Aritmética Modular

MATEMÁTICA DISCRETA I

F. Informática. UPM

La relación de congruencia

Definición

Dado $m \in \mathbb{Z}, m \geq 1$, diremos que $a, b \in \mathbb{Z}$ son congruentes módulo m si y solo si $m|(a-b)$. Se denota $a \equiv b \pmod{m}$. Llamaremos a m módulo de la congruencia.

Proposición

La relación de congruencia módulo m es una relación de equivalencia, para todo $m \in \mathbb{Z}$.

Definición

Llamaremos $\mathbb{Z}_m$ al conjunto cociente de $\mathbb{Z}$ respecto a la relación de congruencia módulo m. A la clase de $a \in \mathbb{Z}$ se le denota por $[a]_m$, $\overline{a}_m$ o simplemente $\overline{a}$.

La relación de congruencia

Teorema

Sea $m \in \mathbb{N}$, entonces

1. $a \equiv b \pmod{m} \Leftrightarrow$ *el resto al dividir a entre m coincide con el resto al dividir b entre m,*
2. *para todo $a \in \mathbb{Z}$ existe $r \in \{0, 1, \ldots, m-1\}$ tal que $a \equiv r \pmod{m}$.*

Observación

Por el teorema anterior $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$, donde

$$[i]_m = \{a \in \mathbb{Z} \mid a \equiv i \pmod{m}\} = \{i + zm \mid z \in \mathbb{Z}\}.$$

Denoteremos, por simplicidad, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ y le llamaremos conjunto de menores residuos no negativos.

Ejemplo

El menor residuo no negativo de 23 en módulo 7 es 2 y el de -48 es 1.

Compatibilidad de la suma y producto en $\mathbb{Z}$

Las operaciones de suma y producto en $\mathbb{Z}$ se pueden trasladar a $\mathbb{Z}_m$ puesto que son compatibles con la estructura de este último conjunto.

Teorema

Sean $n \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$ tales que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$. Entonces

i) $a + c \equiv b + d \pmod{m}$,

ii) $ac \equiv bd \pmod{m}$.

Dem.

Supongamos que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$. Entonces $a = b + k_1 m$ y $c = d + k_2 m$ con $k_1, k_2 \in \mathbb{Z}$ y por tanto $(a+c) = (b+d) + (k_1 + k_2)m$ con $k_1 + k_2 \in \mathbb{Z}$ y $ac = bd + (bk_2 + ck_1 + k_1 k_2)m$ con $bk_2 + ck_1 + k_1 k_2 \in \mathbb{Z}$. □

Compatibilidad de la suma y producto en $\mathbb{Z}$

Ejercicio

Construir las tablas de la suma y el producto en $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

Ejemplo

Como $1234567 \cdot 90213 \equiv 7 \cdot 3 \pmod{10}$ y $21 \equiv 1 \pmod{10}$ se tiene que $1234567 \cdot 90213 = 1$ en $\mathbb{Z}_{10}$.

Ejemplo

El resto al dividir 6^{123} entre 5 es igual al resto al dividir 1^{123} entre 5, que es 1. El resto al dividir 7^{123} entre 5 es igual al resto al dividir 2^{123} entre 5, que no es inmediato. Pero observamos que $2^4 \equiv 1 \pmod{5}$ y por tanto

$$2^{123} = 2^{4 \cdot 30 + 3} = (2^4)^{30} \cdot 2^3 \equiv 2^3 \equiv 3 \pmod{5}.$$

Criterios de divisibilidad y regla del producto

Teorema (Criterios de divisibilidad)

Sea $n = (a_p \dots a_0)_{10} \in \mathbb{N}$ *en base 10. Entonces* $n = a_p 10^p + a_{p-1} 10^{p-1} + a_{p-2} 10^{p-2} + \cdots + a_2 10^2 + a_1 10 + a_0$ *y por tanto,*

i) $n \equiv a_0 \pmod 2$, *luego n es divisible por 2* $\Leftrightarrow$ a_0 *lo es,*

ii) $n \equiv \sum_{i=0}^{p} a_i \pmod 3$, *luego n es divisible por 3* $\Leftrightarrow \sum_{i=1}^{p} a_i$ *lo es,*

iii) $n \equiv 10a_1 + a_0 \equiv 2a_1 + a_0 \pmod 4$, *luego n es divisible por 4* $\Leftrightarrow (a_1 a_0)_{10}$ *lo es,*

iv) $n \equiv a_0 \pmod 5$, *luego n es divisible por 5* $\Leftrightarrow$ a_0 *lo es,*

v) $n \equiv \sum_{i=0}^{p} a_i \pmod 9$, *luego n es divisible por 9* $\Leftrightarrow \sum_{i=1}^{p} a_i$ *lo es,*

vi) $n \equiv \sum_{i=0}^{p} (-1)^i a_i \pmod{11}$, *luego n es divisible por 11* $\Leftrightarrow \sum_{i=1}^{p} (-1)^i a_i$ *lo es.*

Prueba del 9 para la multiplicación

Teorema

Sean $x, y, z \in \mathbb{N}$. *Entonces* $xy = z \Rightarrow \theta(x)\theta(y) \equiv \theta(z) \pmod 9$, *donde* $\theta((a_p \dots a_0)_{10}) = a_p + a_{p-1} + \cdots + a_1 + a_0$.

Ejemplo

Como $\theta(12)\theta(12) = 9 \not\equiv \theta(145) \pmod 9$ se tiene que $12 \cdot 12 \neq 145$. Por otra parte, como $\theta(12)\theta(12) = 9 \equiv \theta(144) \pmod 9$ es posible que $12 \cdot 12 \neq 144$ aunque en principio no tiene porque ser así puesto que también se tiene que $\theta(12)\theta(12) = 9 \equiv \theta(135) \pmod 9$.

Observación

La prueba del 9 también se puede utilizar para la recuperación de datos perdidos. Por ejemplo, si $53928719937 \cdot 376648 = 20312144X06831176$, entonces $\theta(53928719937) \equiv 0 \pmod 9$, $\theta(376648) \equiv 7 \pmod 9$ y $\theta(20312144X06831176) = 49 + X \equiv 4 + X \pmod 9$. Por tanto $0 \equiv 4 + X \pmod 9$ y como $0 \leq X \leq 9$ ha de ser $X = 5$.

Aritmética en $\mathbb{Z}_n$

Definición

En $\mathbb{Z}_m$ podemos definir dos operaciones binarias internas $+$ y $\cdot$ dadas por $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a}\overline{b} = \overline{ab}$.

Propiedades

En $(\mathbb{Z}_m, +, \cdot)$ se verifican las siguientes propiedades:

i) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$, $\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$ para cualesquiera $a, b, c \in \mathbb{Z}$ (asociativa),

ii) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$, $\overline{a}\overline{b} = \overline{b}\overline{a}$, para cualesquiera $a, b \in \mathbb{Z}$ (conmutativa),

iii) $\overline{a} + \overline{0} = \overline{a}$, $\overline{a}\overline{1} = \overline{a}$, para todo $a \in \mathbb{Z}$ (existencia de elemento neutro),

iv) para todo $a \in \mathbb{Z}$ existe $\overline{-a} \in \mathbb{Z}_m$ tal que $\overline{a} + \overline{-a} = 0$ (existencia de elemento opuesto),

v) $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{ac}$, para cualesquiera $a, b, c \in \mathbb{Z}$ (distributiva).

Aritmética en $\mathbb{Z}_n$

En general no se cumple la propiedad cancelativa, por ejemplo $[2]_6 + [1]_6 = [2]_6 + [4]_6$ pero $[1]_6 \neq [4]_6$.

Proposición

Si $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{\mathrm{mcd}(m,c)}}$ *o lo que es equivalente, si* $\overline{ac} = \overline{b}\overline{c}$ *en* $\mathbb{Z}_m \Rightarrow \overline{a} = \overline{b}$ *en* $\mathbb{Z}_{\frac{m}{\mathrm{mcd}(m,c)}}$.

Corolario

$\mathbb{Z}_m$ *tiene la propiedad cancelativa para el producto si m es primo.*

Unidades en $\mathbb{Z}_m$

Definición

Diremos que $\overline{a} \in \mathbb{Z}_m$ es invertible en $\mathbb{Z}_m$ si existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}\overline{b} = 1$ en $\mathbb{Z}_m$.

Proposición

$\overline{a}$ es invertible en $\mathbb{Z}_m \Leftrightarrow$ existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}\overline{b} = \overline{1}$ en $\mathbb{Z}_m \Leftrightarrow$ existen $b, k \in \mathbb{Z}$ tales que $ab + km = 1 \Leftrightarrow \mathrm{mcd}(a, m) = 1$ (en cuyo caso se puede calcular el inverso por el algoritmo de Euclides).

Definición

Si $\overline{a} \in \mathbb{Z}_m$ es invertible en $\mathbb{Z}_m$ y $\overline{a}\overline{b} = \overline{1}$ en $\mathbb{Z}_m$ diremos que $\overline{b}$ es el inverso de $\overline{a}$ módulo m y lo denotamos por $\overline{b} = \overline{a}^{-1}$ (por la propiedad anterior es fácil ver el inverso de un elemento en módulo m es único).

Unidades en $\mathbb{Z}_m$

Definición

Denotaremos por U_m al conjunto de elementos invertibles de $\mathbb{Z}_m$.

Proposición

Si p es primo entonces $|U_p| = p - 1$.

Propiedades

En $\mathbb{Z}_m$ se verifican las siguientes propiedades:

i) Si $\overline{a}, \overline{b} \in U_m$ entonces $\overline{a}\overline{b} \in U_m$ y $\overline{a}^{-1} \in U_m$.

ii) Si $\overline{a} \in U_m$ entonces $\overline{a}U_m = \{\overline{a}\overline{b} \mid \overline{b} \in U_m\} = U_m$.

La función de Euler

Definición

Se define la función ϕ de Euler como la función $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ que a cada n le hace corresponder el número de enteros x tales que $1 \leq x \leq n$, $\mathrm{mcd}(x, n) = 1$. Se tiene que $\phi(m) = |U_m|$. En particular

$$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2, \phi(7) = 6, \ldots$$

Propiedades

i) Si p es primo $\Rightarrow \phi(p^r) = p^r - p^{r-1}$.

ii) Si $\mathrm{mcd}(a, b) = 1 \Rightarrow \phi(ab) = \phi(a)\phi(b)$.

iii) Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \Rightarrow \phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right)$.

iv) $\sum_{d|n} \phi(d) = n$.

Teoremas de Euler y Fermat

Teorema (Teorema de Euler)

Si $\overline{a} \in U_m$ *entonces* $\overline{a}^{\phi(m)} = \overline{1}$ *en* $\mathbb{Z}_m$. *Por tanto, si* $b \in \mathbb{Z}$ *verifica que* $\mathrm{mcd}(b, m) = 1$ *entonces* $b^{\phi(m)} \equiv 1 \pmod{m}$.

Dem.

Supongamos que $U_m = \{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}\}$ (por tanto $\phi(m) = |U_m| = r$). Sea $\overline{a} \in U_m$. Entonces $\overline{a}U_m = \{\overline{aa_1}, \overline{aa_2}, \ldots, \overline{aa_r}\} = U_m$ y por tanto $\overline{a_1 a_2} \cdots \overline{a_r} = (\overline{aa_1})(\overline{aa_2}) \cdots (\overline{aa_r}) = \overline{a}^r \overline{a_1 a_2} \cdots \overline{a_r}$ en $\mathbb{Z}_m$. Además, como $\overline{a_1 a_2} \cdots \overline{a_r}$ es invertible, podemos multiplicar por su inverso y obtenemos que $a^r \equiv 1 \pmod{m}$.
Por otra parte, si $b \in \mathbb{Z}$ existe $r \in \{0, 1, 2, \ldots, p-1\}$ tal que $b \equiv r \pmod{p}$. Entonces $\mathrm{mcd}(p, r) = \mathrm{mcd}(b, p) = 1$ y por tanto $\overline{r} \in U_m$. Por tanto $b^{\phi(m)} \equiv r^{\phi(m)} \equiv 1 \pmod{m}$. □

Teoremas de Euler y Fermat

Teorema (Teorema de Fermat)

Si p es primo y $p \not| a$ entonces $a^{p-1} \equiv 1 \pmod{p}$.
En particular $2^{p-1} \equiv 1 \pmod{p}$ para todo número primo p. Sin embargo, el recíproco no es cierto (basta considerar $341 = 11 \cdot 13$ que verifica que $2^{340} \equiv 1 \pmod{p}$).

Dem.

Si p es primo y $p \not| a$ entonces $\mathrm{mcd}(a, p) = 1$. Por otra parte, como p es primo se tiene que $\phi(p) = p - 1$. Por tanto $a^{p-1} = a^{\phi(p)} \equiv 1 \pmod{p}$. □

Ejercicio

Usar el teorema de Fermat para calcular el resto de dividir 3^{47} entre 23.

Solución

Como 23 es primo y $23 \not| 3$ entonces $3^{22} \equiv 1 \pmod{23}$. Entonces $3^{44} = 3^{22}3^{22} \equiv 1 \pmod{23}$ y $3^{47} = 3^{44}3^3 \equiv 3^3 \pmod{23} \equiv 4 \pmod{23}$.
Por tanto el resto de dividir 3^{47} entre 23 es 4.

Ecuaciones de congruencias

La ecuación de congruencias $ax \equiv c \pmod{m}$ tiene solución en x si y solo si existen $x, y \in \mathbb{Z}$ tales que $ax = c + my$, y esto es equivalente a que la ecuación diofántica $ax + my = c$ tenga solución. Este hecho justifica el siguiente teorema.

Teorema

La ecuación de congruencias $ax \equiv c \pmod{m}$ *tiene solución en* x *si y solo si* $d = \mathrm{mcd}(a, m) | c$ *en cuyo caso tiene exactamente* d *soluciones distintas en* $\mathbb{Z}_m$ *de la forma*

$$x = x_1 + \frac{mt}{d}, t = 0, 1, 2, \ldots, d - 1,$$

siendo x_1 *una solución particular de la ecuación diofántica* $ax + my = c$.

Ecuaciones de congruencias

Dem.

Por el teorema 2.4.10 y la observación anterior, las únicas soluciones posibles son las de la forma $x = x_1 + \frac{mt}{d}$ con $t \in \mathbb{Z}$.
Vamos a ver primero que cualquier solución de éstas es congruente en módulo m a una de las del enunciado. Por el teorema de la división se tiene que $t = qd + r$ con $0 \leq r < d$. Entonces $\frac{mt}{d} = qm + \frac{rt}{d}$ y por tanto $x_1 + \frac{mt}{d} \equiv x_1 + \frac{mr}{d} \pmod{m}$.
Veamos ahora que todas las soluciones del enunciado del teorema son distintas. Supongamos que existen $0 \leq t_1 < t_2 \leq d-1$ tales que $x_1 + \frac{mt_1}{d} \equiv x_1 + \frac{mt_2}{d} \pmod{m}$. Entonces

$$\left(x_1 + \frac{mt_1}{d}\right) - \left(x_1 + \frac{mt_2}{d}\right) = qm.$$

Luego $m(t_1 - t_2) = qmd$ y por tanto $t_1 - t_2 = qd$ y $d | t_1 - t_2$ con $0 \leq t_1 < t_2 \leq d-1$. Contradicción.

Sistemas de congruencias

Teorema (Teorema del resto chino)

El sistema de congruencias

$$\begin{cases} x \equiv c_1 & (\text{mod } m_1) \\ x \equiv c_2 & (\text{mod } m_2) \\ \quad \vdots & \\ x \equiv c_r & (\text{mod } m_r) \end{cases}$$

donde $\text{mcd}(m_i, m_j) = 1$ *para todo* $i \neq j$*, tiene solución única en* $\mathbb{Z}_{m_1 m_2 \cdots m_r}$.

Sistemas de congruencias

Dem.

Para hallar una solución del sistema consideramos, para $i \in \{1, 2, \ldots, r\}$, $t_i = \dfrac{\prod_{j=1}^{r} m_j}{m_i}$ que cumplen $\mathrm{mcd}(m_i, t_i) = 1$. Entonces para todo $i \in \{1, 2, \ldots, r\}$ existe $y_i \in \mathbb{Z}$ tal que $t_i y_i \equiv 1 \pmod{m_i}$. Por otra parte, como $m_j | t_i$ para todo $i \neq j$ se tiene que $t_i y_i \equiv 0 \pmod{m_j}$. Entonces

$$\begin{cases} c_i t_i y_i \equiv c_i \pmod{m_i} \\ c_i t_i y_j \equiv 0 \pmod{m_j} \text{ si } j \neq i \end{cases}$$

Sea $x_0 = \sum_{i=1}^{r} c_i t_i y_i$. Entonces x_0 es solución del sistema inicial.

Para hallar la solución general, observamos que si x_1 es otra solución, entonces $x_0 \equiv x_1 \pmod{m_i}$ para todo $i \in \{1, 2, \ldots, r\}$ y por tanto $m_i | x_0 - x_1$ y, como $\mathrm{mcd}(m_i, m_j) = 1$ para todo $i \neq j$, entonces $m_1 m_2 \cdots m_r | x_0 - x_1$ y por tanto $x_1 \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$. Por tanto, la solución general es $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$. □

Sistemas de congruencias

Corolario

Sean $x, y \in \mathbb{Z}$ *tales que*

$$\begin{aligned} x &\equiv y \pmod{m_1} \\ x &\equiv y \pmod{m_2} \\ &\vdots \\ x &\equiv y \pmod{m_r} \end{aligned}$$

donde $\mathrm{mcd}(m_i, m_j) = 1$ *para todo* $i \neq j$. *Entonces* $x \equiv y \pmod{m_1 m_2 \cdots m_r}$.

Ejercicio

¿Qué entero al dividirlo por 2 da de resto 1 y al dividirlo por 3 da también de resto 1?

Ejercicio

Aritmética con números grandes

Casi todos los procesadores trabajan mucho más rápido con números pequeños que con números grandes. Este problema puede resolverse utilizando congruencias. Para ello consideramos un conjunto $\{m_1, m_2, \ldots, m_k\}$ de números primos entre sí (esto es $\mathrm{mcd}(m_i, m_j) = 1$ para todo $i \neq j$). Entonces cualquier número positivo s menor que $m = m_1 m_2 \cdots m_k$ se puede expresar mediante una n-upla $(r_1, r_2, \ldots, r_k)$ (con $0 \leq r_i < m_i$ para todo $i \in \{1, 2, \ldots, k\}$) donde

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ \vdots \\ x \equiv r_k \pmod{m_k} \end{cases}$$

Además, por el teorema del resto chino existe un único $x \in \{0, 1, 2, \ldots, m\}$ satisfaciendo estas condiciones. Además, si

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ \vdots \\ x \equiv r_k \pmod{m_k} \end{cases} \quad \text{y} \quad \begin{cases} x' \equiv r'_1 \pmod{m_1} \\ \vdots \\ x' \equiv r'_k \pmod{m_k} \end{cases}$$

Aritmética con números grandes

Por tanto, las operaciones aritméticas se pueden realizar entre las r-uplas – cuyas coordenadas son todas menores o iguales que $\max_{1\leq i\leq r} m_i$ –, pudiendose realizar estas operaciones en paralelo. Esto es, para sumar n y n' se suman los vectores asociados $(r_1, r_2, \ldots, r_k)$ y $(r'_1, r'_2, \ldots, r'_k)$ y para multiplicar n y n' se multiplican escalarmente los vectores asociados. Finalmente $x + x'$ y xx' serán las soluciones (únicas en $\mathbb{Z}_m$) de los sistemas anteriores.

Por ejemplo se pueden considerar $m_1 = 99$, $m_2 = 98$, $m_3 = 97$ y $m_4 = 95$ para trabajar con números menores o iguales que $m = m_1 m_2 m_3 m_4 = 89403930$.

Otros enteros que pueden escogerse son los de la forma $2^k - 1$ con $k \in \mathbb{N}$ puesto que es relativamente fácil encontrar conjuntos de estos enteros primos entre sí $(\mathrm{mcd}(2^a - 1, 2^b - 1) = 2^{\mathrm{mcd}(a,b)} - 1)$. Además con estos enteros es fácil trabajar en base 2. Por ejemplo, $2^{35} - 1$, $2^{34} - 1$, $2^{33} - 1$, $2^{31} - 1$, $2^{29} - 1$ y $2^{23} - 1$ son primos entre sí y el producto de ellos es mayor que 2^{184}.

Aritmética con números grandes

Ejemplo

Si tomamos $m_1 = 3$, $m_2 = 4$ se tiene que

$$\begin{array}{llllll} 0 = (0,0) & 1 = (1,1) & 2 = (2,2) & 3 = (0,3) & 4 = (1,0) & 5 = (2,1) \\ 6 = (0,2) & 7 = (1,3) & 8 = (2,0) & 9 = (0,1) & 10 = (1,2) & 11 = (2,3) \end{array}$$

y $5 + 6 \equiv (2,1) + (0,2) = (2,3) \equiv 11$. Por otra parte y $2 \cdot 3 \equiv (2,2) \cdot (0,3) = (0,6) \equiv (0,2) \equiv 6$. Sin embargo $5 \cdot 6$ no es calculable, puesto que el resultado es mayor o igual que 12.

Criptografía

Una de las principales aplicaciones de las congruencias es la codificación y decodificación de mensajes. La teoría de congruencias se utiliza de la siguiente manera:

- A cada letra del alfabeto se le asigna el valor numérico (entre 01 y 27) de su posición.
- Se sustituye cada letra del mensaje por su correspondiente valor numérico.
- El número resultante se cifra mediante una transformación numérica.

Criptografía

Código privado de César. Uno de los primeros métodos de codificación es el llamado "Código privado de César", utilizado por Julio César. Consta de una sola clave para cifrar y descifrar que solo conocen el emisor y el receptor de mensaje. Es por eso que estos métodos de codificación se conocen como de clave privada. Para codificar el mensaje cifrado se toma una función lineal del tipo $f(x) = ax + b$ con $\mathrm{mcd}(a, 27) = 1$ (César tomaba $a = 1$ y $b = 3$) y se reemplaza cada par de cifras p del mensaje, empezando por la derecha, por $ap + b \pmod{27}$.
Para decodificar el mensaje hay que calcular $f^{-1}(q) = a^{-1}(q - b) \pmod{27}$ y por eso es necesario que $\mathrm{mcd}(a, 27) = 1$.

Criptografía

Código Público. Existen otros métodos de codificación de "clave pública". Uno de ellos es el RSA, creado en 1976 en el M.I.T. Se diferencia del anterior en que existen dos claves, una de cifrado que es pública y conocida por cualquiera y una clave privada de descifrado. Está basado en exponenciación modular módulo el producto de dos números primos grandes. La seguridad de la codificación se basa en el hecho de que la factorización de números grandes en sus factores primos (cuando estos factores son también grandes, es practicamente imposible.

Criptografía

Para cifrar el mensaje consideramos dos números primos p y q suficientemente grandes (de unas 200 cifras, por ejemplo) que serán conocidos solamente por la persona que recibe el mensaje. Consideramos $n = pq$ y un exponente e primo con $(p-1)(q-1)$. Ambos números podrán ser conocidos por cualquiera. El mensaje M se codifica reemplazandolo por $C \equiv M^e \pmod{n}$.
Para decodificar el mensaje, como $\mathrm{mcd}(e,(p-1)(q-1)=1$ existen $d, k \in \mathbb{Z}$ tales que $ed = 1 + k(p-1)(q-1)$. Entonces

$$C^d = (M^e)^d = M^{ed} = M^{1+k(p-1)(q-1)} = M(M^{p-1})^{k(q-1)} = M(M^{q-1})^{k(p-1)}$$

Pero en general se tendrá que $\mathrm{mcd}(M,p) = \mathrm{mcd}(M,q) = 1$ y, por el Teorema de Fermat se tiene que $M^{p-1} \equiv 1 \pmod{p}$ y $M^{q-1} \equiv 1 \pmod{q}$. Por tanto $C^d \equiv M \pmod{p}$ y $C^d \equiv M \pmod{q}$. Luego, por el Teorema del resto chino, $C^d \equiv M \pmod{pq}$.

Criptografía

El método del código público tiene la limitación de que el emisor de un mensaje dado puede ser en principio cualquiera. Para que el emisor pueda identificarse se utiliza el siguiente método. El emisor E del mensaje M lo codifica primeramente usando su función de decodificación (privada) y el mensaje resultante lo codifica nuevamente usando ahora la función de codificación (pública) del futuro receptor R del mensaje. E envia el mensaje final a R. Éste lo decodifica usando su función de decodificación (privada) y el mensaje resultante lo codifica nuevamente usando ahora la función de codificación (pública) de E. Si el mensaje resultante es un mensaje comprensible, necesariamente habrá sido emitido por E. A todo este proceso se le conoce como Firma Digital.