Aritmética modular

Jose Salvador Cánovas Peña.
Departamento de Matemática Aplicada y Estadística.

Índice general

Capítulo 1

Aritmética modular

En este tema vamos a trabajar con los números enteros $\mathbb{Z}$. Sabemos que en este conjunto hay definidas unas operaciones suma "+" y producto "$\cdot$" de forma que se cumplen las siguientes propiedades:

1. La suma es asociativa, conmutativa, existe elemento neutro 0 y cada $n \in \mathbb{Z}$ tiene un elemento inverso que denotamos $-n$, de forma que $n + (-n) = 0$. Esta última propiedad suele escribirse $n - n = 0$, introduciendo aparentemente la resta como una nueva operación, inversa de la suma.

2. El producto es asociativo, conmutativo, existe elemento neutro 1.

3. Se cumple la propiedad distributiva $n \cdot (m + l) = n \cdot m + n \cdot l \ \forall n, m, l \in \mathbb{Z}$.

Además, $0 \cdot n = 0$ para todo $n \in \mathbb{Z}$, ya que $0 + 0 = 0$, por lo que $n \cdot (0 + 0) = n \cdot 0$, y por la propiedad distributiva $n \cdot 0 + n \cdot 0 = n \cdot 0$. Sumando en ambos miembros $(-n \cdot 0)$ obtenemos $n \cdot 0 = 0$.

En este tema vamos a tratar con la operación inversa del producto, la división. Veremos que a partir de ésta pueden derivarse estructuras y nociones complejas.

1.1. División entera

Empezamos el tema con el algoritmo de la divisón. Supondremos por comodidad en este tema que 0 es un número natural.

Theorem 1 *Sean $p, q \in \mathbb{N}$. Entonces existen únicos $d, r \in \mathbb{N}$, $0 \leq r < q$ de forma que $p = q \cdot d + r$.*

Demostración. Sea $d = \text{máx}\{s \in \mathbb{N} : q \cdot s \leq p\}$ de forma que $q \cdot d \leq p < q \cdot (d+1) = q \cdot d + q$. Por tanto existira $r = p - q \cdot d \in \{0, 1, ..., q - 1\}$ tal que $p = q \cdot d + r$. Para comprobar la unicidad, supondremos por reducción al absurdo que existen d_i, r_i, $i = 1, 2$, de forma que $p = q \cdot d_i + r_i$. Podemos suponer que $d_1 \geq d_2$. Entonces $q \cdot d_1 + r_1 = q \cdot d_2 + r_2$, de donde

$q \cdot (d_1 - d_2) = r_2 - r_1$. Si $d_1 = d_2$, se obtiene que $r_1 = r_2$. Así suponemos que $d_1 - d_2 > 1$. Como $r_1 < q$, de $q \cdot (d_1 - d_2) = r_2 - r_1$ se tiene que r_2 debe ser mayor que q, que es una contradicción.□

Los números p, q, d, r se llaman dividendo, divisor, cociente y resto. Dados $a, b \in \mathbb{Z}$, se dice que a divide b si en el algortimo de la división $r = 0$. Se denotará por $a \mid b$, y a se dirá divisor de b. Si a no divide b escribiremos $a \nmid b$. Por ejemplo $4 \mid 16$ pero $5 \nmid 16$. Se verifica la siguiente propiedad.

Proposition 2 *Sean $a, b, c \in \mathbb{Z}$. Entonces:*

(a) Si $a \mid b$, entonces $a \mid b \cdot c$.

(b) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

(c) Si $a \mid b$ y $a \mid c$, entonces $a \mid b \cdot x + c \cdot y$ para cualesquiera $x, y \in \mathbb{Z}$.

(d) Si $a, b \in \mathbb{N} \setminus \{0\}$ y $a \mid b$, entonces $a \leq b$.

(e) Si $a \mid b$ y $b \mid a$, entonces $a = b$ o $a = -b$.

Demostración. (a) Si $a \mid b$, existe $d \in \mathbb{Z}$ tal que $b = a \cdot d$. Entonces $b \cdot c = a \cdot (d \cdot c)$, por lo que $a \mid b \cdot c$.

(b) Si $a \mid b$, existe $d_1 \in \mathbb{Z}$ tal que $b = a \cdot d_1$. Si $b \mid c$, existe $d_2 \in \mathbb{Z}$ tal que $c = b \cdot d_2$. Entonces $c = b \cdot d_2 = a \cdot (d_1 \cdot d_2)$, por lo que $a \mid c$.

(c) Si $a \mid b$, existe $d_1 \in \mathbb{Z}$ tal que $b = a \cdot d_1$. Si $a \mid c$, existe $d_2 \in \mathbb{Z}$ tal que $c = a \cdot d_2$. Entonces

$$b \cdot x + c \cdot y = a \cdot d_1 \cdot x + a \cdot d_2 \cdot y = a \cdot (d_1 \cdot x + d_2 \cdot y),$$

por lo que $a \mid b \cdot x + c \cdot y$.

(d) Si $a \mid b$, existe $d \in \mathbb{Z}$ tal que $b = a \cdot d$. Claramente $d \geq 0$. Si $d = 0$, entonces $b = 0$, que es imposible. Por tanto $d \geq 1$, de donde $b \geq a$.

(e) Si $a \mid b$, existe $d_1 \in \mathbb{Z}$ tal que $b = a \cdot d_1$. Si $b \mid a$, existe $d_2 \in \mathbb{Z}$ tal que $a = b \cdot d_2$. Si $a = 0$, entonces $b = 0$. Supongamos que ambos a y b son no nulos. Entonces $a = (d_2 \cdot d_1) \cdot a$, de donde $d_1 \cdot d_2 = 1$. Entonces o bien $d_1 = d_2 = 1$ y $a = b$, o bien $d_1 = d_2 = -1$ y $a = -b$.□

1.2. Máximo común divisor

Dados $a, b \in \mathbb{Z} \setminus \{0\}$, decimos que d es el máximo común divisor de a y b si es el mayor entero positivo que divide a a y b, es decir, $d \mid a$, $d \mid b$, y si c es tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$. Se denotará por $\gcd(a, b)$. Es fácil darse cuenta de que el máximo común divisor de dos números enteros no nulos es único. Todos sabemos de la enseñanza básica que $\gcd(4, 10) = 2$ mediante un algoritmo de factorización en números primos. No obstante ese algoritmo no es útil si los números son más grandes, al contrario que el algoritmo de Euclides que presentamos a continuación.

Proposition 3 *Sean $a, b \in \mathbb{N} \setminus \{0\}$, con $b \leq a$. Sean $p, r \in \mathbb{N}$, $r < b$ tales que $a = b \cdot p + r$. Entonces $\gcd(a, b) = \gcd(r, b)$.*

Demostración. Sea $c \in \mathbb{N}$ tal que $c \mid a$ y $c \mid b$. Como $r = a - b \cdot p$, por la Proposición 2 (c) se tiene que $c \mid r$. Si $c = \gcd(a, b)$, entonces $c \leq \gcd(r, b)$. Análogamente, sea $d \in \mathbb{N}$ tal que $d \mid r$ y $d \mid b$. Por la Proposición 2 (c) se tiene que $d \mid a$, y si $d = \gcd(r, b)$, entonces $d \leq \gcd(a, b)$. Como consecuencia, $\gcd(a, b) = \gcd(r, b)$.$\square$

El algoritmo de Euclides consiste en aplicar sucesivamente la proposición anterior a una par de números enteros a, b, hasta que se llegue a un resto nulo en un número finito de pasos. El menor de los enteros que queden cuando se produce un resto nulo, que es el resto de la etapa anterior, será el $\gcd(a, b)$. Por ejemplo, vamos a calcular $\gcd(1050, 173)$. En un primer paso dividimos $1050 = 173 \cdot 6 + 12$, por lo que $\gcd(1050, 173) = \gcd(173, 12)$. Ahora $173 = 14 \cdot 12 + 5$, por lo que $\gcd(173, 12) = \gcd(12, 5)$. Ahora $12 = 5 \cdot 2 + 2$, por lo que $\gcd(12, 5) = \gcd(5, 2)$, y $5 = 2 \cdot 2 + 1$, de donde $\gcd(5, 2) = \gcd(2, 1)$. Finalmente $2 = 1 \cdot 2 + 0$, por lo que $\gcd(1050, 173) = 1$.

El siguiente resultado está ligado al algoritmo de Euclides.

Theorem 4 (Bezout) *Sean $a, b \in \mathbb{Z} \setminus \{0\}$ y $d = \gcd(a, b)$. Entonces d es el menor entero positivo tal que $d = a \cdot x + b \cdot y$ para $x, y \in \mathbb{Z}$.*

Demostración. Sea $M := \{m \in \mathbb{N} \setminus \{0\} : m = a \cdot x + b \cdot y,\ x, y \in \mathbb{Z}\}$. $M \neq \emptyset$ ya que $|a| \in M$ al ser de la forma $|a| = (\pm 1) \cdot a + 0 \cdot b$. Así, sea $d := \text{mín}\, M$. Nótese que no es restrictivo suponer que a y b son positivos y sean $x_0, y_0 \in \mathbb{Z}$ tales que $d = a \cdot x_0 + b \cdot y_0$.

Veamos que $d \mid a$ y $d \mid b$. Supongamos que $d \nmid a$ y lleguemos a una contradicción. Si $d \nmid a$, existen enteros p, r, $0 < r < d$ tales que $a = d \cdot p + r$. Entonces $r = a - d \cdot p = a - (a \cdot x_0 + b \cdot y_0) \cdot p = a \cdot (1 - x_0 \cdot p) + b \cdot y_0 \cdot p$, por lo que $r \in M$. Como $r < d$, se contradice que d sea el mínimo de M. Por tanto $d \mid a$ y análogamente $d \mid b$.

Finalmente, veamos que $d = \gcd(a, b)$. Sea $c = \gcd(a, b)$, $c \geq d$. Por la Proposición 2, (c) $c \mid a \cdot x_0 + b \cdot y_0$, esto es, $c \mid d$. Por definición de máximo común divisor $c = d$. $\square$

A partir del algoritmo de Euclides podemos calcular los valores x_0 e y_0 a los que hace referencia el Teorema de Bezout. Por ejemplo, para los números 1050 y 173 del ejemplo anterior, basta ir hacia atrás en el algoritmo de Euclides para obtener

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 5 \cdot 2) = 5 \cdot 5 - 2 \cdot 12 \\ &= 5 \cdot (173 - 12 \cdot 14) - 2 \cdot 12 = 5 \cdot 173 - 72 \cdot 12 \\ &= 173 \cdot 5 - 72 \cdot (1050 - 173 \cdot 6) = -72 \cdot 1050 + 437 \cdot 173, \end{aligned}$$

de donde $x_0 = -73$ e $y_0 = 437$. No obstante, el siguiente algoritmo de Euclides extendido permite obtener tanto en máximo común divisor como los números x_0 e y_0 del Teorema de Bezout de una forma compacta. Se basa en el algoritmo de la división y el método de Gauss de operaciones elementales con matrices.

Algoritmo de Euclides extendido. Sean $a, b \in \mathbb{N}$, $b < a$.

1. Sean d_0 y r_0 tales que $a = b \cdot d_0 + r_0$ y la matriz

$$\begin{pmatrix} b & 1 & 0 \\ a & 0 & 1 \end{pmatrix}.$$

   Denotamos la filas de la matriz por F_1 y F_2 y aplicamos la operación elemental fila $F_2 - d_0 \cdot F_1$ obteniendo la matriz

$$\begin{pmatrix} b & 1 & 0 \\ r_0 & -d_0 & 1 \end{pmatrix}.$$

2. Como $r_0 < b$, cambiamos de orden las filas con la operación elemental $F_1 \times F_2$, obteniendo la matriz
$$\begin{pmatrix} r_0 & -d_0 & 1 \\ b & 1 & 0 \end{pmatrix}.$$

3. Sean d_1 y r_1 tales que $b = r_1 \cdot d_1 + r_1$ y aplicamos la operación elemental $F_2 - d_1 \cdot F_1$, obteniendo la matriz
$$\begin{pmatrix} r_0 & -d_0 & 1 \\ r_1 & 1 + d_0 d_1 & -d_1 \end{pmatrix}.$$

4. Aplicamos la operación elemental $F_1 \times F_2$, obteniendo la matriz
$$\begin{pmatrix} r_1 & 1 + d_0 d_1 & -d_1 \\ r_0 & -d_0 & 1 \end{pmatrix}.$$

5. Repetimos el proceso hasta obtener un resto nulo y una matriz de la forma
$$\begin{pmatrix} d & x_0 & y_0 \\ 0 & x_1 & y_1 \end{pmatrix},$$
es decir, $d = \gcd(a, b)$ y $d = a \cdot x_0 + b \cdot y_0$.

1.3. Números primos

Un número $n \in \mathbb{N} \setminus \{0, 1\}$ se dice primo si sus únicos divisores son el 1 y él mismo. Es decir, si $a \mid n$, entonces $a = 1$ o $a = n$. Dos números $a, b \in \mathbb{Z} \setminus \{0\}$ se dicen coprimos si $\gcd(a, b) = 1$. Como sabemos, el número 3 es primo y a su vez es coprimo con 4, que no es primo al tener 2 como divisor. Se verifica el siguiente resultado.

Theorem 5 *Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$ con $\gcd(a, b) = 1$. Si $a \mid b \cdot c$ entonces $a \mid c$.*

Demostración. Por el Teorema de Bezout, existen enteros no nulos x e y tales que $1 = \gcd(a, b) = a \cdot x + b \cdot y$. Entonces $c = a \cdot x \cdot c + b \cdot y \cdot c$. Como $a \mid b \cdot c$, por la Proposición 2 (a) se tiene que $a \mid b \cdot c \cdot y$, esto es $a \cdot k_1 = b \cdot c \cdot y$. Como obviamente, $a \mid a \cdot x \cdot c$, tenemos que $c = a \cdot x \cdot c + b \cdot y \cdot c = a \cdot (x \cdot c + k_1)$, por lo que $a|c$.□

Si aplicamos el teorema anterior a números primos tenemos el siguiente resultado.

Theorem 6 *Sea $p \in \mathbb{N} \setminus \{0, 1\}$ un número primo y $n_1, ...n_k$ naturales positivos tal que $p \mid n_1 \cdot ... \cdot n_k$. Entonces $p \mid n_i$ para algún $i \in \{1, 2, ..., k\}$.*

Demostración. Lo probamos por inducción. Suponemos en primer lugar que $k = 2$ y $p \mid n_1 \cdot n_2$. Sea $d = \gcd(p, n_1) \in \{1, p\}$. Si $d = 1$ por el Teorema 5 tenemos que $p \mid n_2$. Si $d = p$ obviamente $p \mid n_1$. Ahora supongamos el resultado cierto para k y probémoslo para $k + 1$. Para ello basta con agrupar $m = n_k \cdot n_{k+1}$ y aplicar la hipótesis inductiva a $n_1 \cdot ... \cdot n_{k-1} \cdot m$ resultando que o bien $p \mid n_i$ para $i \in \{1, 2, ..., k - 1\}$, o bien $p \mid m$. En el primer caso el resultado estaría probado, y en el segundo basta aplicar el caso $k = 2$.□

Este resultado se utilizará para probar el Teorema fundamental de la aritmética.

Theorem 7 (Teorema fundamental de la artimética) *Sea $n \in \mathbb{N} \setminus \{0,1\}$. Entonces existen primos $p_1 \leq p_2 \leq .... \leq p_m$ tales que*

$$n = p_1 \cdot p_2 \cdot ... \cdot p_m.$$

Esta descomposición es única, es decir, si existen otros primos $q_1 \leq q_2 \leq ... \leq q_k$, tales que $n = q_1 \cdot q_2 \cdot ... \cdot q_k$, entonces $k = m$ y $p_i = q_i$ para todo $i \in \{1, 2, ..., m\}$.

Demostración. En primer lugar vemos que la descomposición en primos existe. Dado n, si es primo ya existe la descomposición. Si no lo es, debe ser producto de dos naturales $n = n_1 \cdot n_2$. Repetimos el proceso para n_1 y n_2. Como el conjunto de los naturales esta acotado inferiormente, este proceso es finito y la descomposición existe.

Veamos que es única. Supongamos que

$$n = p_1 \cdot p_2 \cdot ... \cdot p_m = q_1 \cdot q_2 \cdot ... \cdot q_k.$$

Como $p_1 \mid q_1 \cdot q_2 \cdot ... \cdot q_k$, por el Teorema 6, $p_1 \mid q_i$ para algún $i \in \{1, 2, ..., k\}$. Podemos suponer que $i = 1$ cambiando de orden si es necesario. Entonces $p_1 = q_1$. Eliminando p_1 de la igualdad en ambos miembros, tenemos que $p_2 \cdot ... \cdot p_m = q_2 \cdot ... \cdot q_k$. Repitiendo este proceso un número finito de veces tenemos que $m = k$ y los primos son iguales.□

La siguiente versión agrupada del teorema anterior debe ser conocida y la descomposición se llama factorización canónica de los números naturales.

Corollary 8 *Sea $n \in \mathbb{N} \setminus \{0,1\}$. Entonces existen primos $p_1 < p_2 < .... < p_m$ y enteros positivos $n_1, ..., n_k$ únicos tales que*

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot ... \cdot p_m^{n_m}.$$

Como vemos, los números primos tienen un papel muy importante en el estudio de los números enteros. El siguiente resultado muestra que son infinitos, lo cual tiene importancia a la hora de encriptar información de forma que su desencriptación sea lo más difícil posible.

Theorem 9 *El conjunto de los números primos en infinito.*

Demostración. Supongamos por reduccón al absurdo que el conjunto de primos es finito y $p_1, ..., p_k$ son todos los primos. El número $n = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$ no es primo ni divisible por los primos anteriores, ya que el resto de la división es 1. Por lo tanto, debe ser primo, lo que es una contradicción.□

1.3.1. Mínimo común múltiplo

Dados $a, b \in \mathbb{Z} \setminus \{0\}$ se define el mínimo común múltiplo de a y b como el menor entero positivo m tal que $a \mid m$ y $b \mid m$. Se denotará $m = \text{lcm}(a, b)$. El siguiente resultado muestra que en realidad está íntimamente ligado al máximo común divisor.

Theorem 10 *Sean $a, b \in \mathbb{Z} \setminus \{0\}$. Entonces*

$$\text{lcm}(a, b) = \frac{|a \cdot b|}{\gcd(a, b)}.$$

Demostración. Basta descomponer en primos y hacer las cuentas.□

1.4. Sistemas de numeración

El sistema de numeración que usamos habitualmente se debe a los árabes y se basa en el orden en que una cifra aparece en el número, y una base. En nuestro caso, la base es 10, de forma que hay 10 cifras, del 0 al 9. Así, el número

$$2379 = 2 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10 + 9.$$

Es decir, podemos escribir números muy altos con una candidad finita de cifras, que se llama base. En general, si la base es $b \in \mathbb{N} \setminus \{0, 1\}$, las cifras $0, 1, ..., b-1$ permiten escribir cualquier número de la forma

$$c_{k-1}c_{k-2}...c_1c_0 = c_{k-1} \cdot b^{k-1} + c_{k-2} \cdot b^{k-2} + ... + c_1 \cdot b + c_0.$$

Son conocidas y utilizadas las bases 2, numeración binaria y 16, donde a las cifras del 0 al 9 se le añaden las letras a, b, c, d, e y f para denotar los números 10, 11, 12, 13, 14, 15.

Cualquier número se puede representar en cualquie base. A modo de ejemplo vamos a representar 2379 en binario. Buscamos k tal que 2^k sea mayor que 2379, en nuestro caso $k = 12$. Dividimos 2379 por $2^{k-1} = 2^{11} = 2048$, cuyo cociente es 1 y resto 331. Por lo tanto

$$2379 = 1 \cdot 2^{11} + 331.$$

Procedemos con el resto de igual forma, buscando k tal que $2^k > 331$, en este caso $k = 9$, y dividimos 331 entre $2^8 = 256$, con cociente 1 y resto 75, de forma que

$$2379 = 1 \cdot 2^{11} + 1 \cdot 2^8 + 75.$$

Repetimos el proceso hasta llegar a un resto nulo, teniendo

$$2379 = 1 \cdot 2^{11} + 1 \cdot 2^8 + 1 \cdot 2^6 + 1 \cdot 2^3 + 1 \cdot 2 + 1.$$

Ahora solo falta rellenar con 0 las potencias de 2 que no aparecen en la suma, es decir,

$$2379 = 1 \cdot 2^{11} + 0 \cdot 2^{10} + 0 \cdot 2^9 + 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1,$$

y el número en forma binaria será

$$100101001011,$$

o

$$100101001011_2$$

para indicar la base 2. Nótese que para recuperar la forma decimal basta con simplificar la suma anterior.

Vamos a representarlo ahora con 16 cifras. Para ello

$$2379 = 9 \cdot 16^2 + 75 = 9 \cdot 16^2 + 4 \cdot 16 + 11,$$

y como 11 lo representamos como b, el número se escribirá

$$94b \quad o \quad 94b_{16}.$$

1.5. Aritmética modular

Es frecuente encontrar situaciones en las que un cantidad finita de números naturales es suficiente para describir o caracterizar el fenómeno. Por ejemplo, las horas del día se cuentan del 0 al 23, y cuando el nuevo día empieza no pasamos a la hora 24, sino a la hora 0. Una situación análoga encontramos al contar minutos y segundos, meses y días del año. Para estos fenómenos tenemos la aritmética modular que pasamos a describir.

Dados $m \in \mathbb{N} \setminus \{0,1\}$ y $a, b \in \mathbb{Z}$, decimos que a es congruente con b módulo m si $m \mid a-b$, es decir, si existe $d \in \mathbb{Z}$ tal que $a - b = m \cdot d$. Se denotará $a \equiv b (\mathrm{mod}\, m)$. La siguiente proposición caracteriza los números que son congruentes.

Proposition 11 *Sean $m \in \mathbb{N} \setminus \{0,1\}$ y $a, b \in \mathbb{Z}$. $a \equiv b (\mathrm{mod}\, m)$ si y sólo si los restos de dividir a y b entre m son iguales.*

Demostración. Sean $d_i \in \mathbb{Z}$, y $r_i \in \{0, 1, ..., m-1\}$, $i = 1, 2$, tales que $a = m \cdot d_1 + r_1$ y $b = m \cdot d_2 + r_2$. Entonces $a - b = m \cdot (d_1 - d_2) + r_1 - r_2$. Si $a \equiv b (\mathrm{mod}\, m)$ entonces $r_1 - r_2 = 0$, con lo que $r_1 = r_2$. Si $r_1 = r_2$, entonces $a - b = m \cdot (d_1 - d_2)$ con lo que $a \equiv b (\mathrm{mod}\, m)$.□

La congruencia permite establecer una relación en el conjunto de los números enteros de forma que $a \sim b$ si y solo si $a \equiv b (\mathrm{mod}\, m)$. La proposición anterior permite ver fácilmente que se trata de una relación de equivalencia. Las clases de equivalencia las podemos identificar con los números $0, 1, ..., m-1$ que son todos los posibles restos que pueden darse al dividir un número entero por m, y definir el conjunto de las clases como $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$, donde $\overline{i} = \{a \in \mathbb{Z} : a = m \cdot d + i, \text{ para algún } d \in \mathbb{Z}\}$, $0 \leq i < m$. Recordemos que, al tratarse de una clase de equivalencia, para todo $a \in \overline{i}$ se tiene que $\overline{i} = \overline{a}$.

La propiedad de las clases de equivalencia anterior permite definir las operaciones suma y producto en $\mathbb{Z}_m$ de la siguiente manera. Dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$, definimos $\overline{a} + \overline{b} = \overline{a+b}$ y $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Tenemos entonces las siguiente propiedad.

Proposition 12 *Las operaciones suma y producto definidas sobre $\mathbb{Z}_m$ están bien definidas, y no dependen del elemento de la clase de equivalencia elegido.*

Demostración. Sean $\overline{a}, \overline{b} \in \mathbb{Z}_m$ y $a_1 \in \overline{a}$ y $b_1 \in \overline{b}$. Entonces $a - a_1 = m \cdot d_1$ y $b - b_1 = m \cdot d_2$ para $d_1, d_2 \in \mathbb{Z}$. Así

$$a + b = a_1 + b_1 + m \cdot (d_1 + d_2),$$

con lo que $\overline{a+b} = \overline{a_1 + b_1}$ y

$$a \cdot b = (a_1 + m \cdot d_1) \cdot (a_2 + m \cdot d_2) = a_1 \cdot a_2 + m \cdot (a_1 \cdot d_2 + a_2 \cdot d_1 + m \cdot d_1 \cdot d_2),$$

con lo que $\overline{a \cdot b} = \overline{a_1 \cdot b_1}$ y la prueba concuye.□

A partir de ahora por simplicidad, dejaremos de escribir la barra superior en las clases. Por ejemplo, en $\mathbb{Z}_4$ se pueden construir las siguientes tablas de suma y producto.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Puede comprobarse que la suma cumple las propiedades conmutativa y asociativa, existe el neutro "0" y cada elemento $a \in \mathbb{Z}_m$ tiene inverso que será la clase de $-a$. Para el producto se cumplen las propiedades conmutativa y asociativa, existe elemento neutro "1", pero no todo elemento tiene inverso como por ejemplo el 2 en $\mathbb{Z}_4$. Además se cumple la propiedad distributiva y $0 \cdot a = 0$ para todo $a \in \mathbb{Z}_m$.

Se dice que $a \in \mathbb{Z}_m$ es invertible si existe $a^{-1} \in \mathbb{Z}_m$ tal que $a \cdot a^{-1} = 1$. Obsérvese que en $\mathbb{Z}_4$, 2 no es invertible, pero $3^{-1} = 3$. El siguiente resultado caracteriza los elementos invertibles en $\mathbb{Z}_m$.

Proposition 13 *Sea $a \in \mathbb{Z}_m$. Entonces:*

(a) a es invertible si y sólo si $\gcd(a, m) = 1$. En particular, si m es primo todos los elementos no nulos de $\mathbb{Z}_m$ son invertibles.

(b) $\gcd(a, m) \neq 1$ si y sólo si existe $b \in \mathbb{Z}_m \setminus \{0\}$ tal que $a \cdot b = 0$.

Demostración. (a) Supongamos que existe $a^{-1} \in \mathbb{Z}_m$ tal que $a \cdot a^{-1} = 1$. Entonces $a \cdot a^{-1} - 1 = m \cdot d$ para algún $d \in \mathbb{Z}$. Así, $a \cdot a^{-1} - m \cdot d = 1$, y por el Teorema de Bezout $\gcd(a, m) = 1$. Siguiendo el razonamiento anterior en sentido inverso, obtenemos la implicación inversa y la prueba concluye.

(b) Sea $d = \gcd(a, m) \neq 1$. Sean a_1 y m_1 tales que $a = a_1 \cdot d$ y $m = m_1 \cdot d$. Ahora $a \cdot m_1 = a_1 \cdot d \cdot m_1 = a_1 \cdot m$, y por tanto $a \cdot m_1 = 0$ y $b = m_1$. Recíprocamente, supongamos que $a \cdot b = 0$ y $\gcd(a, m) = 1$. Entonces a es invertible y por tanto $b = 1 \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$, lo que contracice que $b \neq 0$, y la prueba concluye.□

La existencia de elementos sin inversa en los conjuntos $\mathbb{Z}_m$ hace que haya que tener un cuidado especial a la hora de hacer simplificaciones. En los números reales, si $a \cdot b = a \cdot c$ y $a \neq 0$, entonces $b = c$ porque podemos multiplicar en ambos lados de la igualdad por $a^{-1} = 1/a$. En $\mathbb{Z}_4$ sabemos que $2 \cdot 3 = 2 \cdot 1 = 2$, pero $1 \neq 3$. A continuación resumimos las leyes de simplificación que se pueden aplicar.

Proposition 14 *Sea $m \in \mathbb{N} \setminus \{0, 1\}$ y $a, b, c \in \mathbb{Z}_m$. Entonces:*

(a) Si $a \cdot b = a \cdot c$ y $\gcd(a, m) = 1$, entonces $b = c$.

(b) Si $a \cdot b = a \cdot c$ y $\gcd(a, m) = d$, entonces $b \equiv c (\mathrm{mod}\, \frac{m}{d})$, es decir, $b = c$ en $\mathbb{Z}_{\frac{m}{d}}$.

(c) Si m es primo y $a \cdot b = a \cdot c$, entonces $b = c$.

Demostración. Tanto (a) como (c) son consecuencia de que existe elemento inverso de a por la Proposición 13. Para probar (b) nótese que $a \cdot b - a \cdot c = m \cdot q$ para algún entero q. Como $a = a_1 \cdot d$ con $\gcd(a_1, m) = 1$, entonces $a_1 \cdot d \cdot b - a_1 \cdot d \cdot c = m \cdot q$, por lo que $a_1 \cdot b = a_1 \cdot c = \frac{m}{d} \cdot q$, con lo que $a_1 \cdot b = a_1 \cdot c$ en $\mathbb{Z}_{\frac{m}{d}}$. Aplicando el apartado (a) se concluye la prueba.□

Volviendo al ejemplo anterior en $\mathbb{Z}_4$, sabemos que $2 \cdot 3 = 2 \cdot 1$ y $\gcd(2, 4) = 2$, por lo que $3 = 1$ en $\mathbb{Z}_2$, que es cierta.

1.5.1. Ecuaciones diofánticas y teorema chino de los restos

En esta sección vamos a resolver ecuaciones de la forma

$$a \cdot x + b \cdot y = c,$$

donde $a, b, c \in \mathbb{Z}$ y sólo vamos a buscar soluciones enteras, esto es, x e y deben pertenecer a $\mathbb{Z}$. Estas ecuaciones se llaman diofánticas. Nótese que es equivalente a resolver la ecuación

$$a \cdot x \equiv c (\mathrm{mod}\, b).$$

Por el Teorema de Bezout, sabemos que si $d = \gcd(a, b)$, entonces la ecuación diofántica $a \cdot x + b \cdot y = d$ tiene solución entera. Es más, por la demostración de dicho Teorema de Bezout, para que el problema tenga solución entera, c debe ser un múltiplo del máximo común divisor de a y b, es decir $c = k \cdot \gcd(a, b)$ para algún entero k. Si x_0 e y_0 son enteros tales que

$$a \cdot x_0 + b \cdot y_0 = d$$

entonces $k \cdot x_0$ e $k \cdot y_0$ son las soluciones de $a \cdot x + b \cdot y = c = k \cdot d$. Recordemos que x_0 e y_0 se pueden obtener mediante los algoritmos de Euclides y Euclides extendido.

Relacionado con la ecuaciones anteriores tenemos el Teorema chino de los restos. Un antiguo acertijo chino preguntaba "¿Hay algún entero positivo x tal que cuando x se divide entre 3 se obtiene un resto igual a 2, cuando x se divide entre 5 se obtiene un resto igual a 4 y cuando x se divide entre 7 se obtiene un resto igual a 6?" En nuestro lenguaje esto es equivalente a resolver el sistema de ecuaciones

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 3), \\ x \equiv 4 (\mathrm{mod}\, 5), \\ x \equiv 6 (\mathrm{mod}\, 7). \end{cases}$$

El Teorema chino de los restos resuelve este problema.

Theorem 15 (Teorema chino de los restos) *Consideremos el sistema*

$$\begin{cases} x \equiv r_1 (\mathrm{mod}\, m_1), \\ x \equiv r_2 (\mathrm{mod}\, m_2), \\ \quad \ldots\ldots\ldots\ldots\ldots \\ x \equiv r_k (\mathrm{mod}\, m_k), \end{cases}$$

donde $m_1, ..., m_k$ son coprimos dos a dos. Entonces el sistema tiene solución única módulo $M = m_1 \cdot m_2 \cdot ... \cdot m_k$.

Demostración. Sean $M_i = M/m_i$, $i = 1, 2, ..., k$. Nótese que $\gcd(m_i, M_i) = 1$ para $i = 1, 2, ..., k$. Sean $s_1, s_2, ..., s_k$ las soluciones de las ecuaciones

$$\begin{cases} M_1 \cdot x \equiv 1 (\mathrm{mod}\, m_1), \\ M_2 \cdot x \equiv 1 (\mathrm{mod}\, m_2), \\ \quad \ldots\ldots\ldots\ldots\ldots \\ M_k \cdot x \equiv 1 (\mathrm{mod}\, m_k), \end{cases}$$

esto es, $s_i \equiv M_i^{\varphi(m_i)-1} (\mathrm{mod}\, m_i)$ para $i = 1, 2, ..., k$. Veamos que

$$x_0 = M_1 \cdot r_1 \cdot s_1 + M_2 \cdot r_2 \cdot s_2 + ... + M_k \cdot r_k \cdot s_k,$$

es solución del sistema de congruencias. Para ello, fijamos $i \in \{1, 2, ..., k\}$ y démonos cuenta de que $M_j \cdot r_j \cdot s_j \equiv 0 (\mathrm{mod}\, m_i)$ para $j \neq i$. Entonces

$$x_0 (\mathrm{mod}\, m_i) \equiv M_i \cdot s_i \cdot r_i (\mathrm{mod}\, m_i) \equiv r_i (\mathrm{mod}\, m_i).$$

Además, si x_1 es otra solución del sistema, entonces $x_1 - x_0$ debe ser m´ultiplo de cada m_i. Como los m_i son coprimos entre sí, entonces $x_1 - x_0$ es múltiplo de $M = m_1 \cdot ... \cdot m_k$, lo que concluye la demostración.□

Veamos ahora como resolver el acertijo. Las ecuaciones

$$\begin{cases} 35 \cdot x \equiv 1 (\mathrm{mod}\, 3), \\ 21 \cdot x \equiv 1 (\mathrm{mod}\, 5), \\ 15 \cdot x \equiv 1 (\mathrm{mod}\, 7), \end{cases}$$

pueden simplificarse a

$$\begin{cases} 2 \cdot x \equiv 1 (\mathrm{mod}\, 3), \\ x \equiv 1 (\mathrm{mod}\, 5), \\ x \equiv 1 (\mathrm{mod}\, 7), \end{cases}$$

y tienen por soluciones $s_1 = 2$, $s_2 = s_3 = 1$ por lo que

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 4 \cdot 1 + 15 \cdot 6 \cdot 1 = 314 \equiv 104 (\mathrm{mod}\, 105).$$

1.5.2. Función φ de Euler

El cálculo de inversos en crucial para poder resolver ecuaciones. En $\mathbb{Z}_m$ resulta de gran ayuda la función φ de Euler. Dado $m \in \mathbb{N} \setminus \{0\}$, definimos $\varphi(m)$ como el cardinal del conjunto $\{k \in \{1, 2, ..., m-1\} : \gcd(k, m) = 1\} = \{k \in \mathbb{Z}_m : k \text{ es invertible}\}$. En general no es inmediato calcular el valor de la función de Euler para cualquier número natural, pero sí cuando conocemos sus descomposición en primos a partir del siguiente resultado.

Theorem 16 *Sean $m, n \in \mathbb{N} \setminus \{0\}$. Entonces:*

(a) Si m es primo, entonces $\varphi(m) = m - 1$.

(b) Si m es primo, entonces $\varphi(m^k) = m^k - m^{k-1}$.

(c) Si $\gcd(n, m) = 1$, entonces $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

Demostración. (a) se sigue de que m no tiene divisores. Para (b) hay que darse cuenta de que si $d \mid m^k$, entonces $d = 1$ o múltiplo de m, por lo que los elementos no invertibles de $\mathbb{Z}_{m^k}$ son $m, 2 \cdot m, ...m^{k-1} \cdot m$, que en total son $m^{k-1} - 1$. Como hay $m^k - 1$ elementos distintos de 0 en $\mathbb{Z}_{m^k}$, tenemos que

$$\varphi(m^k) = m^k - 1 - \left(m^{k-1} - 1\right) = m^k - m^{k-1}.$$

Finalmente, para (c) tomamos el conjunto $A_n = \{k \in \{1, 2, ..., n \cdot m - 1\} : \gcd(k, n) = 1\}$. Vamos a establecer una aplicación biyectiva entre los conjuntos $A_{n \cdot m}$ y $A_n \times A_m$. Así, probaremos que $\varphi(n \cdot m) = |A_{n \cdot m}| = |A_n \times A_m| = |A_n| \cdot |A_m| = \varphi(n) \cdot \varphi(m)$.

Así, dado $k \in A_{n \cdot m}$, definimos $f(k) = (k_1, k_2) \in A_n \times A_m$ de forma que k_1 es el único número menor que n tal que $k \equiv k_1 (\mathrm{mod}\, n)$ y k_2 es el único número menor que m tal que $k \equiv k_2 (\mathrm{mod}\, m)$. Vamos a ver que la aplicación $f : A_{n \cdot m} \to A_n \times A_m$ está bien definida, es decir, que $k_1 \in A_n$ y $k_2 \in A_m$. Probamos que $k_1 \in A_n$ (el caso $k_2 \in A_m$ es análogo). Supongamos que $\gcd(k_1, n) = d > 1$. Por el Teorema de Bezout, sabemos que existen $a, b \in \mathbb{Z}$ tales que $d = k_1 \cdot a + n \cdot b$. Como $k \equiv k_1 (\mathrm{mod}\, n)$, se tiene que $k_1 = k + c \cdot n$ para $c \in \mathbb{Z}$. Combinado ambas expresiones tenemos que $d = k \cdot a + n \cdot (a \cdot c + b)$, y por lo tanto $\gcd(k, n) \neq 1$ y entonces $\gcd(k, n \cdot m) \neq 1$, lo que es una contradicción.

Veamos ahora que f es inyectiva. Para ello sean $k, l \in A_{n \cdot m}$ tales que

$$\begin{cases} k \equiv k_1 (\mathrm{mod}\, n), \\ k \equiv k_2 (\mathrm{mod}\, m), \end{cases}$$

y

$$\begin{cases} l \equiv k_1 (\mathrm{mod}\, n), \\ l \equiv k_2 (\mathrm{mod}\, m). \end{cases}$$

Por ser relación de equivalencia, se tiene que

$$\begin{cases} l \equiv k (\mathrm{mod}\, n), \\ l \equiv k (\mathrm{mod}\, m), \end{cases}$$

y así $l \equiv k (\mathrm{mod}\, n \cdot m)$, y como l y k son menores que $n \cdot m$, se tiene que $l = k$.

Veamos ahora que f es sobreyectiva. Fijamos $(k_1, k_2) \in A_n \times A_m$ y consideramos las ecuaciones

$$\begin{cases} x \equiv k_1 (\mathrm{mod}\, n), \\ x \equiv k_2 (\mathrm{mod}\, m). \end{cases}$$

Por el Teorema chino de los restos, existe un único $k < n \cdot m$ tal que es solución. Veamos que $k \in A_{n \cdot m}$. Supongamos que $\gcd(k, n \cdot m) = d > 1$. Como $\gcd(n, m) = 1$, se tiene que o bien $\gcd(k, n) = d$ o bien $\gcd(k, m) = d$. Supongamos por ejemplo que $\gcd(k, m) = d$. Por el algoritmo de Euclides, $\gcd(k, m) = \gcd(k_2, m) = d$, lo que contradice que $k_2 \in A_m$.□

A partir del resultado anterior sabemos que $\varphi(5) = 4$, $\varphi(4) = \varphi(2^2) = 2^2 - 2 = 2$ y que $\varphi(20) = \varphi(5) \cdot \varphi(4) = 8$. Veamos que utilidad tiene la función de Euler.

Theorem 17 (Euler) *Sean $a, m \in \mathbb{Z} \setminus \{0\}$ con $m > 1$ tal que $\gcd(a, m) = 1$. Entonces*

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Demostración. Sean $A := \{m_1, ..., m_{\varphi(m)}\}$ todos los elementos invertibles en $\mathbb{Z}_m$ y $B := \{a \cdot m_1, ..., a \cdot m_{\varphi(m)}\}$. Por la leyes de simplificación de la Proposición 14 todos los elementos de B son distintos. Además, todos los elementos de B son invertibles ya que $\gcd(a \cdot m_i, m) = 1$ para todo $i = 1, 2, ..., \varphi(m)$. Entonces $A = B$. En particular,

$$m_1 \cdot m_2 \cdot ... \cdot m_{\varphi(m)} = (a \cdot m_1) \cdot (a \cdot m_2) \cdot ... \cdot (a \cdot m_{\varphi(m)}).$$

Multiplicando por m_1^{-1} se tiene que

$$m_2 \cdot ... \cdot m_{\varphi(m)} = a \cdot (a \cdot m_2) \cdot ... \cdot (a \cdot m_{\varphi(m)}).$$

Multiplicando sucesivamente por m_2^{-1},...,$m_{\varphi(m)}^{-1}$ tenemos que

$$1 = a^{\varphi(m)},$$

es decir, $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.□

Como corolario se obtiene lo que se conoce como pequeño teorema de Fermat.

Corollary 18 *Sean $a, m \in \mathbb{Z} \setminus \{0\}$ con m primo tal que $\gcd(a, m) = 1$. Entonces*

$$a^{m-1} \equiv 1 (\mathrm{mod}\, m).$$

Para calcular el inverso de 4 en $\mathbb{Z}_7$ basta usar el corolario anterior $4^6 \equiv 1 (\mathrm{mod}\, 7)$, por lo que $4^{-1} = 4^5 = 1024 \equiv 2 (\mathrm{mod}\, 7)$. Es decir, $4^{-1} = 2$. Para calcular el inverso de 3 en $\mathbb{Z}_{20}$ utilizamos el Teorema de Euler $3^{\varphi(20)} = 3^8 \equiv 1 (\mathrm{mod}\, 20)$, por lo que $3^{-1} = 3^7 = 2187 \equiv 7 (\mathrm{mod}\, 20)$, esto es, $3^{-1} = 7$.

Para resolver una ecuación lineal $a \cdot x = b$ en $\mathbb{Z}_m$ el elemento a debe tener inverso siendo la solución $x = a^{-1} \cdot b$. La ecuación puede escribirse como

$$a \cdot x \equiv b (\mathrm{mod}\, m),$$

y a tendrá inverso si y sólo si $\gcd(a, m) = 1$. La solución puede escribirse a partir de la función de Euler como

$$x = a^{\varphi(m)-1} \cdot b (\mathrm{mod}\, m).$$

Por ejemplo, la ecuación $7 \cdot x \equiv 2 (\mathrm{mod}\, 10)$ tiene por solución

$$x = 2 \cdot 7^{\varphi(10)-1} (\mathrm{mod}\, 10) = 2 \cdot 7^3 (\mathrm{mod}\, 10) = 6 (\mathrm{mod}\, 10),$$

esto es $x = 6$ en $\mathbb{Z}_{10}$.

1.6. Ejercicios

1. Calcular $\gcd(215, 36)$ y $\gcd(334, 562)$. Encontrar el mínimo común múltiplo de ambos pares de números y los x_0 e y_0 del Teorema de Bezout.

2. Demostrar que $\sqrt{2}$ no es un número racional.

3. Calcular $\gcd(18, 256)$ y $\gcd(8316, 10920)$. Encontrar el mínimo común múltiplo de ambos pares de números y los x_0 e y_0 del Teorema de Bezout.

4. Enumerar todos los primos menores de 100.

5. Sabiendo que $\gcd(a, b) = 1$ probar las siguientes propiedades:

a) $\gcd(a+b, a-b) = 1$ o 2.

b) $\gcd(3a+b, 2a+b) = 1$.

6. Si $\gcd(a, b) = 2$, obtener $\gcd(a-b, a^2-b^2)$.

7. Sea $d = gcd(a, b)$. Demostrar que a/d y b/d son coprimos.

8. Realizar las siguientes operaciones y devolver el resultado en base 8

$$234_5 + 31_4 \cdot 21_3.$$

9. Encontrar un número entre 0 y 10000 que verifique todas las siguientes propiedades:

a) Las dos últimas cifras al escribirlo en base 8 son 03.

b) Su última cifra en base 9 es 4.

c) Es múltiplo de 7.

10. Realizar las siguientes operaciones en $\mathbb{Z}_{12}$

$$234 + 128 \cdot 54 - (123 + 48 \cdot 7)$$

11. Establecer cuáles de las siguientes congruencias son verdaderas.

a) $446 \equiv 278 (\mathrm{mod}\, 7)$.

b) $269 \equiv 413 (\mathrm{mod}\, 12)$.

c) $445 \equiv 536 (\mathrm{mod}\, 18)$.

d) $793 \equiv 682 (\mathrm{mod}\, 9)$.

e) $473 \equiv 369 (\mathrm{mod}\, 26)$.

f) $383 \equiv 126 (\mathrm{mod}\, 15)$.

12. Encontrar todos los números comprendidos entre -50 y 50 congruentes con 12 módulo 21.

13. Encontrar $\varphi(37)$, $\varphi(137)$, $\varphi(275)$, $\varphi(700)$ y $\varphi(201)$.

14. Escribir las tablas de suma y multiplicación de $\mathbb{Z}_6$ y $\mathbb{Z}_7$.

15. Encontrar usando el teorema de Bezout los inversos siguientes, en caso de que sea posible.

a) 12^{-1} en $\mathbb{Z}_5$.

b) 20^{-1} en $\mathbb{Z}_{14}$.

c) $(\text{-}21)^{-1}$ en $\mathbb{Z}_{13}$.

16. Encontrar a^{-1} en $\mathbb{Z}_m$ donde: a) $a = 37$ y $m = 249$; b) $a = 15$ y $m = 234$.

17. Resolver si es posible las siguientes ecuaciones en $\mathbb{Z}_5$.

    a) $3x^2 - 7x + 1 = 0$.

    b) $x^2 + 5x = 1$.

18. Resolver en $\mathbb{Z}_7$ el siguiente sistema de ecuaciones

$$\begin{cases} 2x + 3y = 1, \\ 3x - 2y = 2. \end{cases}$$

19. Resolver la ecuación lineal de congruencia:

    a) $3x \equiv 2 (\mathrm{mod}\, 8)$.

    b) $6x \equiv 5 (\mathrm{mod}\, 9)$.

    c) $4x \equiv 6 (\mathrm{mod}\, 10)$.

20. Encontrar el menor entero positivo x tal que cuando x se divide entre 3 se obtiene un resto igual a 2, cuando x se divide entre 7 se obtiene un resto igual a 4 y cuando x se divide entre 10 se obtiene un resto igual a 6.

21. Encontrar soluciones enteras de las siguientes ecuaciones, cuando sea posible.

    a) $5x + 7y = 4$.

    b) $6x + 24y = 21$.

    c) $14x + 21y = 49$.

22. Encontrar los inversos siguientes a partir de la función φ de Euler:

    a) 20^{-1} en $\mathbb{Z}_9$.

    b) 7^{-1} en $\mathbb{Z}_{12}$.

23. Resolver el siguiente sistema:

$$\begin{cases} 2x \equiv 3 (\mathrm{mod}\, 7), \\ x \equiv 1 (\mathrm{mod}\, 9), \\ x \equiv 3 (\mathrm{mod}\, 8), \\ x \equiv 0 (\mathrm{mod}\, 11). \end{cases}$$

24. Probar que si son ciertas las siguientes propiedades, y si no lo son, dar un ejemplo que muestre que son falsas.

    a) Si $a|b$, $a|c$, $a|d$, entonces $a|b \cdot p + c \cdot q + d \cdot r$, donde $a, b, c, d, p, q, r \in \mathbb{Z}$.

    b) Si $a|b$, $a|c \cdot d$ entonces $a|b \cdot k + c \cdot l$, donde $a, b, c, d, k, l \in \mathbb{Z}$.

25. Resuelve las siguientes ecuaciones en congruencias:

a) $28x + 13 = 0$ en $\mathbb{Z}_{45}$.

b) $51x + 32 = 0$ en $\mathbb{Z}_{60}$.

c) $36x + 44y = 28$, $x, y \in \mathbb{Z}$.

d) $x \equiv 7 (\mathrm{mod}\, 9)$.

e) $x \equiv 13 (\mathrm{mod}\, 12)$.

26. Cada vez que Pablo va a la tienda se compra tres camisetas, mientras que cada vez que Antonio visita la tienda se compra seis. ¿Es posible que se hayan acabado comprando un total de 152 camisetas? ¿Y 153? En los casos en los que sea posible, ¿cuántas visitas hizo cada uno a la tienda?

27. Una empresa fabrica dos modelos de coche. Para el primero, requiere 24 tornillos, mientras que para el segundo requiere 26.

    a) Si el uno de mayo se requirieron 224 tornillos, ¿cuántos coches se hicieron de cada modelo?

    b) Si el primer modelo se vende por 10000 euros, mientras que el segundo se vende por 12000 euros, ¿cuántos modelos deber´ıa vender la empresa para obtener el máximo beneficio?

Bibliografía

[1] S. Lipschutz y M. L. Lipson, Matemáticas discretas, McGraw-Hill.

[2] M .Díaz Toca, F. Guil Asensio y L. Marín, Matemáticas para la computación, Ed. Diego Marín.