Capítulo 8

Ecuaciones diofánticas

§8.1. Ecuaciones diofánticas

8.1.1. En el sentido más general, una ***ecuación diofántica*** es una ecuación en la que buscamos soluciones con valores enteros. El nombre de estas ecuaciones recuerda a Diofanto de Alejandría, conocido como "el padre del álgebra" y autor de una serie de libros, la *Arithmetica*, sobre la solución de ecuaciones algebraicas.

8.1.2. Vamos algunos ejemplos.

(*a*) *Ecuaciones diofánticas lineales.* Si $r \in \mathbb{N}$ y $a_1, \ldots, a_r, b \in \mathbb{Z}$, la ***ecuación diofánticas lineal*** consiste en decidir si existen r-uplas $(x_1, \ldots, x_r)$ de enteros tales que

$$a_1x_1 + \cdots + a_rx_r = b$$

y, cuando ese es el caso, encontrarlos.

(*b*) *La ecuación de Pitágoras.* En este caso, buscamos las ternas (x, y, z) de enteros tales que

$$x^2 + y^2 = z^2,$$

a las que llamamos ternas pitagóricas.

(*c*) *La ecuación de Pell.* Fijamos $n \in \mathbb{N}$. El problema de encontrar enteros x e y tales que

$$x^2 - ny^2 = 1$$

es una ecuación diofántica, la *ecuación de Pell*, por John Pell, aunque esta ecuación fue estudiada mucho tiempo antes — de hecho, la ecuación se conoce con el nombre de Pell porque Leonhard Euler equivocadamente atribuyó a este un método para su solución que fue en realidad fue desarrollado por William Brouncker.

(*d*) *La ecuación de Fermat.* Fijemos un entero positivo n. La ***ecuación de Fermat de exponente n*** es el problema de encontrar enteros x, y y z tales que

$$x^n + y^n = z^n. \tag{1}$$

Famosamente Fermat hizo la siguiente anotación en un margen de su copia del libro de Diofanto, al lado de donde está enunciado el Problema VIII, que es precisamente el de la ecuación de Pitágoras, que mencionamos recién:

> *Es imposible separar un cubo en dos cubos, o una potencia cuarta en dos potencias cuartas, o en general cualquier potencia más alta que la segunda en dos potencias similares. He descubierto una demostración verdaderamente maravillosa de esto, pero este margen es demaciado angosto para contenerla.*

Lo que ahí afirma Fermat es que la ecuación (1) no tiene soluciones (salvo las "triviales") cuando $n \geq 3$. Hoy hay acuerdo en que Fermat no tenía ninguna prueba de esto y fue recién en 1993 que Andrew Wiles pudo probar que la afirmación de Fermat es cierta —aunque hubo muchos resultados parciales antes.

(*e*) *La ecuación Ramanujan–Nagell.* Así es conocido el problema de encontrar enteros x y n tales que

$$2^n - 7 = x^2.$$

Notemos que en esta ecuación, a diferencia de todas las anteriores, hay una incógnita que aparece como un exponente. El problema fue planteado originalmente por Srinivasa Ramanujan en 1913, quien además conjeturó que hay exactamente diez soluciones, y esta conjetura fue probada por Trygve Nagell en 1948. Las diez soluciones (x, n) de la ecuación son los pares

$$(\pm 1, 3), \qquad (\pm 3, 4), \qquad (\pm 5, 5), \qquad (\pm 11, 7), \qquad (\pm 181, 15).$$

La ecuación de Ramanujan–Nagell parece a primera vista bastante exótica y antojadiza, pero aparece en realidad en varios contextos. Por ejemplo, es equivalente al problema de encontrar los números de Mersenne, es decir, de la forma $2^a - 1$ con $a \in \mathbb{N}_0$, que son triangulares, esto es, de la forma $b(b+1)/2$ con $b \in \mathbb{N}_0$. En efecto,

$$\begin{aligned} 2^a - 1 = \frac{b(b+1)}{2} &\iff 8(2^a - 1) = 4b(b+1) \\ &\iff 2^{a+3} - 8 = 4b^2 + 4b \\ &\iff 2^{a+3} - 7 = 4b^2 + 4b + 1 \\ &\iff 2^{a+3} - 7 = (2b+1)^2. \end{aligned}$$

Esto nos dice que el número de Mersenne $2^a - 1$ es igual al número triangular $b(b+1)/2$ si y solamente si el par $(x, n) = (2b+1, a+3)$ es una solución de la ecuación de Ramanujan–Nagell. Por supuesto, el problema de encontrar números de Mersenne que son triangulares no parece mucho menos antojadizo que la ecuación de Ramanujan–Nagell! En el trabajo [BS1956] de Georges Browkin y André Schinzel hay un estudio de este problema.

De todas formas, la ecuación de Ramanujan–Nagell aparece de forma natural en el estudio de los códigos con corrección de errores [SS1959], en teoría de álgebra diferencial [Mea1973] y en computación cuántica [PR2013]. No podemos aquí explicar cómo.

§8.2. Ecuaciones lineales con dos incógnitas

8.2.1. Como dijimos, una ***ecuación diofántica lineal*** es un problema de la siguiente forma: dados $r \in \mathbb{N}$ y $a_1, \ldots, a_r, b \in \mathbb{Z}$, decidir si hay r-uplas de enteros $(x_1, \ldots, x_r)$ tales que

$$a_1x_1 + \cdots a_rx_r = b$$

y, si ese es el caso, encontrarlas. Supondremos siempre que todos los coeficientes $a_1, \ldots, a_r$ son no nulos, ya que esto no nos restringe en nada. Nuestro objetivo en esta sección es resolver este problema completamente.

8.2.2. Empecemos por el caso más sencillo: aquel en que $r = 1$ y hay, por lo tanto, una sola incógnita. Así, tenemos dos enteros a y b y queremos determinar si existen enteros x tales que $ax = b$ y, cuando los hay, encontrarlos. Reconocemos inmediatamente aquí el problema de la división entera, que ya sabemos resolver:

Proposición. *Sean a y b dos enteros y supongamos que $a \neq 0$. Consideremos el problema de encontrar enteros x tales que*

$$ax = b.$$

Hay soluciones si y solamente si a divide a b. Si ese es el caso, entonces hay exactamente una solución, que es $x = b/a$.

Demostración. Si hay una solución al problema, esto es, si existe un entero x tal que $ax = b$, entonces a divide a b simplemente por definición: esto muestra que la condición del enunciado es necesaria para que exista una solución. Recíprocamente, si suponemos que esa condición se cumple, de manera que a divide a b y existe un entero c tal que $ac = b$, entonces claramente ese

entero c, que es b/a, es una solución a la ecuación. Esto muestra que la condición es también suficiente.

Supongamos ahora que x y x' son dos soluciones a la ecuación. En ese caso, tenemos que $ax = b = ax'$ y, por lo tanto, $a(x-x') = 0$. Como a no es nulo, esto es solo posible si $x-x' = 0$, esto es, si $x = x'$. Vemos así que cuando $a \neq 0$ y hay soluciones, hay de hecho una única solución. □

8.2.3. Consideremos ahora el caso en que hay dos variables, es decir, en que $r = 2$ en la situación de 8.2.1. Así, tenemos tres enteros a, b y c con $ab \neq 0$ y buscamos pares ordenados (x, y) de enteros tales que

$$ax + by = c.$$

Empezamos analizando el ***caso homogéneo***, es decir, aquel en el que $c = 0$.

Proposición. *Sean a y b dos enteros no nulos, sea $d \coloneqq \mathsf{mcd}(a, b)$, y sean a' y b' los enteros tales que $a = da'$ y $b = db'$. Las soluciones de la ecuación*

$$ax + by = 0, \tag{2}$$

son los pares de la forma $(tb', -ta')$ con $t \in \mathbb{Z}$.

Demostración. Supongamos que (x, y) es una solución de la ecuación (2), de manera que

$$0 = ax + by = da'x + db'y = d(a'x + b'y).$$

Como $d \neq 0$, esto nos dice que $a'x + b'y = 0$, así que $b'y = -a'x$. En particular, el entero b' divide a $-a'x$ y, como es coprimo con a', divide a x: existe entonces un entero t tal que $x = tb'$. Usando esto vemos que también $b'y = -a'x = -a'b't$, así que, como $b' \neq 0$, es $y = -a't$. Se sigue de esto que todas las soluciones de la ecuación son de la forma $(tb', -ta')$ con $t \in \mathbb{Z}$.

Por otro lado, si t es un entero, entonces $a \cdot (tb') + b \cdot (-ta') = 0$, así que el par $(tb', -ta')$ es una solución de la ecuación (2). Esto prueba la proposición. □

8.2.4. Podemos enunciar esta proposición de una forma equivalente que es a veces útil. Digamos que un par de enteros (x, y) es ***primitivo*** si $\mathsf{mcd}(x, y) = 1$. Notemos que si (x, y) es un par de enteros cualquiera no simultáneamente nulos y ponemos $d \coloneqq \mathsf{mcd}(x, y)$, entonces hay enteros x' e y' tales que $x = dx'$ e $y = dy'$ y es, por lo tanto, $(x, y) = (dx', dy')$ y el par (x', y') es primitivo: esto nos dice que todo par distinto de $(0, 0)$ es un múltiplo de un par primitivo.

Proposición. *Sean a y b dos enteros no nulos, y sean a' y b' los enteros tales que $a = da'$ y $b = db'$.*

(*i*) *La ecuación*

$$ax + by = 0, \tag{3}$$

tiene exactamente dos soluciones primitivas, $(b', -a')$ *y* $(-b', a')$.

(*ii*) *Si* (x_0, y_0) *es una solución primitiva de esa ecuación, entonces las soluciones de la ecuación son todos los pares de la forma* (tx_0, ty_0) *con* $t \in \mathbb{Z}$.

Demostración. Sabemos de la Proposición 8.2.3 que los pares $(b', -a')$ y $(-b', a')$ son soluciones de la ecuación y, como $\mathsf{mcd}(a', b') = 1$, se trata de soluciones primitivas. Más aún, como a' y b' son no nulos, ya que a y b son no nulos, estas dos soluciones son distintas. Por otro lado, si (x, y) es una solución primitiva de la ecuación (3), entonces esa proposición nos dice que $(x, y) = (tb', -ta')$ para exactamente un entero t, y es

$$1 = \mathsf{mcd}(x, y) = \mathsf{mcd}(tb', -ta') = |t|\,\mathsf{mcd}(b', -a') = |t|,$$

así que (x, y) es o $(b', -a')$ o $(-b', a')$. Esto prueba la primera afirmación de la proposición. La segunda afirmación, por su parte, es ahora consecuencia inmediata de la descripción de las soluciones de la ecuación dada por la Proposición 8.2.3. □

8.2.5. Nos ocupamos ahora del caso general de la ecuación diofántica lineal con dos incógnitas:

Proposición. *Sean* a, b *y* c *tres enteros tales que* $ab \neq 0$ *y consideremos el problema de encontrar pares de enteros* (x, y) *tales que*

$$ax + by = c. \tag{4}$$

(*i*) *Hay soluciones a este problema si y solamente si el entero* $d := \mathsf{mcd}(a, b)$ *divide a* c.

(*ii*) *Si ese es el caso y* a', b', c' *enteros tales que* $ax_0 + by_0 = d$, $a = da'$ *y* $b = db'$, *entonces el par* (x_0c', y_0c') *es una solución de* (4).

(*iii*) *Más aún, si* (x_0, y_0) *es una solución cualquiera de la ecuación* (4), *entonces toda solución esa ecuación es de la forma* $(x_0 + x_1, y_0 + y_1)$ *con* (x_1, y_1) *una y solo una solución de la ecuación homogénea*

$$ax + by = 0. \tag{5}$$

La primera parte de esta proposición nos permite decidir cuándo una ecuación diofánticas lineal no homogénea tiene soluciones. Por otro lado, la segunda nos permite encontrar una solución particular de la ecuación, y la tercera nos dice que si tenemos una solución cualquiera, entonces el problema de resolver la ecuación (4) se reduce al de resolver la ecuación homogénea (5) asociada

— y a este último problema sabemos resolverlo, de acuerdo a la Proposición 8.2.3.

Demostración. Supongamos primero que el problema (4) tiene soluciones y sea (x, y) una de ellas. En ese caso, como d divide a a y a b, tenemos que $d \mid ax + by = c$: esto muestra que la condición del enunciado es necesaria para que existan soluciones.

Supongamos ahora que d divide a c y sean x_0, y_0, a', b', c' enteros tales que $ax_0 + by_0 = d$, $a = da'$, $b = db'$ y $c = dc'$. Como

$$ax_0c' + by_0c' = (ax_0 + by_0)c' = dc' = c,$$

es claro que (x_0c', y_0c') es una solución al problema (4). Esto prueba que la condición del enunciado es también suficiente para la existencia de soluciones y, por lo tanto, completa la prueba de las partes (*i*) y (*ii*) de la proposición.

Probemos ahora la parte (*iii*). Sea (x_0, y_0) una solución cualquiera de la ecuación (4). Si (x, y) es otra solución de esa ecuación, entonces tenemos que

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

y esto nos dice que $(x_1, y_1) \coloneqq (x - x_0, y - y_0)$ es una solución de la ecuación homogénea (5) tal que $(x, y) = (x_0 + x_1, y_0 + y_1)$.

Recíprocamente, si (x_1, y_1) es una solución cualquiera de la ecuación homogénea (5), de manera que $ax_1 + by_1 = 0$, entonces tenemos que

$$a(x_0 + x_1) + b(x_0 + x_1) = (ax_0 + by_0) + (ax_1 + by_1) = c + 0 = c,$$

así que el par $(x_0 + x_1, y_0 + y_1)$ es una solución de la ecuación (4). Esto prueba (*iii*). □

8.2.6. De acuerdo a esta proposición y su demostración, para resolver una ecuación de la forma

$$ax + by = c \tag{6}$$

con a, b y c tres enteros tales que $ab \neq 0$ podemos proceder de la siguiente manera.

- En primer lugar, calculamos $d \coloneqq \mathsf{mcd}(a, b)$. Si d no divide a c, entonces sabemos que no hay soluciones de la ecuación y no hay más nada que hacer.
- Supongamos entonces que d sí divide a c. Usando el algoritmo de Euclides extendido buscamos enteros u y v tales que $ua + vb = d$, y dividiendo buscamos el entero c' tal que $c = c'd$. El par $(c'u, c'v)$ es entonces una solución de la ecuación (6)
- Dos divisiones nos dan enteros a', b' tales que $a = a'd$, $b = b'd$, y sabemos que las soluciones de la ecuación homogénea $ax + by = 0$ son las de la forma $(b't, -a't)$ con $t \in \mathbb{Z}$.
- Con todo esto podemos concluir que todas las soluciones de la ecuación (6) son las de la

```haskell
import EMCD

resolverH :: Integer -> Integer -> (Integer,Integer)
resolverH a b = (b `div` d, - a `div` d)
  where (d, x, y) = emcd a b

resolverNH :: Integer -> Integer -> Integer -> Maybe (Integer, Integer)
resolverNH a b c
  | c `mod` d /= 0 = Nothing
  | otherwise      = Just (c * u, c * v)
  where (d, u, v) = emcd a b
        c'        = c `div` d
```

Programa 8.1. Un programa en Haskell para resolver ecuaciones diofánticas lineales con dos incógnitas. Cuando `a` y `b` son enteros no simultáneamente nulos, la expresión `resolverH a b` tiene como valor un par ordenado `(x, y)` que es una solución primitiva de la ecuaciones diofántica homogénea $ax + by = 0$. Por otro lado, cuando `a` y `b` son enteros no simultáneamente nulos, la expresión `resolverNH a b c` tiene o valor `Just (x, y)`, y en ese caso la ecuación $ax + by = c$ tiene soluciones y `(x, y)` es una de ellas, o valor `Nothing`, y en ese caso esa ecuación no tiene ninguna solución. Este código necesita alguna implementación del algoritmo de Euclides extendido.

forma $(c'u + b't, c'v - a't)$ con $t \in \mathbb{Z}$.

El programa 8.1 da una implementación de esto en Haskell.

§8.3. Ecuaciones lineales con un número arbitrario de incógnitas

8.3.1. Exactamente las mismas ideas nos permiten estudiar las ecuaciones diofánticas lineales en un número arbitrario de variables.

Proposición. *Sea $r \in \mathbb{N}$, sean $a_1, \ldots, a_r$ enteros todos distintos de 0, sea b un entero, y consideremos la ecuación*

$$a_1x_1 + \cdots + a_rx_r = b. \tag{7}$$

(*i*) *Hay soluciones a esta ecuación si y solamente si el entero* $d \coloneqq \mathsf{mcd}(a_1, \ldots, a_r)$ *divide a* b.

(*ii*) *Si ese es el caso y* $a'_1, \ldots, a'_r$ *y* b' *son los enteros tales que* $a_i = da'_i$ *para cada* $i \in \{1, \ldots, d\}$ *y* $b = db'$, *y* $u_1, \ldots, u_r$ *son enteros tales que* $a_1u_1 + \cdots + a_ru_d = d$, *entonces* $(u_1b', \ldots, u_rb')$ *es una solución de la ecuación* (7).

(*iii*) *Más aún, si* $(x_1^0, x_2^0, \ldots, x_r^0)$ *es una solución cualquiera de la ecuación* (7), *entonces toda solución de esa ecuación es de la forma* $(x_1^0 + x_1^1, \ldots, x_r^0 + x_r^1)$ *con* $(x_1^1, \ldots, x_r^1)$ *una solución de la ecuación homogénea*

$$a_1x_1 + \cdots + a_rx_r = 0. \tag{8}$$

Demostración. Si hay una solución $(x_1, \ldots, x_r)$ a la ecuación (7), entonces claramente el entero $d \coloneqq \mathsf{mcd}(a_1, \ldots, a_r)$ divide a $a_1x_1 + \cdots + a_rx_r = b$. Para ver que vale la implicación recíproca, supongamos que d divide a b y sea b' el entero tal que $b = db'$. La identidad de Bézout nos dice que existen enteros $u_1, \ldots, u_r$ tales que $a_1u_1 + \cdots + a_ru_r = d$ y entonces $a_1u_1b' + \cdots + a_ru_rb' = db' = b$, así que la r-upla $(u_1b', \ldots, u_rb')$ es una solución de la ecuación. Esto prueba las afirmaciones (*i*) y (*ii*) de la proposición.

Sea ahora $(x_1^0, x_2^0, \ldots, x_r^0)$ una solución cualquiera de la ecuación (7). Si $(x_1, \ldots, x_r)$ es otra solución, entonces la r-upla $(x_1^1, \ldots, x_r^1) \coloneqq (x_1 - x_1^0, \ldots, x_r - x_r^0)$ es una solución de la ecuación homogénea (8), ya que

$$a_1(x_1 - x_1^0) + \cdots + a_r(x_r - x_r^0) = (a_1x_1 + \cdots + a_rx_r) + (a_1x_1^0 + \cdots + a_rx_r^0) = b - b = 0,$$

y es $(x_1, \ldots, x_r) = (x_1^0 + x_1^1, \ldots, x_r^0 + x_r^1)$. Esto prueba la afirmación (*iii*) de la proposición. □

8.3.2. Una diferencia entre la situación de la que se ocupa esta última proposición y la de la Proposición **8.2.5** es que no tenemos una fórmula explícita para las soluciones de la ecuación homogénea como la que da la Proposición 8.2.3 en el caso en que solo hay dos incógnitas. Podemos describir, de todas formas, un *procedimiento* para resolverla. Veamos esto.

Supongamos que $r \geq 2$, que $a_1, \ldots, a_r$ son enteros no nulos, y que buscamos las soluciones de la ecuación diofántica lineal homogénea

$$a_1x_1 + \cdots + a_rx_r = 0. \tag{9}$$

Escribamos $\mathsf{Sol}(a_1, \ldots, a_r)$ al conjunto de todas las r-uplas $(x_1, \ldots, x_r)$ de enteros que son soluciones de esta ecuación. Nuestro objetivo, entonces, es describir este subconjunto de $\mathbb{Z}^r$.

Sin pérdida de generalidad podemos suponer que $\mathsf{mcd}(a_1, \ldots, a_r) = 1$. En efecto, si ese no es el caso, podemos poner $d \coloneqq \mathsf{mcd}(a_1, \ldots, a_r)$ y $a'_i \coloneqq a_i/d$ para cada $i \in \{1, \ldots, r\}$ y considerar en lugar de (9) la ecuación $a'_1x_1 + \cdots + a'_rx_r = 0$, que tiene exactamente las mismas soluciones que la ecuación original y cuyos coeficientes son tales que $\mathsf{mcd}(a'_1, \ldots, a'_r) = 1$.

Sea $e \coloneqq \mathsf{mcd}(a_2, \ldots, a_r)$ y supongamos que $(x_1, \ldots, x_r)$ es una solución de la ecuación (9). Como $\mathsf{mcd}(a_1, e) = \mathsf{mcd}(a_1, \ldots, a_r) = 1$ y

$$e \mid a_2x_2 + \cdots + a_rx_r = -a_1x_1,$$

el entero e divide a x_1 y existe un entero t tal que $x_1 = et$. Por otro lado, el algoritmo de Euclides extendido nos permite encontrar $r-1$ enteros $u_2, \ldots, u_r$ tales que

$$a_2u_2 + \cdots + a_ru_r = e.$$

Calculando vemos que

$$\begin{aligned} a_2(x_2 + a_1tu_2) + \cdots + a_r(x_r + a_1tu_r) &= (a_2x_2 + \cdots + a_rx_r) + a_1t\,(a_2u_2 + \cdots + a_ru_r) \\ &= -a_1x_1 + a_1te = 0, \end{aligned}$$

y esto nos dice que la $(r-1)$-upla $(x_2 + a_1tu_2, \ldots, x_r + a_1tu_r)$ es una solución de la ecuación

$$a_2y_2 + \cdots + a_ry_r = 0 \tag{10}$$

en $r-1$ incógnitas $y_2, \ldots, y_r$.

Recíprocamente, cada vez que $(y_2, \ldots, y_r)$ es una solución de esta última ecuación (10) e t es un entero cualquiera, tenemos que

$$\begin{aligned} a_1et + a_2(y_2 - a_1tu_2) + \cdots + a_r(y_r - a_1tu_r) & \\ = ea_1t - a_1t\,(a_2u_2 + \cdots + a_ru_r) + (a_2y_2 + \cdots + a_ry_r) &= 0, \end{aligned}$$

y esto nos dice que la r-upla $(et, y_2 - a_1tu_2, \ldots, y_r - a_1tu_r)$ es una solución de la ecuación (9), que es claramente equivalente a

$$\frac{a_2}{e}u_2 + \cdots + \frac{a_r}{e}u_r = e.$$

Hemos probado la siguiente proposición.

8.3.3. Proposición. *Supongamos que r y $a_1, \ldots, a_r$ son enteros tales que $r \geq 2$ y $\mathsf{mcd}(a_1, \ldots, a_r) = 1$, sea $e \coloneqq \mathsf{mcd}(a_2, \ldots, a_r)$ y sean $u_2, \ldots, u_r$ enteros tales que $a_2u_2 + \cdots + a_ru_r = e$. El conjunto $\mathsf{Sol}(a_1, \ldots, a_r)$ de las soluciones de la ecuación $a_1x_1 + \cdots + a_rx_r = 0$ es*

$$\{(et, z_2 - a_1tu_2, \ldots, z_r - a_1tu_r) : t \in \mathbb{Z}, (z_2, \ldots, z_r) \in \mathsf{Sol}(a_2/e, \ldots, a_r/e)\}. \qquad \square$$

El punto de esto es que nos permite reduce el problema de encontrar todas las soluciones de una ecuación diofántica lineal homogénea con r incógnitas al de encontrar todas las soluciones de una ecuación del mismo tipo pero con una incógnita menos. Repitiendo esto podemos resolver completamente el problema.

8.3.4. Veamos un ejemplo de este procedimiento. Consideremos la ecuación

$$6 \cdot x_1 + 105 \cdot x_2 + 30 \cdot x_3 + 70 \cdot x_4 = 0. \tag{11}$$

Los coeficientes son coprimos, es $\mathsf{mcd}(105, 30, 70) = 5$, y usando el algoritmo de Euclides extendido encontramos que

$$1 \cdot 105 + 20 \cdot 30 + (-10) \cdot 70 = 5.$$

La proposición nos dice entonces que $\mathsf{Sol}(6, 105, 30, 70)$ es el conjunto de las 4-uplas de la forma

$$(5 \cdot t_1, y_2 - 6 \cdot t_1, y_3 - 120 \cdot t_1, y_4 + 60 \cdot t_1) \tag{12}$$

con $t_1 \in \mathbb{Z}$ y $(y_2, y_3, y_4) \in \mathsf{Sol}(21, 6, 14)$.

Tenemos ahora que resolver la ecuación

$$21 \cdot y_2 + 6 \cdot y_3 + 14 \cdot y_4 = 0, \tag{13}$$

que tiene coeficientes coprimos. Es $\mathsf{mcd}(6, 14) = 2$ y el algoritmo de Euclides extendido nos dice que

$$(-2) \cdot 6 + 1 \cdot 14 = 2.$$

Usando el resultado de la proposición, podemos concluir entonces que las soluciones de la ecuación (13) son las 3-uplas de la forma

$$(2 \cdot t_2, z_3 + 42 \cdot t_2, z_4 - 21 \cdot t_2) \tag{14}$$

con $t_2 \in \mathbb{Z}$ y (z_3, z_4) un elemento de $\mathsf{Sol}(3, 7)$.

Finalmente, tenemos que resolver la ecuación

$$3 \cdot z_3 + 7 \cdot z_4 = 0$$

en dos incógnitas: sus soluciones son los pares de la forma

$$(7 \cdot t_3, -3 \cdot t_3)$$

con $t_3 \in \mathbb{Z}$. Usando esto en (14) vemos que las soluciones de la ecuación (13) son las 3-uplas de la forma

$$(2 \cdot t_2, 7 \cdot t_3 + 42 \cdot t_2, -3 \cdot t_3 - 21 \cdot t_2)$$

con $t_2, t_3 \in \mathbb{Z}$. A su vez, usando esto en (12) vemos que las soluciones de la ecuación (11) con la que empezamos son las 4-uplas de la forma

$$(5 \cdot t_1, 2 \cdot t_2 - 6 \cdot t_1, 7 \cdot t_3 + 42 \cdot t_2 - 120 \cdot t_1, -3 \cdot t_3 - 21 \cdot t_2 + 60 \cdot t_1)$$

con t_1, t_2, $t_3 \in \mathbb{Z}$. En otras palabras, las soluciones de la ecuación (11) son todas las que 4-uplas (x_1, x_2, x_3, x_4) que se obtienen eligiendo tres enteros t_1, t_2, y t_3 y poniendo

$$\begin{aligned} x_1 &\coloneqq \cdot t_1, \\ x_2 &\coloneqq -\cdot t_1 + \cdot t_2, \\ x_3 &\coloneqq -120\cdot t_1 + 42\cdot t_2 + 7\cdot t_3, \\ x_4 &\coloneqq 60\cdot t_1 - 21\cdot t_2 - 3\cdot t_3 \end{aligned} \tag{15}$$

8.3.5. Las soluciones de una ecuación homogénea siempre tienen una forma similar a la de las del ejemplo que acabamos de dar:

Proposición. *Sea $r \in \mathbb{N}$ tal que $r \geq 2$, y sean $a_1, \ldots, a_r$ enteros no nulos tales que $\mathsf{mcd}(a_1, \ldots, a_r) = 1$. Hay $r-1$ elementos*

$$u_1 = (u_{1,1}, \ldots, u_{1,r}), \quad u_2 = (u_{2,1}, \ldots, u_{2,r}), \quad \ldots, \quad u_{r-1} = (u_{r-1,1}, \ldots, u_{r-1,r})$$

de $\mathbb{Z}^r$ tales que las soluciones de la ecuación homogénea

$$a_1x_1 + \cdots + a_rx_r = 0 \tag{16}$$

son todas las r-uplas $(x_1, \ldots, x_r)$ que se obtienen eligiendo $r-1$ enteros $t_1, \ldots, t_{r-1}$ y poniendo

$$\begin{aligned} x_1 &= t_1u_{1,1} + t_2u_{2,1} + \cdots + t_{r-1}u_{r-1,1}, \\ x_2 &= t_1u_{1,2} + t_2u_{2,2} + \cdots + t_{r-1}u_{r-1,2}, \\ &\vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \\ x_r &= t_1u_{1,r} + t_2u_{2,r} + \cdots + t_{r-1}u_{r-1,r}. \end{aligned}$$

En el ejemplo que hicimos arriba sobre la ecuación (11) es $r = 4$ y como los 3 elementos u_1, u_2 y u_3 a los que se refiere esta proposición podemos elegir a

$$(5, -30, 90, 6), \qquad (0, 2, 42, -21), \qquad (0, 0, 7, -3).$$

Demostración. Demostraremos esto procediendo por inducción con respecto al número r de incógnitas de la ecuación (16).

Supongamos primero que $r = 2$. Tenemos entonces dos enteros a_1 y a_2 que son nulos y tales que $\mathsf{mcd}(a_1, a_2) = 1$. De acuerdo a la Proposición 8.2.3, las soluciones de la ecuación $a_1x_1 + a_2x_2 = 0$ son todos los pares ordenados (x_1, x_2) de la forma $(t_1a_2, -t_1a_1)$ con t_1 un entero, y esto nos dice que si ponemos $u_1 \coloneqq (a_2, -a_1)$ entonces la afirmación de la proposición vale.

Supongamos ahora que es $r \geq 3$. Sean $a_1, \ldots, a_r$ enteros tales que $\mathsf{mcd}(a_1, \ldots, a_r) = 1$, y consideremos el número $e \coloneqq \mathsf{mcd}(a_2, \ldots, a_r)$. La ecuación

$$\frac{a_2}{e}y_2 + \cdots + \frac{a_r}{e}y_r = 0 \tag{17}$$

tiene $r-1$ incógnitas y sus coeficientes son coprimos, así que la hipótesis inductiva evidente implica que hay $r-2$ elementos

$$v_2 = (v_{2,2}, v_{2,3}, \ldots, v_{2,r}), \quad v_3 = (v_{3,2}, v_{3,3}, \ldots, v_{3,r}), \quad \ldots, \quad v_{r-1} = (v_{r-1,2}, v_{r-1,3}, \ldots, v_{r-1,r})$$

de $\mathbb{Z}^{t-1}$ tales que las soluciones de la ecuación (17) son las $(r-1)$-uplas $(y_2, \ldots, y_r)$ que se obtienen eligiendo $r-2$ enteros $t_2, \ldots, t_{r-1}$ y poniendo

$$\begin{aligned}
y_2 &= t_2 v_{2,2} + t_3 v_{3,2} + \cdots + t_{r-1} v_{r-1,2}, \\
y_3 &= t_2 v_{2,3} + t_3 v_{3,3} + \cdots + t_{r-1} v_{r-1,3}, \\
&\vdots \qquad \vdots \qquad \vdots \qquad\qquad \vdots \\
y_r &= t_2 v_{2,r} + t_3 v_{3,r} + \cdots + t_{r-1} v_{r-1,r}.
\end{aligned}$$

Por otro lado, como $\mathsf{mcd}(a_1, \ldots, a_r) = 1$, hay enteros $w_1, \ldots, w_r$ tales que $w_1 a_1 + \cdots + w_r a_r = 1$ y la Proposición 8.3.3 nos dice que

> *las soluciones de la ecuación* (16) *del enunciado son las r-uplas de la forma* $(et, y_2 - a_1 t w_2, \ldots, y_r - a_1 t w_r)$ *con* $t \in \mathbb{Z}$ *e* $(y_2, \ldots, y_r)$ *una solución de la ecuación* (17). (18)

Consideremos ahora los $r-1$ elementos

$$\begin{aligned}
u_1 &\coloneqq (e, -a_1 w_2, -a_1 w_3, \ldots, -a_1 w_r), \\
u_2 &\coloneqq (0, \quad v_{2,2}, \quad v_{2,3}, \ldots, \quad v_{2,r}), \\
u_3 &\coloneqq (0, \quad v_{3,2}, \quad v_{3,3}, \ldots, \quad v_{3,r}), \\
&\vdots \qquad\qquad\qquad \vdots \\
u_{r-1} &\coloneqq (0, \quad v_{r-1,2}, \quad v_{r-1,3}, \ldots, \quad v_{r-1,r})
\end{aligned}$$

de $\mathbb{Z}^r$ y para cada $i \in \{1, \ldots, r-1\}$ y cada $j \in \{1, \ldots, r\}$ escribamos $u_{i,j}$ a la componente j-ésima de u_i. Unos momentos de reflexión deberían ser suficientes para convencer al lector que las r-uplas $(x_1, \ldots, x_r)$ que se obtienen eligiendo $r-1$ enteros $t_1, \ldots, t_r$ y poniendo

$$\begin{aligned}
x_1 &= t_1 u_{1,1} + t_2 u_{2,1} + \cdots + t_{r-1} u_{r-1,1}, \\
x_2 &= t_1 u_{1,2} + t_2 u_{2,2} + \cdots + t_{r-1} u_{r-1,2}, \\
&\vdots \qquad \vdots \qquad \vdots \qquad\qquad \vdots \\
x_r &= t_1 u_{1,r} + t_2 u_{2,r} + \cdots + t_{r-1} u_{r-1,r}.
\end{aligned}$$

son precisamente las soluciones de la ecuación (16), de acuerdo a (18). Esto completa la inducción y, por lo tanto, la prueba de la proposición. □

```
import EMCD

resolverH :: [Integer] -> [[Integer]]
resolverH [a]      = []
resolverH (a : as) = primera : [ 0 : s | s <- resolverH as]
  where (e,us)     = emcdN as
        (d,_,_)    = emcd a e
        primera    = e `div` d : [ - u * a `div` d | u <- us]

resolverNH :: [Integer] -> Integer -> Maybe [Integer]
resolverNH as b
  | r /= 0    = Nothing
  | otherwise = Just (map (q *) us)
  where (d, us) = emcdN as
        (q, r) = divMod b d

emcdN :: [Integer] -> (Integer, [Integer])
emcdN [a]    = (a, [1])
emcdN (a:as) = (d, x : [y * u | u <- us])
  where (e, us) = emcdN as
        (d, x, y) = emcd a e
```

Programa 8.2. Funciones en HASKELL que resuelven ecuaciones diofánticas lineales homogéneas y no homogéneas con una cantidad arbitraria de incógnitas. Ambas asumen que todos los coeficientes son distintos de 0. Usamos aquí el código del Programa 6.5 en la página 186 para calcular los coeficientes de la identidad de Bézout.

8.3.6. Ejercicio. Muestre que en la situación de la proposición que acabamos de probar los $r-1$ elementos $u_1, \ldots, u_{r-1}$ de $\mathbb{Z}^r$ pueden elegirse de manera que para toda elección de i en $\{1, \ldots, r-1\}$ y de j en $\{1, \ldots, r\}$ valga

$$1 \leq j < i \implies u_{j,i} = 0.$$

Esto es la generalización del hecho observado en nuestro ejemplo de 8.3.4 de que la solución final (15) de la ecuación allí considerada es «triangular»

8.3.7. El programa 8.2 da una implementación sencilla de este algoritmo para resolver ecuaciones diofánticas lineales homogéneas y la correspondiente aplicación para encontrar una solución particular de las no homogéneas. Por ejemplo, podemos evaluar

```
*Ecuaciones> resolverH [6, 105, 30, 70]
[[5,-6,-120,60],[0,2,42,-21],[0,0,7,-3]]
```

El resultado es la lista de las 4-uplas que encontramos en 8.3.4, de manera que las soluciones de la ecuación

$$6x_1 + 105x_2 + 30x_3 + 70x_4 = 0$$

que consideramos ahí son las 4-uplas (x_1, x_2, x_3, x_4) que se obtienen eligiendo t_1, t_2 y t_3 en $\mathbb{Z}$ y poniendo

$$\begin{aligned} x_1 &:= \ 5 \cdot t_1, \\ x_2 &:= -\ 6 \cdot t_1 + \ 2 \cdot t_2, \\ x_3 &:= -\ 120 \cdot t_1 + 42 \cdot t_2 + 7 \cdot t_3, \\ x_4 &:= \ 60 \cdot t_1 - \ 21 \cdot t_2 - 3 \cdot t_3 \end{aligned}$$

Las tres listas del valor de `resolverH [6, 105, 30, 70]` son los coeficientes de t_1, t_2 y t_3 en estas fórmulas.

De manera similar, las soluciones de la ecuación

$$30x_1 + 14x_2 + 105x_3 + 231x_4 = 0$$

son las 4-uplas (x_1, x_2, x_3, x_4) que se obtienen eligiendo t_1, t_2 y t_3 en $\mathbb{Z}$ y poniendo

$$\begin{aligned} x_1 &= \ 7t_1 \\ x_2 &= \ 30t_1 + 3t_2 \\ x_3 &= -\ 60t_1 + 4t_2 + 11t_3 \\ x_4 &= -\ 30t_1 - 2t_2 - \ 5t_3 \end{aligned}$$

ya que evaluando `resolverH [30,14,105,231]` obtenemos

```
Ecuaciones*> resolverH [30,14,105,231]
[[7,30,60,-30],[0,3,4,-2],[0,0,11,-5]]
```

Por otro lado, la función `resolverNH` nos da una solución de una ecuación no homogénea, si es que hay alguna: podemos evaluar

```
*Ecuaciones> resolverNH [90, 15, -78] 24
Just [24,360,72]
```

y esto nos dice que una solución de la ecuación

$$90x_1 + 15x_2 - 78x_3 = 24$$

es $(x_1, x_2, x_3) = (24, 306, 72)$. Por otro lado,

```
*Ecuaciones> resolverNH [30, 14, 106] 7
Nothing
```

y esto nos dice que la ecuación

$$30x_1 + 14x_2 + 106x_3 = 7$$

no tiene soluciones.

§8.4. Ecuaciones lineales en congruencias

8.4.1. En esta sección nos ocupamos de siguiente problema: dados $m \in \mathbb{N}$ y enteros a y b, queremos decidir si hay enteros x tales que

$$ax \equiv b \mod m$$

y, cuando los haya, encontrarlos.

Proposición. *Sea $m \in \mathbb{N}$, sean a y b dos enteros y sea $d := \mathsf{mcd}(a, m)$. Hay enteros x tales que*

$$ax \equiv b \mod m \tag{19}$$

si y solamente si d divide a b. Si ese es el caso y si u_0, v_0, a', m' y b' son enteros tales que $au_0 + mv_0 = d$, $a = da'$, $m = dm'$ y $b = db'$, entonces los d enteros

$$u_0b' + 0m', \quad u_0b' + 1m', \quad u_0b' + 2m', \quad \dots, \quad u_0b' + (d-1)m'.$$

son soluciones de la ecuación no congruentes módulo m dos a dos y toda otra solución es congruente a una de ellas.

Demostración. Si existe un entero x tal que $ax \equiv b \mod m$, entonces m divide a $ax - b$ y, por lo tanto, existe un entero y tal que $ax - b = my$. Se tiene entonces que

$$d \mid ax - my = b.$$

Supongamos, para ver la recíproca, que d divide a b. La Proposición 8.2.5 nos dice que hay dos enteros x e y tales que $ax + my = b$: como entonces se tiene que $ax \equiv b \mod m$, vemos que la ecuación (19) tiene soluciones. Esto prueba la primera afirmación del enunciado.

Sean u_0, v_0, a', m' y b' enteros tales que $au_0 + mv_0 = d$, $a = da'$, $m = dm'$ y $b = db'$. Para cada entero x tenemos que

$$\begin{aligned} ax \equiv b \mod m &\iff dx \equiv u_0 ax \equiv u_0 b \equiv u_0 db' \mod m \\ &\iff x \equiv u_0 b' \mod m'. \end{aligned}$$

Esto nos dice que toda solución de la ecuación (19) es de la forma

$$x = u_0 b' + m' t$$

para un t unívocamente determinado.

Más aún, las soluciones $u_0 b' + m' t$ y $u_0 b' + m' s$ correspondientes a dos enteros t y s son congruentes módulo m si y solamente si

$$m' d = m \mid (x_0 b' + m' t) - (x_0 b' + m' s) = m'(t - s),$$

lo que ocurre si y solamente si t y s son congruentes módulo d. Esto implica inmediatamente que las d soluciones

$$u_0 b' + 0m', \quad u_0 b' + 1m', \quad u_0 b' + 2m', \quad \ldots, \quad u_0 b' + (d-1)m'$$

son no congruentes módulo m dos a dos y que toda solución de la ecuación es congruente a una de ellas, □

8.4.2. Proposición. *Sean m_1, $m_2 \in \mathbb{N}$, sean b_1, $b_2 \in \mathbb{Z}$ y sea $d = \mathsf{mcd}(m_1, m_2)$. Existen enteros x tales que*

$$\begin{cases} x \equiv b_1 \mod m_1, \\ x \equiv b_2 \mod m_2 \end{cases} \tag{20}$$

si y solamente si $b_1 \equiv b_2 \mod d$. Más aún, si ese es el caso y n_1, n_2 son enteros tales que $n_1 m_1 + n_2 m_2 = d$ y $M = \mathsf{mcm}(m_1, m_2)$, entonces el número

$$u = \frac{n_2 m_2 b_1 + n_1 m_1 b_2}{d}$$

es entero y el conjunto de soluciones de (21) es precisamente la clase de congruencia de u módulo M.

Demostración. Supongamos primero que hay un entero x que satisface las dos ecuaciones (20). En ese caso, como d divide tanto a m_1 como a m_2 tenemos que también $x \equiv b_1 \mod d$ y $x \equiv b_2 \mod d$, de manera que $b_1 \equiv b_2 \mod d$.

Supongamos ahora que $b_1 \equiv b_2 \mod d$. Un entero x satisface la primera de las ecuaciones de (21) si y solamente si existe un entero t tal que $x = b_1 + m_1 t$, y entonces también satisface la segunda de esas ecuaciones si además $b_1 + m_1 t \equiv b_2 \mod m_2$, esto es, si

$$m_1 t \equiv b_2 - b_1 \mod m_2.$$

Como d divide a $b_2 - b_1$, esta ecuación tiene soluciones, en vista del criterio que nos da la Proposición 8.4.1, así que el sistema (20) también. □

8.4.3. La generalización del resultado de la Proposición 8.4.2 al caso de sistemas de un número arbitrario de congruencias es conocida usualmente como el *Teorema Chino del Resto*. El nombre con el que es conocido el teorema se debe a que la primera aparición registrada de este resultado es en el libro *Sunzi Suanjing*, escrito en China en algún momento entre el siglo III y el V de la era cristiana. En el libro se plantea y se resuelve el siguiente problema:

> *Hay ciertas cosas cuyo número se desconoce. Si las contamos de a tres, sobran dos; si de a cinco, sobran tres; y si de a siete, sobran dos. ¿Cuántas cosas hay?*

que es equivalente al de resolver el sistema de congruencias

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5, \\ x \equiv 2 \mod 7. \end{cases}$$

De todas maneras, no menciona ni el enunciado general ni una demostración. Brahmagupta, en el siglo VII en la India, también conocía casos particulares y en su libro *Brāhmasphuṭasiddhānta* plantea el siguiente problema:

> *Una anciana va al mercado y un caballo pisa su canasta y aplasta los huevos que llevaba. El jinete ofrece pagarle los huevos y le pregunta cuántos tenía. Ella no recuerda el número exacto, pero sí que cuando los había ordenado en filas de dos había sobrado uno, y que lo mismo había ocurrido cuando había intentado ordenarlos en filas de tres, de cuatro, de cinco y de seis, y que solo cuando había intentado ponerlos en filas de siete habían quedado parejos. ¿Cuál es la menor cantidad de huevos que pudo haber tenido?*

Por supuesto, lo que quiere Brahmagupta es la menor solución positiva del sistema de congruencias

$$\begin{cases} x \equiv 1 \mod 2, \\ x \equiv 1 \mod 3, \\ x \equiv 1 \mod 4, \\ x \equiv 1 \mod 5, \\ x \equiv 1 \mod 6, \\ x \equiv 0 \mod 7. \end{cases}$$

Más tarde, Fibonacci da varios ejemplos en su libro *Liber Abaci* de 1202. Uno de ellos es el siguiente: se le pide a alguien que piense un número y que nos diga el resto de dividirlo por 5, por 7 y por 9 y el problema consiste en «adivinarlo».

El primero en enunciar el teorema con total generalidad y probarlo fue Gauss, en sus *Disquisitiones* de 1801. Gauss plantea, a partir del párrafo 33, el problema general de «encontrar los números que tienen residuos dados, con respecto a módulos cualesquiera» y después de explicar un método general para resolver ese tipo de problemas y dar varios ejemplos numéricos, plantea la siguiente aplicación práctica a un «problema de cronología»:

> *Encontrar el número de un año del que se conoce la indicción, el número áureo y el ciclo solar.*

La ***indicción*** de un año es el resto de dividir por 15 la suma de su número más 3 (por ejemplo, la indicción del año 2018 es 11) y es uno de los periodos del calendario bizantino, junto con el mes y el año, y que se usaba para la liquidación de impuestos. Por otro lado, el ***número áureo*** de un año (que no tiene nada que ver con el número $(1+\sqrt{5})/2$) es 1 más el resto de dividirlo por 19: este número se usó desde el año 432 a.C. para poder calcular los ciclos lunares con precisión, usando un amétodo debido al griego Metón. Finalmente, el ***ciclo solar*** de un año A es uno más el resto de dividir $A+1$ por 28. Así, el problema que plantea Gauss es el de determinar el año x con indicción i, número aureo a y ciclo solar s es equivalente al de resolver el sistema de congruencias

$$\begin{cases} x \equiv i-3 \mod 15, \\ x \equiv a-1 \mod 19, \\ x \equiv s-1 \mod 28. \end{cases}$$

El mínimo común múltiplo de 15, 19 y 28 es 7980: veremos más abajo que eso implica que cada año desde el primero hasta el 7979 está completamente determinado por su indicción, su número áureo y su ciclo solar.

El problema que plantea Gauss parece hoy bastante extraño, pero en su época era de gran interés. Gauss había tenido un gran éxito un año antes de la publicación de sus *Disquisitiones* al hacer conocer un método algorítmico —el primero en la historia— para el cálculo de la fecha de Pascua. Ese método tenía ciertas falencias y en 1816 publicó finalmente un algoritmo mejorado que permitía calcular exactamente la fecha de Pascua de todos los años a partir del año 1583 del calendario gregoriano.

8.4.4. Empecemos con un caso particular del Teorema Chino del Resto, aquel en el que lo módulos son coprimos dos a dos. La demostración de este caso es más sencilla que la del general y, a la vez, es el que más usamos en la práctica:

Proposición. *Sea $r \in \mathbb{N}$, sean $m_1, \ldots, m_r$ enteros positivos coprimos dos a dos y sean $b_1, \ldots, b_r$ enteros. Hay enteros x tales que*

$$\begin{cases} x \equiv b_1 \mod m_1, \\ \vdots \quad \vdots \qquad \vdots \\ x \equiv b_r \mod m_r \end{cases} \tag{21}$$

y el conjunto de tales enteros es una clase de congruencia módulo $m_1 \cdots m_r$.

Demostración. Sea $M = m_1 \cdots m_r$. Veamos primero que si hay soluciones al sistema de congruencias (21), entonces el conjunto de esas soluciones es precisamente una clase de congruencia módulo M. Esto probará la segunda afirmación del enunciado.

Supongamos entonces que hay un entero x_0 tal que $x_0 \equiv b_i \mod m_i$ para cada $i \in \{1, \ldots, r\}$. Si x es otro entero que satisface las mismas congruencias, entonces tenemos que $x - x_0 \equiv b_i - b_i \mod m_i$ y, por lo tanto, la diferencia $x - x_0$ es divisible por cada uno de los números $m_1, \ldots, m_r$. Como estos r números son coprimos dos a dos, el Corolario 6.5.8 nos dice que su producto M también divide a $x - x_0$ y, por lo tanto que $x \equiv x_0 \mod M$.

Recíprocamente, si x es un entero que es congruente con x_0 módulo M, entonces para cada $i \in \{1, \ldots, r\}$ tenemos que $x \equiv x_0 \mod m_i$, porque m_i divide a M, y entonces que $x \equiv x_0 \equiv b_i \mod m_i$. Así, x es una solución del sistema de congruencias (21).

Concluimos de esta forma que si x_0 es una solución del sistema (21) entonces el conjunto de todas las soluciones es precisamente la clase de congruencia de x_0 módulo M, como queríamos.

Veamos ahora que existen soluciones. Procederemos por inducción. Para cada $r \in \mathbb{N}$ sea $P(r)$ la afirmación

> *si $m_1, \ldots, m_r$ son enteros positivos coprimos dos a dos y $b_1, \ldots, b_r$ son enteros, entonces existe un entero x tal que $x \equiv b_i \mod m_i$ para cada $i \in \{1, \ldots, r\}$.*

Que $P(1)$ vale es evidente y que $P(2)$ vale es un caso particular de la Proposición 8.4.2. Sea, para hacer inducción, s un entero tal que $s \geq 2$, supongamos que $P(s)$ vale y mostremos que entonces $P(s+1)$ también vale. Sean, para eso, $m_1, \ldots, m_{s+1}$ enteros positivos coprimos dos a dos y sean $b_1, \ldots, b_{s+1}$ enteros.

Como m_s y m_{s+1} son coprimos, la Proposición 8.4.2 nos dice que hay un entero a tal que para cada $x \in \mathbb{Z}$ se tiene que

$$x \equiv a \mod m_1 m_2 \iff \begin{cases} x \equiv b_s \mod m_s, \\ x \equiv b_{s+1} \mod m_{s+1} \end{cases} \tag{22}$$

Por otro lado, la hipótesis inductiva implica que existe un entero x_0 que satisface el sistema de

s congruencias

$$\begin{cases} x_0 \equiv b_1 & \text{mód } m_1, \\ \vdots \quad \vdots & \vdots \\ x_0 \equiv b_{s-1} & \text{mód } m_{s-1} \\ x_0 \equiv a & \text{mód } m_s m_s \end{cases}$$

ya que los enteros $m_1, \ldots, m_{s-1}, m_s m_{s+1}$ son coprimos dos a dos, y de esta última congruencia y de (22) deducimos que además $x_0 \equiv b_s \mod m_s$ y $x_0 \equiv b_{s+1} \equiv m_{s+1}$. Así, tenemos que

$$\begin{cases} x_0 \equiv b_1 & \text{mód } m_1, \\ \vdots \quad \vdots & \vdots \\ x_0 \equiv b_{s+1} & \text{mód } m_{s+1} \end{cases}$$

si y solamente si satisface el sistema de s congruencias

$$\begin{cases} x \equiv b_1 & \text{mód } m_1, \\ \vdots \quad \vdots & \vdots \\ x \equiv b_{s+1} & \text{mód } m_{s+1} \end{cases}$$

y, en definitiva, el entero x_0 es una solución al sistema de congruencias (21) del enunciado. Esto prueba que este sistema posee soluciones, por supuesto. □

8.4.5. La prueba de existencia que acabamos de hacer nos da un algoritmo que podemos usar en la práctica. Por ejemplo, supongamos que queremos encontrar un entero x que satisfaga las congruencias

$$\begin{cases} x \equiv 1 & \text{mód } 2, \\ x \equiv 2 & \text{mód } 3, \\ x \equiv 3 & \text{mód } 5, \\ x \equiv 4 & \text{mód } 7. \end{cases} \tag{23}$$

La identidad de Bézout para 2 y 3 es $2 \cdot (-1) + 3 \cdot 1 = 1$ y

$$3 \cdot 1 \cdot 1 + 2 \cdot (-1) \cdot 2 = -1 \equiv 5 \mod 6,$$

así que la Proposición 8.4.2 nos dice que para cada $x \in \mathbb{Z}$ es

$$x \equiv 5 \mod 6 \iff \begin{cases} x \equiv 1 & \text{mód } 2, \\ x \equiv 2 & \text{mód } 3. \end{cases}$$

El sistema (23) es por lo tanto equivalente a

$$\begin{cases} x \equiv 5 \mod 6, \\ x \equiv 3 \mod 5, \\ x \equiv 4 \mod 7. \end{cases} \tag{24}$$

Otra vez, la identidad de Bézout para 6 y 5 es $6 \cdot 1 + 5 \cdot (-1) = 1$, y

$$5 \cdot (-1) \cdot 5 + 6 \cdot 1 \cdot 3 = -7 \equiv 23 \mod 30.$$

De acuerdo a la Proposición 8.4.2, entonces,

$$x \equiv 23 \mod 30 \iff \begin{cases} x \equiv 5 \mod 6, \\ x \equiv 3 \mod 5 \end{cases}$$

y el sistema (24) es equivalente a

$$\begin{cases} x \equiv 23 \mod 30, \\ x \equiv 4 \mod 7. \end{cases} \tag{25}$$

Finalmente, la identidad de Bézout para 30 y 7 es $30 \cdot (-3) + 7 \cdot 13 = 1$ y

$$7 \cdot 13 \cdot 23 + 30 \cdot (-3) \cdot 4 = 1733 \equiv 53 \mod 210,$$

así que el sistema (25) es equivalente a la congruencia

$$x \equiv 53 \mod 210.$$

Ésta es entonces la solución del sistema (23) con el que empezamos.

8.4.6. El procedimiento para resolver un sistema de congruencias que se deduce de la prueba que dimos para la Proposición 8.4.4 es iterativo: vamos resolviendo parcialmente el sistema de a una congruencia por vez. También podemos construir una solución de una sola vez:

Proposición. *Sea $r \in \mathbb{N}$, sean $m_1, \ldots, m_r$ enteros positivos coprimos dos a dos y sean $b_1, \ldots, b_r$ enteros. Pongamos $M = m_1 \cdots m_r$ y para cada $i \in \{1, \ldots, r\}$ sea $q_i = M/m_i$. Para cada $i \in \{1, \ldots, r\}$ existen enteros s_i y t_i tales que $s_i q_i + t_i m_i = 1$ y el entero*

$$x = s_1 q_1 b_1 + \cdots + s_r q_r b_r$$

es una solución del sistema de congruencias

$$\begin{cases} x \equiv b_1 \mod m_1, \\ \vdots \quad \vdots \qquad \vdots \\ x \equiv b_r \mod m_r \end{cases} \tag{26}$$

Demostración. Sea $i \in \{1, \dots, r\}$. Como $q_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_r$ y los $r-1$ factores en este producto son coprimos dos a dos, tenemos que

$$\begin{aligned} \mathsf{mcd}(m_i, q_i) &= \mathsf{mcd}(m_i, m_1) \cdots \mathsf{mcd}(m_i, m_{i-1}) \, \mathsf{mcd}(m_i, m_{i+1}) \cdots \mathsf{mcd}(m_i, m_r) \\ &= 1. \end{aligned}$$

De la identidad de Bézout, entonces, sabemos que existen enteros s_i y t_i tales que

$$s_i q_i + t_i m_i = 1.$$

Esto prueba la primera afirmación del enunciado.

Sea, por otro lado, $x = s_1 q_1 b_1 + \cdots + s_r q_r b_r$, como en el enunciado de la proposición, y sea $i \in \{1, \dots, r\}$. Si j es otro elemento de $\{1, \dots, r\}$ distinto de i, entonces m_j divide a q_i, así que

$$x = s_1 q_1 b_1 + \cdots + s_r q_r b_r \equiv s_i q_i b_i (1 - t_i m_i) b_i \equiv b_i \mod m_i.$$

Vemos así que x es una solución a cada una de las congruencias del sistema (26). □

8.4.7. Resolvamos el sistema de congruencias (23) de 8.4.5 usando esta vez el resultado que acabamos de probar. Tenemos $r = 4$ y

$$m_1 = 2, \quad m_2 = 3, \quad m_3 = 5, \quad m_4 = 7, \quad b_1 = 1, \quad b_2 = 2, \quad b_3 = 3, \quad b_4 = 4.$$

Ponemos $q_1 = 3 \cdot 5 \cdot 7 = 105$, $q_2 = 2 \cdot 5 \cdot 7 = 70$; $q_3 = 2 \cdot 3 \cdot 7 = 42$ y $q_4 = 2 \cdot 3 \cdot 5 = 30$ y, usando el algoritmo de Euclides extendido cuatro veces encontramos que

$$\begin{aligned} q_1 + (-52) m_1 &= 1, & q_2 + (-23) m_2 &= 1, \\ (-2) q_3 + 17 m_3 &= 1, & (-3) q_4 + 13 m_4 &= 1, \end{aligned}$$

así que podemos elegir $s_1 = s_2 = 1$, $s_3 = -2$ y $s_4 = -3$. La proposición nos dice entonces que el entero

$$x = 1 \cdot q_1 \cdot 1 + 1 \cdot q_2 \cdot 2 + (-2) \cdot q_3 \cdot 3 + (-3) \cdot q_4 \cdot 4 = -367$$

es una solución del sistema (23). Esto es consistente, por supuesto, con lo que hicimos antes, ya que $-367 \equiv 53 \mod 2 \cdot 3 \cdot 5 \cdot 7$.

En la práctica, el procedimiento iterativo para resolver sistemas de congruencias es más conveniente, ya que generalmente puede llevarse a cabo sin necesidad de considerar en el proceso enteros tan grandes como los que aparecen usando la idea de la Proposición 8.4.6.

8.4.8. Consideremos ahora la versión general del Teorema Chino del Resto. Cuando los módulos de las congruencias no son coprimos dos a dos, es necesario imponer una condición aritmética para que existan soluciones:

Proposición. *Sea $r \in \mathbb{N}$. Si $m_1, \ldots, m_r$ son enteros positivos y $b_1, \ldots, b_r \in \mathbb{Z}$, entonces hay enteros x tales que*

$$\begin{cases} x \equiv b_1 \mod m_1, \\ \vdots \quad \vdots \qquad \vdots \\ x \equiv b_r \mod m_r \end{cases} \tag{27}$$

si y solamente si se tiene que $b_i \equiv b_j \mod \mathsf{mcd}(m_i, m_j)$ para cada elección de i y j en $\{1, \ldots, r\}$. Cuando ese es el caso, el conjunto de los tales enteros es una clase de congruencia módulo $\mathsf{mcm}(m_1, \ldots, m_r)$.

Demostración. Sean $r \in \mathbb{N}$, $m_1, \ldots, m_r \in \mathbb{N}$ y $b_1, \ldots, b_r \in \mathbb{Z}$ y supongamos que existe un entero x tal que $x \equiv b_t \mod m_t$ para cada $t \in \{1, \ldots, r\}$. Si i y j son dos elementos de $\{1, \ldots, r\}$, tenemos en particular que

$$\begin{cases} x \equiv b_i \mod m_i, \\ x \equiv b_j \mod m_j \end{cases}$$

y la Proposición 8.4.2 nos dice que $b_i \equiv b_j \mod \mathsf{mcd}(m_i, m_j)$. Esto muestra que la condición del enunciado es necesaria para que existan soluciones del sistema de congruencias (27).

Probemos que también es suficiente y la última afirmación del enunciado haciendo inducción con respecto a r. Si r es 1, esto es evidente, y si r es 2 esto es parte de lo que afirma la Proposición 8.4.2.

Supongamos que s es un entero tal que $s \geq 2$ y que lo que afirma la proposición es cierto cuando r es s, y sean $m_1, \ldots, m_{s+1}$ enteros positivos y $b_1, \ldots, b_{s+1}$ enteros tales que $b_i \equiv b_j \mod \mathsf{gcd}(m_i, m_j)$ cada vez que i y j son elementos de $\{1, \ldots, r\}$.

La Proposición 8.4.2 nos dice que hay enteros x tales que

$$\begin{cases} x \equiv b_s \mod m_s, \\ x \equiv b_{s+1} \mod m_{s+1} \end{cases} \tag{28}$$

y, más aún, que el conjunto de tales enteros es una clase de congruencia módulo $\mathsf{mcm}(m_s, m_{s+1})$: así, existe $a \in \mathbb{Z}$ tal que un entero x satisface las congruencias (28) si y solamente si $x \equiv a$

$\mod \operatorname{mcm}(m_s, m_{s+1})$. Observemos que, en particular, tenemos que $a \equiv b_s \mod m_1$ y $a \equiv b_{s+1} \mod m_{s+1}$.

Como consecuencia de esto, es claro que un entero x satisface el sistema de $s+1$ congruencias

$$\begin{cases} x \equiv b_1 & \mod m_1, \\ \vdots \quad \vdots & \vdots \\ x \equiv b_{s+1} & \mod m_{s+1} \end{cases}$$

si y solamente si satisface el sistema de s congruencias

$$\begin{cases} x \equiv \tilde{b}_1 & \mod \tilde{m}_1, \\ \vdots \quad \vdots & \vdots \\ x \equiv \tilde{b}_{s-1} & \mod \tilde{m}_{s-1}, \\ x \equiv \tilde{b}_s & \mod \tilde{m}_s \end{cases}$$

en el que

$$\tilde{b}_1 = b_1, \quad \ldots, \quad \tilde{b}_{s-1} = b_{s-1}, \quad \tilde{b}_s = a,$$

y

$$\tilde{m}_1 = m_1, \quad \ldots, \quad \tilde{m}_{s-1} = m_{s-1}, \quad \tilde{m}_s = \operatorname{mcm}(m_s, m_{s+1}).$$

□

```
module TCR where

import EMCD

resolverTCR :: [(Integer, Integer)] -> Maybe (Integer, Integer)
resolverTCR [(a, m)]               = Just (a `mod` m, m)
resolverTCR ((a, m) : (b, n) : eqs)
  | (a - b) `mod` d == 0           = resolverTCR ((c, p) : eqs)
  | otherwise                      = Nothing
  where (d, x, y) = emcd m n
        c         = (x * m * b + y * n * a) `div` d
        p         = m * n `div` d
```

Programa 8.3. Con esta definición, si `eqs` es una lista de pares de enteros de la forma `[(a1,m1), ..., (ar,mr)]`, entonce s la expresión `resolverTCD eqs` se evalúa o bien a `Just (c,s)`, en caso de que el sistema de congruencias $x \equiv a_1 \mod m_1, \ldots, x \equiv a_r \mod m_r$ tenga como soluciones a los enteros congruentes con `c` módulo `s`, o bien a `Nothing`, en caso de que ese sistema de ecuaciones no posee ninguna solución. Este código depende del Programa 6.5 en la página 186.

§8.5. Ejercicios

Una demostración alternativa del Teorema Chino del Resto

8.5.1. Ejercicio. Sea $r \in \mathbb{N}$, sean $m_1, \ldots, m_r$ enteros coprimos dos a dos y pongamos $M = m_1 \cdots m_r$. Para cada $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ escribamos $[a]_m$ a la clase de congruencia de a módulo m, que es un elemento del conjunto $\mathbb{Z}_m$.

(*a*) La función $\varphi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ tal que

$$\varphi([a]_M) = ([a]_{m_1}, \ldots, [a]_{m_r})$$

para todo $a \in \mathbb{Z}$ es inyectiva.

(*b*) El dominio y el codominio de la función φ tienen el mismo cardinal, así que φ también es sobreyectiva.

(*c*) Si $b_1, \ldots, b_r$ son enteros, entonces existe un entero x tal que

$$\varphi([x]_M) = ([b_1]_{m_1}, \ldots, [b_r]_{m_r})$$

y si y es otro entero con la misma propiedad entonces $[x]_M = [y]_M$. Deduzca de esto que el Teorema Chino del Resto 8.4.4 vale.