \mid a^2 - 1$.

Proposición. Sean $a, b \in \mathbb{Z}$, alguno de ellos no nulo, y sea $c \in \mathbb{Z}$, $c > 0$. Entonces $(c.a : c.b) = c.(a : b)$.

Demostración: Sea $d = (a : b)$. Probaremos que $(c.a : c.b) = c.d$, para lo cual debemos mostrar que
i) $c.d \in \mathbb{N}$
ii) $c.d \mid c.a$ y $c.d \mid c.b$
iii) Sea $k \in \mathbb{Z}$. Si $k \mid c.a$ y $k \mid c.b$ entonces $k \mid c.d$

i) y ii) son triviales pues $d \in \mathbb{N}$, $d \mid a$ y $d \mid b$. Probemos iii): Sea $k \in \mathbb{Z}$ tal que $k \mid c.a$ y $k \mid c.b$. Como $d = (a : b)$ entonces existen $t, s \in \mathbb{Z}$ tales que $d = ta + sb$. Luego, $c.d = t.c.a + s.c.b$. Como $k \mid c.a$ y $k \mid c.b$ entonces $k \mid t.c.a$ y $k \mid s.c.b$ de donde $k \mid t.c.a + s.c.b = c.d$. Luego, $k \mid c.d$ como queríamos probar. □

Ejemplos.

1) Sean a y b enteros coprimos. Veamos que $(2a - b : a + 3b) = 1$ o 7.
Sea $d = (2a - b : a + 3b)$. Entonces $d \mid 2a - b$ y $d \mid a + 3b$. Luego, $d \mid 6a - 3b$ y $d \mid a + 3b$ de donde $d \mid 7a$.
Además, como $d \mid 2a - b$ y $d \mid a + 3b$ entonces $d \mid 2a - b$ y $d \mid 2a + 6b$ de donde $d \mid 7b$.
Por lo tanto, $d \mid 7a$ y $d \mid 7b$ lo que implica que $d \mid (7a : 7b) = 7(a : b) = 7$ pues $(a : b) = 1$.
Luego, $d \mid 7$ y $d \in \mathbb{N}$ de manera que $d = 1$ o 7.

2) Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 6$. Veamos que $(7a - 3b : 2a + 5b) = 6$ o 246.
Sea $d = (7a - 3b : 2a + 5b)$. Entonces $d \mid 7a - 3b$ y $d \mid 2a + 5b$.

$$\left.\begin{array}{l} d \mid 7a - 3b \Longrightarrow d \mid 14a - 6b \\ d \mid 2a + 5b \Longrightarrow d \mid 14a + 35b \end{array}\right\} \Longrightarrow d \mid 41b$$

$$\Longrightarrow d \mid (41a : 41b) = 41(a : b) = 6.41$$

$$\left.\begin{array}{l} d \mid 7a - 3b \Longrightarrow d \mid 35a - 15b \\ d \mid 2a + 5b \Longrightarrow d \mid 6a + 15b \end{array}\right\} \Longrightarrow d \mid 41a$$

Luego, $d = 1, 2, 3, 6, 41, 2.41, 3.41$ o 6.41. Pero como $6 \mid a$ y $6 \mid b$ entonces $6 \mid 7a - 3b$ y $6 \mid 2a + 5b$ de donde $6 \mid d$. Luego, $d = 6$ o $d = 6.41 = 246$.

Otra manera de hacer esto es la siguiente: como $6 \mid a$ y $6 \mid b$ entonces $a = 6k$ y $b = 6q$ $(k, q \in \mathbb{Z})$. Luego $6 = (a : b) = (6k : 6q) = 6(k : q)$ de donde se tiene que $(k : q) = 1$.
Por otra parte, $d = (7a - 3b : 2a + 5b) = (7.6k - 3.6q : 2.6k + 5.6q) = 6(7k - 3q : 2k + 5q)$.
Luego, basta ver que si $(k : q) = 1$ entonces $(7k - 3q : 2k + 5q) = 1$ o 41, lo que dejamos como ejercicio.

3) Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 3$. Veamos que $(3ab : a^2 + b^2) = 9$.
Como $3 \mid a$ y $3 \mid b$ entonces $a = 3k$ y $b = 3q$ donde $k, q \in \mathbb{Z}$. Como $3 = (3k : 3q) = 3(k : q)$ entonces $(k : q) = 1$.
Por otra parte, $(3ab : a^2 + b^2) = (3.3k.3q : 9k^2 + 9q^2) = 9(3kq : k^2 + q^2)$. Luego basta ver que si $(k : q) = 1$ entonces $(3kq : k^2 + q^2) = 1$.

Sean k y q enteros coprimos y supongamos que $(3kq : k^2 + q^2) \neq 1$. Entonces existe un primo positivo p tal que $p \mid 3kq$ y $p \mid k^2 + q^2$.
Como $p \mid 3kq$ y p es primo entonces $p \mid 3$ o $p \mid k$ o $p \mid q$.
Si $p \mid 3$, como p es un primo positivo entonces $p = 3$. Luego, $3 \mid k^2 + q^2$. Pero esto, por el ejercicio 16. v) de la práctica 4, implica que $3 \mid k$ y $3 \mid q$ lo que es absurdo pues k y q son coprimos.
Si $p \mid k$ entonces $p \mid k^2$ y como $p \mid k^2 + q^2$ entonces $p \mid q^2$ de donde resulta que $p \mid q$ pues p es primo. Pero entonces $p \mid k$ y $p \mid q$ lo que no puede ocurrir pues k y q son coprimos.
Análogamente se ve que si Si $p \mid q$ entonces $p \mid k$ y $p \mid q$.

Por lo tanto, debe ser $(3kq : k^2 + q^2) = 1$ con lo cual se tiene que $(3ab : a^2 + b^2) = 9$.

Proposición. Sean $a, b \in \mathbb{Z}$, alguno de ellos no nulo, y sea $n \in \mathbb{N}$. Entonces se verifican:
i) Si $(a : b) = 1$ entonces $(a^n : b^n) = 1$
ii) Si $(a : b) = d$ entonces $(a^n : b^n) = d^n$

Demostración: Ejercicio.

Ejemplo. Veamos que $(2^n + 7^{n+1} : 2^{n+1} + 7^n) = 1$ o 13.
Sea $d = (2^n + 7^{n+1} : 2^{n+1} + 7^n)$. Entonces

$$\left.\begin{array}{l} d \mid 2^n + 7^{n+1} \Longrightarrow d \mid 2^{n+1} + 2.7^{n+1} \\ d \mid 2^{n+1} + 7^n \Longrightarrow d \mid 2^{n+1} + 7^n \end{array}\right\} \Longrightarrow d \mid 13.7^n$$

$$\Longrightarrow d \mid (13.7^n : 13.2^n) = 13(7^n : 2^n)$$

$$\left.\begin{array}{l} d \mid 2^n + 7^{n+1} \Longrightarrow d \mid 2^n + 7^{n+1} \\ d \mid 2^{n+1} + 7^n \Longrightarrow d \mid 7.2^{n+1} + 7^{n+1} \end{array}\right\} \Longrightarrow d \mid 13.2^n$$

y como $(7^n : 2^n) = 1$ pues $(7 : 2) = 1$ entonces $d \mid 13$ y, como $d \in \mathbb{N}$, esto implica que $d = 1$ o $d = 13$.

En realidad, d nunca es 13. Veremos esto más adelante.

6. Ecuaciones diofánticas.

Una ecuación diofántica es una ecuación donde las constantes y las variables son números enteros, es decir, se pretende hallar las soluciones enteras de una ecuación con coeficientes enteros. Por ejemplo, hallar todos los $x, y, z \in \mathbb{Z}$ tales que $3x^2 + y^2 = 2z^2$. Nosotros nos restringiremos a estudiar las ecuaciones diofánticas lineales con dos variables, es decir, las de la forma $ax + by = c$ donde a, b y c son enteros dados.

Supongamos que queremos hallar las soluciones enteras de $12x + 26y = 7$, es decir, todos los $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ que satisfacen la ecuación $12x + 26y = 7$. Como el miembro izquierdo es un entero par y el derecho no lo es, entonces en seguida concluímos que no hay solución.

Lo mismo ocurre con la ecuación $350x + 120y = 45$. En este caso el miembro izquierdo es un entero divisible por 10 y el derecho no.
En general, supongamos que buscamos los $x, y \in \mathbb{Z}$ que sean solución de $ax + by = c$. Si $d = (a : b)$ entonces el miembro izquierdo es un entero divisible por d pues $d \mid a$ y $d \mid b$. Por lo tanto, si $d \not| c$ entonces la ecuación no puede tener solución. Hemos probado entonces que si la ecuación $ax + by = c$ tiene una solución $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ entonces $(a : b) \mid c$.
A continuación veremos que vale la recíproca, es decir, vamos a probar que si $(a : b) \mid c$ entonces la ecuación $ax+by = c$ tiene infinitas soluciones $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ y también veremos cómo hallar todas estas soluciones.

Veamos primero el caso en que $(a : b) = 1$: como a y b son coprimos entonces existen $r, s \in \mathbb{Z}$ tales que $1 = ra+sb$. Luego $c = c.1 = (cr)a+(cs)b$. Por lo tanto, $(x_0, y_0) = (cr, cs)$ es una solución de la ecuación. Veamos ahora cómo podemos obtener todas las soluciones a partir de (x_0, y_0).

Sean $x, y \in \mathbb{Z}$ tales que $ax + by = c$. Como $ax_0 + by_0 = c$ entonces $ax + by = ax_0 + by_0$. Luego,

$$a(x - x_0) = b(y_0 - y) \tag{4}$$

Por lo tanto, $a \mid y_0 - y$ y $b \mid x - x_0$. Luego, existen $q, k \in \mathbb{Z}$ tales que $y_0 - y = aq$ y $x - x_0 = bk$. Por (4), se tiene entonces que $abk = baq$ de donde resulta que $k = q$.
Hemos probado entonces que si $x, y \in \mathbb{Z}$ satisfacen $ax + by = c$ entonces $x = x_0 + bq$ e $y = y_0 - aq$. Recíprocamente, si $x = x_0 + bq$ e $y = y_0 - aq$, con $q \in \mathbb{Z}$, entonces

$$ax + by = a(x_0 + bq) + b(y_0 - aq) = ax_0 + by_0 = c$$

Se tiene entonces que $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ es solución de $ax + by = c$ si y sólo si $x = x_0 + bq$ e $y = y_0 - aq$ para algún $q \in \mathbb{Z}$.
Veamos ahora el caso general. Sea $d = (a : b)$ y supongamos que $d \mid c$. Entonces, dado $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ vale

$$ax + by = c \iff \frac{a}{d}\, x + \frac{b}{d}\, y = \frac{c}{d}$$

donde ahora $\frac{a}{d}$ y $\frac{b}{d}$ son enteros coprimos. Entonces, por lo que probamos para el caso coprimo, $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ es solución de $ax + by = c$ si y sólo si $x = x_0 + \frac{b}{d}q$ e $y = y_0 - \frac{a}{d}q$ para algún $q \in \mathbb{Z}$, donde (x_0, y_0) es una solución particular de $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$.

Ejemplo. Hallemos todos los $x, y \in \mathbb{Z}$ tales que $14x + 22y = 160$.
Primero calculamos $d = (14 : 22)$ para ver si hay solución. Como $d = 2$ y $2 \mid 160$ entonces hay solución.
Para hallar las soluciones, observamos que $14x+22y = 160 \iff 7x+11y = 80$. Resolvamos entonces esta última ecuación donde ahora $(7 : 11) = 1$. Ahora hallamos una solución particular escribiendo al 1 como combinación lineal entera de 7 y 11: $1 = 7.8 + 11.(-5)$

lo que implica que $80 = 7(640) + 11(-400)$. Luego, $x_0 = 640$ e $y_0 = -400$. Por lo tanto todas las soluciones enteras de la ecuación son $x = 640 + 11q$ e $y = -400 - 7q$ con $q \in \mathbb{Z}$.

Ejercicio. Si se reparten 106 monedas iguales entre una cierta cantidad de personas de manera que cada hombre reciba 14 monedas y cada mujer reciba 10 monedas, ¿cuántos hombres y cuántas mujeres hay?

7. Ecuaciones lineales de congruencia.

Dados $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$, queremos hallar todos los $x \in \mathbb{Z}$ que satisfacen $ax \equiv b\ (m)$. Notemos que $\exists\, x \in \mathbb{Z}$ solución de $ax \equiv b\ (m)$ si y sólo si $\exists\, x \in \mathbb{Z}$ tal que $m \mid ax - b$, si y sólo si $\exists\, x, y \in \mathbb{Z}$ tales que $ax - b = ym$ si y sólo si $\exists\, x, y \in \mathbb{Z}$ tales que $ax + (-m)y = b$. Luego, la ecuación lineal de congruencia $ax \equiv b\ (m)$ tiene solución si y sólo si la ecuación diofántica $ax + (-m)y = b$ tiene solución si y sólo si $(a : m) \mid b$. Por ejemplo, la ecuación $14x \equiv 5\ (21)$ no tiene solución pues $(14 : 21) = 7$ y $7 \not| 5$.

Sea $d = (a : m)$ y supongamos que $d \mid b$. Hallaremos las soluciones de $ax \equiv b\ (m)$. Notemos que si hallamos todas las soluciones $x, y \in \mathbb{Z}$ de la ecuación diofántica $ax + (-m)y = b$ entonces los x hallados son todas las soluciones de $ax \equiv b\ (m)$. Veamos otra manera de resolver la ecuación de congruencia.

Como $d \mid a$, $d \mid b$ y $d \mid m$ entonces $\frac{a}{d}$, $\frac{b}{d}$ y $\frac{m}{d}$ son enteros. Luego, por la propiedad 12) de la congruencia,

$$ax \equiv b\ (m) \Longleftrightarrow d.\frac{a}{d}\ x \equiv d.\frac{b}{d}\ (d.\frac{m}{d}) \Longleftrightarrow \frac{a}{d}\ x \equiv \frac{b}{d}\ (\frac{m}{d})$$

Como $\frac{a}{d}$ y $\frac{m}{d}$ son enteros coprimos entonces existen $k, s \in \mathbb{Z}$ tales que $1 = k.\frac{a}{d} + s.\frac{m}{d}$ y como $\frac{m}{d} \equiv 0\ (\frac{m}{d})$ entonces se tiene que

$$1 = k.\frac{a}{d} + s.\frac{m}{d} \equiv k.\frac{a}{d} + s.0 = k.\frac{a}{d} \quad (\frac{m}{d})$$

Es decir, $k.\frac{a}{d} \equiv 1\ (\frac{m}{d})$. Además, como $1 = k.\frac{a}{d} + s.\frac{m}{d}$ entonces k y $\frac{m}{d}$ son enteros coprimos pues 1 es combinación lineal entera de k y $\frac{m}{d}$. Luego,

$$ax \equiv b\ (m) \Longleftrightarrow \frac{a}{d}\ x \equiv \frac{b}{d}\ (\frac{m}{d}) \Longleftrightarrow k.\frac{a}{d}\ x \equiv k.\frac{b}{d}\ (\frac{m}{d}) \Longleftrightarrow 1.x \equiv k.\frac{b}{d}\ (\frac{m}{d})$$

Por lo tanto hemos probado que

$$ax \equiv b\ (m) \Longleftrightarrow x \equiv k.\frac{b}{d}\ (\frac{m}{d}) \Longleftrightarrow x \equiv x_0\ (\frac{m}{d})$$

donde x_0 es el resto de la división de $k.\frac{b}{d}$ por $\frac{m}{d}$.

Luego, las soluciones de $ax \equiv b\ (m)$ son $x = x_0 + q\frac{m}{d}$, con $q \in \mathbb{Z}$. Además hay $d = (a : m)$ soluciones de $ax \equiv b\ (m)$, que satisfacen $0 \leq x < m$ y estas son: $x = x_0 + q.\frac{m}{d}$ donde

$q \in \mathbb{Z}$ tal que $0 \leq q < d$. Dejamos la demostración de esta afirmación como ejercicio (usar que $0 \leq x_0 < \frac{m}{d}$ y ver que $0 \leq x_0 + q\frac{m}{d} < m$ si y sólo si $0 \leq q < d$).

Ejemplos.

1) Hallar todos los $x \in \mathbb{Z}$ tales que $39x \equiv 24\ (45)$.
En primer lugar, esta ecuación tiene solución pues $d = (39 : 45) = 3$ y $3 \mid 24$. Además, $39x \equiv 24\ (45) \iff 13x \equiv 8\ (15)$ por lo tanto resolveremos $13x \equiv 8\ (15)$. La ventaja es que ahora 13 y 15 son coprimos. Luego, 1 es combinación lineal entera de 13 y 15: $1 = 7.13 + (-6).15$. Por lo tanto $7.13 \equiv 1\ (15)$ y como 7 y 15 son coprimos,

$$13x \equiv 8\ (15) \iff 7.13x \equiv 7.8\ (15) \iff x \equiv 56 \equiv 11(15)$$

Luego, las soluciones buscadas son $x = 11 + 15q$, con $q \in \mathbb{Z}$.

¿Cuáles son todas las soluciones de $39x \equiv 24\ (45)$ que satisfacen $0 \leq x < 45$?
Debemos ver para cuáles valores de q se satisface que $0 \leq 11 + 15q < 45$. Dejamos como ejercicio verificar que estos son $q = 0, 1$ y 2. Por lo tanto los x buscados son $x = 11, 26, 41$.

2) Hallar todos los $a \in \mathbb{Z}$ tales que $(7a + 2 : 5a + 3) \neq 1$.
Sea $d = (7a + 2 : 5a + 3)$. Veamos cuáles son los posibles valores de d. Como $d \mid 7a + 2$ y $d \mid 5a + 3$ entonces $d \mid 35a + 10$ y $d \mid 35a + 21$. Luego, $d \mid 11$, de donde $d = 1$ o $d = 11$.
Entonces lo que queremos es hallar todos los $a \in \mathbb{Z}$ tales que $(7a + 2 : 5a + 3) = 11$.
Notemos que como $(7a + 2 : 5a + 3) = 1$ o 11 entonces $(7a + 2 : 5a + 3) = 11$ si y sólo si $11 \mid 7a + 2$ y $11 \mid 5a + 3$.
Hallemos los $a \in \mathbb{Z}$ tales que $11 \mid 7a + 2$:

$$11 \mid 7a + 2 \iff 7a + 2 \equiv 0\ (11) \iff 7a \equiv -2\ (11)$$

Luego, debemos resolver la ecuación lineal de congruencia $7a \equiv -2\ (11)$.
En este caso $d = (7 : 11) = 1$. Escribimos al 1 como combinación lineal entera de 7 y 11: $1 = 7.(-3) + 11.2$. Luego, $7(-3) \equiv 1\ (11)$ y, como -3 y 11 son coprimos se tiene que

$$7a \equiv -2\ (11) \iff (-3)7a \equiv (-3)(-2)\ (11) \iff a \equiv 6\ (11)$$

Luego, $11 \mid 7a + 2$ si y sólo si $a \equiv 6\ (11)$.

Ahora hallemos los $a \in \mathbb{Z}$ tales que $11 \mid 5a + 3$, es decir, resolvamos la ecuación lineal de congruencia $5a \equiv -3\ (11)$. En este caso $d = (5 : 11) = 1$. Escribimos al 1 como combinación lineal entera de 5 y 11: $1 = 5(-2) + 11.1$. Luego, $5(-2) \equiv 1\ (11)$ y, como -2 y 11 son coprimos se tiene que

$$5a \equiv -3\ (11) \iff (-2)5a \equiv (-2)(-3)\ (11) \iff a \equiv 6\ (11)$$

Luego, los $a \in \mathbb{Z}$ tales que $(7a + 2 : 5a + 3) \neq 1$ son los de la forma $a = 6 + 11q$ con $q \in \mathbb{Z}$.

8. Mínimo común múltiplo.

Sea $\mathcal{R}$ la relación de orden en $\mathbb{N}$ definida por $a\,\mathcal{R}\,b \iff a \mid b$ Dados $a, b \in \mathbb{Z}$, ambos no nulos, diremos que m es el *mínimo común múltiplo* entre a y b si es el menor, respecto del orden $\mathcal{R}$, de los múltiplos positivos comunes de a y b. Es decir, m es el único número entero que satisface las condiciones:

i) $m \in \mathbb{N}$ (m es positivo)
ii) $a \mid m$ y $b \mid m$ (m es un múltiplo de a y de b)
iii) Dado $c \in \mathbb{N}$, si $a \mid c$ y $b \mid c$ entonces $m \mid c$ (Si c es un múltiplo positivo de a y de b entonces $m\,\mathcal{R}\,c$, es decir, m es menor o igual que c respecto de la relación de orden $\mathcal{R}$).
Notemos que m es también el menor, respecto del orden usual, de los múltiplos positivos de a y b. En efecto si c es un múltiplo positivo de a y de b entonces por iii) se tiene que $m \mid c$ de donde $m \leq c$.
Notemos además que la condición iii) es equivalente a la condición: "dado $c \in \mathbb{Z}$, si $a \mid c$ y $b \mid c$ entonces $m \mid c$".

El siguiente teorema garantiza que un tal m existe y es único.

Teorema. Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ y $b \neq 0$. Entonces $\exists!\, m \in \mathbb{Z}$ que satisface:

i) $m \in \mathbb{N}$
ii) $a \mid m$ y $b \mid m$
iii) Dado $c \in \mathbb{Z}$, si $a \mid c$ y $b \mid c$ entonces $m \mid c$

Demostración: Existencia: Sea $H = \{n \in \mathbb{N} \,/\, a \mid n \text{ y } b \mid n\}$. Como H es un subconjunto no vacío de $\mathbb{N}$ ya que $|ab| \in H$ entonces, por el principio de buena ordenación, posee un primer elemento m. Luego $m \in H$ y $m \leq h$ para todo $h \in H$.
Es trivial que m satisface i) y ii) pues $m \in H$. Veamos que satisface iii):
Sea $c \in \mathbb{Z}$ tal que $a \mid c$ y $b \mid c$ y sean $q, r \in \mathbb{Z}$ el cociente y el resto de la división de c por m, es decir, $c = mq + r$ y $0 \leq r < m$. Queremos probar que $r = 0$.
Supongamos que $r > 0$. Entonces $r \in \mathbb{N}$ y como $a \mid c$ y $a \mid m$ entonces $a \mid r$. Del mismo modo se ve que $b \mid r$. Luego, $r \in H$, lo cual no puede ocurrir pues $r < m$ y m es el primer elemento de H.

Unicidad: Ejercicio □

Notación. Denotaremos por $[a : b]$ al mínimo común múltiplo entre a y b, es decir, al único $d \in \mathbb{Z}$ que satisface las condiciones i), ii) y iii) del teorema.

Propiedades del mínimo común múltiplo. Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ y $b \neq 0$. Entonces valen

1) $[a : b] = [b : a]$

2) $[a : b] = [-a : b] = [a : -b] = [-a : -b]$

3) Si $a \mid b$ entonces $[a : b] = |b|$.

Demostración: Ejercicio.

Proposición. Sean $a, b \in \mathbb{Z}$ tales que $a > 0$ y $b > 0$. Entonces $(a : b).[a : b] = ab$.

Demostración: Sea $m = \frac{ab}{(a:b)}$. Probaremos que m es el mínimo común múltiplo entre a y b mostrando que satisface las condiciones i), ii) y iii) del teorema.

i) Como $(a : b) \mid a$ entonces $\frac{a}{(a:b)} \in \mathbb{Z}$. Luego $\frac{ab}{(a:b)} \in \mathbb{Z}$ y es positivo, por lo tanto $\frac{ab}{(a:b)} \in \mathbb{N}$.

ii) Como $(a : b) \mid b$ entonces $\frac{b}{(a:b)} \in \mathbb{Z}$ y $m = \frac{ab}{(a:b)} = a\,\frac{b}{(a:b)}$. Luego, $a \mid m$. Del mismo modo se ve que $b \mid m$.

iii) Sea $c \in \mathbb{Z}$ tal que $a \mid c$ y $b \mid c$. Entonces $c = aq$ y $c = bk$ $(q, k \in \mathbb{Z})$. Como $\frac{a}{(a:b)}$ y $\frac{b}{(a:b)}$ son enteros coprimos entonces existen $r, s \in \mathbb{Z}$ tales que $1 = r\frac{a}{(a:b)} + s\frac{b}{(a:b)}$. Entonces

$$c = cr\frac{a}{(a:b)} + cs\frac{b}{(a:b)} = bkr\frac{a}{(a:b)} + aqs\frac{b}{(a:b)} = \frac{ab}{(a:b)}(kr + qs) = m(kr + qs)$$

y como $kr + qs \in \mathbb{Z}$ esto implica que $m \mid c$.

Luego, por la unicidad del mínimo común múltiplo, $m = [a : b]$ como queríamos probar. □

Corolario. Sean $a, b \in \mathbb{Z}$ tales que $a > 0$ y $b > 0$. Entonces a y b son coprimos si y sólo si $[a : b] = ab$.

9. Teorema fundamental de la aritmética.

Veremos que todo número natural mayor que 1 se factoriza como producto de primos positivos, de manera única salvo el orden de los factores.

Teorema. (Teorema Fundamental de la Aritmética) Sea $a \in \mathbb{N}$. Si $a > 1$ entonces existen primos positivos $p_1 < p_2 < \ldots < p_r$ y números naturales $n_1, n_2, \ldots, n_r$ tales que

$$a = \prod_{i=1}^{r} p_i^{n_i}$$

Además, esta escritura es única, es decir, si $a = \prod_{i=1}^{s} q_i^{m_i}$ donde $q_1 < q_2 < \ldots < q_s$ son primos positivos y $m_1, m_2, \ldots, m_s \in \mathbb{N}$ entonces $r = s$, $q_i = p_i$ y $m_i = n_i$, $\forall\, i = 1, 2, \ldots, s$.

Demostración: Demostraremos que el teorema vale para todo $a \in \mathbb{N}$, $a \geq 2$, por inducción global en a.

Si $a = p$, con p primo, entonces basta tomar $r = 1$, $p_1 = p$ y $n_1 = 1$. Veamos que esta escritura es única: si $p = q_1^{m_1} q_2^{m_2} \ldots q_s^{m_s}$ donde $q_1 < q_2 < \ldots < q_s$ son primos positivos y $m_1, m_2, \ldots, m_s \in \mathbb{N}$ entonces $q_i \mid p$ para todo i. Como p es un primo positivo y $q_i > 1$ entonces debe ser $q_i = p$ para todo i. Pero como $q_1 < q_2 < \ldots < q_s$ esto implica que $s = 1$ y $q_1 = p$. Luego $p = p^{m_1}$ y por lo tanto debe ser $m_1 = 1$.

Luego, $s = 1$, $q_1 = p$ y $m_1 = 1$. Hemos probado entonces que el teorema es cierto si a es primo. En particular, el teorema es cierto para $a = 2$.

Paso inductivo: sea $a \in \mathbb{N}$, $a > 1$ y supongamos que el teorema es cierto para todo $b \in \mathbb{N}$ tal que $1 < b < a$ y veamos que entonces vale para a.
Como ya probamos que el teorema es cierto cuando a es primo, supongamos entonces que a no es primo.
Sea p el menor primo positivo que divide a a (el conjunto de todos los primos positivos que dividen a a es no vacío y por lo tanto posee un primer elemento). Entonces $\exists\, b \in \mathbb{Z}$ tal que $a = p.b$ y, como a no es primo, entonces $1 < b < a$. Luego, por hipótesis inductiva, existen únicos primos positivos $p_1 < p_2 < \ldots < p_r$ y números naturales $n_1, n_2, \ldots, n_r$ tales que $b = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$. Luego $a = p.b = p.p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$. Como p_1 es un primo positivo que divide a a y p es el menor primo positivo que divide a a entonces $p \leq p_1$. Luego, $p = p_1$ o $p < p_1$.

Primer caso: Si $p = p_1$, como $a = p.p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ entonces

$$a = p_1^{n_1+1} p_2^{n_2} \ldots p_r^{n_r}$$

donde $p_1 < p_2 < \ldots < p_r$ y $n_1 + 1, n_2, \ldots, n_r \in \mathbb{N}$. Veremos que esta escritura es única.
Antes notemos que en este caso $b = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} = p^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ de donde deducimos que $p \mid b$ pues $n_1 \geq 1$.
Supongamos que $a = q_1^{m_1} q_2^{m_2} \ldots q_s^{m_s}$ donde $q_1 < q_2 < \ldots < q_s$ son primos positivos y $m_1, m_2, \ldots, m_s \in \mathbb{N}$. Probaremos que $r = s$, $q_i = p_i$ $(1 \leq i \leq s)$, $m_1 = n_1 + 1$, $m_2 = n_2, \ldots, m_s = n_s$.
Como q_1 es un primo positivo, $q_1 \mid a$ y p es el menor primo positivo que divide a a entonces $p \leq q_1$. Además, como $p \mid a$ entonces $p \mid q_1^{m_1} q_2^{m_2} \ldots q_s^{m_s}$ y como p es primo entonces $p \mid q_j$ para algún j. Como p y q_j son primos positivos entonces $p = q_j$. Luego, $q_j = p \leq q_1 \leq q_j$ de donde resulta que $p = q_1$. Luego $p.b = a = p^{m_1} q_2^{m_2} \ldots q_s^{m_s} = p.p^{m_1-1} q_2^{m_2} \ldots q_s^{m_s}$ y por lo tanto $b = p^{m_1-1} q_2^{m_2} \ldots q_s^{m_s}$. Si fuese $m_1 = 1$ entonces $b = q_2^{m_2} \ldots q_s^{m_s}$ y como $p \mid b$ razonando como antes se tiene que $p = q_j$ para algún $j \geq 2$ lo que no puede ocurrir pues si $j \geq 2$ entonces $p = q_1 < q_j$. Por lo tanto debe ser $m_1 > 1$ de donde $m_1 - 1 \in \mathbb{N}$. Luego, como $p = q_1$,

$$b = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} \quad \text{y} \quad b = q_1^{m_1-1} q_2^{m_2} \ldots q_s^{m_s}$$

Por lo tanto, por la unicidad de la escritura de b, debe ser $r = s$, $q_i = p_i$ $(1 \leq i \leq s)$, $n_1 = m_1 - 1$ (es decir, $m_1 = n_1 + 1$), $m_2 = n_2, \ldots, m_s = n_s$.

Segundo caso: Si $p < p_1$ entonces

$$a = p.p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$$

donde $p < p_1 < p_2 < \ldots < p_r$ y $1, n_1, n_2, \ldots, n_r \in \mathbb{N}$. Veremos que esta escritura es única.

Notemos que en este caso $p \not| b$ (ejercicio).
Supongamos que $a = q_1^{m_1} q_2^{m_2} \dots q_s^{m_s}$ donde $q_1 < q_2 < \dots < q_s$ son primos positivos y $m_1, m_2, \dots, m_s \in \mathbb{N}$. Probaremos que $s = r + 1$, $q_1 = p$, $q_2 = p_1, \dots, q_s = p_r$, $m_1 = 1$, $m_2 = n_1, \dots, m_s = n_r$.
Razonando igual que en el caso anterior se ve que $p = q_1$. Luego

$$p.b = a = p^{m_1} q_2^{m_2} \dots q_s^{m_s} = p.p^{m_1 - 1} q_2^{m_2} \dots q_s^{m_s}$$

y por lo tanto $b = p^{m_1 - 1} q_2^{m_2} \dots q_s^{m_s}$.
Si fuese $m_1 > 1$ entonces $p \mid b$ lo que no ocurre en este caso. Por lo tanto, $m_1 = 1$ de donde

$$b = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r} \quad \text{y} \quad b = q_2^{m_2} \dots q_s^{m_s}$$

Por lo tanto, por la unicidad de la escritura de b, debe ser $r = s - 1$ (es decir, $s = r + 1$), $q_2 = p_1, \dots, q_s = p_r$, $m_2 = n_1, \dots, m_s = n_r$ y como ya vimos que $q_1 = p$ y $m_1 = 1$ esto prueba que la escritura de a es única. □

Corolario. Sea $a \in \mathbb{Z}$, $a \neq 0, 1, -1$. Entonces existen primos positivos $p_1 < p_2 < \dots < p_r$, números naturales $n_1, n_2, \dots, n_r$ y $\delta \in \{1, -1\}$ tales que

$$a = \delta \prod_{i=1}^{r} p_i^{n_i}$$

Además, esta escritura es única, es decir, si $a = \delta' \prod_{i=1}^{s} q_i^{m_i}$ donde $q_1 < q_2 < \dots < q_s$ son primos positivos, $m_1, m_2, \dots, m_s \in \mathbb{N}$ y $\delta' \in \{1, -1\}$ entonces $\delta = \delta'$, $r = s$, $q_i = p_i$ y $m_i = n_i$, $\forall\, i = 1, 2, \dots, s$.

Ejemplos.

1) $1536 = 2^9.3$

2) ¿Cuántos divisores positivos tiene $2^{15}.5^4.11^{33}$?
a es un divisor positivo de $2^{15}.5^4.11^{33}$ si y sólo si la factorización de a es de la forma $a = 2^n.5^m.11^r$, donde $0 \leq n \leq 15, 0 \leq m \leq 4$ y $0 \leq r \leq 33$. Luego, n puede tomar 16 valores, para cada uno de ellos m puede tomar 5 valores y r puede tomar 34. Luego la cantidad de divisores positivos es 16.5.34

3) ¿Cuál es la suma de los divisores positivos de $3^{11}.7^{27}$?
Debemos sumar los números de la forma $3^i.7^j$ para $0 \leq i \leq 11, 0 \leq j \leq 27$. Luego, la suma de los divisores positivos de $3^{11}.7^{27}$ es

$$\sum_{i=0}^{11} \sum_{j=0}^{27} 3^i.7^j = \sum_{i=0}^{11} 3^i . \sum_{j=0}^{27} 7^j = \frac{3^{12} - 1}{3 - 1} \frac{7^{28} - 1}{7 - 1}$$

4) Factoricemos 22!

$$22! = 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16.17.18.19.20.21.22$$

Los primos que aparecen en la factorización de 22! son los primos menores que 22, es decir, $2, 3, 5, 7, 11, 13, 17$ y 19. Veamos a qué potencia aparece cada uno de ellos en la factorización.
Al multiplicar los números naturales menores o iguales que 22 se tiene que cada dos números hay un múltiplo de 2, pero cada 4 números hay otro factor 2, cada 8 hay otro y cada 16 otro. Luego hay $11 + 5 + 2 + 1 = 19$ factores 2.
Análogamente hay $7 + 2 = 9$ factores 3, 4 factores 5, 3 factores 7, 2 factores 11, y uno solo de cada uno de los restantes primos. Luego, la factorización de 22! es

$$22! = 2^{19}.3^9.5^4.7^3.11^2.13.17.19$$

5) Hallar todos los $a, b \in \mathbb{N}$ tales que $(a : b) = 35$ y $[a : b] = 3.5^2.7^3$
Como $a.b = (a : b).[a : b] = 35.3.5^2.7^3 = 3.5^3.7^4$. Luego los únicos primos que pueden aparecer en la factorización de a y b son $3, 5$ y 7. Además, como $(a : b) = 35$ entonces $35 \mid a$ y $35 \mid b$ de donde 5 y 7 necesariamente aparecen en la factorización de ambos. Por lo tanto $a = 3^r.5^n.7^s$ y $b = 3^t.5^m.7^k$ con $n, s, m, k \geq 1$ y como $3.5^3.7^4 = a.b = 3^{r+t}.5^{n+m}.7^{s+k}$, por la unicidad de la factorización debe ser $r + t = 1$, $n + m = 3$ y $s + k = 4$.
Entonces $r = 1$ y $t = 0$ o $r = 0$ y $t = 1$, $n = 2$ y $m = 1$ o $n = 1$ y $m = 2$ y $s = 3$, $k = 1$ o $s = 2 = k$ o $s = 1$, $k = 3$. Pero notemos que si $s = 2 = k$ entonces $7^2 \mid a$ y $7^2 \mid b$ de donde $7^2 \mid (a : b) = 35$. Luego no puede ser que $s = 2 = k$. Por lo tanto los posibles $a, b \in \mathbb{N}$ que satisfacen lo pedido son

$$a = 3.5^2.7^3 \text{ y } b = 5.7 \qquad a = 5^2.7^3 \text{ y } b = 3.5.7$$
$$a = 3.5^2.7 \text{ y } b = 5.7^3 \qquad a = 5^2.7 \text{ y } b = 3.5.7^3$$
$$a = 3.5.7^3 \text{ y } b = 5^2.7 \qquad a = 5.7^3 \text{ y } b = 3.5^2.7$$
$$a = 3.5.7 \text{ y } b = 5^2.7^3 \qquad a = 5.7 \text{ y } b = 3.5^2.7^3$$

Ejercicio. Probar que si tenemos la factorización de a y b como producto de primos entonces $(a : b)$ es el producto de los primos comunes con el menor exponente y $[a : b]$ es el producto de los primos comunes y no comunes con el mayor exponente.

10. Números racionales. Consideremos el conjunto de los números racionales,

$$\mathbb{Q} = \left\{ \frac{a}{b} \,/\, a \in \mathbb{Z} \text{ y } b \in \mathbb{N} \right\}$$

Dejamos como ejercicio verificar que $\mathbb{Q}$ es cerrado para la suma, la resta, la multiplicación y la división. Pitágoras pensaba que todos los números eran racionales hasta que uno de

sus discípulos descubrió que $\sqrt{2}$ (lo que mide la hipotenusa de un triángulo rectángulo cuyos catetos miden 1) no es racional. Probemos esto:
Supongamos que $\sqrt{2} \in \mathbb{Q}$. Entonces existen $a \in \mathbb{Z}$ y $b \in \mathbb{N}$ tales que $\sqrt{2} = \frac{a}{b}$. Elevando al cuadrado y pasando de miembro al denominador se tiene que $2b^2 = a^2$. Luego $2 \mid a^2$ y por lo tanto $2 \mid a$. Pero entonces $4 \mid a^2$ y por lo tanto $2 \mid b^2$ con lo cual $2 \mid b$. Hemos probado entonces que el primo 2 aparece en la factorización de a y de b. Si en la factorización de a el primo 2 aparece a la potencia n y en la de b a la m entonces en la factorización de a^2 aparece a la potencia $2n$ y en $2b^2$ aparece a la potencia $2m+1$. Entonces, por la unicidad de la factorización de $2b^2 = a^2$ debe ser $2n = 2m+1$ lo cual es absurdo. Por lo tanto $\sqrt{2}$ no puede ser racional.

Ejercicio. Probar que $\sqrt[3]{2} \notin \mathbb{Q}$. En general, si $n \in \mathbb{N}$, $n \geq 2$, y p es un primo positivo entonces $\sqrt[n]{p} \notin \mathbb{Q}$.

Dado $a \in \mathbb{R}$ diremos que a es *irracional* si $a \notin \mathbb{Q}$. En realidad, Pitágoras estaba bastante errado: hay muchos más números irracionales que números racionales.

11. Pequeño teorema de Fermat.

En el año 1640 Pierre de Fermat descubrió que si p es un primo positivo y a es un entero entonces $a^p \equiv a\ (p)$ o, equivalentemente, si a es un entero no divisible por p entonces $a^{p-1} \equiv 1\ (p)$. Este teorema, conocido como el pequeño teorema de Fermat, fue utilizado por Rivest, Shamir y Adleman muchos años más tarde, en 1978, para crear uno de los sistemas criptográficos de clave pública más populares, el RSA, cuyo nombre lleva las iniciales de sus creadores.

Para demostrar el teorema de Fermat necesitaremos antes probar el siguiente resultado

Lema. Sea p un primo positivo y sea $a \in \mathbb{Z}$ tal que $p \not| a$. Entonces

$$\{r_p(a), r_p(2a), r_p(3a), \ldots, r_p((p-1)a)\} = \{1, 2, 3, \ldots, p-1\}$$

Demostración: $\subseteq$: queremos ver que para todo k tal que $1 \leq k \leq p-1$ el resto de la división de ka por p pertenece al conjunto $\{1, 2, 3, \ldots, p-1\}$. Como el resto de la división por p siempre es mayor o igual que cero y menor o igual que $p-1$ entonces sólo debemos probar que si $1 \leq k \leq p-1$ entonces $r_p(ka) \neq 0$. Supongamos que no, entonces $p \mid ka$ y como p es primo entonces $p \mid k$ o $p \mid a$. Pero ninguna de estas dos cosas puede ocurrir ya que $1 \leq k \leq p-1$ y por hipótesis a no es divisible por p.
$\supseteq$: Sea $b \in \{1, 2, 3, \ldots, p-1\}$. Queremos ver $b = r_p(ka)$ para algún k tal que $1 \leq k \leq p-1$. Como $p \not| a$ entonces $(a : p) = 1$. Luego, la ecuación lineal de congruencia $ax \equiv b\ (p)$ tiene una solución k tal que $0 \leq k \leq p-1$. Luego $ak \equiv b\ (p)$. Además, $k \neq 0$ pues b no es divisible por p. Por lo tanto, $1 \leq k \leq p-1$ y como $ak \equiv b\ (p)$ y $1 \leq b \leq p-1$ entonces $r_p(ka) = b$. □

Teorema. (Pequeño teorema de Fermat) Sea p un primo positivo y sea $a \in \mathbb{Z}$. Si $p \not| a$ entonces $a^{p-1} \equiv 1\ (p)$ (es decir, $p \mid a^{p-1} - 1$).

Demostración: Por el lema, se tiene que

$$1.2.3\ldots(p-1) \equiv r_p(a).r_p(2a).r_p(3a).\ldots.r_p((p-1)a) \equiv a.2a.3a\ldots(p-1)a\ \ (p)$$

Luego, $(p-1)! \equiv (p-1)!\, a^{p-1}\ (p)$ y como $(p-1)!$ y p son coprimos esto implica que $1 \equiv a^{p-1}\ (p)$. □

Corolario. Sea p un primo positivo y sea $a \in \mathbb{Z}$. Entonces $a^p \equiv a\ (p)$.

Ejemplos.

1) Hallar $r_{13}(7^{45206})$
Como 13 es primo y $13 \not| 7$ entonces, por el teorema de Fermat, $7^{12} \equiv 1\ (13)$. Luego, como $45206 = 12q + 2$, se tiene que

$$7^{45206} = 7^{12q+2} = \left(7^{12}\right)^q .7^2 \equiv 7^2 = 49 \equiv 10\ \ (13)$$

2) Hallar todos los $n \in \mathbb{N}$ tales que $5^n \equiv 3\ (11)$
Como 11 es primo y $11 \not| 5$ entonces, por el teorema de Fermat, $5^{10} \equiv 1\ (11)$. Sea r el resto de la división de n por 10. Entonces $n = 10q + r$, con $0 \leq r < 10$, de donde resulta que $5^n \equiv 5^r\ (11)$. Veamos entonces para cuáles valores de r se verifica lo pedido:
Si $r = 0$ entonces $5^r \equiv 1\ (11)$, si $r = 1$ entonces $5^r \equiv 5\ (11)$, si $r = 2$ entonces $5^r \equiv 3\ (11)$, si $r = 3$ entonces $5^r \equiv 4\ (11)$, si $r = 4$ entonces $5^r \equiv 9\ (11)$, si $r = 5$ entonces $5^r \equiv 1\ (11)$, si $r = 6$ entonces $5^r \equiv 5\ (11)$, si $r = 7$ entonces $5^r \equiv 3\ (11)$, si $r = 8$ entonces $5^r \equiv 4\ (11)$ y si $r = 9$ entonces $5^r \equiv 9\ (11)$. Luego, los n que satisfacen lo pedido son los de la forma $n = 10q + 2$ o $n = 10q + 7$.

3) Hallar todos los $x \in \mathbb{Z}$ tales que $12^{38}\, x \equiv -5\ (41)$
Como 41 es primo y no divide a 12 entonces $12^{40} \equiv 1\ (41)$. Además, como $(41 : 12^2) = 1$,

$$12^{38}\, x \equiv -5\ (41) \Longleftrightarrow 12^2 12^{38}\, x \equiv 12^2(-5)\ (41) \Longleftrightarrow 12^{40}\, x \equiv 12^2(-5)\ (41)$$

y como $12^2 = 144 \equiv -20\ (41)$ y $12^{40} \equiv 1\ (41)$ entonces

$$12^{38}\, x \equiv -5\ (41) \Longleftrightarrow x \equiv (-20)(-5) = 100 \equiv 18\ (41)$$

4) Veamos que $(2^n + 7^{n+1} : 2^{n+1} + 7^n) = 1$ para todo $n \in \mathbb{N}$. Habíamos visto antes que $(2^n + 7^{n+1} : 2^{n+1} + 7^n) = 1$ o 13, por lo tanto basta ver que $13 \not| 2^{n+1} + 7^n$.
Sea r el resto de la división de n por 12. Entonces $n = 12q + r$, con $0 \leq r < 12$. Como 13 es primo y no divide a 2 ni a 7 entonces, por el teorema de Fermat, $2^{12} \equiv 1\ (13)$ y $7^{12} \equiv 1\ (13)$. Luego $2^{n+1} + 7^n \equiv 2^{r+1} + 7^r\ (13)$. Dejamos como ejercicio verificar que

si $0 \leq r \leq 11$ entonces $2^{r+1} + 7^r$ no es conguente a cero módulo 13, lo que prueba que $13 \not| 2^{n+1} + 7^n$.

5) Hallar el resto de la división de $3^{5^{1001}}$ por 7.
Como 7 es primo y no divide a 3, entonces $3^6 \equiv 1\ (7)$. Luego, si $n = 6q + r$, se tiene que $3^n \equiv 3^r\ (7)$. Por lo tanto, para hallar el resto de la división de $3^{5^{1001}}$ por 7 nos basta calcular el resto de la división de $n = 5^{1001}$ por 6.
Como $5 \equiv -1\ (6)$ entonces $5^{1001} \equiv -1 \equiv 5\ (6)$. Por lo tanto, $5^{1001} = 6q + 5$ de donde

$$3^{5^{1001}} = 3^{6q+5} = (3^6)^q.3^5 \equiv 3^5 = 9.9.3 \equiv 2.2.3 = 12 \equiv 5\ \ (7)$$

12. Teorema chino del resto.

Antes vimos cómo resolver una ecuación lineal de congruencia. Ahora veremos cómo resolver un sistema de ecuaciones lineales de congruencia. Por ejemplo, supongamos que queremos hallar todos los $x \in \mathbb{Z}$ que satisfacen simultáneamente

$$\begin{cases} 2x \equiv -7\ (35) \\ 5x \equiv -1\ (26) \end{cases}$$

Como

$$2x \equiv -7\ (35) \Longleftrightarrow 2x \equiv 28\ (35) \Longleftrightarrow x \equiv 14\ (35)$$

pues $(2 : 35) = 1$, y como

$$5x \equiv -1\ (26) \Longleftrightarrow 5x \equiv 25\ (26) \Longleftrightarrow x \equiv 5\ (26)$$

pues $(5 : 26) = 1$, entonces el sistema que queremos resolver es equivalente a

$$\begin{cases} x \equiv 14\ (35) \\ x \equiv 5\ \ (26) \end{cases}$$

Luego, $x \in \mathbb{Z}$ es una solución del sistema si y sólo si $x = 35k + 14$ y $35k + 14 \equiv 5\ (26)$ si y sólo si $x = 35k + 14$ y $35k \equiv -9\ (26)$. Notemos que existe un k tal que $35k \equiv -9\ (26)$ pues $(35 : 26) = 1$. Como

$$35k \equiv -9\ (26) \Longleftrightarrow 9k \equiv -9\ (26) \Longleftrightarrow k \equiv -1\ (26)$$

pues $(9 : 26) = 1$ entonces $35k \equiv -9\ (26) \Longleftrightarrow k = 26q - 1\ (q \in \mathbb{Z})$.
Por lo tanto, $x \in \mathbb{Z}$ es una solución del sistema si y sólo si $x = 35k + 14$ y $k = 26q - 1$ para algún $q \in \mathbb{Z}$, es decir, si y sólo si $x = 35(26q - 1) + 14 = 35.26.q - 35 + 14 = 35.26.q - 21$.
Observemos que el hecho de que $(35 : 26) = 1$ garantiza que haya solución. Los próximos dos ejemplos muestran que cuando los módulos no son coprimos entonces puede haber o no solución.

Supongamos ahora que queremos resolver el sistema

$$\begin{cases} 7x \equiv 1\ (30) \\ 5x \equiv 31\ (84) \end{cases}$$

Dejamos como ejercicio probar que el sistema dado es equivalente a

$$\begin{cases} x \equiv 13\ (30) \\ x \equiv 23\ (84) \end{cases}$$

Entonces $x \in \mathbb{Z}$ es solución si y sólo si $x = 30k + 13$ y $30k + 13 \equiv 23\ (84)$ si y sólo si $x = 30k + 13$ y $30k \equiv 10\ (84)$. Pero ahora no existe k que satisfaga la ecuación de congruencia pues $(30 : 84) = 6$ y $6 \not| 10$. Luego, en este caso el sistema dado no tiene solución. En este ejemplo $(30 : 84) \neq 1$ y no hay solución.

Finalmente, veamos un ejemplo donde los módulos no son coprimos pero el sistema admite solución:

$$\begin{cases} 3x \equiv 13\ (14) \\ 7x \equiv -13\ (20) \end{cases}$$

Dejamos como ejercicio probar que el sistema dado es equivalente a

$$\begin{cases} x \equiv 9\ (14) \\ x \equiv 1\ (20) \end{cases}$$

Por lo tanto, $x \in \mathbb{Z}$ es una solución del sistema si y sólo si $x = 14k + 9$ y $14k + 9 \equiv 1\ (20)$ si y sólo si $x = 14k + 9$ y $14k \equiv -8\ (20)$.
En este caso existe un k que satisface la ecuación de congruencia pues $(14 : 20) = 2$ y $2 \mid -8$. Luego el sistema tiene solución. Dejamos como ejercicio ver que todas las soluciones son $x = 10.14.q - 19$.

En general, un sistema de dos ecuciones lineales de congruencia siempre es equivalente a uno de la forma

$$\begin{cases} x \equiv a_1\ (m_1) \\ x \equiv a_2\ (m_2) \end{cases}$$

Además, si $(m_1 : m_2) = 1$ entonces existe solución y en otro caso puede ser que exista o puede ser que no exista solución.

Supongamos ahora que queremos resolver el sistema

$$\begin{cases} 3x \equiv\ 13\ (14) \\ 7x \equiv -13\ (20) \\ 2x \equiv\ 1\ (11) \end{cases}$$

que es equivalente a

$$\begin{cases} x \equiv 9\ (14) \\ x \equiv 1\ (20) \\ x \equiv 6\ (11) \end{cases}$$

Como x es solución de las primeras dos ecuaciones si y sólo si $x = 10.14.q - 19$ si y sólo si $x \equiv -19\ (140)$ entonces

$$\begin{cases} x \equiv 9\ (14) \\ x \equiv 1\ (20) \\ x \equiv 6\ (11) \end{cases} \iff \begin{cases} x \equiv -19\ (140) \\ x \equiv 6\ (11) \end{cases}$$

Esto muestra que cualquier sistema de ecuaciones lineales de congruencia es equivalente a un sistema de dos ecuaciones.
Volvamos a mirar los dos ejemplos anteriores en que los módulos no eran coprimos. Vimos antes que el primero,

$$\begin{cases} x \equiv 13\ (30) \\ x \equiv 23\ (84) \end{cases}$$

no tiene solución. Veamos el sistema en más detalle: como

$$x \equiv 13\ (30) \iff \begin{cases} x \equiv 13\ (2) \\ x \equiv 13\ (3) \\ x \equiv 13\ (5) \end{cases}$$

y

$$x \equiv 23\ (84) \iff \begin{cases} x \equiv 23\ (3) \\ x \equiv 23\ (4) \\ x \equiv 23\ (7) \end{cases}$$

$$\begin{cases} x \equiv 13\ (30) \\ x \equiv 23\ (84) \end{cases} \iff \begin{cases} x \equiv 13\ (2) \\ x \equiv 13\ (3) \\ x \equiv 13\ (5) \\ x \equiv 23\ (3) \\ x \equiv 23\ (4) \\ x \equiv 23\ (7) \end{cases} \iff \begin{cases} x \equiv 1\ (2) \\ x \equiv 1\ (3) \\ x \equiv 3\ (5) \\ x \equiv 2\ (3) \\ x \equiv 3\ (4) \\ x \equiv 2\ (7) \end{cases}$$

Notamos entonces que claramente no puede tener solución pues una solución debería satisfacer $x \equiv 1\ (3)$ y $x \equiv 2\ (3)$.
Ahora veamos el segundo,

$$\begin{cases} x \equiv 9\ (14) \\ x \equiv 1\ (20) \end{cases}$$

que es equivalente a

$$\begin{cases} x \equiv 9\ (2) \\ x \equiv 9\ (7) \\ x \equiv 1\ (4) \\ x \equiv 1\ (5) \end{cases} \iff \begin{cases} x \equiv 1\ (2) \\ x \equiv 2\ (7) \\ x \equiv 1\ (4) \\ x \equiv 1\ (5) \end{cases} \iff \begin{cases} x \equiv 2\ (7) \\ x \equiv 1\ (4) \\ x \equiv 1\ (5) \end{cases}$$

ya que si $x \equiv 1\ (4)$ entonces necesariamente vale $x \equiv 1\ (2)$.

Notemos que este último sistema tiene solución pues como 7 y 4 son coprimos podemos hallar x_0 tal que

$$\begin{cases} x \equiv 2\ (7) \\ x \equiv 1\ (4) \end{cases} \iff x \equiv x_0\ (28)$$

y como 28 y 5 son coprimos entonces podemos resolver el sistema equivalente al dado que es

$$\begin{cases} x \equiv x_0\ (28) \\ x \equiv 1\ (5) \end{cases}$$

Teorema chino del resto. Sean $a_1, a_2, \ldots a_k \in \mathbb{Z}$ y sean $m_1, m_2, \ldots, m_k \in \mathbb{N}$ tales que $(m_i : m_j) = 1$ para todo $i \neq j$. Si $m = m_1.m_2 \ldots m_k$ entonces el sistema

$$\begin{cases} x \equiv a_1\ (m_1) \\ x \equiv a_2\ (m_2) \\ \quad \vdots \quad \vdots \quad \vdots \\ x \equiv a_k\ (m_k) \end{cases}$$

tiene una única solución x_0 tal que $0 \leq x_0 \leq m$. Además, $x \in \mathbb{Z}$ es solución del sistema si y sólo si $x \equiv x_0\ (m)$

Demostración: Para cada i $(1 \leq i \leq k)$ sea $M_i = \frac{m}{m_i}$, es decir, M_i es el producto de todos los m_j salvo el m_i. Luego $m_i \mid M_j$ para todo $i \neq j$. Además, como $(m_i : m_j) = 1$ si $i \neq j$ entonces $(M_i : m_i) = 1$ para todo i. En efecto, si existiera un primo p tal que $p \mid M_i$ y $p \mid m_i$ entonces $p \mid m_j$ para algún $j \neq i$ y $p \mid m_i$, por lo tanto $p \mid (m_i : m_j) = 1$.
Para cada i sea $x_i \in \mathbb{Z}$ una solución de $M_i\ x \equiv a_i\ (m_i)$ (que existe pues M_i y m_i son coprimos), es decir, x_i satisface $M_i x_i \equiv a_i\ (m_i)$, y sea $a = M_1x_1 + M_2x_2 + \cdots + M_kx_k$.
Como $m_i \mid M_j$ si $i \neq j$ entonces $M_j \equiv 0\ (m_i)$ para todo $i \neq j$. Luego

$$a = M_1x_1 + M_2x_2 + \cdots + M_ix_i + \cdots + M_kx_k \equiv M_ix_i \equiv a_i\ \ (m_i)$$

para todo i.

Sea x_0 el resto de la división de a por m. Entonces $0 \leq x_0 < m$ y como $x_0 \equiv a\ (m)$ y $m_i \mid m$ resulta que $x_0 \equiv a\ (m_i)$ para todo i y como $a \equiv a_i\ (m_i)$ resulta que

$$x_0 \equiv a_i\ (m_i)$$

para todo i, es decir, es solución del sistema.

Veamos ahora que $x \in \mathbb{Z}$ es solución del sistema si y sólo si $x \equiv x_0\ (m)$:
Si x es solución del sistema entonces $x \equiv x_0\ (m_i)\ \forall\, i$ pues $x \equiv a_i\ (m_i)$ y $x_0 \equiv a_i\ (m_i)$. Luego, como $(m_i : m_j) = 1$ si $i \neq j$ entonces $x \equiv x_0\ (m_1.m_2 \ldots m_k)$, es decir, $x \equiv x_0\ (m)$.
Recíprocamente, si $x \equiv x_0\ (m)$ entonces, para todo i, $x \equiv x_0\ (m_i)$ pues $m_i \mid m$ y como $x_0 \equiv a_i\ (m_i)$ entonces $x \equiv a_i\ (m_i)$. Luego x es solución del sistema.

Luego todas las soluciones son $x = x_0 + mq$ con $q \in \mathbb{Z}$ y por lo tanto la única solución mayor o igual que cero y menor que m es x_0. □

Ejemplos.

1) Resolvamos el sistema

$$\begin{cases} x \equiv 1\ (4) \\ x \equiv 2\ (7) \\ x \equiv 4\ (15) \end{cases}$$

En este caso $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $m_1 = 4$, $m_2 = 7$ y $m_3 = 15$. Luego $m = 4.7.15$, $M_1 = 7.15 = 105$, $M_2 = 4.15 = 60$ y $M_3 = 4.7 = 28$. Ahora hallamos, para $i = 1, 2, 3$, una solución x_i de $M_i\, x \equiv a_i\ (m_i)$. Para hallar x_1 resolvemos $M_1\, x \equiv a_1\ (m_1)$, es decir, hallamos una solución de $105\, x \equiv 1\ (4)$. Como $105 \equiv 1\ (4)$ entonces

$$105\, x \equiv 1\ (4) \Longleftrightarrow x \equiv 1\ (4)$$

por lo tanto podemos tomar $x_1 = 1$.
Para hallar x_2 resolvemos $M_2\, x \equiv a_2\ (m_2)$, es decir, hallamos una solución de $60\, x \equiv 2\ (7)$. Como $60 \equiv 4\ (7)$ entonces

$$60\, x \equiv 2\ (7) \Longleftrightarrow 4x \equiv 2\ (7)$$

por lo tanto podemos tomar $x_2 = 4$.
Para hallar x_3 resolvemos $M_3\, x \equiv a_3\ (m_3)$, es decir, hallamos una solución de $28\, x \equiv 4\ (15)$. Como $28 \equiv -2\ (15)$ y $(-2 : 15) = 1$ entonces

$$28\, x \equiv 4\ (15) \Longleftrightarrow (-2)x \equiv (-2)(-2)\ (15) \Longleftrightarrow x \equiv -2\ (15)$$

por lo tanto podemos tomar $x_3 = -2$. Luego

$$a = M_1x_1 + M_2x_2 + M_3x_3 = 105.1 + 60.4 + 28(-2) = 105 + 240 - 56 = 289$$

y por lo tanto $x_0 = r_m(a) = r_{420}(289) = 289$ y todas las soluciones del sistema son $x = 289 + 420q$, con $q \in \mathbb{Z}$.

2) Resolvamos el sistema

$$\begin{cases} x \equiv 2\ (12) \\ x \equiv 4\ (35) \end{cases}$$

En este caso $m = 12.35 = 420$. Luego, el teorema garantiza que el sistema tiene una única solución x_0 tal que $0 \leq x_0 < 420$ y que todas las soluciones son $x = x_0 + 420q$ con $q \in \mathbb{Z}$. Si $x \in \mathbb{N}$ satisface la primera ecuación entonces $x = 2 + 12h$ con $h \in \mathbb{N}_0$, es decir,

$$x = 2, 14, 26, 38, 50, 62, 74, 86.98, \ldots$$

Si $x \in \mathbb{N}$ satisface la segunda ecuación entonces $x = 4 + 35k$ con $k \in \mathbb{N}_0$, es decir,

$$x = 4, 39, 74, 109, 144, \ldots$$

Luego, $x = 74$ satisface ambas ecuaciones, es decir, es solución del sistema y como además $0 \leq 74 < 420$ entonces debe ser $x_0 = 74$. Luego, todas las soluciones son $x = 74 + 420q$ con $q \in \mathbb{Z}$.

3) Hallar $r_{28}(5^{64} + 3^{45})$.

Sea $a = 5^{64} + 3^{45}$. Queremos hallar r tal que $r \equiv a\ (28)$ y $0 \leq r < 28$. Como $28 = 4.7$ y $(4 : 7) = 1$ entonces

$$r \equiv a\ (28) \Longleftrightarrow \begin{cases} r \equiv a\ (4) \\ r \equiv a\ (7) \end{cases}$$

Notemos que $a = 5^{64} + 3^{45} \equiv 1^{64} + (-1)^{45} = 0\ (4)$. Además, por el teorema de Fermat, $5^6 \equiv 1\ (7)$ y $3^6 \equiv 1\ (7)$ por lo tanto $a = 5^{64} + 3^{45} \equiv 5^4 + 3^3 \equiv 2 - 1 = 1\ (7)$.

Por lo tanto buscamos r tal que $0 \leq r < 28$ y

$$\begin{cases} r \equiv 0\ (4) \\ r \equiv 1\ (7) \end{cases}$$

Luego, el resto buscado es la única solución mayor o igual que 0 y menor que $m = 4.7 = 28$ del sistema

$$\begin{cases} x \equiv 0\ (4) \\ x \equiv 1\ (7) \end{cases}$$

que es $r = 8$.

Observemos que conociendo el resto de la división de a por 4 y por 7 hemos calculado el resto de la división de a por $28 = 4.7$.

En general, si $m_1, m_2, \ldots, m_k$ son coprimos de a dos, el teorema chino del resto nos permite calcular el resto de la división de a por $m = m_1.m_2 \ldots m_k$ conociendo el resto de la división de a por $m_1, m_2, \ldots, m_k$.

Ejercicio. Hallar $r_{36}(a)$ sabiendo que $r_9(2a) = 7$ y $r_8(5a) = 6$.