TEMA 1.- ARITMÉTICA

1.1.- ARITMÉTICA ENTERA

Principio del buen orden: Todo subconjunto no vacío de N tiene un primer elemento

Propiedades de la suma y el producto en Z

- Son operaciones internas en Z
- Son asociativas y conmutativas
- Ambas tienen neutro, el de la suma es 0 y el de la multiplicación es 1.
- El producto es distributivo respecto a la suma: $a\cdot(b+c) = (a\cdot b) + (a\cdot c)$
- Todo elemento tiene opuesto respecto a la suma
- Si $a\cdot b = 0 \Rightarrow a = 0$ o $b = 0$

Suelen resumirse las propiedades anteriores diciendo que $(Z,+,\cdot)$ es un dominio con 1, y que $(Z,+)$ es un grupo conmutativo o abeliano.

Definición Siendo $a, b \in Z$, diremos que *b es mayor que a*, si existe un natural n tal que $b=a+n$. Lo denotaremos *por b > a*.

Siendo $b, c \in Z$, diremos que *b divide a c*, si existe un entero q tal que $c = q\cdot b$. Lo denotaremos *b|c*.

Propiedades de Z respecto a la división y el producto

1. $a\cdot 0 = 0$
2. $a(-b) = -ab$
3. Si $a \neq 0$, $ab = ac \Rightarrow b = c$
4. Si $a \neq 0$ y $a|b \Rightarrow a|bk$, $\forall k \in Z$
5. Si $a \neq 0$, $b \neq 0$ $a|b$ y $b|c \Rightarrow a|c$
6. Sea $a \neq 0$ si $a|b$, $a|c \Rightarrow a|(xb+yc)$ para cualquier par de enteros x e y
7. $a,b > 0$, $a|b \Rightarrow a \leq b$
8. $a \neq 0$, $b \neq 0$, $a|b$, $b|a \Rightarrow a = b$ ó $a = -b$
9. Si $a \leq b$, $m > 0 \Rightarrow am \leq bm$
   Si $a \leq b$, $m < 0 \Rightarrow am \geq bm$

Demostración (usando las propiedades de la suma y el producto):

1. $a\cdot 0 = a\cdot(0+0) \rightarrow a\cdot 0 + a\cdot 0 = a\cdot 0$. Sumando su opuesto $-a\cdot 0$ nos queda $0 + a\cdot 0 = 0$. Pero, como 0 es el neutro de la suma, nos queda $a\cdot 0 = 0$
2. Veamos que $a(-b) = -ab$. Como el opuesto es único, basta ver que $ab + a(-b) = 0$. Esto es así porque $ab + a(-b) = a(b-b) = a\cdot 0 = 0$
3. Sea $a \neq 0$ y $ab = ac$. Luego $ab + (-ac) = ac + (-ac)$, y $ab-ac = 0$ y $a(b-c) = 0$. Como $a \neq 0$ tendrá que ser $b-c = 0 \Rightarrow b = c$.
4. $a|b \Rightarrow b = aq$, luego $bk = aqk$. Sea $q' = qk$, entonces $bk = aq'$ y por tanto $a|bk$.
5. Se cumple porque $c = bk$, y $a|b \Rightarrow a|bk$
6. $a|b$, $a|c \Rightarrow b = aq_1$, $c = aq_2$.
   $bx + cy = aq_1x + aq_2y = a(q_1x + q_2y) = aq \Rightarrow a|bx + cy$
7. $a|b \Rightarrow b = aq$. Como a, b son positivos, q es positivo. Por tanto, podemos escribir
$$b = a + \overset{q \text{ veces}}{\ldots} + a = a + (a + \overset{q-1 \text{ veces}}{\ldots} + a) = a + s$$
   Como q es positivo y entero, $q-1 \geq 0$, por tanto $s \geq 0$. De $b = a + s$ se deduce que $a \leq b$.

8. $\left.\begin{array}{l} a \mid b \Rightarrow b = aq_1 \\ b \mid a \Rightarrow a = bq_2 \end{array}\right\}$ $a = (aq_1)q_2 \Rightarrow q_1 \cdot q_2 = 1 \Rightarrow q_1 = q_2 = 1$ ó $q_1 = q_2 = -1$, por lo que $a = b$ ó $a = -b$.
9. Si $a \leq b$, debe existir un natural n con $b = a + n$. Ahora, al multiplicar por m, tenemos $bm = am + nm$ y, dado que nm es un número natural porque $m > 0$, tenemos que $am \leq bm$. La otra afirmación se demuestra de forma semejante.

Valor absoluto

Llamaremos valor absoluto a la aplicación $f : Z \to Z$ que a cada $m \in Z$ le asocia $|m|$, definido por $|m|=\max\{m,-m\}$

Propiedades del valor absoluto en Z

1. $|a| = 0 \Leftrightarrow a = 0$
2. $|a \cdot b| = |a| \cdot |b|$
3. $|a + b| \leq |a| + |b|$
4. $k > 0$ y $|a| \leq k \Leftrightarrow -k \leq a \leq k$

Demostración:
Vamos a demostrar solamente que $|a + b| \leq |a| + |b|$:
Se presentan tres casos:
1. $a, b \geq 0$, en este caso $a + b \geq 0$. Por tanto $|a + b| = a + b = |a| + |b|$
2. $a, b < 0$, luego $a + b < 0$. Tendremos $|a + b| = -(a + b) = (-a) + (-b) = |a| + |b|$
3. $a \geq 0$, $b<0$. Se presentan 2 subcasos:
   3.1. $a \geq -b$, entonces $a + b \geq 0$ y $|a + b| = a + b = |a| - |b| \leq |a| + |b|$
   3.2. $a < -b$ con lo que $a + b < 0$, tendremos $|a + b| = -(a + b) = -a - b = -|a| + |b| \leq |a| + |b|$

Teorema de la división
Para $a \in Z$, $b \in N$. Existen unos únicos $q, r \in Z$ tales que $a = q \cdot b + r$, $0 \leq r < b$
A los números a, b, q y r se les llama *dividendo*, *divisor*, *cociente* y *resto*.

Demostración

1.- Demostramos que existen $q, r \in Z$ tales que $a = q \cdot b + r$, $0 \leq r < b$:

Consideremos el conjunto $\{b \cdot q / q \in Z, b \cdot q \leq a\}$ que es un conjunto acotado superiormente. Sea bq el mayor múltiplo de b que es menor o igual que a, se cumple que $b \cdot q \leq a < b \cdot (q+1)$

Restando bq en la desigualdad anterior tenemos que

$0 \leq a - bq < b(q+1) - bq = b \Rightarrow$ si tomamos $r = a - bq$ tendremos $0 \leq r < b$

2.- Demostremos la unicidad de q y r.

Si existiesen r_1, q_1, y r_2, q_2 con $a = bq_1 + r_1 = bq_2 + r_2$, entonces $b(q_2 - q_1) = r_1 - r_2$ y, por tanto, $b \mid (r_1 - r_2)$.

Pero, si fuese $r_1 - r_2 \neq 0$

- Si $b \mid x \Rightarrow |x| \geq |b|$. Por tanto $|r_1 - r_2| \geq |b|$.
- Como $0 \leq r_1 < b$ y $0 \leq r_2 < b$, es obvio que $|r_1 - r_2| < b$.

Esto nos lleva a una contradicción entre $|r_1 - r_2| < |b|$ y $|r_1 - r_2| \geq |b|$. Esta contradicción no existiría si $r_1 - r_2 = 0$, por lo que es un error suponer $r_1 \neq r_2$. Viendo que $r_1 = r_2 \Rightarrow q_1 = q_2$.

Máximo Común Divisor

Sean $a, b \in Z$, $d \in Z^+$, se dice que d es *divisor común* de a, b si $d \mid a$ y $d \mid b$.
Además, el divisor común d será un *máximo común divisor* de a, b si es divisible por cualquier otro divisor de a, b. Lo denotaremos por *mcd(a,b)*.

Todo lo anterior también es válido sustituyendo a, b por una sucesión finita $a_1, a_2, \ldots a_n$.

Ejemplo: Los divisores comunes de 42 y 70 son 1,2,7,14. El mcd(42,70) es 14.

Teorema de Bezout

Para a, b, enteros distintos de 0 y d = mcd(a,b), d es el entero positivo más pequeño que puede expresarse de la forma ax + by, con x, $y \in Z$ (d es, por tanto, único).

Demostración:

Sea M ={m = ax + by / ax + by > 0 con x, $y \in Z$}. Como |a| = a (± 1) + 0b, y |a|>0, tendremos que |a| está en M y este conjunto es no vacío. Por el principio de la buena ordenación M tiene un primer elemento que llamaremos d. Como $d \in M$, existen x_1, $y_1 \in Z$ tal que $d = ax_1 + by_1$. Llegados a este punto tenemos que:

- d es divisor común de a y b:

Si d no dividiese al número a, se cumpliría $a = dq + r$ con $0 < r < d$ (algoritmo de la división). Por tanto $r = a - dq = a - (ax_1 + by_1)\cdot q = a\cdot(1 - x_1\cdot q) + b(-y_1\cdot q)$, con lo que vemos que $r \in M$. Sin embargo no es posible que $r \in M$ y $r < d$ porque definimos d como el primer elemento de M.
La contradicción se resolvería si r = 0, por tanto d|a y, análogamente, podemos probar que d|b.

- d es el máximo común divisor:

Sea d' tal que d'|a, d'|b. Esto implica d´|(ax + by), pero como d = ax + by entonces d´|d.

- d es único:

Si existieran d_1, d_2 = mcd(a,b), por definición de mcd cumplirían $d_1|d_2$ y $d_2|d_1$. Como ambos son positivos, tendremos que $d_2=d_1$.

Algoritmo de Euclides básico y extendido

Algoritmo de Euclides

Sirve para calcular el máximo común divisor de dos números a y b. Para enunciar este algoritmo nos serviremos de una proposición y un teorema previos.

Proposición Sean $a \leq b$ con $b \neq 0$, por el algoritmo de la división tendremos que $a = bq + r$. Entonces se cumple:

1) Los divisores comunes de a y b también son divisores de r
2) Los divisores comunes de b y r también son divisores de a

Demostración:

(1) Sea c tal que c|a, c|b, entonces $a = cq_1$, $b = cq_2$. Luego $cq_2q + r = cq_1 \Rightarrow r = c(q_1 - q_2\cdot q) \Rightarrow c|r$.

(2) Supongamos ahora c tal que c|b, c|r. Por tanto $b = cq_1$, $r = cq_2$ y tendremos $a = cq_1q + cq_2 \Rightarrow a = c(q_1q+q_2) \Rightarrow c|a$.

Teorema En una división el máximo común divisor del dividendo y el divisor es igual al máximo común divisor del divisor y el resto, es decir, si $a = bq + r$, con a, b, q, $r \in Z$, $b \neq 0$, se cumple mcd(a,b) = mcd(b,r).

Demostración:

Como vimos antes, dividendo y divisor tienen los mismos divisores que divisor y resto. Por tanto, ambos tendrán el mismo máximo común divisor.

Algoritmo de Euclides

Como mcd(a,b) = mcd(|a|,|b|), podemos suponer sin perdida de generalidad que $a \geq b > 0$.

Dividimos a por b, $a = bq_1 + r_1$, con $0 \leq r_1 < b$

Si $r_1 = 0$, ya que $a \leq b$, es obvio que b = mcd(a,b) y hemos terminado.

Si $r_1 \neq 0$, dividimos b por r_1, $b = r_1q_2 + r_2$, con $0 \leq r_2 < b$

Si $r_2 = 0$, entonces mcd(b,r_1) = r_1 y por el teorema anterior mcd(b,r_1) = r_1 = mcd(a,b).

Si $r_2 \neq 0$ continuamos dividiendo r_1 por r_2, y así sucesivamente

De este modo obtenemos un conjunto de números $r_1 > r_2 > \ldots$, de modo que llegaremos a un $r_n = 0$. Entonces:

$$r_{n-1} = mcd(r_{n-2}, r_{n-1}) = \ldots = mcd(b, r_1) = mcd(a,b)$$

Nota.- El número de pasos necesarios es como máximo 5 veces el número de dígitos del número más pequeño de entre los a, b por los que comenzamos a calcular el máximo común denominador

Algoritmo extendido de Euclides

Sirve para hallar los términos de la combinación lineal que da origen al máximo común divisor. Para ello se realiza el proceso inverso al seguido en el algoritmo de Euclides. Vamos a verlo con un ejemplo:

Ejemplo: Calcular mcd(3120,270) y los números x, y tales que mcd(3120,270) = 3120x + 270y.

1.- Algoritmo de Euclides:

$3120 = 11 \cdot 270 + 150$

$270 = 1 \cdot 150 + 120$

$150 = 1 \cdot 120 + 30$

$120 = 4 \cdot 30 + 0$

$30 = mcd(120,30) = mcd(150,120) = mcd(270,150) = mcd(3120,270)$

$30 = mcd(3120,270)$

2.- Algoritmo extendido de Euclides:

Realizamos el camino inverso al algoritmo de Euclides empezando por la expresión donde el máximo común divisor es igual al resto.

Iremos sustituyendo valores con el objeto de llegar a los números de los que se hallo el máximo común denominador.

$150 - 1 \cdot 120 = 30$

$150 - 1 \cdot (270 - 1 \cdot 150) = 30 \rightarrow 150 - 270 + 150 = 30 \rightarrow 2 \cdot 150 - 270 = 30$

$2 \cdot (3120 - 11 \cdot 270) - 270 = 30 \rightarrow 2 \cdot 3120 - 22 \cdot 270 - 270 = 30 \rightarrow 2 \cdot 3120 - 23 \cdot 270 - 270 = 30$

Así pues, $mcd(3120, 270) = 30 = 2 \cdot 3120 + (-23) \cdot 270$. Luego, $x = 2$, $y = -23$.

Números primos

Decimos que $p \in Z$ con $p > 1$, es *primo* si sus únicos divisores positivos son 1 y p.

En caso contrario decimos que es *compuesto* y puede expresarse como $p = a \cdot b$ con $1 < a < p$ y $1 < b < p$

Decimos que dos números son *primos entre sí*, cuando $mcd(a,b) = 1$

Observación: Todo entero puede expresarse como xk, xk+1, xk+2, ... xk+(x–2), xk+(x–1)

Lema de Euclides Sean a, b, $c \in Z$ con $mcd(a,b) = 1$. Entonces si $a|bc$, debe cumplirse que $a|c$.

Demostración:

$d = mcd(a,b) = 1 \Rightarrow d = ax + by$ para algun x, $y \in Z$

$c \cdot ax + c \cdot by = c \cdot 1$

Por hipótesis $a|bc$, por tanto, $a|cby$. Es obvio que $a|cax$.

Y así, $\left.\begin{matrix} a \mid cby \\ a \mid cax \end{matrix}\right\} \Rightarrow a|(cax + cby) = c$, luego $a|c$

Corolario: SeaN p, a, b, $c \in Z$, $p > 1$. Entonces p primo $\Leftrightarrow$ si $p|ab$ entonces $p|a$ o $p|b$.

Demostración:

"⇒" Sea p primo, p|ab. Si p es primo con a, basta usar el Lema de Euclides. Si no es primo con a, entonces mcd(p,a) = d ≠ 1, y por tanto d|p, d|a. Como p es primo, d|p ⇒ d = p y por tanto p|a.

"⇐" En el caso de que p no fuese primo, existirían a, b∈Z tal que p = ab con 1 < a < p, 1 < b < p. Con lo que p|ab pero no dividiría a ninguno de los dos.

Corolario: Sea p primo. Si $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_r)$, entonces $p|a_i$ para algun i.

Teorema fundamental de la aritmética

Sea n>1,n∈Z, entonces existen números primos $p_1,\ldots,p_k$ tales que $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ con $p_1 \leq p_2 \leq \ldots \leq p_k$

Esta factorización es única, es decir, si $n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ con $q_1 \leq q_2 \leq \ldots \leq q_m$ entonces k = m y $q_i = p_i$ para i=1,2,..,k

Demostración :

Demostremos primero que todo número es factorizable.

Si el número es primo, la consecuencia es obvia. En otro caso, podrá ponerse de la forma n = ab con a, b < n. Repitiendo el procedimiento con a y b, obtenemos que n puede ponerse como producto de números cada vez menores. Como N está acotado inferiormente por 1, este proceso ha de pararse alguna vez. En ese momento, n estará puesto como producto de números que no pueden factorizarse más, es decir, de números primos.

Si $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ con $p_1 \leq p_2 \leq \ldots \leq p_k$ y $n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ con $q_1 \leq q_2 \leq \ldots \leq q_m$, obtenemos $p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_m$, por lo que $p_1 | q_1 \cdot q_2 \cdot \ldots \cdot q_m$. Así pues, $p_1 | q_i$ para algún i. Esto quiere decir, teniendo en cuenta que q_i es primo, que $p_1 = q_i$. Podemos pues simplificar la expresión anterior y, razonando análogamente, demostrar que existe un j con que $p_2 = q_j$, y así sucesivamente. Reiterando el proceso, obtenemos que cada p_i es igual a un q_j distinto (y recíprocamente). Por tanto, k = m y los conjuntos $\{p_1,p_2,\ldots,p_k\}$ y $\{q_1,q_2,\ldots,q_m\}$ son iguales. Dado que ambos conjuntos están ordenados de forma creciente, tendremos que $q_i = p_i$ para cada i=1,2,..,k

Corolario Sea n∈Z con |n| > 1. Entonces n tiene una factorización única de la forma $n = \pm p_1^{\alpha 1} \ldots p_t^{\alpha t}$ formada de 1 o más primos distintos, cuyos exponentes son ≥ 1. Esta expresión se llama la factorización canónica de n.

Ejemplos

$-48 = -(24 \cdot 2) = -(12 \cdot 2 \cdot 2) = -(3 \cdot 2 \cdot 2 \cdot 2 \cdot 2) = -(3 \cdot 2^4)$

$363 = 121 \cdot 3 = 11^2 \cdot 3$

Teorema El número de primos es infinito

Demostración:

Supongamos que $P = \{p_1,\ldots,p_t\}$, es el conjunto finito de números primos y hallemos la contradicción buscando un número primo que no se halle en ese conjunto

Sea $m = (p_1 \cdot p_2 \cdot \ldots p)+1$. Al ser m entero mayor que 1, podemos factorizarlo $m = q_1 \cdot \ldots q_s$ siendo los q_i números primos. Como m no es divisible por ningún p_i, en particular tampoco lo será q_1. Por tanto q_1 es un primo que no está en $P=\{p_1,\ldots,p_t\}$

Teorema Sea a∈**Z**, a > 1. Si para todo primo $p \leq \sqrt{a}$ no se cumple p|a, entonces a es primo

Demostración:

Sea un número a compuesto: a = b·c con 1 < b <a, 1 < c < a, tal que no es divisible por algún primo $\leq \sqrt{a}$.

Podemos suponer sin perdida de generalidad que $b \leq c$. Como $b \leq c$, $b^2 \leq b \cdot c$ y $b \leq \sqrt{a}$. Pero esto es una contradicción porque:

- Si b es primo llegamos a una contradicción por suponer que a no es divisible por

algún primo $p \leq \sqrt{a}$

- Si b es compuesto llegamos a una contradicción, pues b compuesto podría expresarse como producto de primos, y siendo p uno de ellos: b|a, p|b $\Rightarrow$ p|a, siendo $p < b \leq \sqrt{a}$.

Contradicción en ambos casos, que se deshace si el número a es primo.

Cálculo del m.c.d. a partir de la factorización de a y b

Siendo a, b enteros, consideremos sus factorizaciones canónicas. Podemos pasar a una factorización "común" de a y b de la forma $a = \pm(p^{\alpha 1})_1 \dots (p^{\alpha t})_t$, $b = \pm(p^{\beta 1})_1 \dots (p^{\beta t})_t$ sin más que añadir, con exponente 0, los factores primos que le falten a cada uno respecto al otro.

Por ejemplo, la factorización "común" de 350 (= $2 \cdot 5^2 \cdot 7$) y 198 (= $2 \cdot 3^2 \cdot 11$) serían $2 \cdot 3^0 \cdot 5^2 \cdot 7 \cdot 11^0$ y $2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11$.

Teorema *Sean* $a = \pm(p^{\alpha 1})_1 \dots (p^{\alpha t})_t$, $b = \pm(p^{\beta 1})_1 \dots (p^{\beta t})_t$ *donde algunos exponentes pueden ser 0. Entonces* $d = mcd(a,b) = p_1^{min(\alpha 1, \beta 1)} \dots p_t^{min(\alpha t, \beta t)}$

Demostración:

Sea $d = p_1^{\min(\alpha 1, \beta 1)} \dots p_t^{\min(\alpha t, \beta t)}$. Es claro que d|a y d|b. Supongamos que existe c tal que c|a, c|b.

Entonces $c = p_1^{\delta_1} \cdot \dots \cdot p_t^{\delta_t}$ donde $\delta_i \leq \alpha_i$, $\delta_i \leq \beta_i$. Por tanto, $\delta_i \leq \min(\alpha_i, \beta_i)$ y c|d. Entonces d = mcd(a,b).

Definición Sean $a,b \in Z$. Llamamos mínimo común múltiplo de a y b al menor entero positivo que sea múltiplo de ambos. Lo designaremos mcm(a,b).

Teorema Sean $a = \pm(p^{\alpha 1})_1 \dots (p^{\alpha t})_t$, $b = \pm(p^{\beta 1})_1 \dots (p^{\beta t})_t$, donde algunos exponentes pueden ser 0. Entonces $d = mcm(a,b) = p_1^{\max(\alpha 1, \beta 1)} \dots p_t^{\max(\alpha t, \beta t)}$

Demostración:

Sea $d = p_1^{\max(\alpha 1, \beta 1)} \dots p_t^{\max(\alpha t, \beta t)}$. Es claro que a|d y b|d. Supongamos que existe c tal que a|c, b|c.

Entonces $c = p_1^{\delta_1} \cdot \dots \cdot p_t^{\delta_t}$ donde $\delta_i \geq \alpha_i$, $\delta_i \geq \beta_i$. Por tanto, $\delta_i \geq$ máx(α_i,β_i) yo d|c. Entonces d = mcm(a,b).

1.2.- ARITMÉTICA MODULAR

Definición Sea m > 0. Dados a, b $\in$ Z se dice que a y b son *congruentes módulo m* si a–b es divisible por m.

Simbólicamente esta relación se escribe $a \equiv b \pmod{m}$.

Ejemplo: El minutero del cronómetro se pone a 0 cada 60 minutos. Si llevo cronometrados 95 minutos, el cronometro marcará 35, que es un número congruente con 95 módulo 60. Se denota $35 \equiv 95 \pmod{60}$.

Teorema Para a, b enteros, se cumple que $a \equiv b \bmod(m) \Leftrightarrow$ a y b tienen el mismo resto al dividirlos por m

Demostración

"$\Leftarrow$" Sean $a = q_1 m + r$, $b = q_2 m + r$. Entonces $a - b = (q_1 m + r) - (q_2 m + r) = (q_1 - q_2)m$, con lo que m|(a – b) y, por tanto, $a \equiv b \pmod{m}$.

"$\Rightarrow$" Como a - b es un múltiplo de m, a = b + (a - b) = b + km. Por tanto, al dividir por m dan

el mismo resto.

Propiedades

1. $\equiv_m$ es una relación de equivalencia en Z
2. Sean a, b, c, d, m $\in$ Z, m $\neq$ 0. Si a $\equiv$ b (mod m), c $\equiv$ d (mod m), se cumple a+c $\equiv$ b+d (mod m), y a·c $\equiv$ b·d (mod m).

Demostración:

$$\left.\begin{array}{l} a = q_1 m + r, b = q_3 m + r \\ c = q_2 m + r', d = q_4 m + r' \end{array}\right\} \rightarrow \left.\begin{array}{l} a + c = m(q_1 + q_2) + (r + r') \\ b + d = m(q_3 + q_4) + (r + r') \end{array}\right\}$$ luego a + c $\equiv$ b + d (mod m)

Para el producto el razonamiento es análogo.

3. Dado m > 1, para cada a existe un único b congruente con él en el conjunto {0,1,2,...,n-1}

Observación.- Identificaremos cada clase de equivalencia respecto a $\equiv$ con su representante en Z_n = {0,1,...,n-1}. En Z_n podemos definir una suma y un producto dados por:

[a]+[b]= [a+b]

[a][b] = [ab]

Es decir, primero se opera y luego se sustituye el resultado por su representante en Z_n.

Obsérvese que [a] = [0] en $Z_n \Leftrightarrow$ a es múltiplo de n.

Cometiendo un cierto abuso de notación, escribiremos [a] = a.

Es fácil comprobar que, con estas operaciones, (Z_n ,+, ·) verifica

- Son operaciones internas en Z
- Son asociativas y conmutativas
- Ambas tienen neutro, el de la suma es 0 y el de la multiplicación es 1.
- El producto es distributivo respecto a la suma: a · (b + c) = (a · b) + (a · c)
- Todo elemento tiene opuesto respecto a la suma

  Pero no tiene por qué verificar
- Si a · b = 0 $\Rightarrow$ a = 0 ó b = 0

Ejemplo.- En Z_6, 2 $\neq$ 0 y 3 $\neq$ 0, pero 2 · 3 = 6 = 0

Definición.- En Z_n un elemento a se dice

a) Un divisor de 0 si a $\neq$ 0 y existe b $\neq$ 0 con a·b = 0
b) Invertible si existe b con a·b = 1

Obsérvese que un elemento no puede ser a la vez invertible y divisor de 0

Teorema Sea 0 $\neq$ a $\in$ Z_n

a) a es divisor de 0 $\Leftrightarrow$ mcd(a,n) $\neq$ 1
b) a es invertible $\Leftrightarrow$ mcd(a,n) = 1

Demostración:

b) a es invertible $\Leftrightarrow$ existe b con a·b = 1 en $Z_n \Leftrightarrow$ existe b con a·b $\equiv$ 1 (mod n) $\Leftrightarrow$ existe b con a·b – 1 = kn $\Leftrightarrow$ existen b, k con a·b –kn = 1. Usando el Teorema de Bezout, esto se da si y sólo si m.c.d.(a,n) = 1

a) "$\Leftarrow$" sea d = mcd(a,n) $\neq$ 1. Ahora a = da' y n = dn' con n' < n. En particular n' $\neq$ 0 en Z_n. Pero entonces an' = a'dn' = a'n = 0 en Z_n. Por tanto, a es divisor de 0.

"$\Rightarrow$" Si fuese mcd(a,n) = 1, a sería invertible y, por tanto, no sería divisor de 0.

Definición.- Dado n > 1, llamaremos ϕ(n) al número de elementos invertibles en Z_n

Proposición.-

a) Si n = p es primo, ϕ (p) = p-1
b) Si n=p^r, con p primo, ϕ (p^r) = p^r-p^{r-1}

Demostración.-

a) Si n = p, con p primo, todos los elementos 1,2,...,p-1 son coprimos con p. Por tanto, todos son invertibles en Z_p y ϕ (p) = p-1
b) Basta observar que los elementos no invertibles son aquellos que tienen un divisor común con p^r, es decir, los múltiplos de p. Pero en {0,1,2,....,p^r –1} los múltiplos de p van de p en p, por tanto hay $p^r /p = p^{r-1}$. Así pues ϕ (p) = nº elementos de Z_n –nº elementos de Z_n no invertibles = $p^r - p^{r-1}$

Teorema (Chino del resto)

El sistema de congruencias $x \equiv a_i \pmod{m_i}$, i=1,2, ..., k con mcd(m_i,m_j) = 1 si i ≠ j, tiene solución x_0 que, además, es única módulo $m_1m_2...m_k$. En particular, todas las demás soluciones son de la forma $x = x_0 + \lambda\ m_1m_2...m_k$, $\lambda \in Z$.

Demostración:

Como los m_i son coprimos dos a dos, si defino q_i = producto de todos los m_j menos el m_i, debe de ser también coprimo con m_i. Sea h_i su inverso módulo m_i. Si consideramos ahora $a_i \cdot q_i \cdot h_i$, verificará que $a_i \cdot (q_i \cdot h_i) = a_i \cdot 1 = a_i$ módulo m_i. Por otro lado, si tomo un j ≠ i, q_i es un múltiplo de m_j, por lo que $a_i \cdot q_i \cdot h_i$ también lo será. Por tanto, $a_i \cdot q_i \cdot h_i$ es 0 módulo m_j. Si cogemos ahora $x_0 = a_1 \cdot q_1 \cdot h_1 + a_2 \cdot q_2 \cdot h_2 + ... + a_k \cdot q_k \cdot h_k$ tendremos una solución.

Si x es otra solución, tendremos que $x - x_0$ debe ser un múltiplo de cada m_i para i = 1,...,k, ya que dan los mismos restos al dividir por los m_i. Como los m_i son coprimos entre sí, debe de ser un múltiplo de su producto.

El resultado anterior nos permite, si $n = m_1m_2...m_k$ con los m_i coprimos dos a dos, identificar un elemento x de Z_n con sus restos módulo los correspondientes m_i, esto es, escribiré $x = (x_1,..,x_k)$, donde cada x_i es el resultado de dividir x entre el correspondiente m_i. Está claro que, al hacer esto, se tienen las siguientes propiedades:

1) La suma se hace componente a componente
2) El producto se realiza componente a componente
3) 1 = (1,1,...,1)
4) Un elemento $x = (x_1,..,x_k)$ tiene inverso ⇔ cada x_i lo tiene.

En particular, tendremos que el número de elementos invertibles módulo n coincidirá con el producto del número de elementos invertibles módulo los diferentes m_i.

Esta última observación nos sirve para calcular de forma general la función ϕ de Euler.

Proposición.- Sea $n = p_1^{\alpha 1} ... p_t^{\alpha t}$, con los p_i primos distintos. Entonces:

$\phi (n) = \phi (p_1^{\alpha 1} ... p_t^{\alpha t}) = \phi (p_1^{\alpha 1})\phi (p_2^{\alpha 2})....\phi (p_t^{\alpha t}) = (p_1^{\alpha 1} - p_1^{\alpha 1 - 1} ...)(p_2^{\alpha 2} - p_2^{\alpha 2 - 1}).....(p_k^{\alpha k} - p_k^{\alpha k - 1})$

Demostración:

Que $\phi (n) = \phi (p_1^{\alpha 1} ... p_t^{\alpha t}) = \phi (p_1^{\alpha 1})\phi (p_2^{\alpha 2})....\phi (p_t^{\alpha t})$ se sigue de la propiedad 4). Finalmente basta recordar que si $n = p^r$, con p primo, entonces $\phi (p^r) = p^r - p^{r-1}$

Teorema (de Euler)

Sean a y m dos números enteros con m ≥ 1. Si mcd(a,m) = 1 se tiene que $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración:

Sean $\{a_1,...,a_{\phi (m)}\}$ los elementos invertibles de Z_m. Multiplicamos todos ellos por a y obtenemos un nuevo conjunto $\{aa_1,...,aa_{\phi (m)}\}$.

Observemos que, como mcd(a,n) = 1, a es invertible en Z_m, por lo que los aa_i vuelven a ser invertibles. Por otro lado, deben de ser todos distintos ya que, si $aa_i = aa_j$, basta dividir por a para obtener $a_i = a_j$.

Por tanto, los $\{aa_1,...,aa_{\phi (m)}\}$ son ϕ (n) elementos invertibles distintos de Z_m, por lo que deben de ser todos los elementos invertibles solamente que quizás en un orden distinto. Como el producto es conmutativo, se dará:

$$a_1...a_{\phi (m)} = aa_1...aa_{\phi (m)}$$

Basta simplificar ahora, dividiendo sucesivamente por a_1, por a_2,.. por $a_{\phi (m)}$ para obtener a...a = 1. Por tanto $a^{\phi (m)} = 1$ en Z_m o, equivalentemente $a^{\phi (m)} \equiv 1 \pmod{m}$.

Pequeño teorema de Fermat

Si p es un número primo que no divide al número a, entonces $a^{p-1} \equiv 1 \pmod{m}$.

Demostración:
Es un caso particular del resultado anterior sin más que tomar n = p.

Observación.- El resultado anterior sirve para calcular directamente el inverso de un número en Z_n. En efecto, si a es invertible en Z_n, su inverso es $a^{\phi(n)-1}$, ya que

$$a\, a^{\phi(n)-1} = a^{\phi(n)} \equiv 1 \pmod{n}$$

1.3.- SISTEMAS DE NUMERACIÓN

En esta sección se estudian sistemas de numeración diferentes al usado convencionalmente, es decir, sistemas no decimales.

Teorema Sea $b \geq 2$ un número natural llamado *base*. Todo número $n \in N$ tiene representación única en base b de la forma

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 ,$$

para algún $k \geq 0$, con $0 \leq a_i < b$, i = 0, 1,..., k, y con $a_k \neq 0$.

Demostración:
Veamos primero que cualquier número se puede escribir de esta forma.
Lo vamos a ver por inducción en n.
Para n = 1 el resultado es claro sin más que tomar k = 0 y $a_0 = 1$.
Supongamos que el resultado es cierto para números menores que n y vamos a probarlo para n. Distinguimos dos casos
Caso 1.- n < b
En este caso basta tomar k = 0 y $a_0 = n$.
Caso 2.- $n \geq b$
Divido n entre b, obteniendo n = mb + r, con $0 < r \leq b$.
Como m < n, por la hipótesis de inducción, puedo encontrar un número $k \geq 0$, y unos a_i entre 0 y b-1 y con $a_k \neq 0$ de forma que $m = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$
Ahora $n = mb + r = (a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0)b + r = a_k b^{k+1} + a_{k-1} b^k + \ldots + a_1 b^2 + a_0 b + r$, que tiene la forma pedida sin más que recordar que $0 < r \leq b$.
Veamos ahora que la expresión es única. Supongamos que tenemos:

$$a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 = c_t b^t + c_{t-1} b^{t-1} + \ldots + c_1 b + c_0$$

verificando $0 \leq a_i < b$, i = 0, 1,..., k, $0 \leq c_i < b$, i = 0, 1,..., t y con $a_k \neq 0$ y $c_t \neq 0$ y vamos a ver que, en este caso, k = t y que $a_i = c_i$ para i = 0,...,k.
En efecto, tomando congruencias módulo b, tendremos

$$a_0 \equiv a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 \equiv c_t b^t + c_{t-1} b^{t-1} + \ldots + c_1 b + c_0 \equiv c_0$$

Ahora, como $a_0 \equiv c_0$ y, además, $0 \leq a_0, c_0 < b$, tendremos que $a_0 = c_0$. Podemos ahora simplificar nuestra igualdad restando a_0 en ambos términos y obtenemos:

$$a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b = c_t b^t + c_{t-1} b^{t-1} + \ldots + c_1 b$$

En esta igualdad podemos dividir por b, obteniendo

$$a_k b^{k-1} + a_{k-1} b^{k-2} + \ldots + a_1 = c_t b^{t-1} + c_{t-1} b^{t-2} + \ldots + c_1$$

Tomando congruencias módulo b, obtenemos:

$$a_1 \equiv a_k b^{k-1} + a_{k-1} b^{k-2} + \ldots + a_1 \equiv c_t b^{t-1} + c_{t-1} b^{t-2} + \ldots + c_1 \equiv c_1$$

Ahora, como $a_1 \equiv c_1$ y, además, $0 \leq a_1, c_1 < b$, tendremos que $a_1 = c_1$.
De forma análoga se va demostrando que $a_2 = c_2$, $a_3 = c_3$, etcétera.

Criterios de divisibilidad
Sea n un número natural, $n = a_t 10^t + a_{t-1} 10^{t-1} + \ldots + a_1 10 + a_0$, que escribiremos $n = \sum_{i=0}^{t} a_i 10^i$.

Consideremos ahora los restos de la división de 10^i por k para i = 0, 1,..., t. Supongamos que estos restos son r_o, r_1, ..., r_t, es decir,

$$10^0 \equiv r_0 \pmod{k},\ 10^1 \equiv r_1 \pmod{k},\ldots,\ 10^t \equiv r_t \pmod{k}.$$

Por tanto $n = \sum_{i=0}^{t} a_i 10^i \equiv \sum_{i=0}^{t} a_i r_i \pmod{k}$, luego n es divisible por k si y solo si $\sum_{i=0}^{t} a_i r_i$ lo es.

Ejemplo El método anterior funciona bien cuando los r_i son bastante simples. Por ejemplo, si tomamos k = 9, tenemos

$10^0 \equiv 1 \pmod 9$, $10^1 \equiv 1 \pmod 9$, $10^2 \equiv 1^2 \equiv 1 \pmod 9$,..., $10^t \equiv 1^t \equiv 1 \pmod 9$

Por tanto, $n = \sum_{i=0}^{t} a_i 10^i \equiv \sum_{i=0}^{t} a_i \pmod 9$, por tanto, un número es divisible por 9 si y sólo si la suma de sus cifras lo es.

Así, para ver si 1236789 es divisible por 9, podemos sustituirlo por 1 + 2 + 3 + 6 + 7 + 8 + 9 que vale 36, y éste a su vez, podemos cambiarlo por 3 + 6 = 9. Como, obviamente, 9 es múltiplo de 9, obtenemos que también 1236789 lo es.

Otros números para los que hay criterios sencillos de divisibilidad son 2, 3, 4, 5, 6, 11.

1.4.- Criptografía y Criptoanálisis

Criptología quiere decir “escritura secreta”. Actualmente tiene el significado de ciencia de la comunicación segura; su objetivo es que dos partes puedan intercambiar información sin que una tercera parte no autorizada, a pesar de que capte los datos, sea capaz de descifrar la información. La criptografía actúa mediante criptosistemas; un criptosistema o sistema cifrado es un sistema que permite cifrar los mensajes de tal forma que una persona no autorizada no pueda descifrar el mensaje. La criptografía es la ciencia de diseñar criptosistemas.

El criptoanálisis trata de romper los criptosistemas para apoderarse de la información cifrada.

Criptosistemas Clásicos(Simétricos)

Un criptosistema clásico está formado por un quinteto de conjuntos (P, C, K, E, D), donde:

P es un conjunto finito cuyos elementos se llaman “textos claros” (plain text), estos serían los mensajes que se quieren enviar tal cual.

C es un conjunto finito cuyos elementos se llaman “criptotextos”, esto sería lo que resulta una vez que la información se cifra.

K es un conjunto finito cuyos elementos se llaman “claves” (keys).

E = $\{E_k / k \in K\}$ donde E_k: P $\rightarrow$C, $E_k \rightarrow$transformaciones criptográficas

D = $\{D_k / k \in K\}$ donde D_k: C $\rightarrow$P, cumpliendo que $D_k(E_k(x)) = x \ \forall x \in P$.

Se basa en que las 2 partes se ponen de acuerdo en la clave y en mantenerla secreta. La clave k da las transformaciones E_k y D_k.

Un criptoanalista intercepta c pero como no conoce la clave k no es capaz de recuperar p. Cualquier persona que conozca la clave k puede descifrar el mensaje. La clave debe intercambiarse por un canal seguro y además el conjunto de las claves debe ser enorme.

Este criptosistema se llama simétrico ya que el conocimiento de la clave permite las operaciones de cifrar y descifrar.

ALGUNOS SISTEMAS CRIPTOGRÁFICOS CLÁSICOS

En general suelen identificarse las letras del alfabeto con números

$$a \to 0$$
$$b \to 1$$
$$\vdots$$
$$z \to 26$$

$$Z_{27} \to \text{Alfabeto}$$

1) $P = C = K = Z_{27}$

Para cada $k \in Z_{27}$

$E_k(x) := x+k \pmod{27} \quad \forall\, x \in Z_{27}$

$D_k(x) := x-k \pmod{27} \quad \forall\, x \in Z_{27}$

Ejemplo.- Para $k = 3$

$E_3(\text{CESAR}) = \text{FHVDQ}$

$E_3(\text{ZAMORA}) = \text{CDORUD}$

Este sistema se conoce como cifra de César.

Como sólo hay 27 posibles claves se prueban todas las posibles claves hasta que se encuentra la correcta.

2) Criptosistema de sustitución

$P = C = Z_{27}$

$K = S_{27} = \{\sigma : Z_{27} \to Z_{27} / \sigma \text{ es biyectiva (permutación)}\}$

$E_\sigma(x) := \sigma(x) \quad \forall\, x \in Z_{27}$

$D_\sigma(x) := \sigma^{-1}(x) \quad \forall\, x \in Z_{27}$

$|K| = 27! > 10^{28}$

El que $|K|$ sea tan grande implica que este criptosistema no se pueda analizar a base de probar todas las posibilidades

3) Criptosistema afín.

$P = C = Z_{27}$

$K = \{(a,b) \in Z_{27} \times Z_{27} / \text{mcd}(a,27) = 1\}$

Si $k = (a,b)$

$E_k(x) := ax+b \pmod{27} \quad \forall\, x \in Z_{27}$

$D_k(x) := a^{-1}(x-b) \pmod{27} \quad \forall\, x \in Z_{27}$

a se toma primo con 27 para que tenga inverso en Z_{27}. En este caso $|K| = 27 \cdot 29$. Este es un subsistema del caso anterior.

Problemas fundamentales de los criptosistemas clásicos:

- El problema de la seguridad (Shanonn 1949, Bell System Journal). Shanonn dio una definición de lo que es la seguridad de un criptosistema; definió la seguridad incondicional, ésta se establece cuando un criptosistema es seguro con independencia de los medios disponibles (infinita potencia de cálculo). Si un criptosistema es incondicionalmente seguro no se puede romper. Se demostró la existencia de criptosistemas de seguridad incondicional (cifrar de Vernann) aunque d.p.v práctico no tienen utilidad. Los criptosistemas más modernos se basan en la seguridad computacional. La idea es considerar un criptosistema computacionalmente seguro cuando aunque haya un algoritmo que rompa el sistema éste requiera un tiempo de computación tan grande que sea inviable llevarlo a la práctica.
- El problema del manejo y distribución de claves. Los criptosistemas clásicos son de clave secreta, cualquiera que conozca la clave puede descifrar la información. Estos criptosistemas son vulnerables aunque no se sepa como criptoanalizarlos si se intercepta la clave secreta.
- El problema de la autentificación. Los criptosistemas convencionales no proporcionan ningún método para que el receptor del mensaje pueda tener la seguridad de que quien envió el mensaje es quien debería haberlo enviado y no una tercera parte. El mensaje podría ser alterado y no se podría saber si esta situación se ha producido.

Criptografía de Clave Pública

En un criptosistema clásico hay un espacio de claves y para cada clave k hay una función E_k de encriptación y otra D_k de desencriptación. Cualquier persona que conozca k conoce E_k y D_k; además si se conoce E_k se conoce D_k y viceversa; así k, E_k y D_k deben ser secretas.

En 1976 se trató de buscar un criptosistema en el cual el conocimiento de cómo encriptar no implicase el conocimiento de cómo desencriptar. Esto permite usar un criptosistema en el cual E_k fuese pública pero no fuese factible calcula D_k. E_k y D_k deben ser inversas pero si uno conoce E_k no se debe poder obtener D_k. La idea apareció por primera vez en un artículo de W. Diffie y M. Hellman (New direction cryptography).

Estos criptosistemas se basan en la función de dirección única. Una función de dirección única:

$$X \xrightarrow{f} Y$$

es una función tal que es “fácil” calcular $f(x)\ \forall\ x \in X$ pero que por el contrario es “difícil” para la mayoría de los $y \in Y$ encontrar un $x \in X$ tal que $f(x) = y$ (suponiendo que exista).

Criptosistemas de Clave Pública (CCP) o Criptosistemas asimétricos:

Cada usuario del criptosistema se construye una función de encriptación E_u y una función de desencriptación D_u que cumplen las siguientes propiedades:

CP1- $D_u(E_u(x)) = x$ para todo mensaje x y todo usuario u.

CP2- Existen algoritmos eficientes para calcular $E_u(x)$ y $D_u(x)$ para todo x.

CP3- Existe una clave secreta (conocida sólo por u) que permite obtener rápidamente D_u a partir de E_u pero el conocimiento de E_u no hace factible hallar un algoritmo D_u^* que ratifica $D_u^*(E_u(x)) = x$ para todo x.

Cada usuario u hace público el algoritmo para calcular E_u, los E_u se ponen en un directorio que es público. El algoritmo que permite calcular D_u es mantenido en secreto por u.

Si A quiere enviar un mensaje m a B, A busca E_B en el directorio y calcula $E_B(m)$, A envía $c = E_B(m)$ y B calcula $D_B(E_B(m))$. Un criptoanalista conoce $c = E_B(m)$.

CP4- $E_u(D_u(x)) = x \ \forall$ x y todo usuario u.

CP5- No es factible encontrar a partir de E_u una función D_u^* tal que $E_u(D_u^*(x)) = x$

El Criptosistema RSA

Riverest-Shamir-Adleman: Criptosistema RSA (A method for obtaining digital signatures and public key cryptosystems- Comunications of the ACM 1978)

Se piensa que el criptosistema RSA es tan seguro como lo era en 1978.

"Exponenciación modular con exponente y módulos fijos"

$$g_{m,n}: Z_m \rightarrow Z_n$$
$$g_{m,n} := x^m \pmod n$$

Se piensa que esta es una función de dirección única con trampa.

"Extracción de raíces módulo n": Dados y, m, $n \in Z^+$ hallar (en caso de que exista) un x tal que $x^m \equiv y \pmod n$

Es fácil calcular las imágenes pero la extracción de raíces módulo n no es factible computacionalmente a menos que se conozca una información adicional, que si se conoce entonces es fácil volver hacia atrás; esto se logra conociendo la factorización de m en números primos ya que es fácil obtener las raíces m-ésimas.

Dados m y n nadie conoce un algoritmo eficiente para la extracción de raíces módulo n pero no se ha demostrado que este algoritmo no exista.

RSA = (P, C, K, E, D) donde:

$P = C = Z_n$, con $n = pq$, p y q primos
$K = \{(n, e, d)/ ed \equiv 1 \pmod{\phi(n)}\}$

Para cada k = (n, e, d)
$E_k(x) := x^e \pmod n \ \forall \ x \in Z_n$
$D_k(x) := x^d \pmod n \ \forall \ x \in Z_n$

En el caso del sistema RSA:

$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$

$|Z_n^*| = p-1$ si p es primo

$\forall x \in Z_n \; D_k(E_k(x)) = x$

$x \in Z_n^*$

$E_k(x) \equiv x^e \pmod n$

$D_k(E_k(x)) \equiv (x^e)^d \pmod n \equiv x^{ed} \pmod n \equiv x^{t\phi(n)+1} \pmod n \equiv (x^{\phi(n)})^t x \pmod n \equiv x \pmod n$,

ya que $ed \equiv 1 \pmod{\phi(n)} \Leftrightarrow ed = t\phi(n) + 1$

El par (n,e) constituye la clave pública mientras que d, p y q se mantienen en secreto.

Cada usuario u elige dos primos distintos grandes (512 bits ≅ 154 dígitos decimales) p_u y q_u y calcula $n_u = p_u q_u$ (n recibe el nombre de módulo).

Se calcula $\phi(n_u) = (p_u - 1)(q_u - 1) = |Z_{n_u}^*|$. u elige un entero e_u tal que $1 < e_u < \phi(n_u)$ y $\text{mcd}(e_u, \phi(n_u)) = 1$. A continuación se calcula el inverso de e_u en $Z_{\phi(n_u)}^*$, es decir, se calcula el entero d_u tal que $1 < d_u < \phi(n_u)$ y $e_u d_u \equiv 1 \pmod{\phi(n_u)}$

$e_u \rightarrow$exponente de encriptación

$d_u \rightarrow$exponente de desencriptación

Clave pública : (n_u, e_u)

$E_u(x) := x^{e_u} \pmod{n_u}$

$D_u(x) := x^{d_u} \pmod{n_u}$

u mantiene secreto p_u, q_u y d_u

Los números más difíciles de factorizar son los que se factorizan como 2 primos que tienen el mismo número de dígitos.

Se presentan dos problemas:

- Reconocimiento de primos (primality test)
- Factorización de enteros.

Al usar el RSA queremos que otra parte no rompa el sistema, cualquier persona que conozca la descomposición de un en factores primos puede desencriptar, esto lleva al problema de la factorización de enteros; nadie conoce un método eficiente para factorizar enteros generales.

Un criptoanalista tiene $x^{e_B} \pmod{n_B}$, debe hallar la raíz e_B de x, para esto debe conocer $\phi(n_B)$ y para ello debe conocer q_B y d_B.

Ejemplo.-

p = 47 q = 59

n = pq = 47·59 = 2773

$\phi(n) = \phi(p)\cdot\phi(q) = 46\cdot 58 = 2668$

e = 1225

	2	5	1	1	1	1	1	1
2668	1225	218	135	83	52	31	21	10
21	135	83	52	31	21	10	1	

mcd(1225,2668) = 1

1 = 257·1225 – 118·2668

$257\cdot 1225 \equiv 1 \pmod{2668}$

d = 257

Clave pública (2773,1225)

Clave privada (2773,257)

$x^{1225} \pmod{2773}$

Exponenciación binaria:

$1225 = (10011001001)_2 = 2^{10} + 2^7 + 2^6 + 2^3 + 2^0$

$$x^{1225} = x^{(2^{10}+2^7+2^6+2^3+2^0)} = x^{2^{10}} x^{2^7} x^{2^5} x^{2^3} x$$

$1 \leftrightarrow cx$

$0 \leftrightarrow c$

c = elevado al cuadrado

x = multiplicar

cxcccxcxcccxccx

$(((((((((x^2)^2)^2\cdot x)^2\cdot x)^2)^2)^2\cdot x)^2)^2)^2)\cdot x \pmod{2773}$

Haciendo esto calculamos directamente $x^{1225} \pmod{2773}$; hacemos esto con sólo 14 multiplicaciones.

Vamos a ver que se cumplen las condiciones CP1...CP5

- CP1 se cumple.
- D y E se calculan mediante algoritmos factibles ya que el algoritmo de exponenciación binaria es eficiente. CP2 se cumple.
- CP3 permite asegurar que el RSA es seguro. E_u es fácil de calcular pero obtener D_u a partir de E_u no es factible. Existe la conjetura de que criptoanalizar RSA es equivalente a poder factorizar n. Lo máximo que se ha llegado a factorizar son números de 130 dígitos. Los mejores algoritmos de factorización que se conocen son subexponenciales pero aún así el tiempo de computación es grande. Existe una creencia de que el RSA requiere la factorización de n y esto es difícil.

<u>Problemas:</u>

- Manejo y distribución de claves. Este sistema de clave pública resuelve este problema inmediatamente ya que 2 partes no tienen necesidad de intercambiarse clave alguna. Un usuario elige los primos y el exponente de Exponenciación y hace pública una clave pero la clave privada no se intercambia con nadie.
- Identificación. Los criptosistemas clásicos no permiten saber que el mensaje proviene de quien realmente dice. Suponiendo que el RSA sea seguro (CP1 ... CP5) se resuelve este problema.
- Seguridad. Este problema está encerrado en la condición CP3. No está demostrado que el RSA es seguro, existen una serie de hechos matemáticos que hacen pensar que el RSA es seguro. La seguridad del RSA se basa en la creencia de que la función de encriptación es una función de dirección única con trampa. El que RSA sea seguro se basa en 2 premisas:

  a) Se cree que romper RSA es equivalente a saber factorizar n. Esta sin demostrar que no puede existir otra forma de romper RSA que no pase por factorizar n. No está demostrado que romper RSA sea equivalente a factorizar n.

  b) Si aceptamos la premisa anterior de que romper RSA pasa por factorizar n tenemos que la factorización de n para tamaños grandes de n es un problema intratable d.p.v. computacional.

Se ha demostrado que factorizar el criptosistema de Rabin, que es parecido al RSA, es equivalente a factorizar el módulo. La factorización de enteros equivale a estudiar RSA.