Capítulo 5

Enteros – Segunda parte.

5.1 Ecuaciones lineales diofánticas.

Vamos a aplicar ahora la teoría del máximo común divisor que vimos a la resolución de ciertas ecuaciones en enteros, que se llaman *Ecuaciones lineales diofánticas*. Las ecuaciones diofánticas son las ecuaciones con coeficientes enteros de las cuales se buscan las soluciones enteras.

El nombre se puso por *Diofanto de Alejandría*, $\sim$200–284, quién fue quién desarrolló ese tipo de ecuaciones en su obra *La Aritmética*.

Las ecuaciones diofánticas más sencillas son las ecuaciones lineales de la forma $a \cdot X + b \cdot Y = c$ con $a, b, c \in \mathbb{Z}$, donde a y b no son ambos nulos, de las cuales se buscan los pares de soluciones *enteras*. Observemos que una ecuación de este tipo es la ecuación de una recta en $\mathbb{R}^2$, que sabemos resolver en $\mathbb{R}^2$, y que nos estamos preguntando por qué puntos de coordenadas ambas enteras pasa esa recta.

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

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

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

Como primer paso queremos decidir si existe al menos una solución entera $(x_0, y_0) \in \mathbb{Z}^2$.

Observación 5.1.1. Si $a = 0$ o $b = 0$ (pongamos $b = 0$), el problema se vuelve un problema de divisibilidad: $a \cdot X + 0 \cdot Y = c$ tiene solución entera si y solo si $a \mid c$, y en ese caso las soluciones son todos los pares $(c/a, j)$, $j \in \mathbb{Z}$. Luego en lo que sigue podemos suponer que a y b son ambos no nulos.

Ejemplos:

- $5\,X + 9\,Y = 1$ tiene por ejemplo como solución entera $x_0 = 2\,,\ y_0 = -1\,.$
- $5\,X + 9\,Y = 10$ tiene como solución entera $x_0 = 2\,,\ y_0 = 0$ pero también tiene como solución entera, usando el ejemplo anterior, $x_0 = 10 \cdot 2 = 20\,,\ y_0 = -1 \cdot 10 = -10\,.$
- $4\,X + 6\,Y = 7$ no tiene solución entera porque el resultado de lo de la izquierda es claramente siempre par. De hecho recordamos que si un número se escribe como combinación entera de a y b, entonces tiene que ser un múltiplo de $(a : b)\,.$
- $4\,X + 6\,Y = 2$ tiene solución ya que $2 = (4 : 6)$ y sabemos que el mcd es combinación entera de los números. Se puede elegir aquí $x_0 = -1,\ y_0 = 1\,.$
- $18\,X - 12\,Y = 2$ no tiene solución entera pues $(18 : 12) = 6$ y $6 \nmid 2\,.$
- $18\,X - 12\,Y = 60$ tiene solución pues $(18 : 12) \mid 60$: 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 $x_0 = 10,\ y_0 = 10\,.$

Deducimos la siguiente afirmación:

Proposición 5.1.2. (Ecuación diofántica y máximo común divisor.)

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

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

admite soluciones enteras si y solo si $(a : b) \mid c\,.$ Es decir:

$$\exists\ (x_0, y_0) \in \mathbb{Z}^2 :\ a\,x_0 + b\,y_0 = c \iff (a : b) \mid c.$$

Demostración.

- $(\Rightarrow)$ Sea $(x_0, y_0) \in \mathbb{Z}^2$ una solución entera, entonces, como siempre, dado que $(a : b) \mid a$ y $(a : b) \mid b\,,$ se concluye que $(a : b) \mid a\,x_0 + b\,y_0 = c\,,$ es decir, $(a : b) \mid c\,.$
- $(\Leftarrow)$ Sabemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s\,a + t\,b\,.$ Luego, dado que $(a : b) \mid c\,,$ existe $k \in \mathbb{Z}$ tal que $c = k\,(a : b)\,,$ y por lo tanto se tiene que $c = a\,(k\,s) + b\,(k\,t)\,.$ Podemos tomar $x_0 := k\,s,\ y_0 := k\,t\,.$

□

Como $1 \mid c\,,\ \forall\, c \in \mathbb{Z}\,,$ se obtiene inmediatamente el corolario siguiente.

Corolario 5.1.3. (Ecuación diofántica con a y b coprimos.)

Sean $a, b \in \mathbb{Z}$ *no nulos y* coprimos. *Entonces la ecuación diofántica*

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

tiene soluciones enteras, para todo $c \in \mathbb{Z}$.

La Proposición 5.1.2 da además una forma de conseguir una solución (x_0, y_0) particular (si existe): cuando no se consigue a ojo o fácilmente, 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"*, como veremos en lo que sigue.

Antes introducimos la definición-notación siguiente que adoptamos en estas notas:

Definición-Notación 5.1.4. (Ecuaciones diofánticas equivalentes.)

Sean $a \cdot X + b \cdot Y = c$ y $a' \cdot X + b' \cdot Y = c'$ dos ecuaciones diofánticas. Decimos que son *equivalentes* si tienen exactamente las mismas soluciones $(x, y) \in \mathbb{Z}^2$. En ese caso adoptamos la notación

$$a \cdot X + b \cdot Y = c \;\leftrightsquigarrow\; a' \cdot X + b' \cdot Y = c'.$$

Observación 5.1.5. (Ecuación diofántica y ecuación "coprimizada".)

Sean $a, b, c \in \mathbb{Z}$ con a, b no nulos tales que $(a : b) \mid c$.
Definamos $a' = \dfrac{a}{(a : b)}$, $b' = \dfrac{b}{(a : b)}$ y $c' = \dfrac{c}{(a : b)}$. Entonces,

$$a \cdot X + b \cdot Y = c \;\leftrightsquigarrow\; a' \cdot X + b' \cdot Y = c'.$$

Demostración. Cuando $(a : b) \mid c$, es claro que $\forall\,(x, y) \in \mathbb{Z}^2$, $ax + by = c \Leftrightarrow a'x + b'y = c'$. Luego las dos ecuaciones tiene exactamente las mismas soluciones. □

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 encontrar todas las soluciones enteras de una ecuación diofántica que admite al menos una solución entera.

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

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

que siempre tiene solución pues $(a : b) \mid 0$ independientemente de quién es $(a : b)$. Miramos primero un ejemplo.

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

La solución más simple es $x_0 = 0, y_0 = 0$. O también se tiene $x_1 = 27, y_1 = -18$. Así que la solución no es única. También por ejemplo $x_2 = -27, y_2 = 18$ o $x_3 = 3, y_3 = -2$ sirven. Vamos a probar que son infinitas. ¿ Cómo se consiguen todas ?

Por lo mencionado arriba, la ecuación original es equivalente a la ecuación "coprimizada":

$$18\,X + 27\,Y = 0 \quad \leftrightsquigarrow \quad 2\,X + 3\,Y = 0.$$

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

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

Volviendo al primer renglón, resulta:

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

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

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

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

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

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

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

Este procedimiento se puede generalizar sin problemas:

Proposición 5.1.6. (La ecuación diofántica $a \cdot X + b \cdot Y = 0$.)

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

El conjunto $\mathcal{S}_0$ de soluciones enteras de la ecuación diofántica $a \cdot X + b \cdot Y = 0$ es

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

Demostración. Se tiene

$$a\,X + b\,Y = 0 \quad \leftrightsquigarrow \quad a'X + b'Y = 0,$$

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

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

$$\begin{aligned} a'\,x + b'\,y = 0 \quad &\iff \quad a'\,x = -b'\,y \\ &\implies \quad a' \mid b'\,y \quad \text{y} \quad b' \mid a'\,x \\ &\underset{a' \perp b'}{\implies} \quad a' \mid y \quad \text{y} \quad b' \mid x \\ &\implies \quad \exists\, j, k \in \mathbb{Z} :\ y = j\,a' \ \text{ y } \ x = k\,b'. \end{aligned}$$

Volviendo al primer renglón, resulta:

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

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 $a'\,x + b'\,y = a'\,(b'\,k) + b'\,(-a'\,k) = 0$. □

La resolución completa de este caso particular nos sirve para resolver completamente una ecuación lineal diofántica arbitraria.

Teorema 5.1.7. (La ecuación diofántica $a \cdot X + b \cdot Y = c$.)

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

El conjunto $\mathcal{S}$ de soluciones enteras de la ecuación diofántica $a \cdot X + b \cdot Y = c$ es:

- $\mathcal{S} = \emptyset$ *cuando* $(a : b) \nmid c$.

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

Demostración. Sabemos que si $(a:b) \nmid c$, la ecuación no admite solución, luego $\mathcal{S} = \emptyset$ en ese caso. Cuando $(a:b) \mid c$, tenemos al menos una solución particular $(x_0, y_0) \in \mathbb{Z}^2$ de la ecuación, es decir $a\,x_0 + b\,y_0 = c$. Sea ahora $(x,y) \in \mathbb{Z}^2$ una solución cualquiera. Se tiene

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

Es decir (x,y) es solución de $a\,X + b\,Y = c$ si y solo si $(x - x_0, y - y_0)$ es solución de $a\,X + b\,Y = 0$, es decir, por la Proposición 5.1.6, si y solo si existe $k \in \mathbb{Z}$ tal que

$$x - x_0 = b'\,k,\ y - y_0 = -a'\,k, \quad \text{o sea} \quad x = x_0 + b'\,k,\ y = y_0 - a'\,k.$$

□

Resumimos el algoritmo que se obtiene a partir del Teorema 5.1.7 en el cuadro siguiente:

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

1. ¿ Tiene solución la ecuación ?
   (a) **no** cuando $(a:b) \nmid c$. En ese caso $\mathcal{S} = \emptyset$.
   (b) **sí** cuando $(a:b) \mid c$. 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 $18\,X + 27\,Y = -90$:
  Hay soluciones pues $(18 : 27) = 9 \mid -90$.
  "Coprimizo": $2\,X + 3\,Y = -10$.
  Solución particular: $(x_0, y_0) := (-5, 0)$.
  Entonces $\mathcal{S} = \{\,(x, y) :\ x = -5 + 3k,\ y = -2k,\ k \in \mathbb{Z}\,\}$.

- Soluciones *naturales* de $175\,X + 275\,Y = 3000$:
  Hay soluciones enteras pues $(175 : 275) = 25 \mid 3000$.
  "Coprimizo": $\dfrac{175}{25}\,X + \dfrac{275}{25}\,Y = \dfrac{3000}{25}$, i.e. $7\,X + 11\,Y = 120$.
  Solución particular?

$$
\begin{aligned}
& 11 = 1 \cdot 7 + 4,\ 7 = 1 \cdot 4 + 3,\ 4 = 1 \cdot 3 + 1 \\
\Rightarrow\ & 1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7 \\
\Rightarrow\ & 1 = 7 \cdot (-3) + 11 \cdot 2 \\
\Rightarrow\ & 120 = 7 \cdot (-3 \cdot 120) + 11 \cdot (2 \cdot 120) \ =\ 7 \cdot (-360) + 11 \cdot 240 \\
\Rightarrow\ & (x_0, y_0) = (-360, 240).
\end{aligned}
$$

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

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

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

5.2 Ecuaciones lineales de congruencia.

El analisis realizado para las ecuaciones diofánticas se aplica directamente a ciertas *ecuaciones lineales de congruencia*. Más especificamente, dado $m \in \mathbb{N}$, a las ecuaciones de la forma

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

para $a, c \in \mathbb{Z}$.

Como en el caso de las ecuaciones diofánticas, vamos a adoptar en estas notas una definición-notación de ecuaciones lineales de congruencia equivalentes.

Definición-Notación 5.2.1. (Ecuaciones de congruencia equivalentes.)

Sean $a\,X \equiv c \pmod{m}$ y $a'\,X \equiv c' \pmod{m'}$ dos ecuaciones de congruencia. Decimos que son *equivalentes* si tienen exactamente las mismas soluciones $x \in \mathbb{Z}$. En ese caso adoptamos la notación

$$a\,X \equiv c \pmod{m} \iff a'\,X \equiv c' \pmod{m'}.$$

Veremos ahora que la ecuación de congruencia $a\,X \equiv c \pmod{m}$ tiene al menos una solución $x_0 \in \mathbb{Z}$ si y solo si la ecuación diofántica $a\,X - m\,Y = c$ admite al menos una solución $(x_0, y_0) \in \mathbb{Z}^2$, y por lo visto en el Teorema 5.1.7, esto es si y solo si $(a : -m) = (a : m) \mid c$.

Proposición 5.2.2. (Ecuación de congruencia, mcd y ecuación "coprimizada".)

Sea $m \in \mathbb{N}$. Dados $a, c \in \mathbb{Z}$, la ecuación de congruencia $a\,X \equiv c \pmod{m}$ tiene soluciones enteras si y solo si $(a : m) \mid c$.

Si ese es el caso, sean $a' := \dfrac{a}{(a : m)}$, $c' := \dfrac{c}{(a : m)}$ y $m' := \dfrac{m}{(a : m)}$. Entonces

$$\boldsymbol{a}\,X \equiv c \pmod{m} \iff a'X \equiv c' \pmod{m'}.$$

Para probar la segunda afirmación, es útil aislar la propiedad siguiente, que es inmediata y cuya demostración se deja a cargo del lector:

Observación 5.2.3. (Simplificando factores comunes en ecuación de congruencia-I.)

Sean $m' \in \mathbb{N}$ y $a', c', d \in \mathbb{Z}$ no nulos. Entonces,

$$\forall\, x \in \mathbb{Z}, \quad (d\,a')\,x \equiv d\,c' \ \big(\bmod (d\,m')\big) \iff a'\,x \equiv c' \pmod{m'}.$$

Demostración. (de la Proposición 5.2.2.)

Si $(a : m) \mid c$, entonces la ecuación diofántica $aX - mY = c$ admite al menos una solución particular $(x_0, y_0) \in \mathbb{Z}^2$. Es decir, $ax_0 - my_0 = c$, o equivalentemente $ax_0 - c = my_0$. Por lo tanto $m | ax_0 - c$, o lo que es lo mismo, $ax_0 \equiv c \pmod{m}$. Luego $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación de congruencia $a\,X \equiv c \pmod{m}$.

Recíprocamente, si $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación de congruencia $a\,X \equiv c \pmod{m}$, entonces existe $y_0 \in \mathbb{Z}$ tal que $ax_0 - c = my_0$, por lo cual la ecuación diofántica $aX - mY = c$ 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 $(a : -m) = (a : m) \mid c$.

Finalmente, cuando $(a : m) \mid c$, se aplica la Proposición 5.2.3 para para $d = (a : m)$, $a = da'$, $c = dc'$ y $m = dm'$: luego

$$\forall\, x \in \mathbb{Z}, \quad a\,x \equiv c \pmod{m} \iff a'\,x \equiv c' \pmod{m'}.$$

Es decir las dos ecuaciones de congruencia tienen exactamente las mismas soluciones. □

En particular, dado que si $(a : m) = 1$, entonces $(a : m) \mid c$, $\forall\, c \in \mathbb{Z}$, se obtiene:

Corolario 5.2.4. (Ecuación de congruencia con a y m coprimos.)

Sean $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ tal que a y m son coprimos. *Entonces, la ecuación de congruencia $a\,X \equiv c \pmod{m}$ tiene soluciones enteras, cualquiera sea $c \in \mathbb{Z}$.*

El teorema siguiente describe todas las soluciones de una ecuación de congruencia.

Teorema 5.2.5. (La ecuación de congruencia $a\,X \equiv c \pmod{m}$.)

Sea $m \in \mathbb{N}$ y sean $a, c \in \mathbb{Z}$ con $a \neq 0$.

El conjunto $\mathcal{S}$ de soluciones enteras de la ecuación de congruencia

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

es

- $\mathcal{S} = \emptyset$, *cuando* $(a : m) \nmid c$.
- $\mathcal{S} = \{x \in \mathbb{Z} : \ x \equiv x_0 \pmod{m'}\}$ *donde $x_0 \in \mathbb{Z}$ es una solución particular cualquiera de la ecuación $a\,X \equiv c \pmod{m}$ o de la ecuación equivalente $a'\,X \equiv c' \pmod{m'}$ donde $a' = \dfrac{a}{(a : m)}$, $c' = \dfrac{c}{(a : m)}$ y $m' = \dfrac{m}{(a : m)}$, cuando $(a : m) \mid c$, ya que*

  $$a\,X \equiv c \pmod{m} \quad \rightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

  Más aún, existe una única solución $x_0 \in \mathbb{Z}$ que satisface $0 \leq x_0 < m'$.

Demostración. Sabemos por la Proposición 5.2.2 que si $(a : m) \nmid c$, no hay solución, luego $\mathcal{S} = \emptyset$ en ese caso. Sea entonces el caso $(a : m) \mid c$. Tenemos que probar que

$$a\,X \equiv c \pmod{m} \quad \rightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

Pero ya sabemos que en ese caso,

$$a\,X \equiv c \pmod{m} \quad \leftrightsquigarrow \quad a'\,X \equiv c' \pmod{m'}.$$

Por lo tanto alcanza con probar que

$$a'\,X \equiv c' \pmod{m'} \quad \leftrightsquigarrow \quad X \equiv x_0 \pmod{m'},$$

o sea tienen las mismas soluciones enteras.

• Verifiquemos primero que si $x \in \mathbb{Z}$ es solución de la ecuación $X \equiv x_0 \pmod{m'}$, es decir satisface $x \equiv x_0 \pmod{m'}$, entonces es también solución de la ecuación $a'\,X \equiv c' \pmod{m'}$:

Se tiene que $x \equiv x_0 \pmod{m'}$ implica $a'\,x \equiv a'\,x_0 \pmod{m'}$. Como $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación $a'\,X \equiv c' \pmod{m'}$, o sea vale $a'\,x_0 \equiv c' \pmod{m'}$, por transitividad se cumple $a'\,x \equiv c' \pmod{m'}$.

• Verifiquemos ahora que una solución x cualquiera de la ecuación $a'\,X \equiv c' \pmod{m'}$ es también solución de la ecuación $X \equiv x_0 \pmod{m'}$:

Si $x \in \mathbb{Z}$ es una solución cualquiera de la ecuación de congruencia $a'\,x \equiv c' \pmod{m'}$, entonces existe $y \in \mathbb{Z}$ tal que (x, y) es solución de la ecuación diofántica $a'\,X - m'\,Y = c'$. Por el Teorema 5.1.7, $x = x_0 + (-m')k$ e $y = y_0 - a'k$ donde (x_0, y_0) es una solución particular cualquiera de la ecuación diofántica y $k \in \mathbb{Z}$. En particular $m' \mid x - x_0$, es decir $x \equiv x_0 \pmod{m'}$ como se quería probar.

Para terminar, mostremos que hay una única solución x_0 con $0 \leq x_0 < m'$. Que existe es obvio pues si la solución encontrada x_0 no está en esas condiciones, se toma $r_{m'}(x_0)$ que satisface la misma ecuación de congruencia ya que $x_0 \equiv r_{m'}(x_0) \pmod{m'}$. Cualquier otra solución x satisface $x \equiv r_{m'}(x_0) \pmod{m'}$, y por lo tanto no puede haber otra solución $x \neq r_{m'}(x_0)$ con $0 \leq x < m'$. □

Antes de resumir el algoritmo que se obtiene a partir del Teorema 5.2.5, hagamos algunos ejemplos.

Ejemplos:

- La ecuación $9\,X \equiv 2 \pmod{15}$ no tiene solución pues $(9 : 15) \nmid 2$.
- La ecuación $9\,X \equiv 6 \pmod{15}$ tiene solución pues $(9 : 15) = 3 \mid 6$:

  $$9\,X \equiv 6 \pmod{15} \quad \leftrightsquigarrow \quad 3\,X \equiv 2 \pmod{5} \quad \leftrightsquigarrow \quad X \equiv 4 \pmod{5}.$$

  (Aquí, $x_0 := 4$ es una solución particular, pues $3{\cdot}4 = 12 \equiv 2 \pmod{5}$.)
  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 4 \pmod{5} \}$.

Si lo que buscamos es expresar todas las soluciones módulo 15 (el módulo correspondiente al planteo original) tenemos que fijarnos todos los números x_0 con $0 \leq x_0 < 15$ que satisfacen $x_0 \equiv 4 \pmod 5$, es decir $x_0 = 4 + 5\,k$ con $k \in \mathbb{Z}$ tales que $0 \leq x_0 < 15$. Estos son $4 = 4 + 0 \cdot 5$, $9 = 4 + 1 \cdot 5$ y $14 = 4 + 2 \cdot 5$. Así,

$$\begin{aligned}\mathcal{S} &= \{\, x \in \mathbb{Z} :\ x \equiv 4 \pmod 5\} \\ &= \{\, x \in \mathbb{Z} :\ x \equiv 4 \pmod{15} \ \text{ o } \ x \equiv 9 \pmod{15} \ \text{ o } x \equiv 14 \pmod{15}\}.\end{aligned}$$

- La ecuación $3\,X \equiv 2 \pmod 4$ tiene solución pues 3 y 4 son coprimos:

$$3\,X \equiv 2 \pmod 4 \quad \rightsquigarrow \quad X \equiv 2 \pmod 4.$$

  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 2 \pmod 4\}$.

- La ecuación $12\,X \equiv 6 \pmod{10}$ 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:

$$12\,X \equiv 6 \pmod{10} \quad \rightsquigarrow \quad 2\,X \equiv 6 \pmod{10} \quad \rightsquigarrow \quad X \equiv 3 \pmod 5.$$

  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 3 \pmod 5\}$,

  o también, $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 3 \pmod{10} \ \text{ o } \ x \equiv 8 \pmod{10}\}$

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

$$120\,X \equiv 60 \pmod{250} \ \rightsquigarrow \ 12\,X \equiv 6 \pmod{25}.$$

  Pero, $\forall\, x \in \mathbb{Z}$,

$$6\,(2\,x) \equiv 6 \cdot 1 \pmod{25} \ \underset{6 \perp 25}{\iff} \ 2\,x \equiv 1 \pmod{25},$$

  pues, como $6 \perp 25$, se tiene $25 \mid 6 \cdot (2\,x - 1) \ \Leftrightarrow \ 25 \mid 2x - 1$.

  Por lo tanto,

$$12\,X \equiv 6 \pmod{25} \ \rightsquigarrow \ 2\,X \equiv 1 \pmod{25} \ \rightsquigarrow \ X \equiv 13 \pmod{25}.$$

  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 13 \pmod{25}\}$. Si queremos expresar las soluciones módulo 250, tendremos 10 soluciones distintas: ¿Cuáles son?

El argumento usado en el último ejemplo vale en general:

Observación 5.2.6. (Simplificando factores comunes en ecuación de congruencia-II.)

Sean $m \in \mathbb{N}$ y $a, c, d \in \mathbb{Z}$, con a, d no nulos.

Si d y m son *coprimos*, entonces se tiene la siguiente equivalencia de ecuaciones de congruencia:

$$(d\,a)\,X \equiv d\,c \pmod{m} \quad \leftrightsquigarrow \quad a\,X \equiv c \pmod{m}.$$

Demostración. Hay que probar que las dos ecuaciones de congruencia tienen las mismas soluciones $x \in \mathbb{Z}$:

($\Rightarrow$): Esto es porque $m \mid d\,(a\,x - c)$ y $m \perp d$ implica $m \mid a\,x - c$.

($\Leftarrow$): Vale siempre. □

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

1. Antes que nada reemplazo, si es necesario, a por $r_m(a)$ y c por $r_m(c)$ sin cambiar las soluciones, ya que $a \equiv r_m(a) \pmod{m}$ y $c \equiv r_m(c) \pmod{m}$, 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 $(a : m) \nmid c$.

   (b) **sí** si $(a : m) \mid c$. En ese caso:

3. "Coprimizo" la ecuación:

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

4. Si es necesario, ahora que $a' \perp m'$, simplifico todos los factores comunes entre a' y c' aplicando la Observación 5.2.6. Esto me simplifica la búsqueda de la solución particular.

5. Busco una solución particular $x_0 \in \mathbb{Z}$ que satisface que $a'x_0 \equiv c' \pmod{m'}$ (a ojo o encontrando una solución particular de la ecuación diofántica $a'X - m'Y = c'$ asociada).

6. Se concluye que

   $$a\,X \equiv c \pmod{m} \quad \leftrightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

O sea, el conjunto de soluciones de la ecuación de congruencia es el conjunto

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

5.3 Teorema chino del resto (TCR).

La primera versión conocida de este teorema, sobre la resolución simultánea de varias congruencias, se encontró en un tratado escrito por el matemático chino *Sun Tzu*, que vivió entre los Siglos III y V. Dicen que le servía al emperador chino para contar su numeroso ejército sin contar los hombres uno por uno...

En la Sección 5.2 aprendimos a resolver ecuaciones de congruencia: para cada ecuación de la forma $aX \equiv c \pmod{m}$ sabemos producir la ecuación equivalente (es decir con las mismas soluciones) más simple posible, que es de la forma $X \equiv x_0 \pmod{m'}$. Ahora se trata de resolver *sistemas* de ecuaciones lineales de congruencia de la forma

$$\left\{ \begin{array}{rcll} X & \equiv & c_1 & \pmod{m_1} \\ X & \equiv & c_2 & \pmod{m_2} \\ & \vdots & & \\ X & \equiv & c_n & \pmod{m_n} \end{array} \right. \tag{5.1}$$

donde $m_1, \ldots, m_n \in \mathbb{N}$ y $c_1, \ldots, c_n \in \mathbb{Z}$. Aquí resolver significa obtener una descripción equivalente via una sola ecuación de congruencia simple (que tenga las mismas soluciones) de la forma

$$X \equiv x_0 \pmod{m},$$

o lo que es lo mismo, describir el conjunto de soluciones como

$$\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv x_0 \pmod{m}\},$$

para algún $m \in \mathbb{N}$ adecuado y algún x_0, $0 \leq x_0 < m$.

Adoptamos como en la Sección 5.2 la notación $\leftrightsquigarrow$ para sistemas de ecuaciones de congruencia equivalentes, o sea con las mismas soluciones.

Analizaremos ahora unos ejemplos sencillos que nos ayudarán a formular propiedades que garantizan la equivalencia y/o incompatibilidad de ciertos sistemas de ecuaciones de congruencias.

<u>*Ejemplos:*</u>

- $$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{5} \\ X & \equiv & 3 \pmod{12} \end{array} \right. \quad \leftrightsquigarrow \quad X \equiv 3 \pmod{60},$$

pues $5 \mid X-3$ y $12 \mid X-3$ es equivalente a $60 = 5 \cdot 12 \mid X-3$ dado que $5 \perp 12$.

- $$\begin{cases} X & \equiv & 3 \pmod 5 \\ X & \equiv & 2 \pmod{10} \end{cases}$$

  es incompatible dado que $X \equiv 2 \pmod{10}$ implica $X \equiv 2 \pmod d$ para todo d divisor de 10 (pues $10 \mid X-2 \;\Rightarrow\; d \mid X-2$ si $d \mid 10$). En particular, para $d = 5$, no puede ser a la vez $X \equiv 2 \pmod 5$ y $X \equiv 3 \pmod 5$.

- $$\begin{cases} X & \equiv & 3 \pmod 5 \\ X & \equiv & 3 \pmod{10} \end{cases} \quad \leftrightsquigarrow \quad X \equiv 3 \pmod{10},$$

  pues $X \equiv 3 \pmod{10}$ automáticamente implica que se cumple también $X \equiv 3 \pmod d$ para todo d divisor de 10 (¿Por qué?), y en particular automáticamente se cumple $X \equiv 3 \pmod 5$.

- $$\begin{cases} X & \equiv & 3 \pmod 5 \\ X & \equiv & 8 \pmod{10} \end{cases} \quad \leftrightsquigarrow \quad X \equiv 8 \pmod{10},$$

  pues $X \equiv 8 \pmod{10}$ automáticamente implica que se cumple también $X \equiv 8 \pmod d$ para todo d divisor de 10, y en particular automáticamente se cumple $X \equiv 8 \pmod 5$, pero dado que $8 \equiv 3 \pmod 5$, automáticamente se cumple $X \equiv 3 \pmod 5$.

Estos ejemplos se generalizan a las propiedades siguientes, que se aplicarán sistemáticamente en lo que sigue.

Proposición 5.3.1. (Sistemas equivalentes.)

1. *Sean* $m_1, \ldots, m_n \in \mathbb{N}$ coprimos dos a dos, *es decir* $m_i \perp m_j$ *para* $i \neq j$. *Entonces,* $\forall\, c \in \mathbb{Z}$,

$$\begin{cases} X & \equiv & c \pmod{m_1} \\ X & \equiv & c \pmod{m_2} \\ & \vdots & \\ X & \equiv & c \pmod{m_n} \end{cases} \quad \leftrightsquigarrow \quad X \equiv c \pmod{m_1 \cdot m_2 \cdots m_n}.$$

2. *Sean* $m, m' \in \mathbb{N}$ *tales que* $m' \mid m$. *Entonces,* $\forall\, c, c' \in \mathbb{Z}$,

   - *Si* $c \not\equiv c' \pmod{m'}$, $\begin{cases} X & \equiv & c' \pmod{m'} \\ X & \equiv & c \pmod m \end{cases}$ *es incompatible,*

   - *Si* $c \equiv c' \pmod{m'}$, $\begin{cases} X & \equiv & c' \pmod{m'} \\ X & \equiv & c \pmod m \end{cases} \leftrightsquigarrow X \equiv c \pmod m.$

Demostración. 1. Hay que probar que el sistema del lado izquierdo tiene exactamente las mismas soluciones $x \in \mathbb{Z}$ que la ecuación del lado derecho.

($\Leftarrow$) Si $x \in \mathbb{Z}$ satisface $x \equiv c \pmod{m_1 \cdot m_2 \cdots m_n}$, es decir $m_1 \cdot m_2 \cdots m_n \mid x - c$, entonces claramente $m_i \mid x - c$, $\forall\, i$, es decir $x \equiv c \pmod{m_i}$, $\forall\, i$.

($\Rightarrow$) Por inducción en la cantidad de factores n.

- Para $n = 1$, no hay nada que probar.
- $n \Rightarrow n+1$: Queremos probar que si $m_1, \ldots, m_{n+1}$ son coprimos dos a dos, entonces $\forall\, c \in \mathbb{Z}$, $\forall\, x \in \mathbb{Z}$

$$\begin{cases} x \equiv c \pmod{m_1} \\ \quad \vdots \\ x \equiv c \pmod{m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases} \implies x \equiv c \pmod{m_1 \cdots m_n \cdot m_{n+1}}$$

Por H.I., como $m_1, \ldots, m_n$ son coprimos dos a dos,

$$\begin{cases} x \equiv c \pmod{m_1} \\ \quad \vdots \\ x \equiv c \pmod{m_n} \end{cases} \implies x \equiv c \pmod{m_1 \cdots m_n}.$$

Es decir,

$$\begin{cases} x \equiv c \pmod{m_1} \\ \quad \vdots \\ x \equiv c \pmod{m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases} \implies \begin{cases} x \equiv c \pmod{m_1 \cdots m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases}.$$

Pero dado que $m_1, \ldots, m_n$ son todos coprimos con m_{n+1}, se deduce que $m_1 \cdots m_n$ es coprimo con m_{n+1}. Luego

$$\begin{cases} x \equiv c \pmod{m_1 \cdots m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases} \implies \begin{cases} m_1 \cdots m_n \mid x - c \\ m_{n+1} \mid x - c \end{cases}$$

$$\underset{m_1 \cdots m_n \perp m_{n+1}}{\implies} (m_1 \cdots m_n) \cdot m_{n+1} \mid x - c$$

$$\implies x \equiv c \pmod{m_1 \cdots m_{n+1}}.$$

2. Cuando $m' \mid m$, $\forall\, x \in \mathbb{Z}$, $x \equiv c \pmod{m}$ implica $x \equiv c \pmod{m'}$ pues $m \mid x - c \Rightarrow m' \mid x - c$. Luego

$$\begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m} \end{cases} \implies \begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m'} \end{cases}$$

Por transitividad, $c \equiv c' \pmod{m'}$. Por lo tanto, si $c \not\equiv c' \pmod{m'}$, el sistema es incompatible. Sean entonces c, c' tales que $c \equiv c' \pmod{m'}$.

Probemos la equivalencia del sistema de la izquierda con la ecuación de la derecha:

$$\left\{ \begin{array}{rcl} x & \equiv & c' \pmod{m'} \\ x & \equiv & c \pmod{m} \end{array} \right. \quad \Longrightarrow \quad x \equiv c \pmod{m},$$

pues nos estamos quedando con una de las dos condiciones. Recíprocamente,

$$x \equiv c \pmod{m} \implies x \equiv c \pmod{m'} \implies x \equiv c' \pmod{m'},$$

y por lo tanto

$$x \equiv c \pmod{m} \quad \Longrightarrow \quad \left\{ \begin{array}{rcl} x & \equiv & c' \pmod{m'} \\ x & \equiv & c \pmod{m} \end{array} \right. ,$$

como se quería probar.

□

Ejemplos:

- $$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{22} \\ X & \equiv & 3 \pmod{5} \\ X & \equiv & 3 \pmod{21} \end{array} \right. \quad \leftrightsquigarrow \quad X \equiv 3 \pmod{22 \cdot 5 \cdot 21},$$

  por la Proposición 5.3.1, pues $22 = 2 \cdot 11$, 5 y $21 = 3 \cdot 7$ son coprimos dos a dos.

- De la misma forma:

$$\begin{aligned} X \equiv 50 \pmod{22 \cdot 5 \cdot 21} &\leftrightsquigarrow \left\{ \begin{array}{rcl} X & \equiv & 50 \pmod{22} \\ X & \equiv & 50 \pmod{5} \\ X & \equiv & 50 \pmod{21} \end{array} \right. \\ &\leftrightsquigarrow \left\{ \begin{array}{rcl} X & \equiv & 6 \pmod{22} \\ X & \equiv & 0 \pmod{5} \\ X & \equiv & 8 \pmod{21} \end{array} \right. . \end{aligned}$$

- $$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{22} \\ X & \equiv & 3 \pmod{18} \\ X & \equiv & 4 \pmod{11} \end{array} \right.$$

  es incompatible, por la Proposición 5.3.1, pues $11 \mid 22$ pero $3 \not\equiv 4 \pmod{11}$.

- $$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{22} \\ X & \equiv & 4 \pmod{8} \end{array} \right. \quad \leftrightsquigarrow \quad \left\{ \begin{array}{rcl} X & \equiv & 1 \pmod{2} \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 4 \pmod{8} \end{array} \right.$$

  y luego es incompatible pues en el sistema de la derecha la primera ecuación y la tercera son incompatibles: $2 \mid 8$ pero $4 \not\equiv 1 \pmod{2}$.

- $$\left\{\begin{array}{lcl} X & \equiv & 1 \pmod 4 \\ X & \equiv & 5 \pmod 8 \\ X & \equiv & 13 \pmod{16} \end{array}\right. \quad \leftrightsquigarrow \quad X \equiv 13 \pmod{16}$$

  por la Proposición 5.3.1: $4 \mid 8$ y $5 \equiv 1 \pmod 4$, $8 \mid 16$ y $13 \equiv 5 \pmod 8$.

- $$\left\{\begin{array}{lcll} X & \equiv & 3 & \pmod{22} \\ X & \equiv & 5 & \pmod 8 \\ X & \equiv & 17 & \pmod{20} \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{lcl} X & \equiv & 1 \pmod 2 \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 5 \pmod 8 \\ X & \equiv & 1 \pmod 4 \\ X & \equiv & 2 \pmod 5 \end{array}\right.$$
  $$\leftrightsquigarrow \left\{\begin{array}{lcl} X & \equiv & 5 \pmod 8 \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 2 \pmod 5 \end{array}\right.$$

  aplicando reiteradamente la Proposición 5.3.1.

En estos ejemplos se ve que cuando el sistema no es incompatible, se reduce a resolver un sistema (5.1) *pero con la condición de que los m_i son coprimos dos a dos.* En esa situación vale el teorema siguiente:

Teorema 5.3.2. (Teorema chino del resto.)

Sean $m_1, \ldots, m_n \in \mathbb{N}$ coprimos dos a dos*, es decir $m_i \perp m_j$ para $i \neq j$. Entonces, $\forall\, c_1, \ldots, c_n \in \mathbb{Z}$, el sistema de ecuaciones de congruencia*

$$\left\{\begin{array}{lcl} X & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ X & \equiv & c_n \pmod{m_n} \end{array}\right.$$

tiene soluciones enteras.
Más aún,

$$\left\{\begin{array}{lcl} X & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ X & \equiv & c_n \pmod{m_n} \end{array}\right. \quad \leftrightsquigarrow \quad X \equiv x_0 \pmod{m_1 \cdots m_n}\ ,$$

donde $x_0 \in \mathbb{Z}$ es una solución particular cualquiera del sistema, y se tiene

$$\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv x_0 \pmod{m_1 \cdots m_n}\}.$$

En particular, existe una única solución $x_0 \in \mathbb{Z}$ que satisface $0 \leq x_0 < m_1 \cdots m_n$.

Lo interesante de la demostración de este teorema es que da un método constructivo, o sea sugiere directamente un algoritmo, para hallar x_0.

Demostración. 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

$$\begin{cases} x_0 & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ x_0 & \equiv & c_n \pmod{m_n} \end{cases}.$$

En ese caso, por transitividad y aplicando la Proposición 5.3.1, tendremos para una solución cualquiera x:

$$\begin{cases} x & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ x & \equiv & c_n \pmod{m_n} \end{cases} \iff \begin{cases} x & \equiv & x_0 \pmod{m_1} \\ x & \equiv & x_0 \pmod{m_2} \\ & \vdots & \\ x & \equiv & x_0 \pmod{m_n} \end{cases}$$
$$\iff x \equiv x_0 \pmod{m_1 \cdots m_n},$$

o sea probamos la equivalencia enunciada en el Teorema.

El único x_0 que satisface $0 \leq x_0 < m_1 \cdots m_n$ se obtiene reemplazando la solución particular elegida por $r_{m_1 \cdots m_n}(x_0)$.

Para probar que existen soluciones (y hallar una solución particular x_0), vamos a subdividir el sistema (5.1) en n sistemas más simples y probar que cada uno de ellos tiene soluciones. Estos sistemas S_1, S_2, ..., S_n son:

$$\underline{S_1}: \quad \begin{cases} X & \equiv & c_1 \pmod{m_1} \\ X & \equiv & 0 \pmod{m_2} \\ X & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ X & \equiv & 0 \pmod{m_n} \end{cases}, \quad \underline{S_2}: \quad \begin{cases} X & \equiv & 0 \pmod{m_1} \\ X & \equiv & c_2 \pmod{m_2} \\ X & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ X & \equiv & 0 \pmod{m_n} \end{cases}, \ \ldots, \quad \underline{S_n}: \quad \begin{cases} X & \equiv & 0 \pmod{m_1} \\ X & \equiv & 0 \pmod{m_2} \\ & \vdots & \\ X & \equiv & 0 \pmod{m_{n-1}} \\ X & \equiv & c_n \pmod{m_n} \end{cases}$$

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:

$$\underline{S_1}: \quad \begin{cases} x_1 & \equiv & c_1 \pmod{m_1} \\ x_1 & \equiv & 0 \pmod{m_2} \\ x_1 & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ x_1 & \equiv & 0 \pmod{m_n} \end{cases}, \quad \underline{S_2}: \quad \begin{cases} x_2 & \equiv & 0 \pmod{m_1} \\ x_2 & \equiv & c_2 \pmod{m_2} \\ x_2 & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ x_2 & \equiv & 0 \pmod{m_n} \end{cases}, \ \ldots, \quad \underline{S_n}: \quad \begin{cases} x_n & \equiv & 0 \pmod{m_1} \\ x_n & \equiv & 0 \pmod{m_2} \\ & \vdots & \\ x_n & \equiv & 0 \pmod{m_{n-1}} \\ x_n & \equiv & c_n \pmod{m_n} \end{cases}$$

Entonces si definimos

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

se satisface que

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_n & \equiv & c_1 + 0 + 0 + \cdots + 0 \pmod{m_1} \\ x_1 + x_2 + x_3 + \cdots + x_n & \equiv & 0 + c_2 + 0 + \cdots + 0 \pmod{m_2} \\ & \vdots & \\ x_1 + x_2 + x_3 + \cdots + x_n & \equiv & 0 + 0 + \cdots + 0 + c_n \pmod{m_n} \end{cases} \implies \begin{cases} x_0 & \equiv & c_1 \pmod{m_1} \\ x_0 & \equiv & c_2 \pmod{m_2} \\ & \vdots & \\ x_0 & \equiv & c_n \pmod{m_n} \end{cases}$$

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

Aplicando los resultados de la Sección 5.2, vamos a ver que todos los sistemas S_ℓ, $1 \leq \ell \leq n$, tienen soluciones enteras y vamos a elegir para cada uno de ellos una solución particular x_ℓ.

Miremos el sistema S_1: Como $m_2, \ldots, m_n$ son coprimos dos a dos, si ponemos $M_1 := m_2 \cdots m_n$, se tiene la equivalencia descrita en la Proposición 5.3.1:

$$\begin{cases} X \equiv c_1 \pmod{m_1} \\ X \equiv 0 \pmod{m_2} \\ \quad \vdots \\ X \equiv 0 \pmod{m_n} \end{cases} \quad \leftrightsquigarrow \quad \begin{cases} X \equiv c_1 \pmod{m_1} \\ X \equiv 0 \pmod{M_1}. \end{cases}$$

La segunda ecuación a la derecha indica que cualquier solución x tiene que satisfacer que $x = M_1\, y$ para algún $y \in \mathbb{Z}$, y luego para cumplir con la primer ecuación, se tiene que satisfacer $M_1\, y \equiv c_1 \pmod{m_1}$, o sea y es una solución de la ecuación

$$M_1\, Y \equiv c_1 \pmod{m_1}. \tag{5.2}$$

Se observa que $M_1 \perp m_1$, por ser $M_1 = m_2 \cdots m_n$ y los m_i coprimos dos a dos. Por lo tanto, sabemos que la ecuación (5.2) tiene soluciones enteras cualquiera sea $c_1 \in \mathbb{Z}$. Si y_1 es una solución particular, entonces $x_1 := M_1\, y_1$ es una solución particular del sistema S_1.

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

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

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

Definamos $M_\ell := \prod_{j \neq \ell} m_j$ y repitamos lo que se hizo arriba para S_1. Se tiene $M_\ell \perp m_\ell$ por ser todos los m_i coprimos dos a dos. Luego, la ecuación de congruencia

$$M_\ell\, Y \equiv c_\ell \pmod{m_\ell}$$

tiene soluciones enteras cualquiera sea $c_\ell \in \mathbb{Z}$, y si y_ℓ es una solución particular, entonces, como arriba, $x_\ell := M_\ell\, y_\ell$ es una solución particular del sistema S_ℓ. □

Ejemplos:

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

  Como 8, 35 y 3 son coprimos 2 a 2, por el Teorema 5.3.2, 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 la única solución con $0 \leq x_0 < 840$. Para hallar esta solución x_0, se consideran los tres sistemas más simples:

  $$\underline{S_1}: \begin{cases} X \equiv 4 \pmod 8 \\ X \equiv 0 \pmod{35} \\ X \equiv 0 \pmod 3 \end{cases}, \quad \underline{S_2}: \begin{cases} X \equiv 0 \pmod 8 \\ X \equiv 10 \pmod{35} \\ X \equiv 0 \pmod 3 \end{cases}, \quad \underline{S_3}: \begin{cases} X \equiv 0 \pmod 8 \\ X \equiv 0 \pmod{35} \\ X \equiv 1 \pmod 3 \end{cases}.$$

  Solución particular para S_1:

  $$\begin{cases} X \equiv 4 \pmod 8 \\ X \equiv 0 \pmod{35} \\ X \equiv 0 \pmod 3 \end{cases} \leftrightsquigarrow \begin{cases} X \equiv 4 \pmod 8 \\ X \equiv 0 \pmod{35 \cdot 3} \end{cases}$$

  Es decir una solución x satisface $x = 35 \cdot 3\,y = 105\,y$ donde y es solución de la ecuación $105\,Y \equiv 4 \pmod 8$, o sea de la ecuación $Y \equiv 4 \pmod 8$. Una solución particular es $y_1 = 4$, y por lo tanto $x_1 = 105\,y_1 = 420$ es una solución particular del sistema S_1.

  Solución particular para S_2:

  $$\begin{cases} X \equiv 0 \pmod 8 \\ X \equiv 10 \pmod{35} \\ X \equiv 0 \pmod 3 \end{cases} \leftrightsquigarrow \begin{cases} X \equiv 10 \pmod{35} \\ X \equiv 0 \pmod{8 \cdot 3} \end{cases}.$$

  Es decir una solución x satisface $x = 8 \cdot 3\,y = 24\,y$ donde y es solución de la ecuación $24\,Y \equiv 10 \pmod{35}$. Dado que $(24 : 10) = 2 \perp 35$, podemos simplificar por 2 y el sistema es equivalente a $12\,Y \equiv 5 \pmod{35}$. Podemos encontrar rápidamente la solución a ojo del modo siguiente:

  $$\begin{aligned} 12 \cdot 3 \equiv 1 \pmod{35} &\Longrightarrow 12 \cdot (3 \cdot 5) \equiv 1 \cdot 5 \pmod{35} \\ &\Longrightarrow 12 \cdot 15 \equiv 5 \pmod{35}. \end{aligned}$$

  Luego, una solución particular es $y_2 = 15$, y por lo tanto $x_2 = 24\,y_2 = 360$ es una solución particular del sistema S_2.

  Solución particular para S_3:

  $$\begin{cases} X \equiv 0 \pmod 8 \\ X \equiv 0 \pmod{35} \\ X \equiv 1 \pmod 3 \end{cases} \leftrightsquigarrow \begin{cases} X \equiv 1 \pmod 3 \\ X \equiv 0 \pmod{8 \cdot 35} \end{cases}.$$

Es decir una solución x satisface $x = 8 \cdot 35\, y = 280\, y$, donde y es solución de la ecuación $280\, Y \equiv 1 \pmod 3$, o sea de la ecuación $Y \equiv 1 \pmod 3$. Una solución particular es $y_3 = 1$, por lo tanto $x_3 = 280\, y_3 = 280$ es una solución particular de S_3.

Por lo tanto, aplicando la construcción del Teorema 5.3.2,

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

es una solución particular del sistema original, y éste es equivalente a $X \equiv 1060 \pmod{840}$. Como $1060 \equiv 220 \pmod{840}$, se tiene que la única solución x_0 con $0 \leq x_0 < 840$ es $x_0 = 220$:

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

Es decir, $\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv 220 \pmod{840}\}$.

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

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 la única solución con $0 \leq x_0 < 770$. Ahora bien, observemos que por la Proposición 5.3.1, la primera ecuación y la tercera 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:

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

Solución particular para S_1:

Una solución particular x_1 satisface $x_1 = 11\, y_1$ donde y_1 es solución particular de la ecuación $11\, Y \equiv 3 \pmod{70}$. Por ejemplo $y_1 = 13$ (pues por el algoritmo de Euclides $1 = 3 \cdot 70 - 19 \cdot 11$, y por lo tanto $y_1 \equiv 3 \cdot (-19) \pmod{70}$, o sea se puede tomar $y_1 = 13$). Luego $x_1 = 11 \cdot 13 = 143$.

Solución particular para S_2:

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

Así, $x_0 := x_1 + x_2 = 143 + 210 = 353$ es solución particular del sistema original. Además es la única solución con $0 \leq x_0 < 770$. Se tiene la equivalencia

$$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{10} \\ X & \equiv & 1 \pmod{11} \\ X & \equiv & 3 \pmod{7} \end{array} \right. \quad \leftrightsquigarrow \quad X \equiv 353 \pmod{770},$$

es decir, $\mathcal{S} = \{x \in \mathbb{Z} : \ x \equiv 353 \pmod{770}\}$.

Pero en este caso este mismo ejemplo se puede resolver más "a mano" usando la fuerza del TCR:

$$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{70} \\ X & \equiv & 1 \pmod{11} \end{array} \right. .$$

Sabemos que el sistema tiene solución y es equivalente a

$$X \equiv x_0 \pmod{770}$$

donde $x_0 \in \mathbb{Z}$ 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 de la forma $3 + 70\,k$, $k \in \mathbb{Z}$, es decir

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

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

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

El número 353 cumple $353 \equiv 1 \pmod{11}$. ¡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:

$$\left\{ \begin{array}{rcll} X & \equiv & 3 & \pmod{22} \\ X & \equiv & 5 & \pmod{8} \\ X & \equiv & 17 & \pmod{20} \end{array} \right. \quad \leftrightsquigarrow \quad \left\{ \begin{array}{rcl} X & \equiv & 5 \pmod{8} \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 2 \pmod{5} \end{array} \right.$$

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

$$X \equiv x_0 \pmod{8 \cdot 11 \cdot 5}, \quad \text{es decir} \quad X \equiv x_0 \pmod{440},$$

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 números entre 0 y

$11 \cdot 8 = 88$ que cumplen la ecuación con el módulo 11, o sea de la forma $3 + 11\,k, k \in \mathbb{Z}$:

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

¿Cuál cumple la condición con el módulo 8?

$$\not{3},\ \not{1}4,\ \not{2}5,\ \not{3}6,\ \not{4}7,\ \not{5}8, 69:$$

El número 69 cumple $69 \equiv 5 \pmod 8$, luego los que resuelven esas dos ecuaciones son $x \equiv 69 \pmod{88}$. Ahora, vamos escribiendo los números entre 0 y 440 que cumplen esa condición, investigando cuál es el que cumple la ecuación con el módulo 5:

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

El número 157 cumple $157 \equiv 2 \pmod 5$ ¡Ya está!

$$\left\{\begin{array}{rcll} X & \equiv & 3 & (\text{mod } 22) \\ X & \equiv & 5 & (\text{mod } 8) \\ X & \equiv & 17 & (\text{mod } 20) \end{array}\right. \quad \leftrightsquigarrow \quad X \equiv 157 \ (\text{mod } 440),$$

es decir, $\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv 157 \pmod{440}\}$.

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

$$\left\{\begin{array}{rcl} 3\,X & \equiv & 2 \ (\text{mod } 7) \\ 7\,X & \equiv & 5 \ (\text{mod } 8) \\ 6\,X & \equiv & 8 \ (\text{mod } 10) \end{array}\right. .$$

Primero se puede simplificar todo lo que se puede (en este caso el factor común 2 en la tercera ecuación), y luego como en lo que resulta los módulos son coprimos dos a dos, resolver cada ecuación por separado, dándola en la forma $X \equiv c_\ell \pmod{m_\ell}$ para aplicar el TCR:

$$\left\{\begin{array}{rcl} 3\,X & \equiv & 2\ (7) \\ 7\,X & \equiv & 5\ (8) \\ 6\,X & \equiv & 8\ (10) \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{rcl} 3\,X & \equiv & 2\ (7) \\ 7\,X & \equiv & 5\ (8) \\ 3\,X & \equiv & 4\ (5) \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{rcl} X & \equiv & 3\ (7) \\ X & \equiv & 3\ (8) \\ X & \equiv & 3\ (5) \end{array}\right. \leftrightsquigarrow X \equiv 3\ (280),$$

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

$$\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv 3 \pmod{280}\}.$$

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

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

por aplicación reiterada de la Proposición 5.3.1. Al resolver este sistema con el método dado por el TCR, se obtiene que el sistema original es equivalente a

$$X \equiv 1607 \ (9 \cdot 7 \cdot 4 \cdot 5 = 1260) \quad \rightsquigarrow \quad X \equiv 347 \ (1260).$$

Luego el resto de dividir a x por 1260 es 347, pero como se quiere 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.

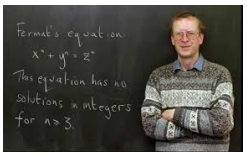
5.4 El Pequeño Teorema de Fermat (PTF)

Este teorema es uno de los tantos que debemos al abogado y mayor matemático amateur de todos los tiempos, el francés *Pierre de Fermat*, 1601–1665. Fermat 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* $a^n + b^n = c^n$.



Esta importante conjetura, que motivó el desarrollo de toda la rama de la matemática conocida como la Teoría de Números, recién fue probada en los años 1993–1994 por el matemático inglés Andrew Wiles (en una parte con su discípulo Richard Taylor).

Teorema 5.4.1. (Pequeño Teorema de Fermat - PTF.)

Sea p *un* primo *positivo. Entonces,* $\forall\, a \in \mathbb{Z}$,

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

Observación 5.4.2.

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 PTF: $a^n \equiv a \pmod n$ para todo $a \in \mathbb{Z}$.

Esos números se suelen llamar "seudoprimos" o "números de Carmichael" por el matemático americano Robert Carmichael, 1879–1967, que descubrió en 1909 el más chico de ellos: el número $n := 561 = 3 \cdot 11 \cdot 17$.

En 1994, los matemáticos Red Alford, Andrew Granville y Carl Pomerance lograron probar la conjetura que afirmaba que existen infinitos seudoprimos.

Observación 5.4.3. Las dos afirmaciones del PTF 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.

Demostración. (del PTF.)

Por la observación anterior, para probar el PTF alcanza con probar el caso (*2*) en que $p \nmid a$, es decir $a \perp p$, que es el caso interesante y no trivial. Vamos a hacer aquí la demostración de Euler, que permite obtener una formulación del teorema para no primos conocida como Teorema de Euler, que no probaremos en estas notas.

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

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

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

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

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

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

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

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

$$\begin{aligned} \Phi(k) = \Phi(j) &\iff r_p(k\,a) = r_p(j\,a) \\ &\iff p \mid k\,a - j\,a = (k-j)\,a \\ &\underset{p \text{ primo}}{\iff} p \mid k-j \;\text{ ó }\; p \mid a, \end{aligned}$$

  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 $k-j \in \{0, \ldots, p-1\}$, luego

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

Por lo tanto Φ es biyectiva, es decir suryectiva también, con lo cual $\mathrm{Im}(\Phi) = \{1, 2, \ldots, p-1\}$. Esto implica

$$\Phi(1) \cdot \Phi(2) \cdots \Phi(p-1) = 1 \cdot 2 \cdots (p-1).$$

Es decir,

$$r_p(a) \cdot r_p(2\,a) \cdots r_p((p-1)\,a) = 1 \cdot 2 \cdots (p-1).$$

Pero como $k\,a \equiv r_p(k\,a) \pmod{p}$ para $1 \leq k \leq p-1$, se deduce

$$a \cdot 2\,a \cdots (p-1)\,a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Es decir

$$(p-1)!\,a^{p-1} \equiv (p-1)! \pmod{p}.$$

Pero 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 k con $1 \leq k \leq p-1$ tal que $p \mid k$), luego

$$a^{p-1} \equiv 1 \pmod{p},$$

como se quería probar. □

Corolario 5.4.4. (Congruencia y potencias.)

Sea p un primo positivo. Entonces $\forall\, a \in \mathbb{Z}$ tal que $p \nmid a$ y $n \in \mathbb{N}$, se tiene

$$n \equiv r \ \big(\mathrm{mod}\,(p-1)\big) \implies a^n \equiv a^r \pmod{p}.$$

En particular,

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

Demostración.

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

□

Ejemplos:

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

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

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

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

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

  $$24^{13^{1521}} \equiv 2^{13^{1521}} \pmod{11}.$$

  Como $11 \nmid 2$, necesitamos calcular $r_{10}(13^{1521})$:

  $$13^{1521} \equiv 3^{1521} \equiv (3^2)^{760}\,3 \equiv (-1)^{760}\,3 \equiv 3 \pmod{10}.$$

  Por lo tanto $r_{10}(13^{1521}) = 3$, y

  $$2^{13^{1521}} \equiv 2^3 \equiv 8 \pmod{11},$$

  es decir $r_{11}(24^{13^{1521}}) = 8$.

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

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

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

  Se concluye que $4^n \equiv 1 \pmod{7} \iff n \equiv 0 \pmod{6}$ o $n \equiv 3 \pmod{6}$, es decir:

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

- Probar que $\forall\ a \in \mathbb{Z},\ 7 \mid a^{362} - a^{62}$:

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

$$\begin{aligned} 7 \mid a &\Longrightarrow a^{362} \equiv 0 \pmod 7 \ \text{ y } \ a^{62} \equiv 0 \pmod 7 \\ &\Longrightarrow a^{362} \equiv a^{62} \pmod 7, \\ 7 \nmid a &\Longrightarrow a^{362} \equiv a^{2} \pmod 7 \ \text{ y } \ a^{62} \equiv a^{2} \pmod 7 \\ &\Longrightarrow a^{362} \equiv a^{62} \pmod 7. \end{aligned}$$

  Por lo tanto, en ambos casos, $a^{362} \equiv a^{62} \pmod 7$.

- Calcular el 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 fuera necesario el PTF) y luego combinar los resultados por medio del TCR.

  - $r_2(n)$:
$$3^{2^{25}} \equiv 1^{2^{25}} \equiv 1 \pmod 2.$$
  - $r_3(n)$:
$$3^{2^{25}} \equiv 0^{2^{25}} \equiv 0 \pmod 3.$$
  - $r_5(n)$:
    Por el PTF (Consecuencia 5.4.4), 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.
$$\begin{aligned} 2^{25} &\underset{\text{PTF},3\nmid 2}{\equiv} 2^{r_2(25)} \equiv 2^1 \equiv 2 \pmod 3 \quad \text{y} \quad 2^{25} \equiv 0 \pmod 4 \\ &\underset{\text{TCR}}{\Longrightarrow} \ 2^{25} \equiv 8 \pmod{12}. \end{aligned}$$
    Así,
$$3^{2^{25}} \equiv 3^{r_{12}(2^{25})} \equiv 3^8 \equiv (3^3)^2 \cdot 3^2 \equiv 9 \pmod{13}.$$

  Podemos ahora calcular $r_{390}(3^{2^{25}})$ por medio del TCR:

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

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

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

  Como $55 = 5 \cdot 11$, para $b \in \mathbb{Z}$ cualquiera, el valor de $(b : 55)$ puede ser 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 $a \in \mathbb{Z}$, $11 \mid 12\,a^{41} - a^{31} - a$ y $5 \nmid 12\,a^{41} - a^{31} - a$:

  - Para el 11:

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

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

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

    Por lo tanto

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

  - Para el 5:

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

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

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

    Por lo tanto

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

  Se concluye aplicando el TCR:

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

- Determinar todos los $a \in \mathbb{Z}$ tales que

$$a \equiv 1 \pmod 4 \quad \text{y} \quad (11\,a + 3 \cdot 2^{150} : 3\,a - 2^{151}) = 31.$$

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

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

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

Ahora bien,

$$d \mid 31 \cdot 2^{150} \ \text{ y } \ d \mid 31 \cdot a \iff d \mid (31 \cdot 2^{150} : 31 \cdot a) = 31\,(2^{150} : a) = 31$$

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

$$\begin{aligned} 31 \mid 11\,a + 3 \cdot 2^{150} &\iff 11\,a + 3 \cdot 2^{150} \equiv 0 \pmod{31} \\ &\underset{\text{PTF}}{\iff} 11\,a + 3 \cdot 2^{r_{30}(150)} \equiv 0 \pmod{31} \\ &\iff 11\,a + 3 \equiv 0 \pmod{31} \\ &\iff a \equiv 11 \pmod{31}. \end{aligned}$$

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

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

Se concluye el ejercicio con el TCR:

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

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

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

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

$$15 \mid 5\,a \implies 3 \mid a, \quad \text{y por lo tanto } 3^2 \mid a^{18}$$
$$15 \mid 7\,b \underset{15\perp 7}{\iff} 15 \mid b, \quad \text{y por lo tanto } 3^2 \mid b^{115}.$$

Luego

$$5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 8^{40} \equiv (-1)^{40} \equiv 1 \pmod{3^2}.$$

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

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

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

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

Se concluye aplicando el TCR:

$$\begin{cases} 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 1 \pmod{3^2} \\ 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 1 \pmod 5 \\ 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 6 \pmod 7 \end{cases} \iff 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 181 \pmod{315}.$$

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

5.4.1 Tests probabilísticos de primalidad.

El PTF permite obtener directamente tests de primalidad, que funcionan muy rápido y son muy utilizados constantemente. Estos tests funcionan de la manera siguiente: dado un número $m \in \mathbb{N}$ del cual se quiere averiguar si es un número primo, se elije al azar un número a, $1 < a < m$, y se hace un test (generalmente se chequea una igualdad que involucra a m y a, asociada al test). Si la igualdad no se satisface, es que m es un número compuesto (y a es un testigo del hecho que m es compuesto). Si la igualdad se satisface, m puede ser primo o compuesto. Repitiendo el test eligiendo al azar otro número a se puede mejorar la probabilidad de éxito del test. La ventaja de estos tests es que son rápidos (más rápidos obviamente que la Criba de Eratóstenes y cualquiera de su variantes, pero también que el test de primalidad AKS que comentamos antes, cuya mejor versión hace del orden de (algo más que) $\log(m)^6$ cuentas), y los números que los pasan pueden ser considerados primos "a efectos prácticos". En la próxima sección,

veremos el sistema criptográfico RSA que necesita generar números primos muy grandes, en forma rápida...

Vamos a describir aquí dos tests probabilísticos de primalidad sencillos, que usan sólo herramientas conocidas, más que nada para dar un sabor de cómo funcionan.

- **El test del Pequeño Teorema de Fermat:** ¿$a^{m-1} \equiv 1 \pmod{m}$?

  Dado $m \in \mathbb{N}$, $m \geq 2$, se elige al azar a, $1 < a < m$, y se calcula $a^{m-1} \pmod{m}$.

  - Si $a^{m-1} \not\equiv 1 \pmod{m}$, claramente m no puede ser primo, luego es compuesto.
  - Si $a^{m-1} \equiv 1 \pmod{m}$, m es declarado "probablemente primo": puede ser primo o compuesto.

  Por ejemplo, para $m = 341 = 11 \cdot 31$, es fácil ver que para $a = 2$, $2^{340} \equiv 1 \pmod{341}$, y sin embargo m es compuesto.

  Lo interesante es que por ejemplo hay solamente 21853 números compuestos menores que $25 \cdot 10^9$ que pasan el test para $a = 2$, o sea menos que $1/1000000$... Este test funciona como una buena limpieza inicial de números compuestos.

  Lo malo es que como sabemos existen números compuestos, los seudoprimos o números de Carmichael, que pasan el test para (casi) cualquier elección de $a < m$ (salvo que uno caiga justo en uno de los divisores de m). O sea que aún eligiendo al azar distintos valores de a no aumentamos la probabilidad de obtener un resultado correcto para esos números, y hay infinitos números de Carmichael!

- **El test de primalidad de Miller-Rabin.**

  Este test fue originalmente propuesto por Gary Miller en 1976, pero dependía de un importante conjetura matemática no probada aún, la *Hipótesis de Riemann*. Fue modificado en 1980 por Michael Rabin para volverlo probabilístico.

  Se basa en el resultado siguiente.

  Proposición 5.4.5. *Sea $p > 2$ un número primo, y sea $p - 1 = 2^s d$ donde d es un número impar. Sea $a \in \mathbb{N}$, $1 \leq a < p$. Entonces se tiene que $a^{2^r d} \equiv -1 \pmod{p}$ para algún r con $s - 1 \geq r \geq 0$ o sino $a^d \equiv 1 \pmod{p}$.*

  Demostración. Sabemos por el PTF que $a^{p-1} = a^{2^s d} \equiv 1 \pmod{p}$ pues $a < p$ implica $a \perp p$. Como $p - 1$ es par, se tiene $s \geq 1$ y por

Miller

Rabin

lo tanto

$$a^{2^s d} - 1 = (a^{2^{s-1} d})^2 - 1 = (a^{2^{s-1} d} + 1)(a^{2^{s-1} d} - 1).$$

Luego

$$p \mid a^{2^s d} - 1 \implies p \mid a^{2^{s-1} d} + 1 \text{ o } p \mid a^{2^{s-1} d} - 1,$$

por ser p primo. Es decir

$$a^{p-1} = a^{2^s d} \equiv 1 \pmod{p} \implies a^{2^{s-1} d} \equiv -1 \pmod{p} \text{ o } a^{2^{s-1} d} \equiv 1 \pmod{p}.$$

Si $a^{2^{s-1} d} \equiv -1 \pmod{p}$ ya está. Sino, $a^{2^{s-1} d} \equiv 1 \pmod{p}$ y podemos repetir el procedimiento (si $s - 1 \geq 1$):

$$a^{2^{s-2} d} \equiv -1 \pmod{p} \text{ o } a^{2^{s-2} d} \equiv 1 \pmod{p}.$$

Nuevamente, si $a^{2^{s-2} d} \equiv -1 \pmod{p}$ ya está. Sino, $a^{2^{s-2} d} \equiv 1 \pmod{p}$ y repetimos el procedimiento, hasta llegar eventualmente a $a^{2d} \equiv 1 \pmod{p}$. Lo que implica

$$a^d \equiv -1 \pmod{p} \text{ o } a^d \equiv 1 \pmod{p}.$$

□

El test de primalidad de Miller-Rabin funciona negando la conclusión de esta proposición.

Dado $m \in \mathbb{N}$, m impar tal que $m - 1 = 2^s d$, se elige al azar $a \in \mathbb{N}$, $1 < a < m$, y se calcula $a^d \pmod{m}$ y $a^{2^r d} \pmod{m}$ para $0 \leq r \leq s - 1$.

- Si $a^d \not\equiv 1 \pmod{m}$ y $a^{2^r d} \not\equiv -1 \pmod{m}$ para $0 \leq r \leq s - 1$, entonces m es compuesto.
- Si $a^d \equiv 1 \pmod{m}$ o $\exists r$, $0 \leq r \leq s - 1$, tal que $a^{2^r d} \equiv -1 \pmod{m}$, entonces am es *probablemente primo*, o sea puede existir la posibilidad que sea compuesto pero "en general" será primo.

Por ejemplo para $m = 221 = 13 \cdot 17$, si se toma $a = 174$, resulta que m pasa el test y sin embargo m es compuesto. Sin embargo en este caso si se toma $a = 137$, a no pasa el test y se concluye que 221 es compuesto.

Lo interesante y que hace funcionar muy bien este test probabilístico, es que para cada número impar compuesto m hay al menos un testigo a para el cual el test falla, o sea que prueba que a es compuesto (en ese sentido es mucho mejor que el test descrito arriba). Es más, para cada m compuesto, se puede probar que hay del orden de $3m/4$ testigos a que prueban que m es compuesto. Por lo tanto, al repetir el test se aumenta la probabilidad de dar una respuesta correcta. Lo malo es que no se sabe a priori, dado un m, quiénes son esos testigos...

Si se corre este algoritmo k veces, la cantidad de cuentas que se hace es el orden de $k \log^3 m$ (lineal en esa cantidad) y la probabilidad de que un número sea declarado probablemente primo siendo compuesto es menor que $1/4^k$.

5.5 El sistema criptográfico RSA.

Este sistema criptográfico, que fue introducido en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, es un sistema de clave pública-clave privada y de firma digital, que se basa en una generalización del Pequeño Teorema de Fermat para números de la forma $n = p \cdot q$, donde p y q son dos primos distintos.

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 bloquecitos si hace falta.

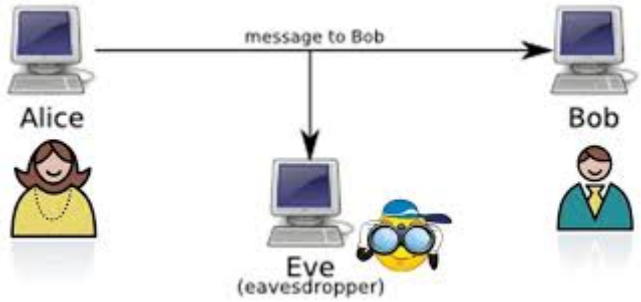
¿Qué se entiende por clave pública-clave privada? Un señor, Bob, va a generar dos claves, una que se llama *clave privada* que va a ser conocida sólo por él, y la otra, que se llama *clave pública* que va a distribuir al resto del mundo. Tanto la clave pública como la privada sirven para codificar o decodificar mensajes, pero una sola de ellas no puede hacer las dos cosas


Rivest


Shamir


Adleman

a la vez. Cuando 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, por ejemplo Eve, 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.

Para seguir con esto, necesitamos esta pequeña generalización del pequeño teorema de Fermat, que es un caso particular del teorema de Euler mencionado previamente.

Proposición 5.5.1. (PTF para $p\,q$.)

Sean p, q dos primos positivos distintos, y sea $a \in \mathbb{Z}$ coprimo con $p\,q$. Entonces

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

Y por lo tanto, $\forall\, m \in \mathbb{N}$,

$$m \equiv r \ \big(\mathrm{mod}\,(p-1)(q-1)\big) \implies a^m \equiv a^r \pmod{p\,q}.$$

Demostración. Como a es coprimo con $p\,q$, es en particular coprimo con p y con q. Luego, por el PTF,

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{y} \quad a^{q-1} \equiv 1 \pmod{q}.$$

Por lo tanto,

$$\begin{aligned} a^{(p-1)(q-1)} &= \big(a^{p-1}\big)^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p} \quad \text{y} \\ a^{(p-1)(q-1)} &= \big(a^{q-1}\big)^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{q}. \end{aligned}$$

Por lo tanto, por la Proposición 5.3.1,

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

La segunda afirmación se prueba como el Corolario 5.4.4:

$$\begin{aligned} &m = k\,(p-1)(q-1) + r \\ &\quad \Longrightarrow\ a^m = a^{k(p-1)(q-1)+r} = (a^{(p-1)(q-1)})^k\,a^r \equiv 1^k\,a^r \equiv a^r \pmod{p\,q}. \end{aligned}$$

□

¿Cómo funciona el sistema criptográfico RSA?

- Bob elige dos primos distintos muy grandes p y q (hay generadores de primos para eso) y los multiplica entre sí creándose el número $n = p\,q$. (Como ya se comentó, una vez multiplicados los dos primos, es muy costoso recuperarlos, es decir es muy costoso factorizar n.)

- Luego elige e coprimo con $(p-1)\,(q-1)$, con $1 \leq e \leq (p-1)\,(q-1)$. (Lo puede hacer ya que conoce p y q, por lo tanto puede calcular $p-1$ y $q-1$, y el producto $(p-1)(q-1)$, y verificar si e es coprimo con $(p-1)(q-1)$ se hace mediante el algoritmo de Euclides.)

- Finalmente calcula d con $1 \leq d \leq (p-1)\,(q-1)$ tal que $e\,d \equiv 1 \pmod{(p-1)(q-1)}$. (Como $e \perp (p-1)(q-1)$ la ecuación tiene solución, que se puede calcular utilizando el algoritmo de Euclides, pero para calcular d se necesita conocer $(p-1)(q-1)$, o sea p y q.)

Ahora fija las claves:

- Clave privada de Bob: (n, e).

- Clave pública de Bob: (n, d).

Observación 5.5.2. (Propiedad clave por la cual funciona el algoritmo RSA.)

Sean $n = p \cdot q$, d, e como arriba. Sea $a \in \mathbb{N}$ con $1 \leq a < n$. Entonces

$$a^{e\,d} \equiv a \pmod{n}.$$

Demostración.

- Si $a \perp p\,q$, entonces $a^{(p-1)(q-1)} \equiv 1 \pmod{n}$ y luego por la Proposición 5.5.1,
$$a^{e\,d} \equiv a^1 \pmod{n}.$$

- Si $p \mid a$ pero $q \nmid a$, entonces

$$\begin{aligned} a \equiv 0 \pmod{p} &\implies a^{e\,d} \equiv 0 \pmod{p} \implies a^{e\,d} \equiv a \pmod{p} \\ a^{q-1} \equiv 1 \pmod{q} &\implies a^{(p-1)(q-1)} \equiv 1 \pmod{q} \\ &\implies a^{e\,d} \equiv a^1 \equiv a \pmod{q}. \end{aligned}$$

  Por lo tanto, $a^{e\,d} \equiv a \pmod{p\,q}$.

  Análogamente se prueba que $a^{e\,d} \equiv a \pmod{p\,q}$ para $p \nmid a$ pero $q \mid a$.

- Si $p \mid a$ y $q \mid a$, entonces

$$a \equiv 0 \pmod{p\,q} \implies a^{e\,d} \equiv 0 \pmod{p\,q} \implies a^{e\,d} \equiv a \pmod{p\,q}.$$

□

Mecanismo del sistema criptográfico RSA:

Dado el mensaje a, $0 \leq a < n$, notemos por $C(a)$ el mensaje encriptado.

1. Caso 1: Alice le quiere mandar a Bob el mensaje a y que solo Bob lo entienda: le manda el mensaje encriptado $C(a)$, donde:

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

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

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

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

2. Caso 2: Bob le quiere mandar el mensaje a "firmado por él" al resto del mundo: manda el mensaje encriptado $C(a)$ donde

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

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

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

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

5.6 El anillo $\mathbb{Z}/m\mathbb{Z}$ y el cuerpo $\mathbb{Z}/p\mathbb{Z}$.

5.6.1 El anillo $\mathbb{Z}/m\mathbb{Z}$.

Ejemplos:

- Consideremos primero la relación de equivalencia congruencia módulo 2, y sus clases de equivalencia. Sabemos que $a \equiv b \pmod{2} \Leftrightarrow r_2(a) = r_2(b)$: todos los pares son congruentes entre sí y todos los impares son congruentes entre sí. Por lo tanto, hay dos clases de equivalencia, determinadas por los dos restos módulo 2, que son 0 y 1:

$$\overline{0} = \{a \in \mathbb{Z} : \ a \equiv 0 \pmod{2}\} = \{a \in \mathbb{Z} : \ a \text{ es par }\},$$
$$\overline{1} = \{a \in \mathbb{Z} : \ a \text{ es impar }\}.$$

Así, $\mathbb{Z} = \overline{0} \cup \overline{1}$ es la partición de $\mathbb{Z}$ asociada a la relación de equivalencia *congruencia módulo* 2. Pero más aún, es claro que la suma de pares siempre da par, la suma de impares siempre da par, la suma de un par y un impar siempre da impar, independientemente de qué par o qué impar se elija. O sea se puede considerar la operación suma en el conjunto $\{\overline{0}, \overline{1}\}$ de las clases de equivalencia:

$$\overline{0} + \overline{0} = \overline{0}, \quad \overline{1} + \overline{0} = \overline{1}, \quad \overline{0} + \overline{1} = \overline{1}, \quad \overline{1} + \overline{1} = \overline{0}.$$

Lo mismo ocurre con el producto: multiplicar un par por cualquier número siempre da par, y multiplicar impar por impar da impar. Así:

$$\overline{0} \cdot \overline{0} = \overline{0}, \quad \overline{1} \cdot \overline{0} = \overline{0}, \quad \overline{0} \cdot \overline{1} = \overline{0}, \quad \overline{1} \cdot \overline{1} = \overline{1}.$$

Estas operaciones $+$ y $\cdot$ en el conjunto $\{\overline{0}, \overline{1}\}$ de clases de equivalencia satisfacen todas las propiedades de anillo conmutativo: la suma es

conmutativa, asociativa, hay un elemento neutro que es el $\overline{0}$ y todo elemento tiene opuesto aditivo: $-\overline{0} = \overline{0}, -\overline{1} = \overline{1}$, o sea $(\{\overline{0}, \overline{1}\}, +)$ es un grupo abeliano. El producto es conmutativo, asociativo, hay un elemento neutro que es el $\overline{1}$. Y además el producto es distributivo sobre la suma. Por lo tanto $(\{\overline{0}, \overline{1}\}, +, \cdot)$ es un anillo conmutativo. Este conjunto de restos módulo 2 se nota $\mathbb{Z}/2\mathbb{Z}$. O sea $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ es un anillo conmutativo con la suma y el producto.

Más aún, en este caso, todo elemento distinto del $\overline{0}$, es decir el $\overline{1}$, tiene inverso multiplicativo pues $\overline{1} \cdot \overline{1} = \overline{1}$ implica $\overline{1}^{-1} = \overline{1}$. Luego $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ es más que un anillo conmutativo, es un *cuerpo*, al igual que $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Pero es un cuerpo finito ¡con solo 2 elementos!

- Miremos ahora la relación de equivalencia congruencia módulo 6: Sabemos que $a \in \mathbb{Z}$ es congruente módulo 6 a su resto $r_6(a)$, y que dos restos distintos no son congruentes entre sí. Dicho de otra manera, en $\mathbb{Z}$ se tienen 6 clases de equivalencia mod 6:

$$\begin{aligned}
\overline{0} &= \{a \in \mathbb{Z} : \ a \equiv 0 \pmod 6\} &&= \{\dots, -12, -6, 0, 6, 12, \dots\} \\
\overline{1} &= \{a \in \mathbb{Z} : \ a \equiv 1 \pmod 6\} &&= \{\dots, -11, -5, 1, 7, 13, \dots\} \\
\overline{2} &= \{a \in \mathbb{Z} : \ a \equiv 2 \pmod 6\} &&= \{\dots, -10, -4, 2, 8, 14, \dots\} \\
\overline{3} &= \{a \in \mathbb{Z} : \ a \equiv 3 \pmod 6\} &&= \{\dots, -9, -3, 3, 9, 15, \dots\} \\
\overline{4} &= \{a \in \mathbb{Z} : \ a \equiv 4 \pmod 6\} &&= \{\dots, -8, -2, 4, 10, 16, \dots\} \\
\overline{5} &= \{a \in \mathbb{Z} : \ a \equiv 5 \pmod 6\} &&= \{\dots, -7, -1, 5, 11, 17, \dots\}
\end{aligned}$$

y $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4} \cup \overline{5}$ es la partición de $\mathbb{Z}$ asociada a esta relación de equivalencia. Notemos

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

También sabemos que si $a \in \overline{r_1}$ y $b \in \overline{r}_2$, eso significa que $a \equiv r_1 \pmod 6$ y $b \equiv r_2 \pmod 6$, y por lo tanto, $a + b \equiv r_1 + r_2 \pmod 6$ y $a \cdot b \equiv r_1 \cdot r_2 \pmod 6$. Es decir, $a + b \in \overline{r_1 + r_2}$ y $a \cdot b \in \overline{r_1 \cdot r_2}$.

Así tiene sentido considerar en el conjunto de clases de restos $\mathbb{Z}/6\mathbb{Z}$ las operaciones suma y producto entre clases dadas por las tablas siguientes:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{2}$	$\overline{4}$

y

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(Aquí no importa en qué sentido se hacen las operaciones: si columna + fila o fila + columna, etc., pues son claramente conmutativas.) Estas operaciones hacen de $(\mathbb{Z}/6\mathbb{Z}), +, \cdot)$ un anillo conmutativo ¡con

6 elementos! El elemento neutro para la suma es el $\overline{0}$ (notemos que $-\overline{0}=\overline{0}$, $-\overline{1}=\overline{5}$, $-\overline{2}=\overline{4}$, $-\overline{3}=\overline{3}$, $-\overline{4}=\overline{2}$ y $-\overline{5}=\overline{1}$) y el elemento neutro para el producto es $\overline{1}$. Pero en este caso $\mathbb{Z}/6\mathbb{Z}$ no es un cuerpo, pues por ejemplo $\overline{2}$ no tiene inverso multiplicativo: no existe otro elemento tal que multiplicado por él de $\overline{1}$.

Enunciemos ahora sin demostrar todos los detalles el resultado en el caso general.

Teorema 5.6.1. (El anillo $\mathbb{Z}/m\mathbb{Z}$.)

Sea $m \in \mathbb{N}$ y consideremos en $\mathbb{Z}$ la relación de equivalencia congruencia módulo m. *Entonces*

1. *Sea $0 \leq r < m$. La clase de equivalencia $\overline{r}$ de r es*

$$\overline{r} = \{a \in \mathbb{Z} : \ a \equiv r \pmod{m}\}$$

y

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{m-1}$$

es la partición de $\mathbb{Z}$ asociada a esta relación de equivalencia.

2. *Notemos*

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

y sean $+$ y $\cdot$ las operaciones en $\mathbb{Z}/m\mathbb{Z}$ definidas por

$$\overline{r}_1 + \overline{r}_2 = \overline{r_1 + r_2} \quad y \quad \overline{r}_1 \cdot \overline{r}_2 = \overline{r_1 \cdot r_2}, \quad para \quad 0 \leq r_1, r_2 < m.$$

Entonces $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

5.6.2 El cuerpo $\mathbb{Z}/p\mathbb{Z}$.

Como vimos en el Corolario 5.2.4, cuando a y m son coprimos, la ecuación de congruencia $a \cdot X \equiv c \pmod{m}$ siempre tiene solución independientemente de quién sea c. En particular tiene solución para $c = 1$. Esto implica directamente el resultado siguiente:

Proposición 5.6.2. (La ecuación de congruencia $a \cdot X \equiv 1 \pmod{m}$.)

Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$. Entonces la ecuación de congruencia $a \cdot X \equiv 1 \pmod{m}$ tiene soluciones si y solo si $a \perp m$. En ese caso, hay una única solución x_0 con $1 \leq x_0 < m$.

Demostración. Cuando $a \not\perp m$, no hay solución pues $(a : m) \nmid 1$.

Por el contrario, cuando $a \perp m$, la ecuación tiene solución. Todas las soluciones son de la forma $X \equiv x_0 \pmod{m}$ donde x_0 es la única solución

que satisface $0 \leq x_0 < m$. Pero no puede ser $x_0 = 0$ pues sino se tendría $a \cdot 0 \equiv 1 \pmod{m}$, contradicción! Luego $1 \leq x_0 < m$.

□

Ejemplo: Soluciones de la ecuación $a \cdot X \equiv 1 \pmod{10}$ para $a = 1, 3, 7, 9$.

- $1 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 1 \pmod{10}$ $(x_0 = 1)$.
- $3 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 7 \pmod{10}$ $(x_0 = 7)$.
- $7 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 3 \pmod{10}$ $(x_0 = 3)$.
- $9 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 9 \pmod{10}$ $(x_0 = 9)$.

Apliquemos la Proposición 5.6.2 al caso en que m es un número primo p.

Corolario 5.6.3. (La ecuación de congruencia $a \cdot X \equiv 1 \pmod{p}$.)

Sea p un primo positivo y sea $a \in \mathbb{N}$ tal que $p \nmid a$. Entonces la ecuación de congruencia $a \cdot X \equiv 1 \pmod{p}$ tiene una única solución x_0 con $1 \leq x_0 < p$.

Ejemplo: Soluciones de la ecuación $a \cdot X \equiv 1 \pmod{7}$ para $a = 1, 2, 3, 4, 5, 6$.

- $1 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 1 \pmod{7}$ $(x_0 = 1)$.
- $2 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 4 \pmod{7}$ $(x_0 = 4)$.
- $3 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 5 \pmod{7}$ $(x_0 = 5)$.
- $4 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 2 \pmod{7}$ $(x_0 = 2)$.
- $5 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 3 \pmod{7}$ $(x_0 = 3)$.
- $6 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 6 \pmod{7}$ $(x_0 = 6)$.

La Proposición 5.6.2 permite también determinar directamente quiénes son los elementos inversibles del anillo $\mathbb{Z}/m\mathbb{Z}$.

Corolario 5.6.4. (Los elementos inversibles de $\mathbb{Z}/m\mathbb{Z}$.)

Sea $m \in \mathbb{N}$, y sea $\overline{r} \in \mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

Entonces, $\overline{r}$ es inversible en $\mathbb{Z}/m\mathbb{Z}$ si y solo si $r \perp m$.

Demostración. Se tiene $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. El elemento $\overline{r}$ es inversible en $\mathbb{Z}/m\mathbb{Z}$ si y solo si existe $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\overline{r} \cdot \overline{x} = \overline{1}$. Pero por la definición del producto en $\mathbb{Z}/m\mathbb{Z}$, $\overline{r} \cdot \overline{x} = \overline{r \cdot x}$, luego hay que determinar x tal que $\overline{r \cdot x} = \overline{1}$, o lo que es lo mismo $r \cdot x \equiv 1 \pmod{m}$. Se concluye por la Proposición 5.6.2. □

Ejemplo: En $\mathbb{Z}/10\mathbb{Z}$,

$$\overline{1}^{\,-1} = \overline{1},\ \overline{3}^{\,-1} = \overline{7},\ \overline{7}^{\,-1} = \overline{3} \text{ y } \overline{9}^{\,-1} = \overline{9}.$$

Traduciendo el Corolario 5.6.4 al anillo $\mathbb{Z}/p\mathbb{Z}$ de enteros módulo p, se obtiene directamente el importante resultado siguiente.

Teorema 5.6.5. ($\mathbb{Z}/p\mathbb{Z}$ es un cuerpo.)

Sea p un primo positivo. Entonces $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un cuerpo.

Es decir, además de ser un anillo conmutativo con la suma y el producto definidos en el Teorema 5.6.1, se satisface que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ es inversible.

Ejemplo: En $\mathbb{Z}/7\mathbb{Z}$,

$$\overline{1}^{\,-1} = \overline{1},\ \overline{2}^{\,-1} = \overline{4},\ \overline{3}^{\,-1} = \overline{5},\ \overline{4}^{\,-1} = \overline{2},\ \overline{5}^{\,-1} = \overline{3} \text{ y } \overline{6}^{\,-1} = \overline{6}.$$

5.7 Ejercicios.

Ecuaciones diofánticas y de congruencia

1. Determinar, cuando existan, todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen

   i) $7a + 11b = 10$
   ii) $20a + 16b = 36$
   iii) $39a - 24b = 6$
   iv) $1555a - 300b = 11$

2. Determinar todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen simultáneamente $4 \mid a$, $8 \mid b$ y $33a + 9b = 120$.

3. Si se sabe que cada unidad de un cierto producto A cuesta 39 pesos y que cada unidad de un cierto producto B cuesta 48 pesos, ¿cuántas unidades de cada producto se pueden comprar gastando exactamente 135 pesos?

4. Hallar, cuando existan, todas las soluciones de las siguientes ecuaciones de congruencia

   i) $17X \equiv 3\ (11)$
   ii) $56X \equiv 28\ (35)$
   iii) $56X \equiv 2\ (884)$
   iv) $78X \equiv 30\ (12126)$

5. Hallar todos los $(a, b) \in \mathbb{Z}^2$ tales que $b \equiv 2a \pmod 5$ y $28a + 10b = 26$.