Álgebra Aplicada y Criptografía

Miguel Ambrona Castellanos

Octubre 2011

Universidad Complutense de Madrid

Índice general

1 Introducción

La criptografía, del griego *krypto* (oculto) y *graphos* (escribir), es la técnica que altera las representaciónes lingüísticas de un mensaje. La criptografía se apoya en las matemáticas para conseguir cierta seguridad en el envío de datos.
A continuación veremos varios ejemplos en cuanto a técnicas de codificación utilizadas.

1.1 Cifrado César

Es una de las técnicas de codificación más simples y usadas. Llamamos $\mathcal{P}$ al conjunto de unidades de texto fuente. Llamamos $\mathcal{C}$ al conjunto de unidades del texto cifrado (normalmente coincide con $\mathcal{P}$). Además nombramos $\mathcal{K}$ al conjunto de claves y e_k a la función de cifrado.

En el Cifrado César tenemos que $\mathcal{P}$={A,B,C,D,...,W,X,Y,Z,' '}= $\mathcal{C}$. A cada letra se le asocia un número del 0 al 25 y al espacio en blanco se le da el número 26. De esta forma tenemos que,

$$\mathcal{P} = \frac{\mathbb{Z}}{< 27 >} = \mathcal{C} = \mathcal{K}$$

Una vez elegida la clave k la función de cifrado es muy sencilla,

$$\begin{aligned} e_k : \mathcal{P} &\longrightarrow \mathcal{C} \\ p &\longmapsto p + k \pmod{27} \end{aligned}$$

Por ejemplo, para cifrar la frase *"Alea jacta est"* con clave $k = 3$ haríamos los siguiente:

A	L	E	A		J	A	C	T	A		E	S	T
0	11	4	0	26	9	0	2	19	0	26	4	18	19

3	14	7	3	2	12	3	5	22	3	2	7	21	22
D	O	H	D	C	M	D	F	W	D	C	H	V	W

La función de descifrado es trivial,

$$\begin{aligned} d_k : \mathcal{C} &\longrightarrow \mathcal{P} \\ q &\longmapsto q - k \pmod{27} \end{aligned}$$

1.2 Cifrado Afín

En este caso, siendo N el número de símbolos del alfabeto, $N = \#\mathcal{P}$, tenemos que,

$$\mathcal{P} = \frac{\mathbb{Z}}{< N^k >}$$

si tomamos las unidades de texto en k-gramas (colecciones de k símbolos).
Además ahora,

$$\mathcal{K} = \left\{ (a, b) \in \frac{\mathbb{Z}}{< N^k >} \times \frac{\mathbb{Z}}{< N^k >} \mid \exists a' : aa' \equiv 1 \pmod{N^k} \right\}$$

Ahora tenemos que

$$e_{(a,b)}(p) = ap + b \pmod{N^k}$$

es la función de cifrado.
Éste es otro ejemplo de cifrado monoalfabético. Débil contra un análisis de frecuencias.

1.3 Matrices de Hill

Propuesto por el matemático Lester Hill. Se trata de un sistema que utiliza una matriz como clave.
$\mathcal{P} = \{\text{unidades de texto original}\} = \{(a_1, \ldots, a_k) : \ a_i \in \frac{\mathbb{Z}}{<N>}\} = \left(\frac{\mathbb{Z}}{<N>}\right)^k$
$\mathcal{K} = \{\text{matrices } k\text{x}k \text{ con entradas en } \frac{\mathbb{Z}}{<N>}\} \times \left(\frac{\mathbb{Z}}{<N>}\right)^k$ Y la función de cifrado es la siguiente,

$$e_{A,b}(p) = Ap^t + b^t.$$

$$\underbrace{\begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_k \end{pmatrix}}_{vector\ cifrado} = (a_{ij})_{i,j=1}^k \cdot \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_k \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_k \end{pmatrix} \quad \text{mód } n$$

Hay que exigir una condición adicional para asegurar la inyectividad y así garantizar la existencia la inversa. Esta condición es que $mcd\,(\det(a_{ij}), N) = 1$.

Para descifrar el mensaje se aplica la siguiente transformación:

$$\begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_k \end{pmatrix} = \left((a_{ij})_{i,j=1}^k\right)^{-1} \cdot \begin{pmatrix} c_1 - b_1 \\ c_2 - b_2 \\ c_3 - b_3 \\ \vdots \\ c_k - b_k \end{pmatrix} \quad \text{mód } n,$$

donde $\left((a_{ij})_{i,j=1}^k\right)^{-1}$ es la matriz inversa de $(a_{ij})_{i,j=1}^k$ módulo n.

1.4 Cifrado de Vigenère

El cifrado de Vigenère es un cifrado polialfabético y de sustitución. En Francia era conocido como el código indescifrable.
En este método la misma letra se cifra de un modo distinto según la posición que ocupa en el mensaje original. Este cifrador soluciona la debilidad del cifrado del César en el que cada letra se cifra siempre de la misma forma.
Se usa una clave m de longitud L y se cifra carácter a carácter sumando módulo n el texto inicial con los elementos de esta clave (obteniendo C). La función de cifrado es: $C_i = (m_i + k_i) \pmod{27}$.
Los métodos de Kasiski y del Índice de Coincidencia, consiguieron atacar este cifrado.

2 Álgebra Modular

Esta sección comienza con el Teorema Chino de los restos, importantísimo en álgebra modular y a la hora de resolver ejercicios. También se exponen algunos conceptos como la función φ de Euler y el desarrollo en base mixta y además se enuncia el algoritmo de exponenciación modular rápida con ejemplos que muestran su utilidad.

2.1 El Teorema Chino de los restos

Teorema 2.1.1 Dados $m_1, \ldots, m_r \in \mathbb{Z}^+$, coprimos dos a dos y $x_1, \ldots, x_r \in \mathbb{Z}$ existe $x \in \mathbb{Z}$ tal que $x \equiv x_i \pmod{m_i}$. Además x es único módulo M. Siendo $M = \prod_{i=1}^{r} m_i$.

También puede ser escrito de la siguiente forma:

Teorema 2.1.2 Dados $m_1, \ldots, m_r \in \mathbb{Z}^+$, coprimos dos a dos, existen $u_1, \ldots, u_r \in \mathbb{Z}$ tales que $u_i \equiv 1 \pmod{m_i}$ y $u_i \equiv 0 \pmod{m_j}$ $\forall j \neq i$

Veamos que **2.1.1** es consecuencia de **2.1.2**. Basta tomar para $x = \sum_{i=1}^{r} x_i u_i$; entonces para cada j se tiene $x - x_j = \sum_{i \neq j}(x_i u_i) + x_j(u_j - 1)$, expresión que es múltiplo de m_j.
Esto prueba que $x \equiv x_i \pmod{m_j}$ $\forall$ j. Ahora, si x y x' son dos soluciones, cada $m_j | x - x'$ y en consecuencia $M | x - x'$, lo que prueba la unicidad.

La ventaja de **2.1.2** es que una vez hechos los cálculos para ciertos módulos, no es necesario volver a hacerlos aunque cambien los restos, por eso en compuatción es más útil la segunda expresión del teorema que demostramos a continuación:

Demostración: Sea $n_i = \prod_{j \neq i} m_j$. Por ser dos a dos coprimos, tenemos que $mcd(m_i, n_i) = 1$ para todo i. Entonces por la identidad de Bézout, $\exists \lambda_i, \mu_i \in \mathbb{Z}$ tales que $\lambda_i m_i + \mu_i n_i = 1$ $\forall i = 1, \ldots, r$. Si tomamos $u_i = \mu_i n_i$ es fácil comprobar que verifican las condiciones del teorema. $\square$

Sabemos entonces que existe una biyección entre,

$$\frac{\mathbb{Z}}{\langle \prod_{i=1}^{r} m_i \rangle} \Longleftrightarrow \frac{\mathbb{Z}}{< m_1 >} \times \frac{\mathbb{Z}}{< m_2 >} \times \cdots \times \frac{\mathbb{Z}}{< m_r >}$$

$$x \left(\mod \prod_{i=1}^{r} m_i \right) \longrightarrow (x \pmod{m_1}, x \pmod{m_2}, \ldots, x \pmod{m_r})$$

$$\sum_i x_i u_i \left(\mod \prod_{j=1}^{r} m_j \right) \longleftarrow (x_1 \pmod{m_1}, x_2 \pmod{m_2}, \ldots, x_r \pmod{m_r})$$

Existe también una biyección análoga entre las unidades de cada anillo.
Supongamos $m = m_1 m_2$ con $mcd(m_1, m_2) = 1$.
$U\left(\frac{\mathbb{Z}}{<m>}\right)$ tiene cardinal $\varphi(m)$ y es isomorfo a $U\left(\frac{\mathbb{Z}}{<m_1>}\right) \times U\left(\frac{\mathbb{Z}}{<m_2>}\right)$. Además, el orden de cada elemento de $U\left(\frac{\mathbb{Z}}{<m>}\right)$ es divisor de $mcm(\varphi(m_1), \varphi(m_2))$.

Ejemplo: Para calcular $a^b \pmod m$, si conocemos e tal que $a^e \equiv 1 \pmod m$, dividiendo b entre e, es decir, $b = qe + r$ con $0 \leq r < e$, llegamos a $a^b = (a^e)^q a^r \equiv a^r \pmod m$.

Ejercicio 2.1.1 Calcular todas las raíces cuadradas de 1 módulo 35, es decir, los elementos que tienen orden 1 ó 2.

Solución: Sabemos que existe una biyección entre,

$$U\left(\frac{\mathbb{Z}}{<35>}\right) \Longleftrightarrow U\left(\frac{\mathbb{Z}}{<5>}\right) \times U\left(\frac{\mathbb{Z}}{<7>}\right)$$

Es fácil ver que en $U\left(\frac{\mathbb{Z}}{<5>}\right)$ las raíces de 1 son $\{1, 4\}$ y que en $U\left(\frac{\mathbb{Z}}{<7>}\right)$ son $\{1, 6\}$. Entonces, las raíces en $U\left(\frac{\mathbb{Z}}{<5>}\right) \times U\left(\frac{\mathbb{Z}}{<7>}\right)$ son $\{(1,1), (1,6), (4,1), (4,6)\}$.

Pero podemos calcular qué elementos son de $U\left(\frac{\mathbb{Z}}{<35>}\right)$ ayudándonos de la biyección que manda $(a, b) \in U\left(\frac{\mathbb{Z}}{<5>}\right) \times U\left(\frac{\mathbb{Z}}{<7>}\right)$ a $au + bv \pmod{35} \in U\left(\frac{\mathbb{Z}}{<35>}\right)$.

Verificando u y v las siguientes congruencias,

$$\begin{array}{ll} u \equiv 1 \pmod 5 & v \equiv 1 \pmod 7 \\ u \equiv 0 \pmod 7 & v \equiv 0 \pmod 5 \end{array}$$

Es fácil comprobar que $u = 21$ y $v = 15$. Entonces las raíces de 1 módulo 35 son $1, 6, 29$ y 34. ✠

Existe una analogía entre el *"Teorema chino de los restos"* y la interpolación polinómica, en el sentido de que dado $\mathbb{F}$ cuerpo, dados $a_i \in \mathbb{F}$ con $i = 0, \ldots, n$ y verificando $a_i \neq a_j$ cuando $i \neq j$ y dados $b_i \in \mathbb{F}$ con $i = 0, 1, \ldots, n$. Existe un único polinomio de grado n, $P(x) \in \mathbb{F}[X]$ tal que $P(a_i) = b_i$

De forma análoga existe una biyección entre,

$$\frac{\mathbb{F}[X]}{\langle \prod_{i=0}^{n}(x - a_i) \rangle} \Longleftrightarrow \frac{\mathbb{F}}{<(x - a_1)>} \times \cdots \times \frac{\mathbb{F}}{<(x - a_n)>}$$

2.2 Algoritmo de exponenciación modular rápida

Utilizado para el cálculo de una exponenciación en un anillo por el método de los cuadrados. Sea $(A, +, \cdot)$ anillo. Sirve para calcular $a^k = a \overset{k)}{\cdots} a$ en el anillo con pocas operaciones en A.

Lo primero que hay que hacer es expresar k en base 2,

$$k = \alpha_r 2^r + \cdots + \alpha_1 2 + \alpha_0 \text{ con } \alpha_i \in \{0, 1\}$$

Entonces, $a^k = a^{\alpha_r 2^r} \cdot a^{\alpha_{r-1} 2^{r-1}} \cdots a^{\alpha_1 2} \cdot a^{\alpha_0}$
Como mucho este algoritmo requiere $2r$ multiplicaciones en el anillo, siendo r el número de dígitos

del exponente en su representación en base 2.
El algoritmo consiste en crear las siguientes sucesiones,

$$\begin{cases} z_0 = 1 \ ; \ b_0 = a \\ z_i = z_{i-1}(b_{i-1})^{\alpha_{i-1}} \\ b_i = (b_{i-1})^2 \end{cases}$$

Para $i = 1, 2, \ldots, r$. Y en ese caso, tenemos que,

$$a^k = z_r b_r.$$

Ejemplo: Para calcular 2^{26} construimos la siguiente tabla,

i	α_i	z_i	b_i
0	**0**	1	**2**
1	**1**	1	4
2	**0**	4	16
3	**1**	4	256
4	**1**	1024	65536
		67108864	

Y obtenemos que $2^{26} = 67108864$.

Ejercicio 2.2.1 Sea $m = 37 \cdot 73$. Calcular $2^{2701} \pmod{m}$.

Solución: Lo primero que hacemos es calcular el mínimo común múltiplo

$$mcm(\varphi(37), \varphi(73)) = mcm(36, 72) = 72.$$

Eso significa que $a^{72} \equiv 1 \pmod{m}$ $\forall a$ tal que $mcd(a, m) = 1$. Ahora, $2^{(72+1)37} = 2^{72 \cdot 37} \cdot 2^{37} \equiv 2^{37} \pmod{m}$.
Por el Teorema de Euler, $2^{37} \equiv 2 \pmod{37}$, y $2^{72} \equiv 1 \pmod{73}$.
Como 73 es primo, $\frac{\mathbb{Z}}{<73>}$ es cuerpo. Entonces la expresión $2^{72} \equiv 1 \pmod{73}$ da lugar a que $2^{36} \equiv \pm 1 \pmod{73}$. Para saber si es $+1$ ó -1, podemos calcular cuánto vale 2^{18} (mód 73) y si resulta ser ± 1 significa que se trataba de $+1$.
Utilizamos el algoritmo de exponenciación modular rápida. Tenemos que $18 = (10010)_2$. Completamos la tabla,

i	α_i	z_i	b_i
0	0	1	2
1	1	1	4
2	0	4	16
3	0	4	37
4	1	4	55
		1	

Con lo cual, hemos llegado a que $2^{36} \equiv 1$ (mód 73) $\Rightarrow 2^{37} \equiv 2$ (mód 73). Y como $2^{37} \equiv 2$ (mód 37), tenemos que $2^{37} \equiv 2$ (mód $37 \cdot 73$) y entonces $2^{2701} \equiv 2$ (mód 2701). ✠

2.3 Desarrollo en base mixta

Sean $m_1, \ldots, m_r \in \mathbb{N}$ coprimos dos a dos. Entonces, dado un número natural x, podemos expresarlo de la siguiente manera,

$$x = y_1 + y_2 m_1 + y_3 m_1 m_2 + \ldots, + y_r \prod_{i=1}^{r-1} m_i$$

De forma única si además $y_i < m_i \ \forall \ i$.

Ejemplo: Sea $r = 3$ y sean $m_1 = 2$, $m_2 = 5$ y $m_3 = 7$. Vamos a expresar el número $x = 23$ en esa base mixta.
Primero calculamos $y_1 \equiv x \ (\text{mód } 2) \ \Rightarrow \ y_1 = 1$.
Ahora calculamos y_2 sabiendo que $x \equiv y_1 + y_2 m_1 \ (\text{mód } m_2)$ es decir, $23 \equiv 1 + 2y_2 \ (\text{mód } 5)$, o lo que es lo mismo, $y_2 \equiv 11 \ (\text{mód } 5) \ \Rightarrow \ y_2 = 1$.
Por último, queda calcular y_3 sabiendo que $x \equiv y_1 + y_2 m_1 + y_3 m_1 m_2 \ (\text{mód } m_3)$. Entonces, $23 \equiv 1 + 1 \cdot 2 + 10 y_3 \ (\text{mód } 7)$, con lo cual $y_3 \equiv 2 \ (\text{mód } 7) \ \Rightarrow \ y_3 = 2$.

Tenemos que

$$23 = (1) + (1) \cdot 2 + (2) \cdot 2 \cdot 5$$

Es decir, $23 = 221$ en base $(2, 5, 7)$.

2.4 La función φ de Euler

Definición 2.4.1 Si n es un número positivo, se define $\varphi(n)$ como el número de enteros positivos menores o iguales que n y coprimos con n.

Es evidente que si p es primo, $\varphi(p) = p - 1$. Además, $\varphi\left(\prod_{i=1}^{r} m_i\right) = \prod_{i=1}^{r} \varphi(m_i)$ siempre que $mcd(m_i, m_j) = 1$ cuando $i \neq j$.

Proposición 2.4.1 Si p es primo, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Demostración: $\varphi(p^\alpha) = \#\{k \text{ con } 1 \leq k \leq p^\alpha \ : \ mcd(k, p^\alpha) = 1\} = p^\alpha - \#\{k \text{ con } 1 \leq k \leq p^\alpha \ : \ p|k\} = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. □

Observación 2.4.1 Si $m = p \cdot q$ siendo p y q primos y conocemos $\varphi(m)$, con "poco esfuerzo" podemos calcular p y q.

Sabemos que $\varphi(m) = (p-1)(q-1) = m - (p+q) + 1$. De donde despejamos p, es decir, $p = m + 1 - \varphi(m) - q$. Por otro lado, $m = pq$, entonces, $m = (m + 1 - \varphi(m) - q)q$ o lo que es lo mismo $q^2 + (\varphi(m) - m - 1)q + m = 0$. Ecuación de segundo grado fácil de resolver.

Teorema 2.4.1

$$p \text{ es primo} \Longrightarrow \frac{\mathbb{Z}}{< p >} \text{ es cuerpo y } \left(\frac{\mathbb{Z}}{< p >}\right)^* \text{ es grupo cíclico.}$$

Para demostrar el teorema es necesario introducir primero un lema:

Lema 2.4.1 (Propiedad φ de Euler)
Sea $m \in \mathbb{N}$. Entonces, $m = \sum_{d|m} \varphi(d)$.

Demostración: Definimos $\Gamma_d = \{j \text{ con } 1 \leq j \leq m \text{ tales que } mcd(j,m) = d\}$. Es fácil ver que para valores distintos de d, los Γ_d son disjuntos. Además, si $d \nmid m$ se tiene que $\Gamma_d = \phi$.
Tenemos que,

$$m = \#\left(\bigcup_{d\leq m} \Gamma_d\right) = \#\left(\bigcup_{d|m} \Gamma_d\right) \Rightarrow m = \sum_{d|m} (\#\Gamma_d)$$

Ahora bien, $\#\Gamma_d$ también puede ser expresado como,

$$\#\Gamma_d = \#\left\{j \text{ con } 1 \leq j \leq m \ : \ mcd\left(\frac{j}{d}, \frac{m}{d}\right) = 1\right\} = \#\left\{l \text{ con } 1 \leq l \leq \frac{m}{d} \ : \ mcd(l, \frac{m}{d}) = 1\right\} = \varphi\left(\frac{m}{d}\right)$$

Hemos llegado a que $m = \sum_{d|m} \varphi(\frac{m}{d})$, pero como $d|m \Rightarrow \frac{m}{d}|m$ podemos decir que $m = \sum_{k|m} \varphi(k)$.
□

Demostración: (Del Teorema 2.4.1)

Sea p primo. Sabemos que $\left(\frac{\mathbb{Z}}{<p>}\right)^*$ es un grupo que tiene $p-1$ elementos.
Sea $a(d)$ el número de elementos de orden d del grupo. Por el *"Teorema de Lagrange"* si d no divide a $p-1$, entonces $a(d) = 0$.

Supongamos que $a(d) \neq 0$, entonces $\exists\ \mu$ tal que $ord(\mu) = d$. Ahora bien,

$$< \mu \bmod p > \leq \left(\frac{\mathbb{Z}}{< p >}\right)^*$$

es un grupo cíclico de cardinal d, que tiene $\varphi(d)$ elementos de orden d. De esta forma hemos visto que $a(d) \neq 0 \ \Rightarrow \ a(d) \geq \varphi(d)$.

Todo elemento de orden d es una raíz del polinomio

$$T^d - 1 \in \frac{\mathbb{Z}}{< p >}[T]$$

Y un polinomio con coeficientes en un cuerpo no puede tener más raíces que su propio grado. Además, los d-elementos de $< \mu \bmod p >$ son raíces de $T^d - 1 \in \frac{\mathbb{Z}}{<p>}[T]$.
Si existiera η tal que η (mod p) $\notin <\mu$ mod p > y $ord(\eta)$(mod p) = d, habría otra raíz más, lo que es imposible. Entonces no puede haber más elementos de orden d.

Hemos probado que si $a(d) \neq 0$, entonces $a(d) = \varphi(d)$.
Ahora utilizamos el Lema 2.4.1 para $m = p-1$ y tenemos que,

$$p - 1 = \sum_{d|p-1} \varphi(d)$$

Por otro lado,

$$p - 1 = \sum_{d=1}^{p-1} a(d) = \sum_{d|p-1} a(d)$$

Con lo cual tenemos que,

$$\sum_{d|p-1} \varphi(d) = \sum_{d|p-1} a(d)$$

Tenemos dos sumas iguales, aunque no necesariamente sumando a sumando. Supongamos que $a(d) = 0$ para algún $d|p-1$. Su sumando correspondiente en la otra suma, $\varphi(d)$ no puede ser cero, entonces tendría que haber algún $a(d') > \varphi(d')$ para compensar sumandos. Pero en este caso, como $\varphi(d') > 0$ tendría que ser $a(d') > 0$ y en concreto $a(d') \neq 0$, lo que daría lugar a que $a(d') = \varphi(d')$ y entonces sería imposbile alcanzar dicha compensación en otro sumando.
Esto prueba que para cada $d|p-1$, $a(d) \neq 0$.

En concreto lo anterior se cumple para $d = p-1$, es decir, $a(p-1) \neq 0$, lo que significa que hay algún elemento de orden $p-1$ y por lo tanto el grupo es cíclico. □

Teorema 2.4.2 (Euler):
Sean $a, m \in \mathbb{Z}$. Si $mcd(a,m) = 1 \ \Rightarrow \ a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demostración:
Definimos $\sum_m = \{a \in \{1, 2, \ldots, m-1\} \ : \ mcd(a,m) = 1\}$.
Sea $a \in \sum_m$. Definimos la aplicación $\mu_a : \sum_m \to \sum_m$ tal que $\mu_a(x) = ax \pmod{m}$. Dicha aplicación es inyectiva ya que si $ax \equiv ay \pmod{m} \Rightarrow a(x-y) \equiv 0 \pmod{m}$. Entonces, $m|a(x-y)$ y como $mcd(a,m) = 1$ tenemos que $m|x-y$ o lo que es lo mismo, $x \equiv y \pmod{m}$. Como es un endomorfismo, entonces también es biyectiva. Es decir,

$$\prod_{x \in \sum_m} (ax) \equiv \prod_{x \in \sum_m} x \pmod{m}$$

Sea $p = \prod_{x \in \sum_m} x$, como $\# \sum_m = \varphi(m)$ tenemos que,

$$a^{\varphi(m)} p \equiv p \pmod{m}$$

Pero $mcd(p,m) = 1 \ \Rightarrow \ \exists p' \in \mathbb{Z}$ tal que $pp' \equiv 1 \pmod{m}$ y multiplicando la expresión anterior por p' llegamos a que,

$$a^{\varphi(m)} \equiv 1 \pmod{m} \ \square$$

3 Extensiones de cuerpos

A continuación se proponen algunos resultados sobre extensiones de cuerpos y extensiones algebraicas. Al final de la sección se presenta la Construcción de Kronecker utilizada para la construcción de cuerpos finitos.

3.1 Conceptos básicos

Definición 3.1.1 Sea L cuerpo y $K \subset L$ subcuerpo. Diremos que L es una extensión de K.

Ejemplos: $\mathbb{Q} \subset \mathbb{R}$ o $\mathbb{R} \subset \mathbb{C}$.

Definición 3.1.2 Dada una extensión de cuerpos $K \subset L$ decimos que $u \in L$ es algebraico sobre K si y sólo si $\exists f(x) \in K[X] - \{0\}$ tal que $f(u) = 0$.

Ejemplos: $\mathbb{Q} \subset \mathbb{R}$; $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$.
$\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ porque tomando $f(x) = x^2 - 2$ tenemos que $f(\sqrt{2}) = 0$.
$\pi \in \mathbb{R} - \mathbb{Q}$ "No es algebraico sobre $\mathbb{Q}$, es trascendente".
$e \in \mathbb{R} - \mathbb{Q}$ "No es algebraico sobre $\mathbb{Q}$, es trascendente".
Aunque probar las dos afirmaciones anteriores no es nada trivial.

Observación 3.1.1 Si $l \in K$, entonces $x - l \in K[X]$ y además, $l - l = 0$. En ese caso l es algebraico sobre K.

Observación 3.1.2 $\#\{r \in \mathbb{R}$ algebraicos sobre $\mathbb{Q}\}$ es numerable.

Si $r \in \mathbb{R}$ es algebraico, vamos a ver que, de todos los polinomios con coeficientes en $\mathbb{Q}$ que se anulan en $\mathbb{R}$, hay uno que es el de menor grado y es mónico (de coeficiente principal 1).
Así, dar r es equivalente a dar ese polinomio llamado "polinomio mínimo" de r sobre $\mathbb{Q}$ y dar el orden que ocupa r entre todas las raíces reales de ese polinomio.

De esta forma, cada número real algebraico tiene asociados los coeficientes de un polinomio y un número de orden (menor que el grado del polinomio).

Si F es un conjunto numerable, entonces $\#\{\sum \subset F$ de forma que $\# \sum$ es finito $\}$ es numerable.

Además, $\{r \in \mathbb{R} : r$ no es algebraico sobre $\mathbb{Q}\}$ es un conjunto no numerable.

Definición 3.1.3 Un polinomio $f(x) \in K[X]$ es irreducible si y sólo si $f(x) \neq 0$, $\deg(f) \geq 1$ y si $g|f$, entonces $g \in K - \{0\}$ o $g = cf$ con $c \in K - \{0\}$.

Ejemplo: Todo polinomio de grado 1 es irreducible.

Observación 3.1.3 Sea $f(x) \in K[X]$ y sea $a \in K$. Entonces, $f(a) = 0 \Leftrightarrow x - a|f$.

Por ejemplo, consideremos $\frac{\mathbb{Z}}{<3>}$ y sea $f(x) = x^3 - x$. Entonces f se anula en todos los elementos del anillo. Y además, $f(x) = x(x+1)(x-1)$.

Lema 3.1.1 Dada una extensión de cuerpos $K \subset L$, $f(x) \in K[X] - \{0\}$ y $u \in L$, son equivalentes las siguientes afirmaciones,

(1) $f(x)$ es un polinomio de grado mínimo de entre los polinomios de $K[X]$ no nulos que se anulan en u.

(2) $f(u) = 0$ y $f(x) \in K[X]$ es irreducible.

Demostración:
$\boxed{1 \Rightarrow 2}$
Hay que ver que $f(x) \in K[X]$ es irreducible si verifica las hipótesis de (1).
Sabemos que $f(u) = 0$ y que $f(x) \in K[X] - \{0\}$, con lo cual $\deg(f) \geq 1$. Además, dado $g \in K[X]$ con $g|f$, entonces $\exists h \in K[X]$ tal que $g \cdot h = f$.

Evaluando en u tenemos, $f(u) = 0 = g(u) \cdot h(u)$ en L, que es cuerpo (y por lo tanto Dominio de Integridad). Entonces deducimos que $g(u) = 0$ ó $h(u) = 0$.

Sin pérdida de generalidad, supongamos que es $g(u) = 0$, entonces, como f es un polinomio de grado mínimo de entre los no nulos que se anulan en u, sería absurdo que $\deg(g) < \deg(f)$. Además, $\deg(f) = \deg(g) + \deg(h)$. Entonces, como $\deg(g) \leq \deg(f)$, necesariamente $\deg(g) = \deg(f)$ y en ese caso, $\deg(h) = 0$, es decir, $h \in K - \{0\}$.

Ahora, llamando $c = h$ hemos llegado a que $f = c \cdot g$, lo que prueba (2), f es irreducible.

$\boxed{2 \Rightarrow 1}$
Suponemos ahora que $f \in K[X] - \{0\}$ es irreducible y que $f(u) = 0$.
Sea $\sum = \{h \in K[X] - \{0\} \ : \ h(u) = 0\}$. En particular $f \in \sum$.
Como todos esos polinomios son distintos del polinomio nulo, sus grados son números naturales y podemos hablar de ν, el menor de los grados de los polinomios de $\sum$.

Sea $h \in \sum$, polinomio de grado ν. Aplicamos la división euclidea en $K[X]$ y obtenemos que,

$$f(x) = q(x) \cdot h(x) + r(x)$$

siendo $r(x) = 0$ ó $\deg(r) < \nu$.
Además, $f(u) = 0$ y $h(u) = 0$, lo que da lugar a que $r(u) = 0$. Entonces $r(x) \equiv 0$, pues de lo contrario sería un polinomio de $\sum$ con grado estrictamente menor que ν.

Tenemos que $f(x) = q(x) \cdot h(x)$ y que f es irreducible, entonces $q(x) \in K - \{0\}$ (pues h no puede ser de grado 0 ya que se anula en u) y por lo tanto $\deg(f) = \deg(h) = \nu$. Lo que prueba (1), el polinomio f es de grado mínimo de entre los polinomios no nulos que se anulan en u. □

Como consecuencia de este lema, dada $K \subset L$ extensión de cuerpos y dado $u \in L$ algebraico, si $f(x) \in K[X] - \{0\}$ tal que $f(u) = 0$ y f es de grado mínimo de entre los que se anulan en u, cualquier otro polinomio $g \in K[X]$ que se anule en u verifica que $f|g$.

Definición 3.1.4 Dada $K \subset L$ extensión de cuerpos y dado $u \in L$ algebraico. El polinomio de grado mínimo de entre los que se anulan en u que además es mónico se llama "polinomio mínimo de u sobre K".

Ejemplos: (de polinomios irreducibles en K[X])

⋆ Todo polinomio de grado 1 es irreducible.

⋆ Sea $f(x) \in K[X]$ con $\deg(f) = 2$, entonces $f(x) = a_2x^2 + a_1x + a_0$ siendo $a_2 \neq 0$ y $a_i \in K \ \forall \ i \in \{0, 1, 2\}$.
Veamos si f es irreducible en K[X].
Supongamos que no lo es. Entonces existe un divisor no trivial $g \in K[X]$ con $g|f \wedge g \notin K \wedge g \neq c \cdot f$ siendo $c \in K$. Esto último da lugar a que $\deg(g) \neq 0$ y que $\deg(g) \neq 2$ entonces, necesariamente $\deg(g) = 1$.

Con lo cual, para un polinomio de grado 2 es lo mismo decir que es reducible que decir que tiene una raíz.

Se puede hacer un razonamiento totalmente análogo (salvo algún ajuste) para polinomios de grado 3, de forma que ver que son irreducibles es equivalente a ver que no tienen raíces.

⋆ Sea $\mathbb{F}_2$ un cuerpo de 2 elementos. ¿Qué polinomios con coeficientes en $\mathbb{F}_2$ son irreducibles?
Sabemos que todos los de grado 1 los son: $x \quad ; \quad x + 1$.
De grado 2, aquellos que no tengan raíces. El único es $x^2 + x + 1$.
Para los de grado 3 también buscamos aquellos sin raíces: $x^3 + x + 1 \quad ; \quad x^3 + x^2 + 1$.
Con grado 4 hay que hacer otro tipo de análisis, ya no es válido el criterio anterior. En este caso serían los polinomios: $x^4 + x^3 + x^2 + x + 1 \quad ; \quad x^4 + x^3 + 1 \quad ; \quad x^4 + x + 1$.
El cálculo se va complicando a medida que aumenta el grado, al igual que es cada vez más difícil a medida que aumenta el número de elementos del cuerpo.

3.2 Extensiones de cuerpos

Sea $K \subset L$ extensión de cuerpos. Sea $B = \{b_1, \ldots, b_r\} \subset L$ subconjunto de L.

¿Cuál es el menor subcuerpo de L que contiene a K y a B?
Lo llamamos $K(B)$ y contiene a K, $\{b_1, \ldots, b_r\}$, expresiones del tipo $\sum(\lambda_{i_1,\ldots,i_r} \cdot b_1^{i_1} \cdots b_r^{i_r})$ y sus inversos en L.
Se trata de una extensión intermedia, $K \subset K(B) \subset L$.

Definimos $K[B]$ como el menor anillo que contiene a K y a B. En ese caso,

$$K[B] = \left\{ \sum_{finita} \lambda_{i_1,\ldots,i_r} \cdot b_1^{i_1} \cdots b_r^{i_r} \text{ con } \lambda_{i_1,\ldots,i_r} \in K \text{ y } i_1, \ldots, i_r \in \mathbb{N} \right\}$$

Es de importancia el caso en el que B tiene un único elemento.
Si $B = \{b\}$ (dividir equivale a multiplicar por el inverso),

$$K(\{b\}) = K(B) = \left\{ \frac{\lambda_0 + \lambda_1 b + \cdots + \lambda_r b^r}{\mu_0 + \mu_1 b + \cdots + \mu_m b^m \neq 0} \text{ con } \lambda_i, \mu_j \in K \text{ en } L \right\}$$

Ejemplo:
Sean $K = \mathbb{Q}$, $L = \mathbb{C}$ y $b = \sqrt{2}$.

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{\text{polinomio evaluado en } \sqrt{2}}{\text{polinomio evaluado en } \sqrt{2}} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \; a,b,c,d \in \mathbb{Q} \; \wedge \; c,d \text{ no ambos nulos} \right\}$$

Racionalizando el denominador obtenemos que

$$\mathbb{Q}(\sqrt{2}) = \left\{ \lambda + \mu\sqrt{2} \text{ con } \lambda, \mu \in \mathbb{Q} \right\}$$

Ahora, si $b = \pi$ no se podría simplificar la expresión de $\mathbb{Q}(\pi)$, habría que dejarla como

$$\mathbb{Q}(\pi) = \left\{ \frac{g(\pi)}{h(\pi)} \text{ con } g, h \in \mathbb{Q}[X] \text{ arbitrarios } \wedge \; h(\pi) \neq 0 \right\}.$$

Definición 3.2.1 Dada $K \subset L$ extensión de cuerpos. Diremos que es algebraica si $\forall \; x \in L$, x es algebraico sobre K.

Definición 3.2.2 Si dada la extensión de cuerpos $K \subset L$ existe un subconjunto finito B de L tal que $L = K(B)$ se dice que L es extensión finitamente generada de K.
Si además existe $B = \{b\}$ tal que $L = K(B)$, decimos que L es una extensión simple de K.

En el ejemplo anterior, tanto $\mathbb{Q}(\sqrt{2})$ como $\mathbb{Q}(\pi)$ son extensiones simples sobre $\mathbb{Q}$.
$\mathbb{Q} \subset \mathbb{Q}(\pi, \sqrt{2}) \subset \mathbb{R}$ es una extensión finitamente generada de $\mathbb{Q}$, no algebraica.

Observación 3.2.1 Si $K \subset F$ es una extensión de anillos, siendo K cuerpo y F anillo, tenemos que F es un K-espacio vectorial.
$K \times F \to F$; $(l, a) \mapsto l \cdot a$ (operación definida en F).

Lema 3.2.1 Sea $K \subset L$ extensión de cuerpos y $u \in L$ algebraico sobre K. Sea $f(x) \in K[X]$ el polinomio mínimo de u sobre K. Entonces, $K(u)$ es K-espacio vectorial de dimensión n y base $\mathcal{B} = \{1, u, u^2, \ldots, u^{n-1}\}$. Y por lo tanto podemos escribir, $K(u) = \{a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$ con $a_i \in K \; \wedge \; n = \deg(f)\}$.

Demostración:
$K(u) \supset K$ es una extensión de cuerpos. Además, $\mathcal{B} \subset K(u)$, es decir, $u^i \in K(u)$.
También sabemos que $(K(u), +)$ es grupo, pues $(K(u), +, \cdot)$ es cuerpo.
Es fácil ver que $K(u)$ es K-espacio vectorial verificando todas las propiedades que se han de cumplir.

Veamos que $\mathcal{B}$ es un conjunto linealmente independiente.
Sean $\lambda_0, \ldots, \lambda_{n-1} \in K$ tales que $\lambda_0 + \lambda_1 u + \cdots + \lambda_{n-1}u^{n-1} = 0$. Si definimos $G(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1}$, la condición es que $G(u) = 0$.

Si $G(x)$ fuera no identicamente nulo ($\exists \; i \in \{1, 2, \ldots, n-1\} \; : \; \lambda_i \neq 0$), sería un polinomio de grado menor que n que se anula en u, lo que es imposible pues f es el polinomio mínimo de u sobre K y tiene grado n. Entonces, todos los coeficientes son cero, con lo cual los elementos de $\mathcal{B}$ son linealmente independientes.

Veamos ahora que $\mathcal{B}$ es un sistema de generadores para concluir la demostración.
Sea $\omega \in K(u)$, consideremos dos casos distintos,

1. El elemento es de la forma $\omega = \lambda_0 + \lambda_1 u + \cdots + \lambda_m u^m$ con $\lambda_i \in K$, $m \in \mathbb{N}$ y en principio $m \geq n$ pues si no sería trivial expresar ω en la base $\mathcal{B}$.

   Sea $g(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_m x^m$. Aplicamos la división euclidea y obtenemos que, $\exists q(x), r(x) \in K[X]$ tales que $g(x) = q(x)f(x) + r(x)$ y además, $r(x) \equiv 0$ ó $\deg(r) < n$.

   Ahora, sustituyendo en u, $g(u) = q(u)f(u) + r(u) \Rightarrow g(u) = r(u)$.
   Como $r(x) = \mu_0 + u_1 x + \cdots + u_s x^s$ siendo $s < n$, tenemos que $\omega = g(u) = r(u) = \mu_0 + \mu_1 u + \cdots + \mu_s u^s$ está expresado en la base $\mathcal{B}$ como queríamos.

2. El elemento es de la forma $\omega = \frac{1}{\lambda_0 + \lambda_1 u + \cdots + \lambda_m u^m \neq 0}$ con $\lambda_i \in K$, $m \in \mathbb{N}$. Queremos expresarlo en la base $\mathcal{B}$.

   Sea $g(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_m x^m \in K[X]$. Sabemos que es imposible que $f|g$ porque $f(u) = 0$ y $g(u) \neq 0$ y entonces, como f es irreducible, tenemos que, en $K[X]$, $mcd(f(x), g(x)) = 1$.

   Ahora, por el lema de Bézout, $\exists A(x), B(x) \in K[X]$ tales que

   $$A(x)f(x) + B(x)g(x) = 1 \Rightarrow \underbrace{A(u)f(u)}_{=0} + B(u)g(u) = 1.$$

   En ese caso, $B(u)$ es el inverso de $g(u) \Rightarrow \omega = B(u)$. Además, se podía escoger $B(x)$ tal que $deg(B) < deg(f)$ y entonces $B(x) = b_0 + b_1 x + \cdots + b_s x^s$ con $b_i \in K$.

   Entonces, hemos escrito $\omega = b_0 + b_1 u + \cdots + b_s u^s$, es decir, en función de la base $\mathcal{B}$ como queríamos.

Ahora, el caso general para un ω cualquiera es consecuencia de los dos casos anteriores. Dado

$$\omega = \frac{\lambda_0 + \lambda_1 u + \cdots + \lambda_r u^r}{\mu_0 + \mu_1 u + \cdots + \mu_m u^m}$$

podemos reescribirlo en función de la base $\mathcal{B}$ utilizando los dos argumentos anteriores. □

Ejercicio:
Racionalizar,

$$\frac{1}{\cos\left(\frac{2\pi}{5}\right) - 1} \in \mathbb{Q}\left(\cos\frac{2\pi}{5}\right)$$

¿Es $\cos\left(\frac{2\pi}{5}\right)$ algebraico? ¿cuál es el polinomio mínimo?

En general, $\xi_n = \cos(\frac{2\pi k}{n}) + i\ \mathrm{sen}(\frac{2\pi k}{n})$ son raíces del polinomio $x^n - 1$.
Y si $(n > 1)$, $x^n - 1$ no es irreducible en $\mathbb{Q}[X]$, ya que $x - 1 | x^n - 1$.

En nuestro caso, considerando la extensión de cuerpos $\mathbb{Q} \subset \mathbb{C}$, $\cos(\frac{2\pi}{5}) + i\ \mathrm{sen}(\frac{2\pi}{5})$ es un número complejo algebraico sobre $\mathbb{Q}$, siendo $f(x) = x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$.
Pero el polinomio $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[X]$ es irreducible.

Además, observemos que, como $|\xi| = 1$, se tiene que $\bar{\xi} = \frac{1}{\xi}$.

Buscamos el polinomio mínimo. Tengamos en cuenta que,

$$\eta = \cos\left(\frac{2\pi}{5}\right) = \frac{\xi + \bar{\xi}}{2} = \left(\xi + \frac{1}{\xi}\right)\frac{1}{2}$$

Intentemos buscar un polinomio que se anule en η y de grado lo más pequeño posible.
Es fácil ver que hay uno de grado 2 que es mónico. Llamémoslo $P(x) = x^2 + bx + c$ con $b, c \in \mathbb{Q}$.
Como $P(x)$ se anula en η, tiene que suceder lo siguiente,

$$\frac{1}{4}\left(\xi + \frac{1}{\xi}\right)^2 + \frac{b}{2}\left(\xi + \frac{1}{\xi}\right) + c = 0$$

Y haciendo los cálculos correspondientes se llega a que $b = \frac{1}{2}$ y que $c = \frac{-1}{4}$. Es decir, el polinomio $P(x) = x^2 + \frac{x}{2} - \frac{1}{4}$ es el polinomio mínimo de $\cos\left(\frac{2\pi}{5}\right)$ sobre $\mathbb{Q}$.
Esto resolvería las dos preguntas planteadas en el enunciado de este ejercicio.

Para racionalizar $\frac{1}{\eta - 1}$, tengamos en cuenta que $mcd(x - 1, x^2 + \frac{x}{2} - \frac{1}{4}) = 1$
Entonces, por el lema de Bézout, $\exists A(x), B(x) \in \mathbb{Q}[X]$ tales que $1 = A(x)(x-1) + B(x)(x^2 + \frac{x}{2} - \frac{1}{4})$.
En este caso, $A(x) = -\frac{4}{5}x - \frac{6}{5}$ mientras que $B(x) = \frac{4}{5}$.

Tenemos que, $1 = A(\eta)(\eta - 1) + B(\eta)(\eta^2 + \frac{\eta}{2} - 1) = A(\eta)(\eta - 1)$. Y tenemos que $A(\eta)$ es el inverso multiplicativo del denominador que queríamos racionalizar. Con lo cual la expresión racionalizada queda,

$$A(\eta) = A\left(\cos\left(\frac{2\pi}{5}\right)\right) = -\frac{4}{5}\cos\left(\frac{2\pi}{5}\right) - \frac{6}{5}. \text{ ✠}$$

ACLARACIÓN

Para ver que $x^4 + x^3 + x^2 + x + 1$ es irreducible, se puede utilizar el criterio de Eisenstein.

Proposición 3.2.1 (Criterio de Eisenstein)
Sea D dominio de factorización única y $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n \in D[X]$ con $n \geq 1$ y primitivo. Supongamos que existe $p \in D$ irreducible verificando $p|a_0,\ p|a_1, \ldots,\ p|a_{n-1}$, $p \not| a_n,\ p^2 \not| a_0$, entonces $f(x)$ es irreducible en $D[X]$.

Entonces, el polinomio satisface el criterio de Eisenstein en una nueva variable y después de establecer $x = y + 1$, y en nuestro caso, para aplicar el criterio, basta tomar $p = 5$.

3.3 Extensiones finitas de cuerpos

Definición 3.3.1 Sea $K \subset L$ extensión de cuerpos. Decimos que es una extensión finita si L es un K-espacio vectorial de dimensión finita.

Ejemplos:

- ⋆ $\mathbb{Q} \subset \mathbb{R}$ no es extensión finita, mientras que $\mathbb{R} \subset \mathbb{C}$ sí lo es, ya que una base de $\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}$ como $\mathbb{R}$-espacio vectorial puede ser $\{1, i\}$.
- ⋆ $\mathbb{Q} \subset \mathbb{Q}(b)$ es una extensión finita si $b \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$.

⋆ $\mathbb{Q} \subset \mathbb{Q}(\pi)$ no es un $\mathbb{Q}$-espacio vectorial de dimensión finita. Supongamos que lo es, entonces los siguientes elementos no pueden ser todos linealmente independientes, $\{1, \pi, \pi^2, \pi^3, \dots\}$ y en ese caso $\exists\ \delta \in \mathbb{N}$ tal que $\pi^\delta = a_0 \cdot 1 + a_1 \cdot \pi + \cdots + a_{\delta-1} \cdot \pi^{\delta-1}$, lo cual es absurdo, pues π no es algebraico.

Por el contrario, si $K \subset L$ es una extensión finita, entonces $\exists\ \{u_1, \dots, u_n\} \subset L$ de forma que $L = \mathcal{L}_K\{u_1, \dots, u_n\}$.
En particular $B = \{u_1, \dots, u_n\}$ y entonces $L = K(B)$, $K \subset L$ es extensión finitamente generada.

Proposición 3.3.1 Las siguientes propiedades sobre extensiones finitas de K cuerpo son ciertas,

(1) Si $K \subset L$ extensión finita $\Rightarrow$ L es extensión finitamente generada de K.

(2) Si $K \subset L$ extensión finita $\Rightarrow$ L es extensión algebraica de K.

(3) (Transitividad) Sea $K \subset L$ extensión finita con $\dim_K L = r$ y sea $L \subset F$ extensión finita con $\dim_L F = s$. Entonces, F es una extensión finita sobre K y $\dim_K F = r \cdot s$.

Demostración:
Para entender (1) basta leer el comentario inmediatamente anterior a esta Proposición.
Veamos cómo demostrar (2),
Sea $u \in L - \{0, 1\}$. Entonces los elementos $\{1, u, u^2, \dots\} \subset L$ son, en principio, distintos. Como L es K-espacio vectorial de dimensión finita, no puede haber un conjunto infinito de vectores distintos que sean linealmente independientes.
Esto da lugar a que $\exists\ \delta \in \mathbb{N}$ con $\delta \leq \dim_K L$ tal que u^δ es combinación lineal de los vectores $\{1, u^2, \dots, u^{\delta-1}\}$.
Es decir, $\exists a_i \in K$ con $i = 0, 1, \dots, \delta - 1$ tales que $u^\delta = a_0 \cdot 1 + a_1 \cdot u + \cdots + a_{\delta-1} u^{\delta-1}$. Ahora definimos $P(x) = x^\delta - a_{\delta-1} x^{\delta-1} - \cdots - a_1 x - a_0 \in K[X]$ y llegamos a que $P(u) = 0$ y por lo tanto u es algebraico sobre K.

Demostremos (3), Sea $B_{L|K} = \{v_1, \dots, v_r\} \subset L$ base de L como K-espacio vectorial.
Sea $B_{F|L} = \{u_1, \dots, u_s\} \subset F$ base de F como L-espacio vectorial.
Afirmamos que $\mathcal{B} = \{v_i u_j \ : \ 1 \leq i \leq r \text{ y } 1 \leq j \leq s\} \subset F$ es una base de F como K-espacio vectorial.
Esto implica (3), aunque es una afirmación aún más fuerte.

1. Veamos que $\mathcal{B}$ es sistema de generadores de F como K-espacio vectorial.
   Sea $z \in F$. Recordemos que F es un L-espacio vectorial con base $B_{F|L}$, entonces podemos expresar z como,
   $$z = \sum_{j=1}^{s} \lambda_j u_j \text{ con } \lambda_j \in L \ \forall\ j = 1, \dots, s$$
   Ahora, los λ_j los podemos escribir en función de $B_{L|K}$, es decir, $\exists\ \mu_{ij} \in K$ tales que $\lambda_j = \sum_{i=1}^{r} \mu_{ij} v_i$ y entonces tenemos que,
   $$z = \sum_{i=1,j=1}^{r,s} \mu_{ij} v_i u_j \ \text{ con } \ \mu_{ij} \in K$$

2. Veamos que $\{v_i u_j \ : \ 1 \leq i \leq r \text{ y } 1 \leq j \leq s\}$ son linealmente independientes sobre K.
   Escribimos una combinación lineal igualada a cero y veamos que necesariamente los coeficientes son cero.

$$\sum_{i=1,j=1}^{r,s} \gamma_{ij} v_i u_j \ \text{ con } \ \gamma_{ij} \in K$$

   Ahora bien, la suma anterior es igual a

$$\sum_{j=1}^{s} \left(\sum_{i=1}^{r} \gamma_{ij} v_i \right) u_j$$

   y como $\{u_1, \ldots, u_s\}$ son linealmente independientes en L tenemos que

$$\sum_{i=1}^{r} \gamma_{ij} v_i = 0 \ \forall j = 1, \ldots, s$$

   pero como $\{v_1, \ldots, v_r\}$ son linealmente independientes en K tenemos que

$$\gamma_{ij} = 0 \ \forall ij. \ \square$$

Ejemplo: Consideremos $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. Tenemos $K \subset L$ extensión finita (adjunto un elemento algebraico) y también $L \subset F$ extensión finita (adjunto un elemento algebraico).
Claramente $B_{L|K} = \{1, \sqrt{2}\}$ es una base de L como K-espacio vectorial. Además, el polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $x^2 - 2$.

Sabemos que $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ es un polinomio que se anula en $\sqrt{3}$, pero ¿es el de grado mínimo en $\mathbb{Q}(\sqrt{2})$? o equivalentemente ¿$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$? o lo que es lo mismo ¿$\sqrt{3} = a + b\sqrt{2}$ siendo $a, b \in \mathbb{Q}$?

Los griegos demostraron que la respuesta a la última pregunta es "no" y por lo tanto la respuesta a las otras dos es "sí".

Esto da lugar a que $B_{F|L} = \{1, \sqrt{3}\}$ es una base de $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ como $\mathbb{Q}(\sqrt{2})$-espacio vectorial. Y por lo tanto, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es una base de $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ como $\mathbb{Q}$-espacio vectorial.

3.4 Construcción de Kronecker

El objetivo es extender un cuerpo "pequeño" sin conocer uno más grande.
Sea K cuerpo y $f(x) \in K[X]$ con $\deg(f) \geq 1$.
Sea $\frac{K[X]}{<f>}$ (ideal de múltiplos de f) el anillo cociente. $[g]_f = \{g + hf \text{ siendo } h \in K[X]\}$.

$$[g_1]_f \pm [g_2]_f = [g_1 \pm g_2]_f \qquad [g_1]_f \cdot [g_2]_f = [g_1 \cdot g_2]_f$$

Proposición 3.4.1 Es $\frac{K[X]}{<f>}$ una extensión de K y por lo tanto es un K-espacio vectorial con base $\{[1]_f, [x]_f, \ldots, [x^{n-1}]_f\}$ siendo $n = \deg(f)$. Y es un cuerpo si y sólo si $f(x) \in K[X]$ es irreducible.
Además, si $f(x) \in K[X]$ es irreducible, el cuerpo $\frac{K[X]}{<f>}$ contiene al menos una raíz de $f(x)$ que es $[x]_f$.

Demostración:
Consideremos la aplicación $\varphi : K \longrightarrow \frac{K[X]}{<f>}$ definida como $\varphi(c) = [c]_f$.
Veamos que φ es inyectiva.
Supongamos que $c, c' \in K$ son tales que $[c]_f = [c']_f$. Entonces, $f|c - c' \in K \Rightarrow c - c' = 0 \Rightarrow c = c'$.
Esto prueba que en $\frac{K[X]}{<f>}$ hay más elementos que en K.
Veamos que $\mathcal{B} = \{[1]_f, [x]_f, \ldots, [x^{n-1}]_f\}$ es base:

1. Es sistema de generadores.

   Sea $[g]_f \in \frac{K[X]}{<f>}$ dado $g \in K[X]$.
   Realizando el algoritmo de Euclides, podemos encontrar $q, r \in K[X]$ tales que $g = q \cdot f + r$.
   Siendo $r(x) = r_0 + r_1 x + \cdots + r_s x^s$ con $r_i \in K$ y $s < n$. En ese caso,

   $$[g]_f = [q \cdot f]_f + [r]_f = [g]_f \cdot \underbrace{[f]_f}_{=0} + [r]_f$$

   y por lo tanto,

   $$[g]_f = [r_0 + r_1 x + \cdots + r_s x^s]_f = r_0 + r_1 [x]_f + \cdots + r_s [x^s]_f$$

   hemos expresado $[g]_f$ en función de los elementos de la base.

2. Es conjunto K-linealmente independiente.

   Sean $\lambda_i \in K$ tales que $\lambda_0 1 + \lambda_1 [x]_f + \cdots + \lambda_{n-1}[x^{n-1}]_f = 0_{\frac{K[X]}{<f>}}$ o lo que es lo mismo, $\lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1} x^{n-1} \in < f >$. Esto da lugar a que todos los λ_i son 0, pues de lo contrario tendríamos un polinomio no nulo de grado menor que f y múltiplo de él, lo que es imposible.

Ahora, un anillo $(A, +, \cdot)$ es cuerpo si y sólo si $\forall\ z \in A : z \neq 0_A\ \exists\ z' \in A$ de forma que $zz' = 1_A$.
Entonces,

$$\frac{K[X]}{< f >} \text{ es cuerpo } \iff \forall g \in K[X] \text{ tal que } f \not| g\ \ \exists\ h \in K[X]\ \wedge\ g \cdot h - 1 \in < f >$$

Y lo anterior es equivalente a que $\forall g \in K[X]$ tal que $f \not| g\ \exists h \in K[X],\ \exists q \in K[X]$ de manera que $g \cdot h - q \cdot f = 1$ en $K[X]$. Si y solamente si $\forall g \in K[X] : f \not| g$, se tiene que $mcd(f, g) = 1 \iff f$ es irreducible.

Por último, suponemos $f \in K[X]$ irreducible. Entonces, $\frac{K[X]}{<f>}$ que abreviaremos como K_f es cuerpo.
Consideremos f como elemento de $K_f[T]$ y vamos a ver que f tiene en K_f una raíz, $[x]_f$.
Sea $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ con $a_i \in K$.

$$f([x]_f) = a_n [x]_f^n + \cdots + a_1 [x]_f + a_0 = [a_n x^n + \cdots + a_1 x + a_0]_f = [0]_f. \ \square$$

Ejemplo: Sea $K = \frac{\mathbb{Z}}{<2>} = \mathbb{F}_2$.
Si $f(x) \in \mathbb{F}_2[X]$ es irreducible, entonces $\frac{\mathbb{F}_2}{<f>}$ es cuerpo.
Como ejemplo,

$$\frac{\mathbb{F}_2}{< x^4 + x^3 + 1 >} \text{ es un cuerpo de 16 elementos.}$$

En general, si $f \in \mathbb{F}_p[X]$ es irreducible y $\deg(f) = n$, la Construcción de Kronecker proporciona un cuerpo de p^n elementos.

Ejemplo: Vamos a construir un cuerpo de 4 elementos y veremos cómo se relacionan.
Tenemos que $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{<x^2+x+1>}$ cuyos elementos son 1, 0, x, $x+1$ y podemos conostruir la tabla de sumas,

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Así como la tabla de multiplicar,

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

en la que se aprecia que todo elemento no nulo tiene inverso.

4 Cuerpos finitos

A continuación estudiaremos los cuerpos finitos y sus propiedades. Estos cuerpos tienen muchas aplicaciones en otros campos, desde resolver una ecuación de congruencias hasta poder controlar el lanzamiento de misiles, por ejemplo.

4.1 Recordando conceptos básicos

Recordemos que si $(A, +, \cdot)$ es anillo, el menor subanillo de A debe contener

$$\Sigma_A = \{1_A;\ 1_A+ \overset{n)}{\ldots}. +1_A;\ (-1_A)+ \overset{n)}{\ldots}. (-1_A) \text{ con } n \in \mathbb{N}\}$$

Además debe contener a,

$$(1_A+ \overset{n)}{\ldots}. +1_A) \cdot (1_A+ \overset{m)}{\ldots}. +1_A) = 1_A+ \overset{n\cdot m}{\ldots}. +1_A$$

$$((-1_A)+ \overset{n)}{\ldots}. +(-1_A)) \cdot ((-1_A)+ \overset{m)}{\ldots}. +(-1_A)) = 1_A+ \overset{n\cdot m}{\ldots}. +1_A$$

$$((-1_A)+ \overset{n)}{\ldots}. +(-1_A)) \cdot (1_A+ \overset{m)}{\ldots}. +1_A) = (-1_A)+ \overset{n\cdot m}{\ldots}. +(-1_A)$$

Entonces existen dos posibilidades excluyentes,

$$\begin{cases} \text{O bien } \exists \delta \in \mathbb{N} \ :\ 1_A+ \overset{\delta}{\ldots}. +1_A = 0_A \\ \text{O bien } \forall\ \delta \in \mathbb{N} \ ||\ 1_A+ \overset{\delta}{\ldots}. +1_A \neq 0_A \end{cases}$$

En el primer caso se dice que A tiene caraterística finita y en el segundo que el anillo tiene característica cero. Se define la característica del anillo como el menor δ natural tal que $1_A+ \overset{\delta}{\ldots}. +1_A = 0_A$.

1. En caso de característica finita, sea δ la característica de A.
   Tenemos que Σ_A es isomorfo a $\frac{\mathbb{Z}}{<\delta>}$.
2. En caso contrario, Σ_A es isomorfo a $\mathbb{Z}$.

En cualquier caso, todo anillo $(A, +, \cdot)$ contiene una copia de $\frac{\mathbb{Z}}{<n>}$ para algún $n \in \mathbb{N}$ o una copia de $\mathbb{Z}$.
Claramente, si $\#A$ es finito, sólo se puede dar el primer caso.

Proposición 4.1.1 Si $(A, +, \cdot)$ es un cuerpo y la característica de A es $n < +\infty$, entones n es un número primo.

Demostración:
Sea $n = r \cdot s$ siendo $r, s > 1$ la característica del anillo A.
Consideramos $1_A+ \overset{n)}{\ldots}. +1_A = (1_A+ \overset{r)}{\ldots}. +1_A) \cdot (1_A+ \overset{s)}{\ldots}. +1_A) = 0_A$.
Entonces, $r_A \cdot s_A = 0_A$ y si A es cuerpo, entonces también es dominio de integridad, es decir, $r_A = 0_A$ ó $s_A = 0_A$.
Sin pérdida de generalidad, sea $r_A = 0_A = 1_A+ \overset{r)}{\ldots}. +1_A \Rightarrow$ como $r < n$ es absurdo que la característica de A sea n. $\square$

Todo cuerpo K, o bien posee una copia de $\frac{\mathbb{Z}}{<p>}$, con p primo, o bien posee una copia de $\mathbb{Q}$ y este es su "cuerpo primo" (el menor subcuerpo de K).
En particular, todo cuerpo finito posee una copia de $\frac{\mathbb{Z}}{<p>}$.

- ⋆ Si $\mathbb{F}$ es un cuerpo finito y $p = \text{caract}(\mathbb{F})$, entonces $\mathbb{F} \supset \frac{\mathbb{Z}}{<p>}$ es un $\frac{\mathbb{Z}}{<p>}$-espacio vectorial de dimensión finita.
- ⋆ Si $\#\mathbb{F} = p^m$ éste puede ser interpretado como m-uplas con entradas en un conjunto de cardinal p.

Proposición 4.1.2 Sea $\mathbb{F}$ un cuerpo finito ($\mathbb{F} \supset \frac{\mathbb{Z}}{<p>}$ y $p = \text{caract}(\mathbb{F})$), entonces

$$\frac{\mathbb{Z}}{< p >} = \{x \in \mathbb{F} \ : \ x^p - x = 0\}\,.$$

Demostración:
Para cada $a \in \frac{\mathbb{Z}}{<p>}$, si $a = 0$, entonces $0^p - 0 = 0$ y si $a \neq 0$, por el pequeño teorema de Fermat, $a^{p-1} \equiv 1$ (mód p) en $\mathbb{F}$ y entonces, $a^p = a$, lo que da lugar a que $a^p - a = 0$.

¿Por qué no hay más elementos en $\mathbb{F}$ que verifiquen $x^p - x = 0$?
Porque $T^p - T \in \mathbb{F}[T]$ es un polinomio de grado p con coeficientes en un cuerpo y por el *Teorema Fundamental del Álgebra* no puede tener más de p raíces. □

Sea $\mathbb{F} \supset \frac{\mathbb{Z}}{<p>}$ extensión finita y por lo tanto extensión algebraica.
Sea $\alpha \in \mathbb{F}$. Nos preguntamos cuál es el polinomio mínimo de α respecto a $\frac{\mathbb{Z}}{<p>}$.

Consideremos el conjunto $\{\alpha^{p^0}, \alpha^{p^1}, \alpha^{p^2}, \ldots, \alpha^{p^{i-1}}\}$. Siendo i el menor número natural tal que $\alpha^{p^i} = \alpha$, o lo que es lo mismo $\alpha^{p^i - 1} = 1 \ \Rightarrow \ \text{ord}(\alpha) | p^i - 1$.
Consideremos ahora

$$f_\alpha(x) = \prod_{l=0}^{i-1} (x - \alpha^{p^l})$$

polinomio de grado i, donde i es el menor natural tal que $p^i \equiv 1$ (mód ord(α)) en $\mathbb{F}$.
Veamos que $f_\alpha(x)$, que pertenece a $\mathbb{F}[X]$, realmente está en $\frac{\mathbb{Z}}{<p>}[X]$.

Para ello hay que ver que todo coeficiente c de $f_\alpha(x)$ verifica $c^p = c$.
Sea $f_\alpha(x) = c_{i-1}x^{i-1} + \cdots + c_1 x + c_0$. En ese caso,

$$(f_\alpha(x))^p = c_i^p x^{p(i-1)} + \cdots + c_1^p x^p + c_0^p = \prod_{l=0}^{i-1} (x - \alpha^{p^l})^p$$

pero la expresión anterior es igual a

$$\prod_{l=0}^{i-1} (x^p - \alpha^{p^{l+1}}) = \prod_{j=0}^{i-1} (x^p - \alpha^{p^j}) = f_\alpha(x^p) = c_{i-1}x^{p(i-1)} + \cdots + c_1 x^p + c_0$$

Y como los coeficientes tienen que ser iguales dos a dos, tenemos que $c_j^p = c_j \ \forall j$, con lo cual los c_j están en realidad en $\frac{\mathbb{Z}}{<p>}$.

ACLARACIÓN

En el razonamiento anterior hemos utilizado el siguiente resultado.

Lema 4.1.1 Sea $(A, +, \cdot)$ anillo abeliano de característica p, número primo.
Entonces se verifica para todo $a, b \in A$ que $(a \pm b)^p = a^p \pm b^p$.

Demostración:
Sabemos que, como A es abeliano,

$$(a \pm b)^p = \sum_{k=0}^{p} \binom{p}{k} (\pm 1)^k a^k b^{p-k}$$

Fijémonos en todos los sumandos menos en el primero y el último. Sea $1 \leq k \leq p-1$, entonces $\binom{p}{k}$ es un múltiplo de p, ya que se puede expresar como,

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{1 \cdot 2 \cdot 3 \cdots k}$$

Y como p es primo, no se puede simplificar con el denominador, entonces tenemos una expresión entera que es múltiplo de p, sea $\binom{p}{k} = c_k \cdot p$.
Ahora bien, podemos ver el sumando k-ésimo de la siguiente forma,

$$c_k \cdot \underbrace{(1_A + \overset{p)}{\ldots} + 1_A)}_{=0_A} \cdot (\pm 1)^k a^k b^{p-k} = 0_A$$

Y por lo tanto, todos los sumandos de la suma desarrollada según el binomio de Newton, excepto el primero y el último, son nulos como queríamos demostrar. □

Ejemplo: Veamos que el polinomio $f(x) = x^6 + x + 1 \in \mathbb{F}_2[X]$ es irreducible.
No tiene factores irreducibles de grado 1. El único polinomio irreducible de grado 2 es el $x^2 + x + 1$ y no divide a f. Y en cuanto a los factores irreducibles de grado 3 sólo podrían ser $x^3 + x + 1$ o $x^3 + x^2 + 1$ y ninguno divide a f.
Esto prueba que f es irreducible.

Sea $\mathbb{F}_{64} = \frac{\mathbb{F}_2[X]}{<f>}$ cuerpo de 64 elementos. Veamos ahora que x (mód f) tiene orden 63 (entonces f es lo que después llamaremos "polinomio primitivo").
Sabemos que el orden de x módulo $f(x)$ es divisor de 63. Entonces tiene que ser 1, 3, 7, 9, 21 o 63.

$$x^3 \not\equiv 1 \text{ (mód } f) \qquad x^6 \equiv x+1 \text{ (mód } f) \qquad x^7 \equiv x^2 + x \text{ (mód } f) \qquad x^9 \equiv x^4 + x^3 \text{ (mód } f)$$

y $x^{21} = (x^9)^2 \cdot x^3 \equiv (x^4 + x^3)^2 \cdot x^3 \equiv (x^8 + x^6) \cdot x^3 \equiv (x^3 + x^2 + x + 1) \cdot x^3 \equiv x^6 + x^5 + x^4 + x^3 \equiv x + 1 + x^5 + x^4 + x^3 \not\equiv 1$ (mód f).
Entonces el orden de x (mód f) necesariamente tiene que ser 63.

En ese caso podemos decir que,

$$\mathbb{F}_{64}^* = \{1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{62}\}$$

Ahora elegimos un elemento, $\omega = x^3 \pmod f$ y vamos a calcular su polinomio mínimo sobre $\mathbb{F}_2$. ¿Qué grado tendrá? Podemos calcular el orden multiplicativo de ω, es decir, su orden como elemento del grupo $\mathbb{F}_{64}^*$,

$$\omega = a^3 \;\Rightarrow\; \text{ord}(\omega) = \frac{\text{ord}(a)}{mcd(\text{ord}(a), 3)} = \frac{63}{mcd(63, 3)} = 21 \;\Rightarrow\; \text{ord}(\omega) = 21.$$

El grado del polinomio mínimo es el menor i tal que $\omega^{2^i} = \omega \;\Leftrightarrow\; 2^i - 1 \equiv 0 \pmod{\text{ord}(\omega)} \;\Leftrightarrow\; 2^i \equiv 1 \pmod{21} \;\Rightarrow\; i = 6$ es el menor.
Ahora, su polinomio mínimo es,

$$(t-\omega)(t-\omega^2)(t-\omega^4)(t-\omega^8)(t-\omega^{16})(t-\omega^{32})$$

expresión difícil de simplificar. Por eso en este caso es mejor calcular el polinomio mínimo de esta otra manera.
Sea $g(t) = t^6 + a_5t^5 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$ con $a_i \in \mathbb{F}_2$. Como g es el polinomio mínimo, se debe anular en $\omega = \bar{x}^3$, entonces,

$$\bar{x}^{18} + a_5\bar{x}^{15} + a_4\bar{x}^{12} + a_3\bar{x}^9 + a_2\bar{x}^6 + a_1\bar{x}^3 + a_0 = \bar{0}_{\mathbb{F}_{64}}$$

es decir,

$$(\bar{x}^3 + \bar{x}^2 + \bar{x} + 1) + a_5(\bar{x}^5 + \bar{x}^3) + a_4(\bar{x}^2 + 1) + a_3(\bar{x}^3 + \bar{x}^4) + a_2(\bar{x} + 1) + a_1\bar{x}^3 + a_0 = \bar{0}_{\mathbb{F}_{64}}$$

y para comparar los dos miembros de la igualdad necesitamos escribirlos en función de la base $\{1, \bar{x}, \ldots, \bar{x}^5\}$.
Entonces llegamos al siguiente sistema de ecuaciones,

$$\begin{cases} 1: & a_0 + a_2 + a_4 + 1 = 0 \longrightarrow a_0 = 1 \\ \bar{x}: & a_2 + 1 = 0 \longrightarrow a_2 = 1 \\ \bar{x}^2: & a_4 + 1 = 0 \longrightarrow a_4 = 1 \\ \bar{x}^3: & a_1 + a_3 + a_5 + 1 = 0 \longrightarrow a_1 = 1 \\ \bar{x}^4: & a_3 = 0 \\ \bar{x}^5: & a_5 = 0 \end{cases}$$

Con lo cual, el polinomio mínimo de ω respecto a $\mathbb{F}_2$ es $g(t) = t^6 + t^4 + t^2 + t + 1$.

ACLARACIÓN

En el ejemplo anterior hemos utilizado el siguiente lema.

Lema 4.1.2 Sea G grupo, $a \in G$ y sea $r = \text{ord}(a)$, entonces,

$$\text{ord}(a^k) = \frac{r}{mcd(r, k)}$$

Demostración:
El orden de a^k es el menor número natural i tal que $(a^k)^i = 1$. Es decir, $a^{i\cdot k} = 1$. Como $a^r = 1$, necesitamos el menor i tal que $r | i \cdot k$. Pero entonces, $i \cdot k = mcm(r, k)$ y tenemos que $i = \frac{mcm(r,k)}{k}$.
Ahora, utilizando que $mcm(r, k) = \frac{r \cdot k}{mcd(r,k)}$ llegamos a que,

$$i = \text{ord}(a^k) = \frac{r \cdot \not{k}}{\not{k} \cdot mcd(r, k)} = \frac{r}{mcd(r, k)}. \;\square$$

4.2 Tabla de logaritmos

Sea K un cuerpo finito, entonces $\#(K) = p^d$ con p primo. Además $1_K + \overset{p)}{\ldots} + 1_K = 0_K$ y $\mathbb{F}_p \subset K = \mathbb{F}_{p^d}$. $\mathbb{F}_{p^d}$ es un $\mathbb{F}_p$-espacio vectorial de dimensión d.

También sabemos que

$$\mathbb{F}_{p^d} = \frac{\mathbb{F}_p[X]}{< x^d + u_{d-1}x^{d-1} + \cdots + u_1 x + u_0 = D(x) >}$$

y para calcular, por ejemplo, $p(x) \cdot q(x)$ en este anillo cociente basta calcular el resto al dividir $p(x) \cdot q(x)$ entre $D(x)$.

Consideramos $\mathbb{F}_{p^d} - \{0\} = \mathbb{F}_{p^d}^*$. Sabemos que $(\mathbb{F}_{p^d}^*, \cdot)$ es un grupo abeliano.

Teorema 4.2.1 (Del elemento primitivo)
Sea $\mathbb{F}_{p^d}$ cuerpo finito de p^d elementos con p primo. Entonces, $(\mathbb{F}_{p^d}^*, \cdot)$ es un grupo cíclico.

Definición 4.2.1 Un elemento primitivo (o raíz primitiva) de $\mathbb{F}_{p^d}^*$ es un generador del grupo cíclico $(\mathbb{F}_{p^d}^*, \cdot)$.

Ejemplo:
Consideremos el cuerpo de 11 elementos, $\mathbb{F}_{11} \sim \frac{\mathbb{Z}}{<11>} = \{\underline{0}, \underline{1}, \ldots, \underline{10}\}$.
Entonces, $\mathbb{F}_{11}^* = \{\underline{1}, \ldots, \underline{10}\}$. Aunque a partir de ahora nos ahorraremos el subrayado para referirnos a la clase de equivalencia.

Busquemos un elemento primitivo. Para ello podemos probar con el 3,

$$3^1 = 3 \qquad 3^2 = 9 \qquad 3^3 = 27 = 5 \qquad 3^4 = 4 \qquad 3^5 = 1$$

En este caso 3 no puede ser primitivo porque no genera todo el grupo. Si probamos con el 2,

$$2^1 = 2 \qquad 2^2 = 4 \qquad 2^3 = 8 \qquad 2^4 = 5 \qquad 2^5 = 10$$

Y ya podemos parar sabiendo que 2 sí es un elemento primitivo.
¿Por qué? Porque el cardinal del grupo es 10 y el orden de cualquier elemento tiene que dividir a dicho cardinal.
En los cálculos anteriores hemos comprobado que el orden de 2 es mayor que 5 y como tiene que dividir a 10, sólo puede ser 10, es decir, 2 es generador y por lo tanto un elemento primitivo de $\mathbb{F}_{11} =< 2 >$.

Definición 4.2.2 (Logaritmo discreto)
Sea $\mathbb{F}_q$ cuerpo finito con $q = p^d$ y p un número primo. Sea α un elemento primitivo de $\mathbb{F}_q^*$. Entonces para cada $b \in \mathbb{F}_q^*$ definimos $\log_\alpha b$ como el número $a \in \mathbb{F}_q^*$ tal que $\alpha^a = b$.

En el ejemplo de $\mathbb{F}_{11}$ podemos construir fácilmente la tabla de logaritmos,

$\mathbb{F}_{11}^*$	1	2	3	4	5	6	7	8	9	10
$\log_\alpha$	10	1	8	2	4	9	7	3	6	5

Además se verifica la siguiente propiedad,

$$\log_\alpha(b \cdot c) = \log_\alpha b + \log_\alpha c$$

lo que hace que a veces sea más rápido para realizar un producto sumar los logaritmos asociados a cada factor y deshacer el cambio que realizar el propio producto.

Veamos otro ejemplo de tabla de logaritmos, en este caso con $\mathbb{F}_8^* = \frac{\mathbb{F}_2[X]}{<x^3+x+1>}$, cuyo cardinal es 7 y por lo tanto todos los elementos del grupo son primitivos.
Sea $\alpha = x$. Entonces,

$$\alpha^2 = x^2 \qquad \alpha^3 = x+1 \qquad \alpha^4 = x^2+x \qquad \alpha^5 = x^2+x+1 \qquad \alpha^6 = x^2+1 \qquad \alpha^7 = 1$$

En este caso la tabla quedaría de la siguiente manera,

$\mathbb{F}_8^*$	x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1
$\log_\alpha$	1	2	3	4	5	6	7

Ahora, si a cada polinomio le asociamos un vector en función de sus coeficientes, por ejemplo, $x^2+x+1 = (1,1,1)$ o $x = (0,1,0)$, es claro que sumando los vectores, estaremos sumando los polinomios.
Pero también se puede multiplicar los polinomios es decir, ¡multiplicar los vectores! ayudándonos de los logaritmos discretos y la propiedad enunciada más arriba.

Como ejemplo, veamos cuánto vale $(0,1,0)\cdot(1,0,1)$. Calculamos sus logaritmos en base x asociados, que son 1 y 6 respectivamente y entonces, el logaritmo asociado al producto debe ser la suma de ambos, $1+6=7$ y por lo tanto el producto de los dos vectores resulta ser el vector $(0,0,1)$.

4.3 Polinomios primitivos sobre cuerpos finitos

En general es un problema difícil encontrar un generador de $\mathbb{F}_p^*$. Hay exactamente $\varphi(p-1)$, con lo cual, la probabilidad de encontrarlo escogiendo uno al azar es $\frac{\varphi(p-1)}{p-2}$.

Vamos a construir la tabla multiplicativa de los elementos de $\mathbb{F}_9^*$.
Sabemos que $\mathbb{F}_9 \simeq \frac{\mathbb{F}_3[X]}{<x^2+x-1>} = \{\alpha+\beta x \ : \ \alpha,\beta \in \{0,1,-1\}\}$.
La tabla (sin contar el cero pues es un caso trivial) quedaría así:

	1	-1	$\bar{x}$	$-\bar{x}$	$\bar{x}+1$	$-\bar{x}-1$	$-\bar{x}+1$	$\bar{x}-1$
1	1	-1	$\bar{x}$	$-\bar{x}$	$\bar{x}+1$	$-\bar{x}-1$	$-\bar{x}+1$	$\bar{x}-1$
-1	-1	1	$-\bar{x}$	$\bar{x}$	$-\bar{x}-1$	$\bar{x}+1$	$\bar{x}-1$	$-\bar{x}+1$
$\bar{x}$	$\bar{x}$	$-\bar{x}$	$-\bar{x}+1$	$\bar{x}-1$	1	-1	$-\bar{x}-1$	$\bar{x}+1$
$-\bar{x}$	$-\bar{x}$	$\bar{x}$	$\bar{x}-1$	$-\bar{x}+1$	-1	1	$\bar{x}+1$	$-\bar{x}-1$
$\bar{x}+1$	$\bar{x}+1$	$-\bar{x}-1$	1	-1	$\bar{x}-1$	$-\bar{x}+1$	$\bar{x}$	$-\bar{x}$
$-\bar{x}-1$	$-\bar{x}-1$	$\bar{x}+1$	-1	1	$-\bar{x}+1$	$\bar{x}-1$	$-\bar{x}$	$\bar{x}$
$-\bar{x}+1$	$-\bar{x}+1$	$\bar{x}-1$	$-\bar{x}-1$	$\bar{x}+1$	$\bar{x}$	$-\bar{x}$	-1	1
$\bar{x}-1$	$\bar{x}-1$	$-\bar{x}+1$	$\bar{x}+1$	$-\bar{x}-1$	$-\bar{x}$	$\bar{x}$	1	-1

Ahora, mirando la tabla podemos comprobar que $\bar{x}$ es un generador de $\mathbb{F}_9$.

$\bar{x}^2 = -\bar{x} + 1 \qquad \bar{x}^3 = -\bar{x} - 1 \qquad \bar{x}^4 = -1 \qquad \bar{x}^5 = -\bar{x} \qquad \bar{x}^6 = \bar{x} - 1 \qquad \bar{x}^7 = \bar{x} + 1 \qquad \bar{x}^8 = 1$

Además vemos que el inverso de $\bar{x}$ es $\bar{x}^7 = \bar{x} + 1$.

Definición 4.3.1 (Polinomio primitivo sobre un cuerpo finito)
Sea p primo. $\mathbb{F}_p = \frac{\mathbb{Z}}{<p>}$ y sea $f(x) \in \mathbb{F}_p[X]$ con $\deg(f) = n > 1$. Decimos que f es primitivo si,

- f(x) es irreducible en $\mathbb{F}_p[X]$.
- Si el cuerpo $\mathbb{F} := \frac{\mathbb{F}_p[X]}{<f(x)>}$, que tiene p^n elementos, tiene a $\bar{x} \equiv x$ (mód f) como generador de $\mathbb{F}^*$.

Ejemplo: El polinomio $x^2 + x - 1$ es primitivo sobre $\mathbb{F}_3$, pero sin embargo $x^2 + 1$ no lo es.

Definición 4.3.2 (Equivalente a la anterior)
Sea p primo. $\mathbb{F}_p = \frac{\mathbb{Z}}{<p>}$ y sea $f(x) \in \mathbb{F}_p[X]$ con $\deg(f) = n > 1$. Decimos que f es primitivo si $x \not| f$ y $\bar{x} \equiv x$ (mód f), en el grupo $U\left(\frac{\mathbb{F}_p[X]}{<f(x)>}\right)$, tiene orden $p^n - 1$.

Proposición 4.3.1 Las definiciones 4.3.1 y 4.3.2 son equivalentes.

Demostración:
En realidad sólo hay que ver que la segunda implica la primera. Bajo las hipótesis de 4.3.2, veamos que $f(x)$ es irreducible. Esto es equivalente a ver que $\frac{\mathbb{F}_p[X]}{<f>}$ es cuerpo. Y esto último sucede si y sólo si todo elemento no nulo del anillo $\frac{\mathbb{F}_p[X]}{<f>}$ tiene inverso, o lo que es lo mismo,

$$U\left(\frac{\mathbb{F}_p[X]}{< f >}\right) = \frac{\mathbb{F}_p[X]}{< f >} - \{\bar{0}\}$$

NOTA: Las equivalencias anteriores se deben a la Proposición 3.4.1.

Tenemos que demostrar la doble inclusión para ver que los dos conjuntos son iguales, pero en realidad una de las dos inclusiones es trivial. Sólo hay que demostrar que

$$U\left(\frac{\mathbb{F}_p[X]}{< f >}\right) \supset \frac{\mathbb{F}_p[X]}{< f >} - \{\bar{0}\}$$

Sea $f \in \mathbb{F}_p[X]$ tal que $x \not| f$. Tenemos que $mcd(x, f) = 1$ en $\mathbb{F}_p[X]$ y por lo tanto $\bar{x} \in U\left(\frac{\mathbb{F}_p[X]}{<f>}\right)$. Además, como por hipótesis, el orden de $\bar{x}$ es $p^n - 1$, $\bar{x}$ es generador del anillo $\left(\frac{\mathbb{F}_p[X]}{<f>}\right)^*$. $\square$

Para ver si un polinomio es primitivo algunas veces es adecuado utilizar la primera de las definiciones y otras veces la segunda.

Ejemplo: Consideremos el cuerpo de 16 elementos, $\mathbb{F}_{16} = \frac{\mathbb{F}_2[X]}{x^4+x+1}$, pues sabemos que $x^4 + x + 1$ es un polinomio irreducible de $\mathbb{F}_2[X]$, pero ¿es un polinomio primitivo?
En este caso es mejor utilizar la primera definición para comprobarlo pues sólo queda ver si el orden

de $\bar{x}$ es 15 en $\mathbb{F}_{16}^*$.

Por el Teorema de Lagrange, el orden de $\bar{x}$ debe dividir a 15, es decir, debe ser 1, 3, 5 o 15.
En realidad no puede tener orden menor que 4, así que vamos a analizar si tiene orden 5.

$$\bar{x}^4 + \bar{x} + 1 = 0 \;\Rightarrow\; \bar{x}^4 = -\bar{x} - 1 = \bar{x} + 1 \;\Rightarrow\; \bar{x}^5 = \bar{x}^2 + \bar{x} \neq 1$$

Eso significa que el orden de $\bar{x}$ no puede ser 5 y por lo tanto debe ser 15, con lo cual $\bar{x}$ es generador de $\mathbb{F}_{16}^*$, lo que significa que el polinomio $x^4 + x + 1$ es primitivo en $\mathbb{F}_2$.

Si en vez de probar con el polinomio anterior, probamos con $x^4 + x^3 + x^2 + x + 1$ obtendremos que $\bar{x}$ tiene orden 5 en $\frac{\mathbb{F}_2[X]}{<x^4+x^3+x^2+x+1>}$ y por lo tanto no es un polinomio primitivo en $\mathbb{F}_2$.

4.4 Fórmula mágica de los cuerpos finitos

Proposición 4.4.1 Sea p un número primo y $m \in \mathbb{N}$. Entonces,

$$x^{p^m} - x = \prod f_d(x)$$

donde $f_d(x)$ es irreducible en $\frac{\mathbb{Z}}{<p>}$, es mónico y además $\deg(f) = d \wedge d|m$.

Ejemplo: Sea $p = 2$ y $m = 4$.

$$x^{2^4} - x = x^{16} - x = \underbrace{x(x+1)}_{\text{grado 1}} \cdot \underbrace{(x^2+x+1)}_{\text{grado 2}} \cdot \underbrace{(x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1)}_{\text{grado 4}}$$

Se puede comprobar que es cierto haciendo las cuentas.

Lema 4.4.1 Sea $a, m, n \in \mathbb{Z}^+$ entonces las siguientes afirmaciones son equivalentes,

(1) $m|n$.

(2) $a^m - 1|a^n - 1$.

(3) $x^{a^m} - x|x^{a^n} - x$ en $\mathbb{Z}[X]$.

Demostración:

$\boxed{1 \Rightarrow 2}$
Suponemos que $m|n$, entonces existe un $\lambda \in \mathbb{Z}^+$ tal que $n = m \cdot \lambda$.
Y ahora, $a^n - 1 = a^{m\cdot\lambda} - 1 = (a^m - 1)(a^{m(\lambda-1)} + a^{m(\lambda-2)} + \cdots + 1) \;\Rightarrow\; a^m - 1|a^n - 1$.

$\boxed{2 \Rightarrow 3}$
Suponemos que $u = a^m - 1|a^n - 1 = v$. Como $u, v \in \mathbb{Z}$ y $u|v$, podemos utilizar la implicación ya demostrada para ver que $t^u - 1|t^v - 1$ en $\mathbb{Z}[T]$ y por lo tanto, $x^{a^m-1} - 1|x^{a^n-1} - 1 \;\Rightarrow x^{a^m} - x|x^{a^n} - x$ en $\mathbb{Z}[X]$.

$\boxed{3 \Rightarrow 2}$
La hipótesis es que $x^{a^m} - x | x^{a^n} - x$ en $\mathbb{Z}[X] \Rightarrow x^{a^m-1} - 1 | x^{a^n-1} - 1$ en $\mathbb{Z}[X]$. Podemos aplicar la división euclídea y obtener que $a^n - 1 = q(a^m - 1) + r$ con $0 \leq r < a^m - 1$. En ese caso tenemos,

$$x^{a^n-1} = x^{(a^m-1)q} \cdot x^r = (x^{(a^m-1)q} - 1)x^r + x^r$$

entonces,

$$x^{a^n-1} - 1 = (x^{(a^m-1)q} - 1)x^r + x^r - 1$$

tengamos en cuenta que

$$x^{a^m-1} - 1 | (x^{a^m-1} - 1)(x^{(a^m-1)(q-1)} + x^{(a^m-1)(q-2)} + \cdots + 1) = x^{(a^m-1)q} - 1$$

y entonces existe un $k \in \mathbb{Z}$ tal que $(x^{a^m-1} - 1)k = x^{(a^m-1)q} - 1$. Con lo cual tenemos,

$$x^{a^n-1} - 1 = (x^{a^m-1} - 1)kx^r + x^r - 1$$

y utilizando la hipótesis vemos que necesariamente

$$x^{a^m-1} - 1 | x^r - 1 \Rightarrow \begin{cases} a^m - 1 \leq r & \rightarrow \text{ imposible.} \\ r = 0. \checkmark \end{cases}$$

$\boxed{2 \Rightarrow 1}$
Para concluir, la hipótesis es que $a^m - 1 | a^n - 1$ y queremos ver que entonces $m | n$.
Realizamos la división euclidea de forma que $\exists\, q, r \in \mathbb{Z} \,:\, n = mq + r$ con $0 \leq r < m$. Tenemos que,

$$a^n - 1 = a^{mq} \cdot a^r - 1 = (a^{mq} - 1)a^r + a^r - 1$$

Sabemos que $a^m - 1 | (a^m - 1)(a^{m(q-1)} + a^{m(q-2)} + \cdots + 1) = a^{mq} - 1$ y entonces existe un $k \in \mathbb{Z}$ tal que $a^{mq} - 1 = (a^m - 1)k$. Con lo cual tenemos que,

$$a^n - 1 = (a^m - 1)ka^r + a^r - 1$$

y como, por hipótesis, $a^m - 1 | a^n - 1$ vemos que necesariamente,

$$a^m - 1 | a^r - 1 \Rightarrow \begin{cases} m \leq r & \rightarrow \text{ imposible.} \\ r = 0. \checkmark \end{cases} \quad \square$$

Demostración: (De la Proposicion 4.4.1)

- Primero vamos a ver que si $f_d(x)$ es irreducible en $\frac{\mathbb{Z}}{<p>}[X]$, es mónico y $d | m$, entonces $f_d(x) | x^{p^m} - x$ en $\frac{\mathbb{Z}}{<p>}[X]$. Para ello definimos

$$\mathbb{F}' := \frac{\mathbb{F}_p[X]}{< f_d(x) >} \text{ que es cuerpo pues } f_d(x) \text{ es irreducible.}$$

  Además es un $\mathbb{F}_p$-espacio vectorial de dimensión d y tenemos que $\#\mathbb{F}' = p^d$ y que $\#\mathbb{F}'^* = p^d - 1$. Sea $\theta = x$ (mód $f_d(x)$), es decir, $\theta \in \mathbb{F}'^*$. Sabemos que $\theta^{(p^d-1)} = 1$ y en particular, $\theta^{p^d} - \theta = 0$. Entonces θ es una raíz del polinomio $x^{p^d} - x$.

  Ahora, como $d | m$ podemos aplicar el Lema 4.4.1 para ver que $x^{p^d} - x | x^{p^m} - x$ en $\mathbb{F}_p[X]$. Y entonces θ también es raíz del polinomio $x^{p^m} - x$.
  Por la Proposición 3.4.1 sabemos que θ es raíz del polinomio $f_d(x)$, pero entonces, éste es un polinomio irreducible, mónico y que se anula en θ, con lo cual es el polinomio mínimo de θ y esto da lugar a que $f_d(x) | x^{p^m} - x$ en $\mathbb{F}_p[X]$, como queríamos ver.

⋆ Como la descomposición en factores irreducibles en un cuerpo ($\mathbb{F}_p[X]$) es única, será suficiente demostrar que si $f(x) \in \mathbb{F}_p[X]$ (mónico) es irreducible y divide a $x^{p^m} - x$, entonces el grado de f divide a m.

Sea $f(x) \in \mathbb{F}_p[X]$ irreducible y sea d el grado de f. Además,

$$\mathbb{F}' := \frac{\mathbb{F}_p[X]}{< f(x) >} \text{ es un cuerpo de } p^d \text{ elementos.}$$

Por hipótesis $f(x)|x^{p^m} - x$ y por la Proposición 3.4.1 $\bar{x}$ es raíz de $f(x)$.
Entonces, $\bar{x}^{p^m} = \bar{x}$ en $\mathbb{F}'$ y como $\mathbb{F}'^*$ es un grupo cíclico de cardinal $p^d - 1$, $\exists\ \theta \in \mathbb{F}'$ tal que $\text{ord}(\theta) = p^d - 1$. Además podemos expresar θ como,

$$\theta = g(\bar{x}) = a_0 + a_1\bar{x} + \cdots + a_{d-1}\bar{x}^{d-1} \quad \text{con } a_i \in \mathbb{F}_p\ \forall i$$

Tenemos que,

$$\theta^{p^m} = (a_0 + a_1\bar{x} + a_{d-1}\bar{x}^{d-1})^{p^m} = a_0^{p^m} + a_1^{p^m}\bar{x}^{p^m} + \cdots + a_{d-1}^{p^m} + (\bar{x}^{d-1})^{p^m}$$

y simplificando llegamos a que

$$\theta^{p^m} = a_0 + a_1\bar{x} + \cdots + a_{d-1}\bar{x}^{d-1} = \theta.$$

Lo que significa que θ es invariante en $\mathbb{F}'$, y entonces $\theta^{p^m-1} = 1$. Con lo cual $\text{ord}(\theta)|p^m - 1$, es decir, $p^d - 1|p^{m-1}$ y aplicando el Lema 4.4.1 llegamos a que $d|m$. □

A continuación exponemos algunos resultados que son consecuencia de la fórmula mágica mencionada en esta sección:

Teorema 4.4.1 Sea $f(x) \in \frac{\mathbb{Z}}{<p>}[X]$ irreducible. Sea $\mathbb{F}'$ cuerpo tal que $\mathbb{F}' \supset \frac{\mathbb{Z}}{<p>}$ (la característica de $\mathbb{F}'$ es p). Entonces son equivalentes las siguientes afirmaciones:

(1) El grado de f divide a m siendo $m = \dim_{\frac{\mathbb{Z}}{<p>}} \mathbb{F}'$.

(2) f tiene una raíz en $\mathbb{F}'$.

(3) $f(x)$ es producto de factores lineales en $\mathbb{F}'[X]$.

Demostración:

$\boxed{1 \Rightarrow 3}$
Sea $f(x) \in \frac{\mathbb{Z}}{<p>}[X]$ irreducible. Dividiendo por el coeficiente principal podemos conseguir que f sea mónico. Sea $\deg(f) = d$. Por hipótesis $d|m$. Y entonces, por la Proposición 4.4.1 tenemos que $f|x^{p^m} - x$.
El cuerpo $\mathbb{F}' \supset \frac{\mathbb{Z}}{<p>}$ y $\#\mathbb{F}' = p^m \ \Rightarrow\ \#\mathbb{F}'^* = p^m - 1$. Entonces,

$$\forall\ a \in \mathbb{F}'\ ||\ a = 0 \vee a^{p^m} = 1 \iff \forall a \in \mathbb{F}'\ ||\ a^{p^m} = a$$

Si y sólo si todo elemento de $\mathbb{F}'$ es raíz de $x^{p^m} - x$. En ese caso,

$$x^{p^m} - x = \prod_{\alpha \in \mathbb{F}'} (x - \alpha)$$

Por otra parte, $\exists g(x) \in \frac{\mathbb{Z}}{<p>}[X]$ tal que $g(x) \cdot f(x) = x^{p^m} - x = \prod_{\alpha \in \mathbb{F}'}(x - \alpha)$, pero en $\mathbb{F}'[X]$ la descomposición en factores irreducibles es única, con lo cual,

$$f(x) = (x - \alpha_{i_1}) \cdots (x - \alpha_{i_d}) \text{ para ciertos } \alpha_{i_1}, \ldots, \alpha_{i_d} \in \mathbb{F}'.$$

Como queríamos ver.

$\boxed{3 \Rightarrow 2}$
Es evidente.

$\boxed{2 \Rightarrow 1}$
La hipótesis ahora es que $f(x)$ es irreducible en $\frac{\mathbb{Z}}{<p>}[X]$ y tiene una raíz en $\mathbb{F}'$. Además, $\#\mathbb{F}' = p^m$. Según la fórmula mágica (Proposición 4.4.1) y por la unicidad de la descomposición en factores irreducibles en $\frac{\mathbb{Z}}{<p>}[X]$, para ver que el grado de f divide a m es suficiente probar que $f | x^{p^m} - x$ en $\frac{\mathbb{Z}}{<p>}[X]$.

Sabemos que f tiene una raíz en $\mathbb{F}'$, llamémosla ω. Tenemos que $\omega \in \mathbb{F}'$ y que $f(\omega) = 0$. Si $\omega = 0$ verifica $\omega^{p^m} - \omega = 0$, así que supongamos que $\omega \neq 0$. Entonces, $\omega \in \mathbb{F}'^*$. Es decir, la raíz pertenece a un grupo de cardinal $p^m - 1$, con lo cual,

$$\omega^{p^m - 1} = 1 \;\Rightarrow\; \omega^{p^m} - \omega = 0$$

y entonces ω es raíz del polinomio $x^{p^m} - x$.
No olvidemos que $f(x)$ es el polinomio mínimo de ω sobre $\frac{Z}{<p>}$, lo que significa que $f | x^{p^m} - x$ en $\frac{\mathbb{Z}}{<p>}[X]$ y por lo tanto el grado de f divide a m. $\square$

Ejemplo:
Sea $\mathbb{F}'$ cuerpo de 9 elementos construido de la forma $\frac{\mathbb{F}_3[X]}{<x^2+1>}$. El polinomio $f(y) = y^2 + y - 1$ es irreducible en $\mathbb{F}_3[Y]$. Entonces, según el Teorema 4.4.1 que acabamos de demostrar, como $\deg(f) = 2$ y $2 | m = 2$, entonces $f(y) = (y - \alpha)(y - \beta)$ en $\mathbb{F}'$.

Busquemos α y β.
$\alpha = a + b\bar{x}$ con $a, b \in \{-1, 0, 1\}$ en $\mathbb{F}_3$.

$$(a + b\bar{x})^2 + (a + b\bar{x}) - 1 = \bar{0} \;\Rightarrow\; a^2 - b^2 - ab\bar{x} + a + b\bar{x} - 1 = \bar{0}$$

Y como $\{1, \bar{x}\}$ es una base de $\mathbb{F}'$ como $\mathbb{F}_3$-espacio vectorial, tenemos,

$$\begin{cases} 1: \; a^2 - b^2 + a - 1 = 0 \\ \bar{x}: \; -ab + b = 0 \end{cases}$$

Y resolviendo el sistema vemos que necesariamente $a = 1$ y $b = \pm 1$. Y entonces,

$$f(y) = (y - (1 + \bar{x}))(y - (1 - \bar{x})).$$

Teorema 4.4.2 (Unicidad de los cuerpos finitos)
Para cada número primo p y para cada $n \in \mathbb{N}$ existe (salvo isomorfismo que conserva $\frac{\mathbb{Z}}{<p>}$) un único cuerpo de p^n elementos.

Demostración:
Sean p primo y $n \in \mathbb{N}$ y sea $\mathbb{F}'$ un cuerpo de p^n elementos.
Como $\mathbb{F}'^*$ es cíclico, sea θ una raíz primitiva de $\mathbb{F}'$, entonces $\mathbb{F}'^* =< \theta >$. Ahora, $\mathbb{F}' \supset \frac{Z}{<p>}[X]$ y sea $f(x)$ el polinomio mínimo de θ sobre $\frac{\mathbb{Z}}{<p>}$.

Veamos que $\frac{\mathbb{F}_p[X]}{<f>}$ es isomorfo a $\mathbb{F}'$. Definimos el homomorfismo de anillos $ev_\theta : \mathbb{F}_p[X] \longrightarrow \mathbb{F}'$ que manda un polinomio con coeficientes en $\mathbb{F}_p$ a su evaluación en θ visto como un polinomio de $\mathbb{F}'$. En particular, $ev_\theta(x) = \theta$.
Por el Primer Teorema de Isomorfía, sabemos que existe una biyección entre $\frac{\mathbb{F}_p[X]}{\ker(ev_\theta)}$ e $Im(ev_\theta)$. Ahora, bien,

$$\ker(ev_\theta) = \{g(x) \in \mathbb{F}_p[X] \ : g(\theta) = 0\}$$

es decir, el núcleo de la aplicación ev_θ son los múltiplos de $f(x)$ (pues f es el polinomio mínimo de θ sobre $\frac{\mathbb{Z}}{<p>}$).

Por otra parte veamos que $Im(ev_\theta) = \mathbb{F}'$. Dado $\alpha \in \mathbb{F}'$, si $\alpha \neq 0$, como $\mathbb{F}'^* =< \theta >$ sabemos que existe un $\delta \in \mathbb{N}$ tal que $\alpha = \theta^\delta$ y en ese caso, $x^\delta \in \frac{\mathbb{Z}}{<p>}[X]$ verifica que $ev_\theta(x^\delta) = \theta^\delta = \alpha$. Si $\alpha = 0$, entonces $ev_\theta(x^{p^n-1} - 1) = 0 = \alpha$.

Hemos probado que,

$$\frac{\mathbb{F}_p[X]}{< f >} = \frac{\mathbb{F}_p[X]}{\ker(ev_\theta)} \approx Im(ev_\theta) = \mathbb{F}'.$$

De nuevo, sea p primo, $n \in \mathbb{N}$ y sean $\mathbb{F}'$ y $\mathbb{F}''$ cuerpos de p^n elementos, construidos de la siguiente forma,

$$\mathbb{F}' = \frac{\mathbb{F}_p[X]}{< f >} \qquad\qquad \mathbb{F}'' = \frac{\mathbb{F}_p[X]}{< g >}$$

con $f(x), g(x) \in \mathbb{F}_p[X]$ polinomios irreducibles, mónicos y ambos de grado n.

Veamos que $\mathbb{F}' \approx \mathbb{F}''$.
Por el Teorema 4.4.1 sabemos que f tiene una raíz en $\mathbb{F}'$, llamémosla ω. Contruimos la aplicación $\varphi_\omega : \mathbb{F}' = \frac{\mathbb{F}_p[X]}{<f>} \longrightarrow \mathbb{F}''$ que manda un polinomio de $\mathbb{F}'$ al polinomio de $\mathbb{F}''$ que resulta de evaluar el primero en ω. La aplicación está bien definida ya que si $P_1(x) \equiv P_2(x)$ (mód f), entonces,

$$\varphi_\omega(P_1(x)) = P_1(\omega) \quad \text{y} \quad \varphi_\omega(P_2(x)) = P_2(\omega)$$

pero $f | P_1 - P_2 \ \Rightarrow \ \exists h \ : \ f \cdot h = P_1 - P_2$ y como $f(\omega) = 0$, tenemos que $P_1(\omega) = P_2(\omega)$.

El núcleo de la aplicación es,

$$\ker(\varphi_\omega) = \left\{ P(x) \in \frac{\mathbb{F}_p[X]}{< f >} \ : \ \varphi_\omega(P(x)) = 0 \right\} = \left\{ P(x) \in \frac{\mathbb{F}_p[X]}{< f >} \ : \ P(\omega) = 0 \right\}$$

Y como f es el polinomio mínimo de ω sobre $\mathbb{F}_p[X]$, el núcleo de la aplicación es la clase del 0, con lo cual la aplicación φ_ω es inyectiva.

Por otra parte, como $\mathbb{F}'$ y $\mathbb{F}''$ tienen el mismo cardinal, la aplicación también es sobreyectiva y por lo tanto define un isomorfismo entre los dos cuerpos. □

Ahora surge una nueva pregunta. Dado p primo supongamos que tenemos dos cuerpos finitos, $\mathbb{F}$ y $\mathbb{F}'$ con de cardinal p^n y p^m respectivamente. ¿Alguno de ellos está contenido en el otro?

Proposición 4.4.2 En las hipótesis anteriores, $\mathbb{F} \subset \mathbb{F}'$, es decir, $\mathbb{F}'$ contiene una copia de $\mathbb{F}$, si y sólo si $n|m$.

Demostración:

"$\Rightarrow$" Supongamos $\mathbb{F}$ es un subcuerpo de $\mathbb{F}'$ ($\mathbb{F} \subset \mathbb{F}'$). Entonces también tenemos que $\mathbb{F}^*$ es un subgrupo de $\mathbb{F}'^*$.

$$p^n - 1 = \#\mathbb{F}^* \mid \#\mathbb{F}'^* = p^m - 1$$

y por el Lema 4.4.1 concluimos que $n|m$.

"$\Leftarrow$" Supongamos que $n|m$. Podemos considerar $\mathbb{F} = \frac{\mathbb{F}_p[X]}{<f>}$ con $f(x) \in \mathbb{F}_p[X]$ polinomio irreducible y de grado n.
Como $n|m$, por el Teorema 4.4.1 tenemos que $\exists \omega \in \mathbb{F}' \ : \ f(\omega) = 0$.
Contruimos el homomorfismo de anillos $ev_\omega : \mathbb{F}_p[X] \longrightarrow \mathbb{F}'$ que manda un polinomio de $\mathbb{F}_p[X]$ a su evaluación en ω visto como un polinomio de $\mathbb{F}'$.
Tenemos que $\ker(ev_\omega) = \{g(x) \in \mathbb{F}_p[X] \ \ g(\omega) = 0\} =< f >$ ya que f es el polinomio mínimo de ω (pues podemos suponer que es mónico).
Entonces la misma aplicación cuyo dominio es $\frac{\mathbb{F}_p[X]}{<f>} = \mathbb{F}$ es inyectiva, lo que significa que $\mathbb{F} \subset \mathbb{F}'$. $\square$

Ejercicio: (Por Eva y Maribel)
¿Qué subcuerpos tiene $\mathbb{F}_{625}$?. Sea α un elemento primitivo de $\mathbb{F}_{625}$, expresar en potencias de α los elementos no nulos de dichos subcuerpos.

Sabemos que $\mathbb{F} \subset \mathbb{F}'$ si y solo si $n|m$ siendo $\#\mathbb{F} = p^n$ y $\#\mathbb{F}' = p^m$.
En nuestro caso $\#F_{625} = 5^4$ y por lo tanto tenemos subcuerpos de cardinal 5^1 y 5^2.
Ahora bien, $\alpha^{624} \equiv 1$ (mód 625).

$\star$ En $\mathbb{F}_5^*$ elegimos $\beta = \alpha^{156}$ y por lo tanto β tiene orden 4 en $\mathbb{F}_{625}^*$ lo que significa que

$$\mathbb{F}_5^* = \{1, \alpha^{156}, \alpha^{312}, \alpha^{468}\}$$

$\star$ En $\mathbb{F}_{5^2}^*$ elegimos $\beta = \alpha^{26}$ y por lo tanto β tiene orden 24 en $\mathbb{F}_{625}^*$ lo que significa que

$$\mathbb{F}_{5^2}^* = \{1, \alpha^{26}, \alpha^{52}, \ldots, \alpha^{598}\} \ \ \clubsuit$$

Ejercicio: (Por Eva y Maribel)
Sea $\mathbb{F}$ un cuerpo de cardinal 81. Demostrar que el polinomio $x^2 + x - 1$ tiene una raíz en $\mathbb{F}$.

Tenemos que $\mathbb{F} = \mathbb{F}_{3^4} = \frac{\mathbb{F}_3[X]}{<f>}$ con $f \in \mathbb{F}_3[X]$ un polinomio irreducible de grado 4.
Veamos que $g(x) = x^2+x-1$ es irreducible en $\mathbb{F}_3[X]$. Como tiene grado 2 es suficiente con comprobar que no tiene raíces y en efecto,

$$g(0) = -1 \qquad g(1) = -1 \qquad g(-1) = -1$$

Ahora, utilizando el Teorema 4.4.1 llegamos a que, como $2|4$, el polinomio $x^2 + x - 1$ tiene una raíz en $\mathbb{F}$.

Demostrar que $\mathbb{F}$ contiene una raíz primitiva quinta de la unidad, ω.
Sabemos que $\mathbb{F}_{81}^*$ es un grupo cíclico de 80 elementos y por lo tanto tiene un elemento que lo genera. Sea α dicho elemento, entonces

$$\text{ord}(\alpha) = 80 \Rightarrow \alpha^{80} \equiv 1 \text{ (mód 81)} \Rightarrow (\alpha^{16})^5 \equiv 1 \text{ (mód 81)}$$

Por lo tanto, $\omega = \alpha^{16}$ es una raíz quinta de la unidad y es primitiva ya que $\text{ord}(\omega) = 5$.

Calcular el polinomio mínimo de ω sobre $\frac{\mathbb{Z}}{<3>}$.
Consideremos el polinomio $f(T) = T^5 - 1$ pues $f(\omega) = \omega^5 - 1 = 0$. ¿Es irreducible en $\frac{\mathbb{Z}}{<3>}$?
No lo es, tenemos que $f(T) = (T-1)(T^4 + T^3 + T^2 + T + 1)$ y como $\omega \neq 1$ entonces

$$\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$$

o lo que es lo mismo, ω es raíz de $h(T) = T^4 + T^3 + T^2 + T + 1$, pero ahora $h(T)$ sí es irreducible en $\frac{\mathbb{Z}}{<3>}$ ya que no tiene raíces y por tanto no tiene factores de grado 1 ni 3,

$$h(0) = 1 \qquad h(1) = -1 \qquad h(-1) = 1$$

ni tampoco tiene factores irreducibles de grado 2 pues éstos en $\frac{\mathbb{Z}}{<3>}$ son x^2+x-1, x^2+1 y x^2-x-1 y ninguno divide a h.
En resumen, $h(T) = T^4 + T^3 + T^2 + T + 1$ es el polinomio de grado mínimo de ω sobre $\frac{\mathbb{Z}}{<3>}$. ✠

5 Cifrado en flujo

En inglés, *Stream Cipher*. Este método de encriptado utiliza una secuencia de bits producida de manera eficiente, con período grande y que debe parecer aleatoria. Dicha secuencia aleatoria es producida por un autómata a partir de una clave inicial.
Es de utilidad, por ejemplo, en conversaciones telefónicas pues se trata de situaciones de cifrado en tiempo real.

5.1 Conceptos básicos

Definición 5.1.1 Un registro de desplazamiento con realimentación de longitud m consiste en una colección de celdas de memoria que, en cada instante, almacenan 0 o 1, y en una función de realimentación.

En cada instante la colección de ceros y unos contenidos en las celdas de memoria se llama estado del registro. El registro pasa del estado $(s_0, \ldots, s_{n-1})$ al estado $(s_1, \ldots, s_n)$, siendo $s_n = f(s_0, \ldots, s_{n-1})$ donde f es la función de realimentación.
El registro se conoce como FSR (*feedback shift register*). Si f es una función lineal se llama $LFSR$.

Definición 5.1.2 El período de una secuencia es el menor p tal que $s_i = s_{i+p}$ para cada $i \in \mathbb{N}$.
El período siempre es menor o igual que 2^m, pues éste es el número de estados distintos.

Ejemplo: Sea $m = 4$ y $f(s_0, s_1, s_2, s_3) = s_0 + s_1 + s_2 + s_3$. Entonces, dado el estado inicial 1010 obtenemos,

1 0 1 0 0 1 0 1 0

que tiene período 5.
Sin embargo, si $m = 4$ y $f(s_0, s_1, s_2, s_3) = s_0 + s_3$, con el mismo estado inicial,

1 0 1 0 1 1 0 0 1 0 0 0 1 1 1 1 0 1 0

tenemos una secuencia de período 15.

Ahora, si $m = 5$ y $f(s_0, \ldots, s_4) = s_0 + s_4$, con el valor inicial $(1, 0, 0, 0, 0)$ obtenemos una secuencia de período 21 mientras que con el valor inicial $(1, 1, 1, 0, 0)$ el período es 7. Obtenemos períodos distintos debido a que el polinomio característico $x^5 + x^4 + 1$ no es irreducible en $\mathbb{F}_2[X]$.

Definición 5.1.3 Dado m y una función de realimentación lineal, $f(s_0, \ldots, s_{m-1}) = c_0 s_0 + \cdots + c_{m-1} s_{m-1}$. Definimos el polinomio característico del $LFSR$ como

$$P(x) = x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0$$

En el ejemplo anterior los polinomios característicos son $x^4 + x^3 + x^2 + x + 1$ y $x^4 + x^3 + 1$ respectivamente.

Definición 5.1.4 Decimos que el $LFSR$ es regular si $c_0 \neq 0$.

Observemos que, en caso de que f sea lineal, $s_m = c_0 s_0 + \cdots + c_{m-1} s_{m-1}$, además $s_{m+1} = c_0 s_1 + \cdots + c_{m-1} s_m$ y en general,

$$s_{m+i} = \sum_{j=0}^{m-1} c_j s_{i+j} \ \forall \ i \geq 0$$

y entonces, si el registro es regular ($c_0 \neq 0$) y el valor inicial es no nulo, el número de estados a los que se va a llegar es menor o igual que $2^m - 1$ ya que nunca se podrá llegar al estado nulo.

Nos reduciremos a estudiar $LFSR's$ regulares ($c_0 \neq 0$).
Es fácil ver que si $c_0 = 0$, podemos obtener la misma secuencia cifrante con un $LFSR$ de longitud menor.

Observación 5.1.1 Sea un $LFSR$ tal que para algún valor inicial $z_0, \ldots, z_{m-1}$, la secuencia producida tiene período máximo, es decir, tiene período $2^m - 1$. En ese caso el registro recorre todos los resgistros menos el registro nulo.
En realidad, si sucede lo anterior, para cualquier estado inicial distinto del nulo, se recorrerán todos los estados.

5.2 Algunos resultados importantes

Vamos a intentar caracterizar la propiedad anterior en términos del polinomio característico del $LFSR$.
Sea $\Omega(f)$ el conjunto de secuencias $(z_i)_{i\geq 0}$ obtenidas por el $LFSR$ a partir del polinomio característico f para un valor inicial $(z_0, \ldots, z_{m-1})$. Tenemos que $\Omega(f) \subset \mathbb{F}_2^{\mathbb{N}}$.

Proposición 5.2.1 $\Omega(f)$ es un $\mathbb{F}_2$-espacio vectorial de dimensión m.

Demostración:
Veamos que $(\Omega(f), +)$, donde $+$ se refiere a la suma módulo 2, es un grupo abeliano.
Es claro que $\mathbb{F}_2^{\mathbb{N}}$ con la suma módulo 2 es un grupo abeliano, así que sólo tenemos que ver que la suma es interna en $\Omega(f)$. Es decir, que si sumamos dos sucesiones de $\Omega(f)$, obtenemos otra sucesión que también está en $\Omega(f)$.

Sea $(z_0, \ldots, z_{m-1}, \ldots) \in \Omega(f)$ y sea $(w_0, \ldots, w_{m-1}, \ldots) \in \Omega(f)$. Además,

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \quad \text{y} \quad w_{i+m} = \sum_{j=0}^{m-1} c_j w_{i+j}.$$

Consideremos la sucesión suma de las dos anteriores y veamos que es la misma sucesión que se genera a partir del valor inicial $(z_0 + w_0, \ldots, z_{m-1} + w_{m-1})$. Para verlo basta que lo comprobemos para el siguiente elemento de la sucesión y haciendo un razonamiento iterativo se podría completar la demostración.

Sabemos que el siguiente término es, $\sum_{j=0}^{m-1} c_j(z_j + w_j)$, pero por linealidad podemos expresarlo como,

$$\sum_{j=0}^{m-1} c_j(z_j + w_j) = \sum_{j=0}^{m-1} c_j z_j + \sum_{j=0}^{m-1} c_j w_j = z_m + w_m$$

Como queríamos ver.
Para ver que $(\Omega(f), +)$ es gurpo abeliano quedaría ver que la sucesión nula está en $\Omega(f)$, pero ésta es la sucesión asociada al valor inicial nulo y quedaría ver que toda sucesión tiene una opuesta, pero esto es muy fácil ya que una sucesión es opuesta a sí misma.
En definitiva, como los únicos escalares de $\mathbb{F}_2$ son el cero y el uno, en realidad ya hemos visto que $\Omega(f)$ es un $\mathbb{F}_2$-espacio vectorial.

Ahora, afirmamos que $\mathcal{B} = \left\{z^{(i)} = (z_n^i)_{n\geq 0} \text{ con } i = 1, \dots, m-1\right\}$, donde cada z^i es la sucesión obtenida por el $LFSR$ de polinomio característico f con valor inicial $(0, \dots, 0, \overset{i)}{1}, 0, \dots, 0)$ es una base de $\Omega(f)$.

$\mathcal{B}$ es un sistema de generadores. Dado $w = (w_0, \dots, w_{m-1}, \dots) \in \Omega(f)$, sean $w_{i_1}, \dots, w_{i_l}$, con $i_1 < \dots < i_l$ los únicos no nulos de entre $w_0, \dots, w_{m-1}$. En ese caso es evidente que $w = z^{(i_1)} + \dots + z^{(i_l)}$ y ya tenemos expresado w en los elementos de $\mathcal{B}$.

Es evidente ver que los elementos de $\mathcal{B}$ son linealmente independientes. □

NOTACIÓN

Sea $(A, +, \cdot)$ anillo. Entonces denotaremos con $A[[X]]$ al anillo de series formales, series de la forma $\{a_0 + a_1 x + \dots + a_n x^n + \dots\}$ con $a_i \in A\ \forall i$.
La suma de dos series formales se realiza término a término, mientras que el producto se define de la siguiente forma,

$$a \cdot b = \sum_k (a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0) x^k.$$

Tenemos entonces que si K es cuerpo, $K[X] \subset K[[X]]$, pero además existe un anillo intermedio en esta inclusión. Éste es el formado por el conjunto

$$\left\{ \frac{p(x)}{q(x)} \ ; \ q(0) \neq 0 \right\}$$

que contiene algunos elementos del cuerpo de fracciones del anillo $K[X]$.

Ejemplo:
Vamos a intentar expresar el elemento $\frac{1}{1-x}$ del conjunto descrito anteriormente (tomando $K = \mathbb{Q}$) como una serie formal. Para ello es suficiente con darse cuenta de que es cierta la siguiente igualdad,

$$(1 + x + x^2 + x^3 + \dots)(1 - x) = 1$$

En ese caso tenemos que $\frac{1}{1-x} \simeq 1 + x + x^2 + x^3 + \dots$

Proposición 5.2.2 Sea K cuerpo y $p(x) \in K[X]$ siendo $p(x) = p_m x^m + \cdots + p_1 x + p_0$ con $p_0 \in K - \{0\}$. Entonces el inverso de $p(x)$ es un elemento de $K[[X]]$.

Demostración:
Vamos a construir el inverso de $p(x)$. Buscamos $q_0, q_1, q_2, \cdots \in K$ de forma que

$$(q_0 + q_1 x + q_2 x^2 + \dots)(p_0 + p_1 x + \cdots + p_m x^m) = 1.$$

Para ello vamos a encontrar recursivamente los $q_i's$.
$\boxed{q_0} \longrightarrow q_0 \cdot p_0 = 1 \Rightarrow q_0 = \frac{1}{p_0} \in K$.
$\boxed{q_1} \longrightarrow q_0 p_1 + q_1 p_0 = 0 \;\Rightarrow\; q_1 p_0 = -q_0 p_1 \;\Rightarrow\; q_1 = \frac{-q_0 p_1}{p_0} \in K$.
$\boxed{q_i} \longrightarrow q_0 p + q_1 p_{i-1} + \cdots + q_i p_0 = 0$. Si $j > m$, por convenio $p_j = 0$. Entonces,

$$q_i = \frac{-q_0 p_i - q_1 p_{i-1} - \cdots - q_{i-1} p_1}{p_0} \in K. \; \square$$

Proposición 5.2.3 Dada una sucesión $\{s_0, s_1, \dots\}$, entonces

$$\exists p \;:\; s_i = s_{i+p} \Longleftrightarrow \sum_{i \geq 0} s_i x^i = \frac{s^{(p)}(x)}{1 - x^p}$$

siendo $s^{(p)}(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{p-1} x^{p-1}$.

Demostración:

$\boxed{\text{“}\Leftarrow\text{”}}$ Por hipótesis tenemos que $(s_0 + s_1 x + s_2 x^2 + \cdots + s_p x^p + \dots)(1 - x^p) = s_0 + s_1 x + \cdots + s_{p-1} x^{p-1}$.
Atendiendo a los coeficientes de x^p tenemos $s_p - s_0 = 0 \;\Rightarrow\; s_p = s_0$.
En general, atendiendo a los coeficientes de x^{p+j} tenemos que $s_{p+j} - s_j = 0 \;\Rightarrow\; s_{p+j} = s_j$ como queríamos ver.

$\boxed{\text{“}\Rightarrow\text{”}}$ Supongamos que $(s_i)_{i \geq 0}$ es una sucesión tal que $s_j = s_{j+p}\ \forall j \geq 0$. Entonces veamos que

$$\left(\sum_{i \geq 0} s_i x^i \right) (1 - x^p) = s_0 + s_1 x + \cdots + s_{p-1} x^{p-1}.$$

Para ello hay que comprobar la igualdad coeficiente a coeficiente. Si $0 \leq j \leq p - 1$ tenemos que el coeficiente de x^j en el miembro de la izquierda es s_j y en el miembro de la derecha es también s_j.

Si $j \geq p$ el coeficiente de x^j en el miembro de la derecha es 0, mientras que en el miembro de la izquierda es $s_j - s_{j-p}$ que es cero por hipótesis. $\square$

NOTACIÓN

Sea K cuerpo y $f(x) \in K[X]$. Denotamos con $f^*(x)$ al polinomio recíproco de f. Si $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$, tenemos que

$$f^*(x) = \sum_{l=0}^{m} c_{m-l}x^l = \sum_{k=0}^{m} c_k x^{m-k}$$

Comúnmente se dice que $f^*(x) = x^m f(\frac{1}{x})$.
Por ejemplo, si $f(x) = x^3 - x + 5$ entonces $f^*(x) = 1 - x^2 + 5x^3$.

Proposición 5.2.4 El recíproco del producto es el producto de los recíprocos, es decir,

$$(f \cdot g)^* = f^* \cdot g^*.$$

Demostración:
Sean los polinomios

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad \text{y} \qquad g(x) = \sum_{j=0}^{m} b_j x^j.$$

En ese caso tenemos que,

$$(f \cdot g)^* = \left(\left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{j=0}^{m} b_j x^j \right) \right)^* = \left(\sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} \right)^*$$

y reordenando sumandos,

$$(f \cdot g)^* = \left(\sum_{k=0}^{n+m} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) x^k \right)^* = \sum_{k=0}^{n+m} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) x^{m+n-k}.$$

Por otra parte,

$$f^* \cdot g^* = \left(\sum_{i=0}^{n} a_i x^{n-i} \right) \left(\sum_{j=0}^{m} b_j x^{m-j} \right) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{m+n-i-j} = \sum_{k=0}^{n+m} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) x^{m+n-k}.$$

Con lo cual las dos expresiones son iguales. □

Proposición 5.2.5 Sea $f \in \mathbb{F}_2[X]$ un polinomio primitivo. Entonces su recípropo f^* también es primitivo.

Demostración: (Por Eva y Maribel)
Sea $f \in \mathbb{F}_2[X]$ un polinomio primitivo de grado n. Sabemos que f es irreducible en $\mathbb{F}_2[X]$ y que $\mathbb{F} = \frac{\mathbb{F}_2[X]}{<f>}$ es un cuerpo de 2^n elementos. Además, la clase $\bar{x} = (x + kf)$ es un generador de $\mathbb{F}^*$

Para ver que f^* es primitivo hay que ver que

⋆ f^* es irreducible en $\mathbb{F}_2[X]$.

$\star$ El cuerpo $\mathbb{K} = \frac{\mathbb{F}_2[X]}{<f^*>}$ de 2^n elementos tiene a la clase $(x + kf^*)$ como generador de $\mathbb{K}^*$.

Primero veamos que f^* es irreducible.
Si no lo fuera, existirían polinomios g y h ambos con grado mayor o igual que 1 y tales que $f^* = gh$ y por lo tanto, $(f^*)^* = (gh)^*$, es decir, $f = g^*h^*$ siendo g^* y h^* polinomios ambos de grado mayor o igual que 1. Esto último contradice que f sea irreducible y por lo tanto f^* tiene que ser irreducible.

Veamos ahora que $< x + kf^* >= \mathbb{K}^*$.
Sea φ una aplicación que va de $\mathbb{F}^*$ a $\mathbb{K}^*$ tal que $\varphi(g+kf) = g+kf^*$. Entonces φ es un homomorfismo de grupos y además,

$$\mathbb{K}^* = \varphi(\mathbb{F}^*) = \varphi(< x + kf >) =< \varphi(x + kf) >=< x + kf^* > \Rightarrow < x + kf^* >= \mathbb{K}^*$$

y por lo tanto $x + kf^*$ es generador de $\mathbb{K}^*$. $\square$

Proposición 5.2.6 Sea $f(x)$ polinomio de $\mathbb{F}_2[X]$ y sea $(s_i)_{i\geq 0}$ sucesión de $\Omega(f)$. Entonces,

$$\sum_{i\geq 0} s_i x^i = \frac{u(x)}{f^*(x)}$$

donde $u(x) \in \mathbb{F}_2[X]$ es un polinomio de grado menor o igual que $m-1$, siendo m el grado de f.

Demostración:
Sea $z_0, \ldots, z_{m-1}$ el valor inicial de una secuencia de $\Omega(f)$, es decir, $z_{m+i} = \sum_{j=0}^{m-1} c_j z_{i+j}\ \forall i \geq 0$.
Tenemos que ver que

$$\left(\sum_{i\geq 0} z_i x^i\right)\left(\sum_{l=0}^{m} c_{m-l} x^l\right)$$

es un polinomio de grado menor o igual que $m-1$.

Sabemos que el producto anterior se puede expresar como

$$\sum_{j=0}^{\infty}\left[\sum_{l=0}^{min(j,m)} z_{j-l}c_{m-l}\right]x^j = \sum_{j=0}^{m-1}\left(\sum_{l=0}^{j} z_{j-l}c_{m-l}\right)x^j + \underbrace{\sum_{j\geq m}\left(\sum_{l=0}^{m} z_{j-l}c_{m-l}\right)x^j}_{=0}$$

Viendo que el segundo sumando es cero habremos concluido la demostración. Vamos a redefinir los subíndices de la siguiente manera:

$$i = j - m \ \ ; \ \ h = m - l \ \ \Rightarrow \ j - l = i + \cancel{m} - \cancel{m} + h$$

Entonces el segundo sumando queda,

$$\sum_{i=0}^{\infty}\left(\sum_{h=0}^{m} z_{i+h}c_h\right)x^{i+m}$$

Pero para cada i mayor o igual que cero se verifica que,

$$\sum_{h=0}^{m} z_{i+h}c_h = z_{m+i} + c_m z_{m+i} = z_{m+i} + z_{m+i} = 0 \qquad \text{ya que } c_m = 1.$$

Hemos visto que cada coeficiente es nulo y por tanto el segundo sumando también. □

Ejemplo: Sea un $LFSR$ con $m = 5$ y polinomio característico asociado $f = x^5 + x^2 + 1 \in \mathbb{F}_2[X]$. Considérese el estado inicial $(1, 1, 0, 1, 0)$. Se pide calcular un polinomio $u(x)$ de grado menor o igual que 4, tal que, denotando $s(x)$ a la función generatriz de la sucesión obtenida por el $LFSR$ se tenga,

$$s(x) = \frac{u(x)}{f^*(x)}.$$

Utilizando el Teorema anterior sabemos que

$$u(x) = \sum_{j=0}^{m-1} \left(\sum_{l=0}^{j} z_{j-l} c_{m-l} \right) x^j$$

donde $(z_0, \ldots, z_4) = (1, 1, 0, 1, 0)$ y $(c_0, \ldots, c_5) = (1, 0, 1, 0, 0, 1)$. Entonoces,

$$u(x) =$$
$$(z_0c_5)+(z_1c_5+z_0c_4)x+(z_2c_5+z_1c_4+z_0c_3)x^2+(z_3c_5+z_2c_4+z_1c_3+z_0c_2)x^3+(z_4c_5+z_3c_4+z_2c_3+z_1c_2+z_0c_1)x^4$$

es decir,

$$u(x) = x^4 + 2x^3 + x + 1.$$

Teorema 5.2.1 Sea $(z_i)_{i\geq 0}$ una sucesión binaria (no identicamente nula) producida por un $LFSR$ de polinomio característico $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0 \in \mathbb{F}_2[X]$ con f regular ($c_0 \neq 0$). Sea r el orden de multiplicidad de x (mód f), entonces $x^r \equiv 1$ (mód f) y por lo tanto $x \not| f$ y $\bar{x} \in U\left(\frac{\mathbb{F}_2[X]}{<f>}\right)$. Sea además p el período de $(z_i)_{i\geq 0}$. Entonces se verifica:

i) r es múltiplo de p.

ii) Si f es irreducible entonces $r = p$.

iii) $r = 2^m - 1 \iff f$ es primitivo.

Demostración:

(i) Tenemos que p es el menor entero ν tal que $z_i + z_{i+\nu}\ \forall i \geq 0$. Vamos a ver que $z_i = z_{i+r}\ \forall i \geq 0$ y por ser p el menor concluiremos que $p|r$.

Por la Proposición 5.2.3, tenemos que ver que la serie formal asignada a la sucesión $(z_i)_{i\geq 0}$ verifica,

$$\sum_{i\geq 0} z_i x^i = \frac{z_0 + z_1x + \cdots + x_{r-1}x^{r-1}}{1 - x^r}$$

Como $x^r \equiv 1$ (mód f), tenemos que $f|x^r - 1$ en $\mathbb{F}_2[X]$ y por lo tanto, $\exists g(x) \in \mathbb{F}_2[X]$ (de grado $r - m$) tal que $f(x) \cdot g(x) = x^r - 1$.
Tomando recíprocos, $(f \cdot g)^* = f^* \cdot g^* = 1 - x^r$. Ahora, por la Proposición 5.2.6,

$$\sum_{i\geq 0} z_i x^i = \frac{u(x)}{f^*(x)}$$

donde $u(x) \in \mathbb{F}_2[X]$ tiene grado menor o igual que $m-1$.
En ese caso,

$$\sum_{i\geq 0} z_i x^i = \frac{u(x)\cdot g^*(x)}{f^*(x)\cdot g^*(x)} = \frac{v(x)}{1-x^r}$$

y además el grado de $v(x)$ es menor o igual que $m-1+r-m = r-1$.

De esta forma hemos visto que $\forall\ i \geq 0$ se verifica que $z_i = z_{i+r}$ y p es el período de $(z_i)_{i\geq 0}$. Concluyamos que $p|r$.
Podemos dividir r entre p y obtener $r = p\cdot q + \delta$ siendo $\delta < p$. Entonces tenemos que,

$$\forall\ i \geq 0 \quad z_{i+\delta} = z_{i+\delta+p} = z_{i+\delta+pq} = z_{i+r} = z_i$$

y si $\delta \neq 0$ es absurdo que p sea el período de $(z_i)_{i\geq 0}$, con lo cual $\delta = 0$ y por lo tanto la división es exacta y $p|r$.

(II) Veamos que si f es irreducible, $r|p$ (ya sabemos que $p|r$ y tendríamos $p = r$).
Sabemos que

$$\sum_{i\geq 0} z_i x^i = \frac{u(x)}{f^*(x)}$$

con $u(x) \in \mathbb{F}_2[X]$ de grado $\leq m-1$.
También sabemos que

$$\sum_{i\geq 0} z_i x^i = \frac{z_0 + z_1 x + \cdots + z_{p-1}x^{p-1}}{1-x^p} = \frac{v(x)}{1-x^p}.$$

Entonces, $u(x)(1-x^p) = v(x)f^*(x)$ en $\mathbb{F}_2[X]$ y tomando recíprocos, $u^*(x)(x^p-1) = v^*(x)f(x)$.
Pero f es irreducible y $f(x)|u^*(x)(x^p-1)$ entonces $f(x)|u^*(x)$ o $f|x^p-1$. La primera opción es imposible ya que f tiene grado m y u^* tiene grado menor o igual que $m-1$.
En ese caso, $f|x^p-1 \Rightarrow x^p \equiv 1$ (mód f) y como el orden de $\bar{x} = x$ (mód f) es r, tenemos que $r|p$.

(III) Sabemos que $x \not| f$ (f es regular) y como r es el orden de $\bar{x}$ tenemos que $r = 2^m - 1 \iff f$ es primitivo, por la Definición 4.3.2. □

5.3 Buenas propiedades que puede verificar un LFSR

A continuación exponemos algunas propiedades interesantes de una secuencia cifrante que se pueden conseguir de un $LFSR$.

Que se produzca fácilmente.	✓
Que tenga período grande.	✓
Que en un período se comporte de una forma aleatoria[1].	✓
Que sea fuerte ante un ataque con texto original parcialmente conocido.	×

Concretamente éste último punto es el fallo de las secuencias cifrantes producidas por un $LFSR$. Si tenemos un polinomio primitivo $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + \underbrace{c_0}_{\neq 0}$, a pesar de que el período

[1] Según los postulados de pseudoaleatoriedad de Golombek.

conseguido es $2^m - 1$, conociendo $2m$ términos consecutivos se puede conocer la secuencia entera.

Supongamos que de la secuencia $z_0, z_1, \ldots, \underbrace{z_k, \ldots, z_{k+2m-1}}_{conocidos}$ conocemos $2m$ términos consecutivos. Utilizando que

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j}$$

podríamos construir y resolver el siguiente sistema en el que la incógnita es el vector c de constantes,

$$\underbrace{\begin{pmatrix} z_k & \cdots & z_{k+m-1} \\ z_{k+1} & \cdots & z_{k+m} \\ \vdots & \ddots & \vdots \\ z_{k+m-1} & \cdots & z_{k+2m-2} \end{pmatrix}}_{A} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} = \begin{pmatrix} z_{k+m} \\ z_{k+m+1} \\ \vdots \\ z_{k+2m-1} \end{pmatrix}$$

que tiene solución única pues, como veremos a continuación, por ser $f(x)$ primitivo el determinante de la matriz A es no nulo.

Proposición 5.3.1 Si el polinomio $f(x)$ es primitivo, el determinante de A es no nulo.

Demostración: Supongamos que $\det(A) = 0$. Entonces existe una fila i-ésima que depende linealmente de las anteriores (pues ninguna fila es identicamente nula). Tenemos entonces que,

$$(z_{k+i}, \ldots, z_{k+i+m-1}) = \sum_{j=0}^{i-1} \lambda_j (z_{k+j}, \ldots, z_{k+j+m-1}) \quad \text{con } \lambda_j \in \mathbb{F}_2$$

o lo que es lo mismo,

$$z_{k+i+h} = \sum_{j=0}^{i-1} \lambda_j z_{k+j+h} \quad \text{con } h \in \{0, \ldots, m-1\}$$

Veamos que el resto de filas, y en general los sucesivos estados, dependen linealmente de los estados $k, \ldots, k+i-1$. Sabemos que,

$$z_{k+i+m} = \sum_{h=0}^{m-1} c_h z_{k+i+h} = \sum_{h=0}^{m-1} c_h \left[\sum_{j=0}^{i-1} \lambda_j z_{k+j+h} \right] = \sum_{j=0}^{i-1} \lambda_j \left[\sum_{h=0}^{m-1} c_h z_{k+j+h} \right] = \sum_{j=0}^{i-1} \lambda_j z_{k+j+m}$$

entonces tenemos que

$$(z_{k+i+1}, \ldots, z_{k+i+m}) = \sum_{j=0}^{i-1} \lambda_j (z_{k+j+1}, \ldots, z_{k+j+m})$$

Es decir, la fila $i+1$-ésima es combinación lineal de los estados $k, \ldots, k+i-1$.
Aplicando inducción tenemos que todos los estados a partir del i-ésimo son combinación lineal de los i primeros estados. Entonces, ¿cuántos estados distintos puede haber? Como mucho podría haber tantos como combinaciones lineales de los i primeros estados y esto es 2^i.

Ahora, como $i \leq m-1$ el número de estados es menor o igual que 2^{m-1}, pero si $f(x)$ es primitivo se deberían recorrer los $2^m - 1$ estados distintos y como $2^{m-1} < 2^m - 1$ deducimos que $f(x)$ no es

primitivo.

En conclusión, si $f(x)$ es primitivo, el determinante de la matriz A es distinto de cero. □

Para subsanar este inconveniente se combinan varios $LFSR$ de polinomios primitivos.

Ejemplo: (Generador de Geffe)
Consideramos tres $LFSR$, es decir, $LFSR_1$, $LFSR_2$ y $LFSR_3$ cada uno con un polinomio primitivo distinto $f_1(x)$, $f_2(x)$ y $f_3(x)$ y se crean tres sucesiones binarias distintas, $(z_i^1)_{i\geq 0}$, $(z_i^2)_{i\geq 0}$ y $(z_i^3)_{i\geq 0}$.

Se define la sucesión $(w_i)_{i\geq 0}$ término a término de la siguiente manera $w_i = z_i^1 z_i^2 + z_i^1 z_i^3 + z_i^2$.
Es decir, si $z_i^1 = 0 \Rightarrow w_i = z_i^2$ y si $z_i^1 = 1 \Rightarrow w_i = z_i^3$.

Observación 5.3.1 Si las secuencias $(z_i^1)_{i\geq 0}$, $(z_i^2)_{i\geq 0}$ y $(z_i^3)_{i\geq 0}$ tienen período p_1, p_2 y p_3 respectivamente, es fácil ver que, en general, la secuencia $(w_i)_{i\geq}$ tiene período $mcm(p_1, p_2, p_3)$.

Observación 5.3.2 Sea $(z_i)_{i\geq 0}$ una sucesión binaria de período p. Entonces se puede considerar como obtenida por un $LFSR$ de polinomio característico $x^p + 1$

Definición 5.3.1 Se llama complejidad lineal de una secuencia $(z_i)_{i\geq 0}$ al menor m natural tal que existe un polinomio $f \in \mathbb{F}_2[X]$ de grado m de forma que $(z_i)_{i\geq 0} \in \Omega(f)$.

6 Complejidad de algoritmos en aritmética de enteros y cuerpos finitos

En este capítulo, dado un algoritmo pretenderemos acotar el número de operaciones que requiere hasta llegar al resultado final. La cota dependerá de los datos con los que se inicie el algoritmo y de la eficiencia de éste.

6.1 Complejidad de un algoritmo en álgebra y complejidad binaria

Definición 6.1.1 La complejidad de un algoritmo en álgebra es el número de pasos del algoritmo desde que recibe una entrada hasta que produce una salida, en términos de ciertos parámetros de la(s) entrada(s) llamados parámetros de la complejidad.

Si el algoritmo trata sobre números enteros (la entrada y salida son uno o varios enteros), entonces el parámetro de la complejidad es el número de bits de la entrada.

Definición 6.1.2 Un paso es una única operación en bits si hablamos de complejidad binaria.
Si se trata de álgebra sobre polinomios con coeficientes en un cuerpo o anillo, se puede considerar la complejidad aritmética.
En este último caso los parámetros son el número de polinomios, los grados de éstos, el número de variables...
Un paso es una operación aritmética de "+" o "·" en el cuerpo o anillo.

Estudiaremos la complejidad binaria de los algoritmos sobre los enteros, pero nos interesará una "medida asintótica" es decir, una cota superior cuando los términos de las entradas sean grandes.

NOTACIÓN

Sean $f, g : \mathbb{N}^r \longrightarrow \mathbb{R}^+$. Decimos que f es una O grande de g y escribimos $f = O(g)$ si y sólo si $\exists \nu \in \mathbb{N}$ y $\exists C \in \mathbb{R}^+$ tales que

$$f(n_1, \ldots, n_r) \leq Cg(n_1, \ldots, n_r) \text{ siempre que } n_i \geq \nu \ \ \forall i = 1, \ldots, r.$$

6.2 Complejidad de los algoritmos con enteros de la escuela

Empecemos por el cálculo de la complejidad binaria del algoritmo de la escuela para la suma de dos números, un k-bit más un l-bit, suponiendo $k \geq l$. Por definición un n-bit es un número cuya representación binaria ocupa n bits o menos.

¿Cuántas operaciones en bits hay que hacer para sumar ambos números?
Es fácil ver que no más de $2k$. En ese caso la complejidad binaria de la suma de dos enteros, uno k-bit y el otro l-bit ($k \geq l$) es $O(k)$ (se pierden las constantes).

En las mismas condiciones, el algoritmo de la escuela para la resta tiene una complejidad $O(l)$.

Para la multiplicación de un k-bit por un l-bit ($k \geq l$) con el algoritmo de la escuela es fácil ver que como mucho habrá que hacer $l-1$ sumas, la i-ésima de complejidad binaria $O(k+i+1)$. En total, el número de operaciones es menor o igual que

$$C(k+1+k+2+\cdots+k+l-1)(l-1) = C\frac{k+1+k+l-1}{2}(l-1) = \frac{2k+l}{2}(l-1)$$

que es menor o igual que $(k+\frac{l}{2})l \leq 2kl$. En definitiva, el algoritmo de la escuela para la multiplicación tiene complejidad binaria $O(kl)$.

A la hora de dividir un k-bit entre un l-bit ($k \geq l$) hay que hacer no más de $k-l$ restas de k-bit's. Es decir, la complejidad binaria de la división es $O((k-l)k)$.

6.3 Complejidad del algoritmo de Euclides y el algoritmo de Euclides extendido

Recordemos el algoritmo de Euclides. Dados $n, m \in \mathbb{Z}^+$ con $n \geq m$. Definimos $r_0 = n$ y $r_1 = m$. Además,

$$r_{i-1} = q_i r_i + r_{i+1} \quad \text{con} \quad 0 \leq r_{i+1} < r_i.$$

Existe $\nu \in \mathbb{N}$ tal que $r_{\nu+1} = 0$ y en ese caso $r_\nu = mcd(n, m)$.

Sea $k_i = \#_2 r_i$ (número de bits de r_i). Nótese que $k_{i+1} \leq k_i \ \forall i$.
Sea $C \in \mathbb{R}^+$ tal que la complejidad binaria de dividir un k-bit entre un l-bit ($k \geq l$) es menor o igual que $C(k-l)k$ para k suficientemente grande.

Entonces la complejidad binaria del algoritmo de Euclides es menor o igual que la suma de la complejidad de cada división.
La división i-ésima "cuesta" $C(k_{i-1}-k_i)k_{i-1}$ operaciones. Entonces la complejidad total es menor o igual que la suma,

$$\sum_i C(k_{i-1}-k_i)k_{i-1} = C((k_0-k_1)k_0 + (k_1-k_2)k_1 + \cdots + (k_\nu - \underbrace{k_{\nu+1}}_{=0})k_\nu)$$

cantidad que es menor o igual que

$$C(k_0^2 - k_1^2 + k_1^2 - k_2^2 + k_2^2 - \cdots - k_\nu^2 + k_\nu^2) = Ck_0^2.$$

En resumen, la complejidad binaria del algoritmo de Euclides es $O(k^2)$ donde $k = \#_2 n$.

Observación 6.3.1 Dado $n \in \mathbb{N}$, si $k = \#_2 n$ entonces $2^{k-1} \leq n < 2^k$ y por lo tanto $k-1 \leq \log_2 n < k$. Es decir, $[\log_2 n] = k-1 \ \Rightarrow \ k = [\log_2 n] + 1$.

Entonces, la complejidad de sumar, restar, multiplicar y dividir con enteros menores o iguales que n es respectivamente $O(\log_2 n)$, $O(\log_2 n)$, $O(\log_2^2 n)$, $O(\log_2^2 n)$.
Y la complejidad binaria del EA (Algoritmo de Euclides) es $O(\log_2^2 n)$.

Recordemos ahora el algoritmo de Euclides extendido. Dados $n, m \in \mathbb{Z}^+$ con $n \geq m$. Una vez hecho el algoritmo de Euclides, definimos $x_0 = 0$, $y_0 = 1$, $x_1 = 1$, $y_1 = 0$ y además,

$$x_{k+1} = q_k x_k + x_{k-1} \quad \text{y} \quad y_{k+1} = q_k y_k + y_{k-1}$$

de esta forma se verifica* que

$$(-1)^k x_k r_0 + (-1)^{k+1} y_k r_1 = r_k$$

y por lo tanto, para $k = \nu$ tenemos una identidad de Bézout.

Demostración*:
Veámoslo por inducción.
Para $k = 0$, tenemos que $r_0 + 0 = r_0$ ✓.
Para $k = 1$, tenemos $0 + r_1 = r_1$ ✓.

Supongamos que es cierto hasta $i - 1$ y veámos que también lo es para i.

$$(-1)^i x_i r_0 + (-1)^{i+1} y_i r_1 = (-1)^i r_0 (q_{i-1} x_{i-1} + x_{i-1}) + (-1)^{i+1} r_1 (q_{i-1} y_{i-1} + y_{i-2})$$

y sacando factor común q_{i-1}

$$q_{i-1} \underbrace{\left((-1)^i r_0 x_{i-1} + (-1)^{i+1} r_1 y_{i-1}\right)}_{-r_{i-1}} + \underbrace{(-1)^i r_0 x_{i-2} + (-1)^{i+1} r_1 y_{i-2}}_{+r_{i-2}} = r_i \ \checkmark \ \square$$

Observación 6.3.2 Se verifica que $q_\nu \neq 0$ porque $r_{\nu+1}$ es el primero que es 0. Además $q_\nu \neq 1$ porque $r_{\nu-1} \neq r_\nu$.
Tenemos que

$$a = q_1 r_1 + r_2 \geq q_1 r_1 = q_1 (q_2 r_2 + r_3) \geq q_1 q_2 r_2 \geq \cdots \geq q_1 \cdots q_\nu$$

y tomando logaritmos

$$\sum_{i=1}^{\nu} \log_2 q_i \leq \log_2 a \ \Rightarrow \ r_1 = b \geq \prod_{j=1}^{\nu} q_j$$

y entonces también se tiene que

$$\sum_{j=2}^{\nu} \log_2 q_j \leq \log_2 b.$$

Observación 6.3.3 Para cada i se tiene que $r_{i+2} \leq \frac{r_i}{2}$.
Supongamos que $2r_{i+2} > r_i$. Pero $r_{i+2} < r_{i+1} < r_i$ y como $r_{i+1} > r_{i+2} > \frac{r_i}{2}$, dividiendo r_i entre r_{i+1} cabe a 1 y entonces

$$r_i = r_{i+1} + r_{i+2} > \frac{r_i}{2} + \frac{r_i}{2} = r_i$$

lo que es absurdo.
Entonces $\nu \simeq 2[\log_2 b] + 1$.

Tratemos de escribir el algoritmo de Euclides extendido en forma matricial,

$$\underbrace{\begin{pmatrix} x_{k+1} & x_k \\ y_{k+1} & y_k \end{pmatrix}}_{T_{k+1}} = \underbrace{\begin{pmatrix} x_k & x_{k-1} \\ y_k & y_{k-1} \end{pmatrix}}_{T_k} \underbrace{\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}}_{E_k}$$

Entonces podemos decir que $T_{k+1} = T_k E_k \ \ \forall k = 1, \ldots, \nu$. Además,

$$T_{k+1} = T_{k-1}E_{k-1}E_k = \cdots = T_1 E_1 \cdots E_k = E_1 \cdots E_k$$

Ahora definimos $S_k = E_{k+1} \cdots E_\nu$ si $k < \nu$ y $S_\nu = Id$ y escribimos,

$$S_k = \begin{pmatrix} u_k & v_k \\ u_{k+1} & v_{k+1} \end{pmatrix} \quad 0 \leq k \leq \nu$$

Por último es fácil ver que $S_{k-1} = E_k S_k$ y entonces

$$\begin{pmatrix} u_{k-1} & v_{k-1} \\ u_k & v_k \end{pmatrix} = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_k & v_k \\ u_{k+1} & v_{k+1} \end{pmatrix}.$$

Lema 6.3.1 Se verifica que

(I) $0 \leq v_k \leq \dfrac{r_k}{2mcd(a,b)} \quad 1 \leq k \leq \nu$

(II) $x_k \leq \dfrac{b}{2mcd(a,b)}$ y $y_k \leq \dfrac{a}{2mcd(a,b)} \quad 1 \leq k \leq \nu$

Demostración:

(I) Razonaremos por inducción decreciente,
Tenemos que $S_\nu = Id$ y entonces $v_\nu = 0$. Además,

$$0 = v_\nu \leq \frac{r_\nu}{2mcd(a,b)} = \frac{r_\nu}{2r_\nu} = \frac{1}{2}$$

Para $\nu - 1$ tenemos que $S_{\nu-1} = E_\nu S_\nu = E_\nu \ \Rightarrow \ v_{\nu-1} = 1$. Por otro lado,

$$\frac{r_{\nu-1}}{2mcd(a,b)} = \frac{r_{\nu-1}}{2r_\nu} \ \checkmark$$

Sabemos que $r_{\nu-1} = q_\nu r_\nu + r_{\nu+1}$ y por la Observación 6.3.2 $q_\nu \neq 0, 1$, es decir, $q_\nu \geq 2$ y entonces $q_\nu r_\nu = r_{\nu-1} \geq 2r_\nu$ y con lo cual

$$0 \leq 1 = v_{\nu-1} \leq \frac{r_{\nu-1}}{2r_\nu} \ \checkmark$$

Supongamos que es cierto desde ν hasta k y veamos que también lo es para $k-1$.

$$0 \leq v_{k-1} = q_\nu v_k + v_{k+1} \leq q_k \frac{r_k}{2mcd(a,b)} + \frac{r_{k+1}}{2mcd(a,b)} = \frac{r_{k-1}}{2mcd(a,b)} \ \checkmark$$

(II) Observemos que las sucesiones de $\{x_k\}$ y $\{y_k\}$ son crecienes, $x_{k+1} = q_k x_k + x_{k-1} \geq x_k$ y lo mismo para y_k. Entonce basta ver que x_ν y que y_ν son menores que las cotas que propone el enunciado.
Tenemos que

$$S_0 = E_1 \cdots E_\nu = T_{\nu+1} \ \Rightarrow \ \begin{pmatrix} u_0 & v_1 \\ u_1 & v_0 \end{pmatrix} = \begin{pmatrix} x_{\nu+1} & x_\nu \\ y_{\nu+1} & y_\nu \end{pmatrix}$$

Y por lo tanto $x_\nu = v_1$ mientras que $y_\nu = v_0$. Ahora, aplicando el primer apartado de este lema tenemos el resultado, ya que $a = r_0$ y $b = r_1$. $\square$

Este lema demuestra que el Algoritmo de Euclides Extendido proporciona los "mejores" coeficientes de la identidad de Bézout.

¿Cuál es el coste de calcular los coeficientes de Bézout?
Sea $\omega(x) = \#_2 x$ el número de bits de x. Por el Lema 6.3 tenemos que

$$\omega(x_k) \leq \omega(a) \qquad \text{y que} \qquad \omega(y_k) \leq \omega(a)$$

Sea $C \in \mathbb{R}^+$ la constante que aparece en la medida asintótica de los algoritmos de la escuela de suma y producto. La complejidad binaria de calcular x_{k+1} es menor o igual que

$$C\omega(q_k)\omega(x_k) + \omega(q_k) + \omega(x_k) \leq C'\omega(q_k)\omega(x_k) \leq C'\omega(q_k)\omega(a)$$

El coste de calcular todos los x_k es menor o igual que

$$C'\omega(a)\sum_{k=1}^{\nu}\omega(x_k)$$

Y podemos razonar de forma totalmente análoga para los y_k.
Como $\omega(x) = \log_2 x + 1$, pordemos decir que la complejidad de calcular los x_k y los q_k es menor o igual que

$$C'\left(\log_2 a + 1\right)\left(\sum_{k=1}^{\nu}(\log_2 q_k + 1)\right) \leq C'\left(\log_2 a + 1\right)\left(n + \sum_{k=1}^{\nu}\log_2 q_k\right)$$

Y ya hemos visto que $\sum_{k=1}^{\nu}\log_2 q_k \leq \log_2 a$ y que $\nu \simeq 2[\log_2 b] + 1$, entonces la complejidad del EEA es el coste de calcular los q_k, los x_k y los y_k.

Decimos que la complejidad del Algoritmo de Euclides Extendido es una $O(\log_2 a \cdot \log_2 b)$. Y suponiendo $a \geq b$ podemos decir que es una $O(\log_2^2 a)$.

Corolario 6.3.1 La complejidad de la aritmética modular: $+$, $\times$, ¿$\div$? (test de inverso) en el anillo $\frac{Z}{<n>}$ es $O(\log_2^2 n)$.

6.4 Complejidad de la aritmética de cuerpos finitos

Sea $\mathbb{F}$ cuerpo finito. Entonces, $\mathbb{F} = \frac{\mathbb{F}_p[X]}{<f>}$ siendo $f(x) \in \mathbb{F}_p[X]$ irreducible y de grado n. Además, $\mathbb{F}$ es un $\mathbb{F}_p$-espacio vectorial de base $\{[1]_f, [x]_f, \ldots, [x^{n-1}]_f\}$.

Un elemento de $\mathbb{F}$ puede ser visto como una n-upla $(a_0, \ldots, a_{n-1})$ con $a_i \in \mathbb{F}_p$. Cuando trabajemos con un cuerpo finito, uno de los parámetros de la complejidad será el máximo número de bits de los a_i con $i = 1, \ldots, n$, es decir

$$\max_{i=0,\ldots,n} \#_2 a_i \leq \#_2 p$$

Proposición 6.4.1 Si $\mathbb{K}$ es cuerpo, multiplicar dos polinomios de grado menor o igual que n en $\mathbb{K}[X]$, con el algoritmo de la escuela, requiere un número de operaciones de suma y producto en $\mathbb{K}$ que es $O(n^2)$.

Demostración:
Para multiplicar dos polinomios (uno de grado n y el otro de grado m) tenemos que hacer $n \cdot m$ multiplicaciones y $n \cdot m$ sumas, en total $2nm$ operaciones en $\mathbb{K}$ que es del orden de $O(n^2)$.

Proposición 6.4.2 Dividir (con resto) dos polinomios de $\mathbb{K}[X]$ con grados menores o iguales que n requiere un número de operaciones aritméticas en $\mathbb{K}$ que es $O(n^2)$.

Demostración:
Al hacer una división de polinomios (uno de grado n y otro de grado m) tenemos que hacer, en cada paso, 1 división en $\mathbb{K}$, m multiplicaciones y n restas. En total hay que dar $n - m + 1$ pasos, con lo cual tenemos que hacer $(n - m + 1)(n + m + 1)$ operaciones en $\mathbb{K}$ que es del orden de $O(n^2)$.

Calculemos la complejidad de las operaciones aritméticas en $\mathbb{F}$.

1. Sumar n-uplas de enteros módulo p tiene complejidad binaria $O(n \log_2 p)$
2. Multiplicar dos n-uplas y reducir módulo f.
   Acotemos el número de operaciones en necesario. Utilizando las dos proposiciones anteriores, $\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right)$ cuesta $O(n^2)$ operaciones en $\mathbb{F}_p$ y la división para encontrar el resto cuesta $O((2n)^2)$.

   En total, tenemos una $O(n^2)$ y por lo tanto, la complejidad binaria es $O(n^2 \log_2^2 p) = O(\log_2^2 p^n) = O((\#\mathbb{F})^2)$.

La consecuencia es que si $\mathbb{F}$ es un cuerpo finito de q elementos, las operaciones aritméticas de $\mathbb{F}$ con los algoritmos de la escuela, tienen complejidad binaria

$$O(\log_2^2 q).$$

Definición 6.4.1 Sea $\mathbb{K}$ cuerpo. Un elemento $x \in \mathbb{K}$ es raíz n-ésima si $x^n = 1$. Si además, n es el menor entero tal que $x^n = 1$ entonces x es raíz primitiva.

Lema 6.4.1 Una condición necesaria y suficiente para que $\mathbb{F}_q$ tenga alguna raíz primitiva n-ésima es que $n|q - 1$.

Lema 6.4.2 Una condición necesaria y suficiente para que $\mathbb{F}_q$ tenga alguna raíz n-ésima distinta de la unidad es que $mcd(n, q - 1) \neq 1$.

Es fácil ver que si $\mathbb{F}_q$ tiene alguna raíz primitiva, ξ, n-ésima, entonces tiene todas. Basta considerar el subgrupo $< \xi >$ y observar que ξ^k con $mcd(k, n) = 1$ también es raíz primitiva n-ésima.

7 Teoría de la complejidad

Jerarquiza la dificultad de los problemas en relación a los algoritmos que los resuelven. Distinguimos dos clases:

- Problemas de decisión.
  Como por ejemplo, dado un $n \in \mathbb{N}$ decidir si es primo o compuesto, si es potencia pura, si es libre de cuadrados, problemas de combinatoria... Dentro de esta clase, según la dificultad de un problema distinguimos:

  a) La clase P, en la que están los problemas para los que se conoce un algoritmo de complejidad polinomial que los resuelve.

  b) La clase NP, en la que están los problemas para los que hay un algoritmo que los resuelve, pero no con complejidad polinomioal y sin embargo, dada una posible solución del problema, verificar que lo es sí se consigue en un tiempo polinomial.

- Problemas de búsqueda.
  Por ejemplo, dado $n \in \mathbb{N}$ que se sabe compuesto, encontrar un factor. O el famoso problema de la mochila.

Algunos problemas de búsqueda se pueden traducir en un problema de decisión.
Por ejemplo, consideremos el problema en el que dado un $n \in \mathbb{N}$ tenemos que encontrar un factor propio. Podemos traducirlo en un problema de decisión que sería el siguiente: dados a, b y n con $a, b < n$ decidir si existe un factor propio de n en $[a, b]$.
Pasaríamos del primer problema al segundo con complejidad binaria $O(\log_2 n)$, es decir, para resolver el primero haría falta hacer del orden de $\log_2 n$ llamadas al segundo.

Hay algunos problemas de la clase NP que en Álgebra han dado lugar a sistemas criptográficos de interés:

1. El problema de factorización de enteros ha dado lugar al RSA (River-Shamir-Adlemann, 1980).

2. El problema del logaritmo discreto[1] ha dado lugar al DHM (Diffie-Hellman-Merkle, 1976).

7.1 Algunos conceptos básicos

Definición 7.1.1 Decimos que una función f es de una dirección si, dado x, existe un algoritmo polinomial para calcular $f(x)$, pero no se conoce ningún algoritmo polinomial para, dado $y \in Im(f)$, calcular x tal que $f(x) = y$.

Definición 7.1.2 Una función, f, de una dirección con trampa es una función de una dirección que es biyectiva de forma que, dada una información adicional llamada trampa, sí se puede calcular $f^{-1}(y)$ con $y \in Im(f)$. También llamadas como "funciones hash". La información adicional es conocida como "trap-door" o clave privada.

[1] Dado un grupo cíclico finito $G =< g >$, siendo $\text{ord}(g) = n$ y dado $x \in G$ el problema del logaritmo discreto consiste en encontrar un $\alpha < n$ tal que $x = g^{\alpha}$.

En un sistema de clave pública, cada usuario u tiene asociadas dos claves, una clave pública k_u que permite cifrar mensajes hacia u y una clave privada k'_u que permite a u descifrar los mensajes enviados.

Un sistema de clave pública resuelve además de la privacidad:

- ⋆ Autentificación.
- ⋆ Integridad.
- ⋆ No repudiación (Firma digital).

7.2 Protocolo de intercambio de claves DHM

Definición 7.2.1 Un protocolo es un conjunto de pasos ordenados que los usuarios de un sistema criptográfico tienen que seguir para realizar una tarea.

En 1976, Diffie-Hellman-Merkle diseñaron un protocolo de intercambio de claves basado en la dificultad de resolver el problema del logaritmo discreto (DLP) en los grupos $\mathbb{F}_p^*$.

(I) Los usuarios de un sistema, A y B convienen en un número primo p grande y g generador de $\mathbb{F}_p^*$. El usuario A elige de modo secreto un $a \in \{2, \ldots, p-2\}$ y calcula $g^a \pmod p$, que se puede hacer con complejidad binaria $O(\log_2^3 p)$ mediante el algoritmo de exponenciación modular rápida. Simultáneamente B elige b y calcula $g^b \pmod p$.

(II) A envía g^a a B y se guarda a, mientras que B envía g^b a A y se guarda b.

(III) Ahora A puede calcular $(g^b)^a$ y B puede calcular $(g^a)^b$, es decir, ambos conocen $g^{ab} \pmod p$.

Si en el intercambio de información alguien consigue conocer g^a o g^b no importa, pues del conocimiento de estos valores no se sabe calcular $g^{ab} \pmod p$ de modo eficiente.

7.3 Protocolo de privacidad RSA

Es el primer protocolo de privacidad basado en la dificultad de factorizar enteros.

Sea N el cardinal de símbolos del alfabeto. Sean $k, l \in \mathbb{N}$ tales que $k < l$ y por lo tanto $N^k < N^l$.
$\mathcal{P}$ representa el conjunto de unidades de texto original, $\frac{\mathbb{Z}}{<N^k>}$.
$\mathcal{C}$ representa el conjunto de unidades de texto cifrado, $\frac{\mathbb{Z}}{<N^l>}$.

(I) Cada usuario u del sistema elige $p_u,\ q_u$ primos "grandes" tales que $p_u \cdot q_u = n_u$ y $N^k < n_u < N_l$. Además elige $e_u \in \{1, \ldots, \varphi(n_u) - 1\}$ siendo $\varphi(n_u) = (p_u - 1)(q_u - 1)$ de forma que $mcd(e_u, \varphi(n_u)) = 1$.
Ahora calcula usando el Algoritmo de Euclides Extendido el inverso multiplicativo de e_u módulo $\varphi(n_u)$, es decir, d_u tal que

$$e_u d_u \equiv 1 \pmod{\varphi(n_u)}$$

(II) A envía a B un mensaje $P \in \frac{\mathbb{Z}}{<N^k>}$, para ello A se entera de cuál es la clave pública de B recibiendo $(e_B,\ n_B)$ y calcula con el algoritmo de exponenciación modular rápida $C = P^{e_B} \pmod{n_B}$ que representa sin confusión un único entero de $\frac{\mathbb{Z}}{<N^l>}$ porque $n_B < N^l$.

(III) B, que conoce la clave privada $(d_B,\ p_B,\ q_B)$ recibe C y lo eleva a d_B de forma que $C^{d_B} \equiv (P^{e_B})^{d_B}$ (mód n_B) que resulta ser $P^{1+\lambda\varphi(n_B)}$ pero aplicando el Lema 7.3.1 tenemos que en realidad es $P^1 = P$.

Lema 7.3.1 Si $n = pq$ siendo p y q primos, entonces $\forall\ a < n$ y $\forall\ s : s \equiv 1$ (mód $\varphi(n)$) se tiene que

$$a^s \equiv a \text{ (mód } n)$$

Demostración:
Sea $s \equiv 1$ (mód $\varphi(n)$), entonces $s = 1 + \lambda\varphi(n)$.
Si $mcd(a, n) = 1$, sabemos que $a^{\varphi(n)} \equiv 1$ (mód n) y por lo tanto

$$a^s = a^{1+\lambda\varphi(n)} = a \cdot (a^{\varphi(n)})^\lambda \equiv a \text{ (mód } n) \ \checkmark$$

Si $mcd(a, n) \neq 1$ y $a < n$, entonces o bien $mcd(a, n) = p$, o bien $mcd(a, n) = q$.
Supongamos sin pérdida de generalidad que $mcd(a, n) = p$ y que $mcd(a, q) = 1$. En ese caso, por el pequeño teorema de Fermat tenemos que $a^{q-1} \equiv 1$ (mód q).
Escribimos $s = 1 + \lambda\varphi(n) = a + \lambda(p-1)(q-1)$ y

$$a^s = a \cdot a^{\lambda(p-1)(q-1)} \stackrel{?}{\equiv} a \text{ (mód } n)$$

O lo que es lo mismo,

$$a\left(a^{\lambda(p-1)(q-1)} - 1\right) \stackrel{?}{\equiv} 0 \text{ (mód } n) \iff pq \stackrel{?}{\mid} a\left(a^{\lambda(p-1)(q-1)} - 1\right)$$

Pero $p|a$ y además,

$$a^{q-1} \equiv 1 \text{ (mód } q) \Rightarrow a^{\lambda(q-1)} \equiv 1 \text{ (mód } q) \Rightarrow a^{\lambda(q-1)(p-1)} \equiv 1 \text{ (mód } q) \Rightarrow q|\left(a^{\lambda(p-1)(q-1)} - 1\right). \ \square$$

Observación 7.3.1 Si se consigue factorizar n, se encuentran p y q y entonces $\varphi(n) = (p-1)(q-1)$ por lo que se puede calcular $d \equiv e^{-1}$ (mód $\varphi(n)$).
Por otro lado, si se conocen $\varphi(n)$ y n se pueden encontrar p y q con complejidad $O(\log_2^3 n)$. Véase la Observación 2.4.1.

Observación 7.3.2 Supongamos que un criptoanalista que intercepta mensajes cifrados dirigidos a u intenta encontrar $d' \in \mathbb{N}$ con $d' < n_u$ tal que $C^{d'}$ (mód n_u) sea igual a P, para muchos P's diferentes.
Para los P's tales que $mcd(P, n_u) = 1$ tendríamos que $P^{e_u d'-1} \equiv 1$ (mód n_u). Entonces el criptoanalista habría encontrado un entero d' tal que $e_u d' - 1$ es múltiplo del orden de todo elemento de $U\left(\frac{\mathbb{Z}}{<n_u>}\right)$, grupo isomorfo a $U(\frac{\mathbb{Z}}{<p_u>}) \times U(\frac{\mathbb{Z}}{<q_u>})$, por lo que sería suficiente encontrar un d' tal que $e_u d' - 1$ sea múltiplo de $mcd(p_u - 1, q_u - 1)$.

Por eso es importante elegir primos p y q tales que $mcd(p-1, q-1)$ sea pequeño, a ser posible 2. Para que $mcm(p-1, q-1)$ se aproxime a $(p-1)(q-1)$.

Algunos criterios de seguridad en el RSA son:

- ⋆ Elección adecuada de p y q.
  - *a*) De forma que $mcm(p-1, q-1) \approx (p-1)(q-1)$.

b) Evitar p cercano a q, pues el Algoritmo de Fermat permite factorizar n si $n = pq$ con p y q cercanos a $\sqrt{n}$.

c) Evitar el método de Pollard[2].

d) Evitar primos de Mersenne[3].

$\star$ Elección de e_u.

a) Queremos que P^{e_u} sea mayor que n_B $\forall P$. Para ello es suficiente pedir que $e_B > \log_2 n_B$ ya que en ese caso $P^{e_B} \geq 2^{e_B} > n_B$.

b) Por último es necesario que d no sea pequeño.

7.4 Protocolo ElGamal

El usuario A quiere enviarle un mensaje a B, para ello convienen en un número primo p y un generador g de $\mathbb{F}_p^*$. La clave privada de B es $b \in \{0, 1, \ldots, p-2\}$ y la clave pública es $e_B = g^b$.

A elige un $r \in \{0, 1, \ldots, p-2\}$ de forma que $mcd(p-1, r) = 1$ y calcula $R = g^r \pmod p$ y $S = M \cdot e_B^r \pmod p$ donde M es el mensaje. Envía a B el par (R, S).

Ahora B, para descifrar el mensaje, sólo tiene que hacer lo siguiente:
Calcular $S(R^b)^{-1} \equiv Mg^{rb}(g^{rb})^{-1} \pmod p \equiv M \pmod p$.
La seguridad de este sistema se basa en la dificultad de resolver el problema del logaritmo discreto.

7.5 Los números primos

Un test de primalidad o algoritmo de primalidad resuelve el problema de decisión en el que, dado un n impar hay que decidir si es primo o compuesto.

- Existe un único algoritmo determinista, publicado en 2002 por los autores Agrawal-Kayal-Saxena.
- Hay otros algoritmos probabilistas que resuelven este problema:

  a) Solovay-Strassen.

  b) Miller (1979, algoritmo determinista polinomial sujeto a GRH[4].)

  c) Rabin (1980, versión probabilista muy eficiente).

  Si un algoritmo probabilista niega que un número sea primo entonces dicho número es compuesto, pero si afirma su primalidad, ésta sólo es cierta con probabilidad $1 - \varepsilon$.
  Para ello se realizan un número de etapas polinomial en $\log\left(\frac{1}{\varepsilon}\right)$, cada una de ellas polinomial en $\log n$.

Teorema 7.5.1 (Wilson)
Una condición necesaria y suficiente para que n sea primo es que $n \mid (n-1)! + 1$.

[2]Si n es producto de primos tales que $p_i - 1$ tienen sólo factores primos pequeños en su descomposición, entonces es fácil factorizar n.

[3]Un primo de Mersenne es de la forma $2^k - 1$ con $k \in \mathbb{N}$.

[4]La Conjetura de Riemann.

Lema 7.5.1 (Fermat)
Una condición necesaria para que n sea primo es que $\forall\ a < n : mcd(a, n) = 1$ se verifique que $a^{n-1} \equiv 1$ (mód n).

Definición 7.5.1 Sea n impar compuesto tal que $\exists a < n$ con $mcd(a, n) = 1$ de forma que que $a^{n-1} \equiv 1$ (mód n).
Se dice que n es un pseudoprimo de Fermat de base a.

Hay infinitos pseudoprimos de Fermat en todas las bases.

Definición 7.5.2 Sea n impar compuesto y $a < n : mcd(a, n) = 1$. Además $n - 1 = 2^s t$ con $2 \not| t$. Entonces decimos que a no es testigo de que n es compuesto si y sólo si

$$\exists s' : 1 \leq s' < s \quad \text{de forma que} \quad a^{2^{s'} t} \equiv -1 \text{ (mód } n) \text{ o } a^t \equiv 1 \text{ (mód } n).$$

Un ejemplo de un algoritmo de primalidad sería el siguiente:

Input: n, *etapas*
$k = 1$
while $k <$ *etapas* **do**
  $a = random(1, n)$
  if $mcd(a, n) \neq 1$ **then**
    return 'False'
  else
    if $a^{n-1} \not\equiv 1$ (mód n) **then**
      return 'False'
    else
      s es tal que $2^s t = n - 1$ y $2 \not| t$
      while $s > 1$ **do**
        if $a^{2^{s-1} t} \not\equiv -1$ (mód n) **then**
          return 'False'
        end if
        $s = s - 1$
      end while
      if $a^t \not\equiv 1$ (mód n) **then**
        return 'False'
      end if
      $k = k + 1$
    end if
  end if
end while
return 'True'

Teorema 7.5.2 (Miller-Rabin) Dado un n impar y compuesto siendo $n > 9$ se tiene que

$$\frac{\#\{a < n : a \text{ no es testigo de que } n \text{ es compuesto }\}}{\#\{a < n : mcd(a, n) = 1\}} \leq \frac{1}{4}$$

Este Teorema da lugar a que, después de un número k de etapas, si el algoritmo ha devuelto el valor 'True', la probabilidad de que el número sea compuesto es menor o igual que $\frac{1}{4^k}$ y de que sea primo

es mayor o igual que $1 - \frac{1}{4^k}$.
Además, cada etapa requiere un número de operaciones binarias polinomial en $\log n$. Esto hace que el algoritmo en la práctica sea muy eficiente.

Por ejemplo, el único número menor que $2{,}5 \times 10^{10}$ que no tiene por testigo de que n es compuesto ningún $a \in \{2, 3, 5, 7\}$ es $n = 3215031751$.

Antes de demostrar el Teorema de Miller-Rabin vamos a ver unos resultados previos.

Lema 7.5.2 Si p es primo y $p \geq 3$, entonces $U\left(\frac{\mathbb{Z}}{<p^\alpha>}\right)$ con $\alpha \geq 2$ es cíclico.

Demostración:
Primero veamos que para $p = 2$ no es cierto. Por ejemplo, si $\alpha = 3$ tenemos que

$$U\left(\frac{\mathbb{Z}}{<8>}\right) = \{1, 3, 5, 7\}$$

todos elementos de orden 2, salvo el 1.

Ahora, sea g tal que $1 \leq g < p$ y g módulo p genera $U\left(\frac{\mathbb{Z}}{<p>}\right)$. Entonces,

$$g^{p-1} \equiv 1 \text{ (mód } p) \;\Rightarrow\; g^{p-1} = 1 + g_1 p \;\text{ con } g_1 \in \mathbb{Z}^+.$$

I) $p \not| g_1$
Entonces, como p es primo, $mcd(p, g_1) = 1$. Vamos a ver que si $g^j \equiv 1$ (mód p^α) se tiene que $(p-1)p^{\alpha-1}|j$ y la consecuencia será que el orden de g módulo p^α es múltiplo de $(p-1)p^{\alpha-1} = \#U\left(\frac{\mathbb{Z}}{<p^\alpha>}\right)$ y tendremos el resultado.

Supongamos que $g^j \equiv 1$ (mód p^α), como $p|p^\alpha$, $g^j \equiv 1$ (mód p), lo que da lugar a que el orden de g módulo p divide a j, es decir, $p-1$ divide a j y entonces $j = (p-1)j_1$. Tenemos que

$$g^j = g^{(p-1)j_1} = (1 + g_1 p)^{j_1} \equiv 1 \text{ (mód } p^\alpha)$$

pero

$$(1 + g_1 p)^{j_1} = 1 + j_1 g_1 p + \underbrace{\binom{j_1}{2} g_1^2 p^2 + \cdots + \binom{j_1}{j_1} g_1^{j_1} p^{j_1}}_{\text{múltiplo de } p^2} \equiv 1 \text{ (mód } p^\alpha)$$

y como $\alpha \geq 2$ tenemos que

$$p^2 | j_1 g_1 p \;\Rightarrow\; p | j_1 g_1 \overset{p \not| g_1}{\Rightarrow} p | j_1$$

Es decir, $j_1 = p^k \cdot i$ con $k \geq 1$. Veamos que si $k < \alpha - 1 \;\Rightarrow\; p|i$.

$$(1 + g_1 p)^{p^k i} = 1 + p^{k+1} i g_1 + \underbrace{\binom{p^k i}{2} g_1^2 p^2 + \cdots + \binom{p^k i}{l} g_1^l p^l + \cdots + \binom{p^k i}{p^k i} g_1^{p^k i} p^{p^k i}}_{\text{múltiplos de } p^{k+2}} \equiv 1 \text{ (mód } p^\alpha)$$

Suponemos que $k < \alpha - 1 \;\Rightarrow\; k + 2 \leq \alpha$ y por lo tanto

$$p^{k+2} | p^{k+1} i g_1 \overset{p \not| g_1}{\Rightarrow} p | i$$

y concluimos que $(p-1)p^{\alpha-1}|j$ ✓.

II) $p|g_1$
Recordemos que $g^{p-1} = 1 + g_1 p$ y sea $g' = (p+1)g$. Entonces $g' \equiv g \pmod{p}$ por lo que g' también genera $U\left(\frac{\mathbb{Z}}{<p>}\right)$. Ahora bien,

$$g'^{p-1} = g^{p-1}(p+1)^{p-1} = g^{p-1}\left(1 + (p-1)p + \binom{p-1}{2}p^2 + \cdots + \binom{p-1}{p-1}p^{p-1}\right)$$

que es igual a

$$(1+g_1 p)\left(1 + (p-1)p + \binom{p-1}{2}p^2 + \cdots + \binom{p-1}{p-1}p^{p-1}\right) = 1 + pg_1'$$

y además tenemos que $p \not| g_1'$ y podemos razonar como en I). □

Demostración: (Miller-Rabin)
Recordemos lo que dice el Teorema. Sea n impar y compuesto mayor que 9 de forma que $n-1 = 2^k m$ y $2 \not| m$. Entonces,

$$\#\underbrace{\{a : 1 \le a < n \text{ y } (\exists i < k : a^{2^i m} \equiv -1 \pmod{n}) \vee (a^m \equiv 1 \pmod{n})\}}_{B} \le \frac{\varphi(n)}{4}.$$

Para cada p_i primo que divide a n tenemos que $p_i - 1 = 2^{l_i} m_i$ y $2 \not| m_i$. Además definimos $l = \min l_i$, es decir, l es el exponente de la mayor potencia de dos que divide a $p_1 - 1$ para cada i.

Vamos a ver que $B \subset B' := \{x : 1 \le x < n \text{ y } x^{m2^{l-1}} \equiv \pm 1 \pmod{n}\}$.
Si $a \in B$ y es porque $a^m \equiv 1 \pmod{n}$ automáticamente $a \in B'$. En otro caso es porque $a^{m2^i} \equiv -1 \pmod{n}$ con $i < k$ y entonces, para cada factor primo p_j se tiene que

$$a^{m2^i} \equiv -1 \pmod{p_j}.$$

Además, el orden de a en $U\left(\frac{\mathbb{Z}}{<p_j>}\right)$ divide a $p_j - 1 = 2^{l_j} m_j$. Veamos que el exponente de 2 en la parte par de $\mathrm{ord}(a)$ módulo p_j es exactamente $i+1$.
Si éste fuera $h < i+1$ entonces tendríamos

$$2^h t = \mathrm{ord}(a) \pmod{p_j} \;\Rightarrow\; a^{2^h t} \equiv 1 \pmod{p_j} \;\Rightarrow\; (a^{2^h t})^{2^{i-h}m} \equiv 1 \pmod{p_j} \;\Rightarrow\; a^{2^i t m} \equiv 1 \pmod{p_j}$$

Lo que contradice que $a^{m2^i} \equiv -1 \pmod{p_j}$ pues esto da lugar a que, como t es impar, $a^{m2^i t} \equiv -1 \pmod{p_j}$.

Hemos visto que el exponente de 2 que aparece en la parte par del orden de a módulo p_j es $i+1$ para cada p_j, lo que da lugar a que, como $ord(a) \pmod{p_j} | p_j - 1$, se tiene que $i + 1 \le l_j \;\; \forall j$ y por lo tanto $i + 1 \le \min l_j = l$, es decir, $i \le l - 1 \;\Rightarrow\; a \in B'$.

Ahora que hemos visto que $B \subset B'$ vamos a ver que $\#B' \le \frac{\varphi(n)}{4}$ y lo haremos por contraposición, es decir, supondremos que $\#B' > \frac{\varphi(n)}{4}$ y llegaremos a que $n \le 9$ o que n no es compuesto.

Es fácil ver que podemos dividir B' en dos conjuntos disjuntos,

$$B'_+ = \{x : 1 \le x < n \text{ y } x^{m2^{l-1}} \equiv +1 \pmod{n}\}$$

y

$$B'_- = \{x : 1 \leq x < n \text{ y } x^{m2^{l-1}} \equiv -1 \text{ (mód } n)\}$$

ambos contenidos en $U\left(\frac{\mathbb{Z}}{<n>}\right)$ y como decíamos, $B' = B'_+ \oplus B'_- \Rightarrow \#B' = \#B'_+ + \#B'_-$.

Recordemos además que, por el Teorema Chino de los Restos, $U\left(\frac{\mathbb{Z}}{<n>}\right) \simeq \prod_{p_j|n} U\left(\frac{\mathbb{Z}}{<p_j^{\alpha_j}>}\right)$ y por lo tanto

$$\#B'_+ = \prod_j \# \left\{ \text{soluciones en } U\left(\frac{\mathbb{Z}}{<p_j^{\alpha}>}\right) \text{ de } x^{m2^{l-1}} \equiv +1 \text{ (mód } p_j^{\alpha_j}) \right\}$$

y

$$\#B'_- = \prod_j \# \left\{ \text{soluciones en } U\left(\frac{\mathbb{Z}}{<p_j^{\alpha}>}\right) \text{ de } x^{m2^{l-1}} \equiv -1 \text{ (mód } p_j^{\alpha_j}) \right\}$$

Vamos primero con $\#B'_+$. Fijado j, cuántas soluciones tiene la ecuación $x^{m2^{l-1}} \equiv +1$ (mód $p_j^{\alpha_j}$). Por el Lema 7.5.2, el grupo $U\left(\frac{\mathbb{Z}}{<p^{\alpha}>}\right)$ es cíclico, por lo que encontrar soluciones x's tales que $x^{m2^{l-1}} \equiv 1$ (mód $p_j^{\alpha_j}$) es equivalente a encontrar e's de forma que, si $< g >= U\left(\frac{\mathbb{Z}}{<p^{\alpha}>}\right)$, $x = g^e$ y entonces $g^{em2^{l-1}} \equiv 1$ (mód $p_j^{\alpha_j}$) equivalente a encontrar e's tales que

$$em2^{l-1} \equiv 0 \text{ (mód } p_j^{\alpha_j - 1}(p_j - 1))$$

luego el número de soluciones es $mcd(p_j^{\alpha_j - 1}(p_j - 1), m2^{l-1}) = 2^{l-1} mcd(p_j - 1, m)$ y entonces,

$$\#B'_+ = \prod_j 2^{l-1} mcd(p_j - 1, m).$$

Por otra parte, para calcular $\#B'_-$ notemos que el número de soluciones es el número de e's tales que $g^{em2^{l-1}} \equiv -1$ (mód p_j^{α}). Sabemos que

$$\left(\underbrace{g^{\frac{p_j - 1}{2} p_j^{\alpha_j - 1}}}_{-1} \right)^2 \equiv 1 \text{ (mód } p_j^{\alpha_j})$$

y entonces $g^{2m2^{l-1}} \equiv g^{\frac{p_j-1}{2} p_j^{\alpha_j - 1}}$ (mód $p_j^{\alpha_j}$) y el número de soluciones es el número de e's tales que

$$em2^{l-1} \equiv \frac{p_j - 1}{2} p_j^{\alpha_j - 1} \text{ (mód } p_j^{\alpha_j - 1}(p_j - 1))$$

y para que exista solución se ha de cumplir que

$$mcd\left(m2^{l-1}, p_j^{\alpha_j - 1}(p_j - 1)\right) \left| \frac{p_j - 1}{2} p_j^{\alpha_j - 1} \right.$$

pero esto sucede pues ese mcd vale $2^{l-1} mcd(m, m_j)$ y entonces

$$2^{l-1} mcd(m, m_j) \left| 2^{l-1} m_j \right| 2^{l_j - 1} m_j = \frac{p_j - 1}{2} \left| \frac{p_j - 1}{2} p_j^{\alpha_j - 1} \right.$$

y entonces hay $2^{l-1}mcd(m,m_j) = 2^{l-1}mcd(m,p_j-1)$ soluciones.

$$\#B'_- = \prod_j 2^{l-1}mcd(p_j-1,m).$$

En definitiva,

$$\#B' = 2\prod_j \frac{2^{l-1}mcd(p_j-1,m)}{(p_j-1)p_j^{\alpha_j-1}} \overset{\star}{>} \frac{1}{4}$$

Ahora examinaremos distintos casos según la factorización de n:

1. Veremos que $\star$ no es posible si el número de factores primos distintos es mayor o igual que 3. En ese caso tendríamos,

$$\frac{1}{4} \overset{\star}{<} 2\prod_j \frac{2^{l-1}}{\frac{(p_j-1)p_j^{\alpha_j-1}}{mcd(p_j-1,m)}} = 2\prod_j \frac{2^{l-1}}{\frac{2^{l_j}m_j p_j^{\alpha_j-1}}{mcd(m_j,m)}} \leq 2\prod_j \frac{1}{2^{l_j-l+1}}$$

   donde hemos suprimido lo rojo y lo azul pues ambos eran mayores que 1 y estaban en el denominador. Además hemos utilizado que $l_j - l + 1 \geq 1$. Ahora, como hay tres o más factores primos distintos,

$$\frac{1}{4} < \text{Algo} \leq 2\left(\frac{1}{2}\right)^3 = \frac{1}{4} \longrightarrow \textsc{Imposible}$$

2. Veamos que si se da $\star$, no puede ser $n = p^\alpha q^\beta$ con p,q primos (mayores o iguales que 3) y $\alpha \geq 2$.

$$\frac{1}{4} \overset{\star}{<} 2\frac{1}{\frac{2^{l_p-l+1}m_p p^{\alpha-1}}{mcd(m_p,m)}} \cdot \frac{1}{\frac{2^{l_q-l+1}m_q q^{\beta-1}}{mcd(m_q,m)}} \leq \cancel{2}\frac{1}{2\cdot 3}\frac{1}{\cancel{2}} = \frac{1}{6} \longrightarrow \textsc{Imposible}$$

3. Veamos que tampoco puede suceder que $n = p^\alpha$ con $\alpha \geq 3$. Tenemos que,

$$\frac{1}{4} \overset{\star}{<} \cancel{2}\frac{\cancel{2^{l_p-1}}}{\frac{\cancel{2^{l_p}}m_p p_j^{\alpha_j-1}}{mcd(m_p-1,m)}} \leq \frac{1}{p^2} \quad (p \geq 3) \longrightarrow \textsc{Imposible}$$

4. Tampoco es posible que $n = p^2$ a menos que $p = 3$,

$$\frac{1}{4} \overset{\star}{<} \cancel{2}\frac{\cancel{2^{l_p-1}}}{\frac{\cancel{2^{l_p}}m_p p_j^{\alpha_j-1}}{mcd(m_p-1,m)}} \leq \frac{1}{p} \quad (p \geq 5) \longrightarrow \textsc{Imposible}$$

5. Por último veamos que tampoco es factible $n = pq$.

$$\frac{1}{8} \overset{\star}{<} \frac{2^{l-1}}{\frac{2^{l_p}m_p}{mcd(m_p,m)}} \cdot \frac{2^{l-1}}{\frac{2^{l_q}m_q}{mcd(m_q,m)}} \Rightarrow 2 > \frac{m_p 2^{l_p-l}}{mcd(m_p,m)} \cdot \frac{m_q 2^{l_q-l}}{mcd(m_q,m)}$$

   y si el producto de dos enteros positivos es menor que 2 es que ambos son 1. Por lo tanto $l_p = l_q = l$ y $m_p = m = m_q$, es decir, p y q son iguales su parte par es igual y su parte impar también, pero habíamos supuesto que eran distintos. □

Podemos convencernos de que la probabilidad de que, tras escoger un número natural éste sea primo es mayor que la probabilidad de que sea un cuadrado perfecto. Sólo hace falta observar que

$$\sum_{p\in\mathbb{P}} \frac{1}{p} \text{ diverge} \qquad \text{y} \qquad \sum_{n\in\mathbb{N}} \frac{1}{n^2} \text{ converge.}$$

Donde $\mathbb{P}$ representa el conjunto de números primos.

Teorema 7.5.3 (Del número primo)
Si consideramos $\pi(x) = \#\{p \in \mathbb{P} : p \leq x\}$, entonces

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = \frac{1}{\ln x}$$

es decir,

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Así que para valores grandes de n, la probabilidad de que un entero menor o igual que n sea primo es $\frac{\ln n}{n}$.

CURIOSIDAD

Existen "huecos" sin primos tan grandes como queramos. Dado un $n \in \mathbb{N}$,

$$n!+2,\ n!+3,\ n!+4, \ldots,\ n!+n$$

son $n-1$ números compuestos consecutivos.

Gauss observó que la integral logarítmica es una mejor aproximación de la función $\pi(x)$ que $\frac{x}{\ln x}$. Su expresión es,

$$L_i(x) = \int_1^x \frac{dt}{\ln t}$$

La Hipótesis de Riemann Generalizada afirma que $L_i(x) - \pi(x) = O(x^{\frac{1}{2}+\varepsilon})$.

7.6 Algoritmos de factorización

No se conocen algoritmos de factorización con complejidad polinomial, ni siquiera probabilísticos, pero el descubrimiento o invención de uno acabaría con la seguridad del *RSA*. Algunos algoritmos son los siguientes:

1. Regla de Eratóstenes, exponencial en $\log n$, complejidad $O(\sqrt{n})$.
2. Algoritmos especiales (válidos para números especiales).
3. Método ρ de Pollard, probabilista con complejidad $O(\sqrt[4]{n}\ \log n)$.
4. Métodos "subexponenciales":

a) E.C.M. Método de las Curvas Elípticas (Lenstra), válido para enteros grandes, de unas 40 cifras decimales, 120 bits. $\longrightarrow$ probabilista.

b) Q.S. Quadratic Sieve (Pomerance), válido para enteros de unas 100 cifras decimales. $O(e^{1+\varepsilon\sqrt{(\ln n)(\ln(\ln n))}}) \longrightarrow$ probabilista.

c) N.F.S. Number Field Sieve[5] $O(e^{1,92+\varepsilon(\ln n)^{\frac{1}{3}}(\ln(\ln n))^{\frac{2}{3}}})$.

Definición 7.6.1 Una función subexponencial es de la forma

$$L_{u|v} = \exp\left[v\,(\ \ln x)^u \cdot (\ \ln(\ln x))^{1-u}\right] \quad \text{con } u \in (0,1).$$

Observación 7.6.1 Si $u = 0$, $v = v_0 \in \mathbb{R}^+$ y $x \in \mathbb{R}^+$ entonces,

$$L_{0|v_0} = \exp(v_0 \ln\ln x) = (\ln x)^{v_0} \quad \text{(polinomial en } \ln x)$$

Si $u = 1$ y $v = v_0$, entonces,

$$L_{1|v_0} = \exp(v_0 \ln x) = x^{v_0} \quad \text{(exponencial en } \ln x).$$

Dado un n compuesto impar, producto de dos primos, $n = pq$, vamos a ver la relación que existe entre factorizar n y calcular las raíces cuadradas módulo n.

Sea $x \in \mathbb{Z}^+$ tal que $\sqrt{n} < x < n$ y sea $c = x^2 \pmod n$. Sabemos que c tiene cuatro raíces cuadradas, de las cuales conocemos dos, x y $-x$. Además, las raíces cuadradas de $c \pmod p$ son $x \pmod p$ y $-x \pmod p$ y las raíces cuadradas de $c \pmod q$ son $x \pmod q$ y $-x \pmod q$.

Por el Teorema Chino de los Restos, podemos encontrar u, v de forma que

$$\begin{cases} u \equiv 1 \pmod p \\ u \equiv 0 \pmod q \end{cases} \quad y \quad \begin{cases} v \equiv 0 \pmod p \\ v \equiv 1 \pmod q \end{cases}$$

y las cuatro raíces cuadradas de $c \pmod n$ serían $\pm ux \pm vx \pmod n$.
Nótese que $ux + vx \equiv x \pmod n$ y que $-ux - vx \equiv -x \pmod n$. A las otras dos raíces las llamamos,

$$z = ux - vx \equiv x \pmod p \equiv -x \pmod q \quad y \quad -z = -ux + vx \equiv -x \pmod p \equiv x \pmod q.$$

Entonces, si conocemos x y z sabemos que $x^2 \equiv c \pmod n \equiv z^2 \pmod n$ y entonces $x^2 \equiv z^2 \pmod n$ o lo que es lo mismo, $(x - z)(x + z) \equiv 0 \pmod n$, pero $p|(x - z)$ y $q \not| (x - z)$, luego basta hacer $mcd(x - z, n) = p$.

Método de las bases de cuadrados
Sea n compuesto impar de forma que $n = pq$ con p, q primos.

I) Se consideran conjuntos de primos (k en total), por ejemplo los k primeros primos.

$$B = \{p_1, \ldots, p_k\} \quad k << n$$

El k óptimo se elige en función de n basándose en Teoría analítica de números y en Experimentación.

[5]Este algoritmo, en 1990, consiguió factorizar el número $2^{2^9} - 1$ en tres primos.

II) Construimos suficientes $b_i : \sqrt{n} < b_i < n$ y tomamos $c_i = b_i^2 \pmod n$ de modo que c_i se pueda factorizar con los primos de B (ensayo y error) aleatoriamente.
Al menos se necesitan $k+1$ $c_i's$ con éxito.

III) Cada c_i está factorizado,

$$c_i = p_1^{u_{i_1}} \cdots p_k^{u_{i_k}} \quad \text{con} \quad u^i = (u_{i_1}, \ldots, u_{i_k}) \in \mathbb{N}_{\geq 0}^k$$

Además consideramos el conjunto

$$\left\{\nu^{(i)} \;\; i = 1, \ldots, k+1\right\} \subset \mathbb{F}_2^k \;\; \text{donde} \;\; \nu^{(i)} = (u_{i_1} \pmod 2, \ldots, u_{i_k} \pmod 2) \in \mathbb{F}_2^k$$

Y como hay $k+1$ vectores, seguro que hay alguna combinación lineal de ellos igual a cero no trivial, es decir, una suma parcial de los vectores que da cero,

$$\nu^{(j_1)} + \cdots + \nu^{(j_s)} = 0$$

entonces $u^{(j_1)} + \cdots + u^{(j_s)}$ es un vector que tiene todas sus coordenadas pares y por lo tanto podemos contruir un cuadrado. Por un lado,

$$c_{j_1} \cdots c_{j_s} = p_1^{\lambda_1} \cdots p_k^{\lambda_k} = (p_1^{\frac{\lambda_1}{2}} \cdots p_k^{\frac{\lambda_k}{2}})^2 = a^2 \qquad \lambda_i \in 2\mathbb{N}$$

por otro lado,

$$c_{j_1} \cdots c_{j_s} = (b_{j_1} \cdots b_{j_s})^2$$

y entonces $b^2 \equiv a^2 \pmod n$

IV) Si hemos tenido la suerte de que a es distinto de $\pm b$, entonces $mcd(b-a, n)$ es un factor propio de n.

7.7 Cálculo de raíces cuadradas

Vamos a ver cómo calcular la parte entera de la raíz cuadrada de un número natural n.
Si sabemos cuántos bits tiene $[\sqrt{n}]$, sabemos qué lugar ocupa el 1 más significativo, entonces, suponemos que el segundo bit es también un 1 y el resto de bits son 0.
Si al elevar este número al cuadrado obtenemos un número mayor que n, significa que el segundo bit no es un 1 sino un 0. En caso contrario estábamos en lo cierto y seguimos el proceso iterativo.

Como mucho deberemos hacer $\log_2 n$ operaciones, cada una de complejidad $O(\log_2^2 n)$ lo que significa que el algoritmo tiene complejidad $O(\log_2^3 n)$.
Es fácil ver que, en general, calcular parte entera de la raíz r-ésima de un número n tiene complejidad $O(\log_2^3 n)$.

Otro problema diferente es averiguar si, dado n, éste se puede expresar como a^s.
Si $n = a^s \geq 2^s$ tenemos que $\log_2 n \geq s$ y por lo tanto responder a la pregunta tiene complejidad $O(\log_2^4 n)$.

Vamos a intentar calcular raíces cuadradas, pero en $\mathbb{F}_p$, para ello necesitamos introducir la siguiente definición.

Observación 7.7.1 Sea $r = \#_2 n$, es fácil darse cuenta de que si r es par, entonces $\#_2[\sqrt{n}] = \frac{r}{2}$ y si r es impar, $\#_2[\sqrt{n}] = \frac{r+1}{2}$.

Definición 7.7.1 (Símbolo de Legendre)
Sea p primo impar. Definimos $\left(\frac{a}{p}\right)$ como 0 si $p|a$, 1 si $\exists c \in \mathbb{Z} : c^2 \equiv a \pmod{p} \not\equiv 0$ y -1 si $\nexists c \in \mathbb{Z} : c^2 \equiv a \pmod{p} \not\equiv 0$.

Observación 7.7.2 Sabemos que $\mathbb{F}_p^*$ es un grupo cíclico, $\mathbb{F}_p^* =< g >$.
Sea $x \in \mathbb{F}_p^*$ de forma que $x = g^\alpha$.
Si α es par, entonces x es un cuadrado módulo p, es decir, $\left(\frac{x}{p}\right) = 1$.
Recíprocamente, si $x \in \mathbb{F}_p^*$ y $\exists c : a \equiv c^2 \pmod{p}$ entonces $a = g^\beta$ y $c = g^\delta$ de forma que $g^\beta \equiv g^{2\delta} \pmod{p}$ y entonces $p-1|\beta - 2\delta$ por lo que como $p-1$ es par, $\beta - 2\delta$ debe ser par y por lo tanto β debe ser par.

Lema 7.7.1 Sea p primo impar y $a \in \mathbb{F}_p^*$ se verifica que,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Demostración:
Si $p|a$ entonces $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$ y también $\left(\frac{a}{p}\right) = 0$.
Supongamos que $p \not| a$.
Si $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ entonces $g^{\alpha\frac{p-1}{2}} \equiv 1 \pmod{p}$ y por lo tanto $p-1|\alpha\frac{p-1}{2} \Rightarrow 2|\alpha$, por lo que α es par y $\left(\frac{a}{p}\right) = 1$. Si $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ entonces $g^{\alpha\frac{p-1}{2}} \equiv -1 \pmod{p}$, pero como $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ tendríamos que

$$g^{\alpha\frac{p-1}{2} - \frac{p-1}{2}} \equiv 1 \pmod{p}$$

lo que significa que $p-1|\frac{(\alpha-1)(p-1)}{2}$ y por lo tanto $2|\alpha - 1$, es decir, α es impar y $\left(\frac{a}{p}\right) = -1$. □

Nótese que el lema proporciona una condición necesaria para que un número sea primo.

Observación 7.7.3 Del lema anterior se deducen algunas propiedades:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
- Si $p \not| b$, se verifica que $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.
- $\left(\frac{1}{p}\right) = 1$ y $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
- $\left(\frac{2}{p}\right) = 1$ si $p = \pm 1 \pmod{8}$ mientras que $\left(\frac{2}{p}\right) = -1$ si $p = \pm 3 \pmod{8}$.
- Ley de Reciprocidad Cuadrática de Gauss.
  $\left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right)$ si $p \equiv q \equiv 3 \pmod{4}$, mientras que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ en caso contrario.

Definición 7.7.2 (Símbolo de Jacobi)
Sea n impar mayor o igual que 3. Sea $a \in \mathbb{Z}$. Definimos,

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i}$$

siendo $\prod_{i=1}^{r} p_i^{\alpha_i}$ la factorización en primos de n.

Se puede comprobar que el símbolo de Jacobi hereda algunas propiedades del Símbolo de Legendre.

Estos días estuve muy vago en clase y esta parte la tengo muy incompleta. Los resultados más importantes son los de la Observación 7.7.3, pero no incluyo la demostración hecha en clase.
Dejo un enlace que puede ser de utilidad como complemento, aunque, de cara al examen, no creo que merezca la pena:

`http://www.famaf.unc.edu.ar/series/pdf/pdfCMat/CMat31-3.pdf`

8 Firma digital

En un sisteama criptográfico de clave pública, uno de los usuarios pretende enviar un mensaje a otro de forma que el segundo esté completamente convencido de que se lo envía el primero. Para ello le envía un mesaje firmado.

Sea f_u la función de encriptado para enviar mensajes al usuario u y f_u^{-1} la función que usa u para descifrarlos.
El usuario A envía a B un mensaje M firmado, mandándole el par $(f_B(M), f_B \circ f_A^{-1}(M))$.
Ahora B aplica f_B^{-1} y obtiene el par $(M, f_A^{-1}(M))$. Para asegurarse de que fue A quien le envió el mensaje aplica f_A a la segunda parte y obtiene M.

Si ambos mensajes coinciden, entonces B está convencido de que el mensaje viene de A pues nadie más conoce f_A^{-1}.

8.1 Firma con funciones hash

En la práctica, como el mensaje puede llegar a ser muy largo, para la firma digital (el segundo elemento del par enviado) se utiliza una *función hash* o *función resumen.*

$$H : \Sigma \longrightarrow \Sigma_l \qquad l \sim 160 \text{ bits}$$

Además, esta función es resistente a imagen inversa ya que, conociendo $y \in \Sigma_l$ es difícil calcular $x \in \Sigma$ de forma que $H(x) = y$ y también es resistente a colisión, es decir, es difícil, conocienco x, calcular un $x' \neq x$ de forma que $H(x') = H(x)$.
En el proceso de envío del mensaje se manda el par $(f_B(M), f_B f_A^{-1}(H(M)))$.

8.2 Firma con RSA

Suponiendo que $n_A < n_B$ tenemos el siguient esquema,

$$\frac{\mathbb{Z}}{< n_A >} \xrightarrow{f_A^{-1}} \frac{\mathbb{Z}}{< n_A >} \xrightarrow{i} \frac{\mathbb{Z}}{< n_B >} \xrightarrow{f_B} \frac{\mathbb{Z}}{< n_B >}$$

$$p \longmapsto p^{d_A} \qquad x \longmapsto x \qquad m \longmapsto m^{e_B}$$

Cuando A quiere enviarle un mensaje a B, le manda el par $(\underbrace{p^{e_b} \pmod{n_B}}_{Q}, \underbrace{(p^{d_A} \pmod{n_A})^{e_B} \pmod{n_B}}_{Q'})$
Ahora B puede descifrar el mensaje elevando Q a d_B y además puede cerciorarse de que el mensaje viene de A utilizando que, $Q' < n_B$. Además $Q'^{d_B} \equiv C^{d_B e_B} \pmod{n_B}$ y quiere conocer C, pero $Q'^{d_B} < n_B$ y como $C < n_A < n_B$ necesariamente $Q'^{d_B} = C$.
Al conocer C, lo eleva a e_A y llega de nuevo al mensaje original.

Nótese que si se hubiera hecho al revés, es decir, si se hubiera mandado como firma

$$(p^{e_B} \pmod{n_B})^{d_A} \pmod{n_A}$$

habría dos mensajes distintos con la misma firma.

8.3 Firma con ElGamal

Los usuarios de este sistema criptográfico convienen en un número primo p y un generador g de $\mathbb{F}_p^*$ (alternativamente un primo p y un polinomio primitivo $f(x) \in \frac{\mathbb{F}_p[X]}{<f>}$).
Cada usuario A, B elige aleatoriamente, en secreto, una clave privada $a, b \in \{0, 1, 2, \ldots, p-2\}$.

I) A selecciona aleatoriamente un $r \in \{0, 1, 2, \ldots, p-2\}$ de forma que $mcd(p-1, r) = 1$ (clave de sesión) y calcula $R = g^r$.
Ahora escribe una ecuación modular llamada "ecuación de firma" utilizando su clave privada, su clave de sesión y el mensaje,

$$M = aR + rS \pmod{p-1}$$

y entonces

$$S = (M - aR)r^{-1} \pmod{p-1}$$

A envía a B el par (R, S).

II) Ahora B verifica que la firma viene de A. Calcula,

$$e_A^R R^S \pmod{p} = g^{aR+rr^{-1}(M-aR)} \pmod{p} = g^{M \pmod{p-1}} \pmod{p}$$

que coincide con $g^M \pmod{p}$.

Como por otro lado B ha conseguido descifrar el mensaje, es capaz de saber si efectivamente el mensaje se lo ha enviado A.

También se puede conseguir el mismo objetivo enviando en la firma un resumen del mensaje en lugar del mensaje entero, para ahorrar cálculos. Para ello se elige un primo q de unos 1024 bits y otro primo p de unos 160 bits de forma que $p|q-1$ (el tamaño del texto resumen será de unos 160 bits).
Ahora hace falta calcular un elemento de orden p de $\mathbb{F}_q^*$. En la práctica se elige un $h \in \mathbb{F}_q^*$ y se calcula $g = h^{\frac{q-1}{p}} \pmod{q}$ si el resultado es distinto de 1 significa que g tiene orden p mientras que si el resultado es 1 se intenta con otro h.

A y B convienen en una función resumen H y A elige aleatoriamente un $r \in \{0, 1, 2, \ldots, p-1\}$ y calcula $R = g^r \pmod{q}$ y $S = (H(M) + aR)r^{-1} \pmod{p}$ para enviar el par (R, S).

B verifica la firma, para ello calcula $\omega = S^{-1} \pmod{p}$, $x = H(M)\omega \pmod{p}$ e $y = R\omega \pmod{p}$.
Nótese que B conoce el mensaje por otro camino, así que puede calcular $H(M)$.
Ahora, si el mensaje viene efectivamente de A, debe suceder que

$$g^x e_A^y \pmod{q} = g^{(H(M)+aR)S^{-1}} \pmod{q} = g^{(H(M)+aR)(H(M)+aR)^{-1}r} \pmod{q} = g^r \pmod{q} = R.$$

9 Ataques al DLP

El mejor algoritmo conocido es probabilista de complejidad subexponencial. También hay algoritmos deterministas (no polinomiales) pero su eficiencia depende de si se conoce la factorización de $p-1$ cuando se trabaja en el grupo $\mathbb{F}_p^*$.

9.1 Algoritmo de Pohlig-Hellman

Sea p un número primo y F_p el cuerpo finito de p elementos. El problema reside en calcular logaritmos discretos en $\mathbb{F}_p^*$, es decir, conociendo un generador g de $\mathbb{F}_p^* =< g >$ y dado un $y \in \mathbb{F}_p^*$, calcular un x tal que $g^x = y$. En ese caso decimos que $x = \log_g y$ módulo p.

Supongamos que conocemos la factorización de $p-1 = \prod q^\alpha$. La idea es que calcular logaritmos discretos en un grupo cíclico de cardinal $p-1$ es equivalente a calcular logaritmos discretos en grupos cíclicos de cardinal q^α.
Buscamos x, entero módulo $p-1$, pero por el Teorema Chino de los Restos es suficiente encontrar x (mód q^α) $\forall q$ primo tal que $q|p-1$ y $q^\alpha||p-1$.

Fijamos q y buscamos x (mód q^α). Para ello, consideremos el desarrollo de x en base q,

$$x = x_0 + x_1 q + x_2 q^2 + \cdots + x_{\alpha-1} q^{\alpha-1} + x_\alpha q^\alpha \qquad x_i \in \{0, 1, \ldots, q-1\}$$

Observemos que si $\eta_q = g^{\frac{p-1}{q}}$ (mód p) entonces η_q tiene orden q, por lo que es una raíz primitiva q-ésima de la unidad. Sea $y_1 = y^{\frac{p-1}{q}}$, con lo cual

$$y_1 = \left(g^{x_0+x_1 q+\cdots+x_\alpha q^\alpha}\right)^{\frac{p-1}{q}} = g^{x_0 \frac{p-1}{q}} \underbrace{(g^{p-1})^{x_1+x_2 q+\cdots+x_\alpha q^{\alpha-1}}}_{1} = g^{x_0 \frac{p-1}{q}} = \eta_q^{x_0}$$

Sabiendo resolver el DLP en $< n_q >$ se calcula $x_0 \in \{0, 1, \ldots, q-1\}$. Esto se puede hacer mediante algoritmos rápidos para encontrar elementos en una lista "sorting" o por el método de "divide y vencerás" con el algoritmo *Baby Step-Giant Step*.

Veamos ahora cómo determinar x_1 (si $\alpha - 1 \geq 1 \Rightarrow \alpha \geq 2 \Rightarrow q^2|p-1$). Sea $y_2 = \frac{y}{g^{x_0} q^1}$. Ahora calculamos

$$y_2^{\frac{p-1}{q^2}} = \left(g^{x_1 q+\cdots+x_\alpha q^\alpha}\right)^{\frac{p-1}{q^2}} = \left(g^{x_1+x_2 q+\cdots+x_\alpha q^{\alpha-1}}\right)^{\frac{p-1}{q}} = g^{x_1 \frac{p-1}{q}} = \eta_q^{x_1}$$

Y resolviendo el DLP de nuevo obtenemos x_1. Análogamente se pueden calcular todos los x_i's.

Ejemplo:
Calcular el logaritmo discreto de 28 en base 2 módulo 37.
Buscamos un x tal que $2^x \equiv 28$ (mód 37). Además sabemos que $\mathbb{F}_{37}^* =< 2 >$.

Tenemos que $37 - 1 = 2^2 3^2$
Fijamos $q = 2$. Entonces $\eta_2 = g^{\frac{36}{2}}$ (mód 37) $\equiv 36$ (mód 37).
Ahora, $y_1 = 28^{\frac{36}{2}} \equiv 1$ (mód 37) $\equiv \eta_2^0 \Rightarrow x_0 = 0$.

Además $y_2 = \frac{28}{2^0} = 28$ y entonces $28^{\frac{36}{4}} \equiv 36 \pmod{37} \equiv \eta_2^1 \Rightarrow x_1 = 1$.
Hemos llegado a que $x \equiv 2 \pmod 4$.

Sea ahora $q = 3$. En este caso $\eta_3 = g^{\frac{36}{3}} \pmod{37} \equiv 26 \pmod{37}$.
Y entonces $y_1 = 28^{\frac{36}{3}} \equiv 26 \pmod{37} \equiv \eta_3^1 \pmod{37} \Rightarrow x_0 = 1$.
Por último $y_2 = \frac{28}{2^1} = 14$ y $14^{\frac{36}{9}} \equiv 10 \pmod{37} \equiv \eta_3^2 \pmod{37} \Rightarrow x_1 = 2$. Y entonces $x \equiv 7 \pmod 9$.

Ahora, resolviendo el siguiente sistema en congruencias

$$\left.\begin{array}{l} x \equiv 2 \pmod 4 \\ x \equiv 7 \pmod 9 \end{array}\right\}$$

llegamos a que $x = 34 \pmod{37}$ con lo cual, el logaritmo discreto de 28 en base 2 módulo 37 es 34.

9.2 Cálculo del índice

Sea $G =< g >$ siendo $\text{ord}(g) = n$. Buscamos un conjunto $S = \{s_1, s_2, \ldots, s_l\} \subset G$ de forma que sean conocidos sus logaritmos discretos.

$$\delta_i \in \{0, 1, 2, \ldots, n-1\} \qquad s_i = g^{\delta_i}$$

Necesitamos escribir $y \in G$, cuyo logaritmo buscamos, como producto de los s_i's y utilizaremos que el logaritmo del producto es la suma de los logaritmos.

I) Es necesario seleccionar $S \subset G$ con la propiedad de que gran proporción de elementos de G se puedan escribir como producto de elementos de S.

II) Hay que encontrar "bastantes" índices $i \in \mathbb{N}$ tales que

$$g^i = s_1^{u_{i1}} \cdots s_l^{u_{il}} \qquad i \equiv u_{i1}\delta_1 + \cdots + u_{il}\delta_l \pmod{n-1}$$

Para ello producimos potencias g^i y las reescribimos en términos de $s_1, \ldots, s_l$ hasta tener l ecuaciones linealmente independientes. Ahora podremos despejar $\delta_1, \ldots, \delta_l \pmod{n-1}$.

III) Dado $y \in G$ buscamos un r tal que $g^r y$ sea fácil de escribir como producto de los s_i's, es decir,

$$g^r y = s_1^{\alpha_1} \cdots s_l^{\alpha_l}$$

y entonces tendremos que $r + x = \alpha_1\delta_1 + \cdots + \alpha_l\delta_l \pmod{n-1}$, de donde conocemos todo salvo la x, por lo que la podemos despejar. Además se verifica que $g^x = y$.

10 Resultante y discriminante

10.1 Recordando conceptos

Recordemos qué significa que $\mathbb{C}$ es un cuerpo algebraicamente cerrado. Todo polinomio $f \in \mathbb{C}[X]$ de grado $n \geq 1$ se puede expresar como,

$$f = \lambda \prod_{i=1}^{n} (x - \alpha_i) \qquad \text{con } \alpha_i \in \mathbb{C}$$

si queremos ser más precisos,

$$f = \lambda \prod_{j=1}^{s} (x - \beta_j)^{e_j} \qquad \text{con } \beta_i \neq \beta_j \text{ si } i \neq j \qquad \text{y} \qquad e_1 + \cdots + e_s = n.$$

Recordemos también el concepto de multiplicidad de una raíz.
Sea $f \in K[X]$, decimos que $\alpha \in K$ es raíz de $f(x)$ si y sólo si $f(x) = 0$. Decimos que α es raíz de multiplicidad mayor o igual que r si

$$f'(\alpha) = f''(\alpha) = \cdots = f^{(r-1)}(\alpha) = 0$$

Si además resulta que $f^{(r)}(\alpha) \neq 0$ entonces α es una raíz de multiplicidad exactamente r.

Definición 10.1.1 Sea $(A, +, \cdot)$ anillo y dominio de integridad. Entonces decimos que A es DFU (dominio de factorización única) si se verifican:

- $\forall\, a \in A^* \,:\, a$ no es unidad $\Rightarrow$ a se puede escribir como $a = a_1 \cdots a_r$ con $a_i \in A^*$ irreducibles.
- La descomposición es única.

Lema 10.1.1 Dado un cuerpo Q y un polinomio $l(x) \in Q[X]$ con $\deg(l) \geq 1$ entonces existe un cuerpo $K \supset Q$ con $\alpha \in K$ de forma que $l(\alpha) = 0$.

Demostración:
Sabemos que Q es un cuerpo y que $l \in Q[X]$. Si l es irreducible en $Q[X]$, tomamos $K = \frac{Q[X]}{<l>}$ que es cuerpo y $\bar{x} \pmod{l}$ es raíz de $l(T)$.

Si l no es irreducible, entonces tiene algún factor irreducible de grado mayor o igual que 1 porque $Q[X]$ es DFU. En ese caso razonamos de forma análoga a la del caso anterior utilizando dicho factor irreducible.

10.2 Resultante de Sylvester

Teorema 10.2.1 Sean $f(x) = a_0 x^n + \cdots + a_n$ y $g = b_0 x^m + \cdots + b_m$ con $\deg(f) \leq n$, $\deg(g) \leq m$ y $f, g \in A[X]$ siendo A DFU. Si además f y g son no ambos constantes, entonces son equivalentes,

(1) $\exists\, h, k \in A[X]$ no ambos identicamente nulos, con $\deg(h) \leq \deg(g) - 1$, $\deg(k) \leq \deg(f) - 1$ y $hf = kg$.

(2) $\exists\, l \in A[X]$ con $\deg(l) \geq 1$ y de forma que $l|f \ \wedge \ l|g$.

(3) Existe K cuerpo que contiene a A donde los polinomios $f(x)$ y $g(x)$ tienen alguna raíz común.

Demostración:

$\boxed{1 \Rightarrow 2}$

Sabemos que $hf = kg$ y que h y g no son ambos nulos.
Supongamos que f o g, uno de los dos es nulo. Sin pérdida de generalidad, $g = 0 \ \Rightarrow \ f \neq 0$ y además $\deg(f) \geq 1$ pues no están ambos en A.
En este caso es fácil ver que se verifica (2) tomando $l = f$.

Ahora supongamos que f y g son ambos no nulos. En ese caso, también h y k son distintos de cero. Por el Lema de Gauss, $A[X]$ también es DFU y como es cierta la igualdad

$$h(x)f(x) = k(x)g(x)$$

no es posible que todo factor irreducible de $f(x)$ de grado mayor o igual que 1 divida a $k(x)$ y el mismo número de veces ya que $\deg(f) > \deg(k) \ \Rightarrow \ \exists\, l(x)$ irreducible con grado mayor o igual que 1 de forma que $l|f$ y $l|g$.

$\boxed{2 \Rightarrow 1}$

Existe $l(x) \in A[X]$ con $\deg(l) \geq 1$ y $l|f \ \wedge \ l|g$. Entonces existen $f_1, g_1 \in A[X]$ tales que $lf_1 = f$ y $lg_1 = g$.
Además, $\deg(f_1) \leq \deg(f) - 1$ y $\deg(g_1) \leq \deg(g) - 1$.
Si fueran $g_1 = f_1 = 0$ tendríamos que f y g son ambos nulos, lo que contradice la hipótesis (no ambos están en A). Esto da lugar a que $g_1 \neq 0$ o $f_1 \neq 0$ y además

$$g_1 f = f_1 g$$

$\boxed{2 \Rightarrow 3}$

Tenemos que $l(x)|f$ y $l(x)|g$. Además $\deg(l) \geq 1$. Utilizando el lema 10.1.1 decudiremos (3).
Tomamos $Q =$"Cuerpo de fracciones de A". Entonces existe $K \supset Q$ y existe $\alpha \in K$ de forma que $l(\alpha) = 0$ lo que da lugar a que $f(\alpha) = g(\alpha) = 0$.

$\boxed{\text{No } 2 \Rightarrow \text{No } 3}$

Como A es DFU, por el Lema de Gauss $A[X]$ es DFU. Por hipótesis, $mcd_{A[X]}(f, g) \in A - \{0\}$ lo que da lugar a que $mcd_{Q[X]}(f, g) = 1$. En ese caso, existen $\lambda(x)$ y $\mu(x)$ en $Q[X]$ tales que $1 = \lambda(x)f + \mu(x)g$ y entonces f y g no pueden tener raíces comunes en K si $K \supset Q[X]$. $\square$

Si escribimos la primera condición del Teorema 10.2.1 en ecuaciones tenemos que $\exists h, k \in A[X]$ no ambos nulos de forma que

$$h(x) = c_0 x^{m-1} + \cdots + c_{m-1} \qquad k(x) = d_0 x^{n-1} + \cdots + d_{n-1}$$

y además,

$$hf = kg \Rightarrow (c_0 x^{m-1} + \cdots + c_{m-1})(a_0 x^n + \cdots + a_n) = (d_0 x^{n-1} + \cdots + d_{n-1})(b_0 x^m + \cdots + b_m)$$

Igualando los coeficientes de $x^{n+m-1},\ x^{n+m-2},\ldots,\ x^1,\ x^0$ llegamos a un sistema homogéneo de $n+m$ ecuaciones con $n+m$ incógnitas $(c,-d)$.
Matricialmente,

$$\underbrace{\begin{pmatrix} a_0 & \ldots & a_n & 0 & \ldots & \ldots & 0 \\ 0 & a_0 & \ldots & a_n & 0 & \ldots & 0 \\ & & \ddots & & \ddots & & \\ 0 & \ldots & \ldots & 0 & a_0 & \ldots & a_n \\ b_0 & \ldots & \ldots & b_m & 0 & \ldots & 0 \\ & \ddots & & & \ddots & & \\ 0 & \ldots & 0 & b_0 & \ldots & \ldots & b_m \end{pmatrix}}_{S_{n,m}(f,g)} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \\ -d_0 \\ \vdots \\ -d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Al determinante de la matriz del sistema lo llamamos "resultante de Sylvester" y lo denotamos como $R_{n,m}(f,g) = Res(f,g)$

Corolario 10.2.1 Sea A anillo DFU. Sean $f(x) = a_0x^n + \cdots + a_n$ y $g = b_0x^m + \cdots + b_m$ con $\deg(f) \leq n$, $\deg(g) \leq m$ y $f, g \in A[X]$. Entonces son equivalentes,

(1) $R_{n,m}(f,g) = 0$

(2) $a_0 = b_0 = 0 \vee f(x)$ y $g(x)$ tienen un factor común de grado mayor o igual que 1 en $A[X]$.

(3) $a_0 = b_0 = 0 \vee f(x)$ y $g(x)$ tienen alguna raíz común en algún cuerpo $K \supset A$.

Demostración:
$\boxed{1 \Rightarrow 2}$
Hay que demostrar que si $R_{n,m}(f,g) = 0$ y No $(a_0 = b_0 = 0)$, entonces $f(x)$ y $g(x)$ tienen un facctor común de grado mayor o igual que 1 en $A[X]$.

Supongamos que $a_0 \neq 0$, entonces $\deg(f) = n$. Aplicando el Teorema 10.2.1, ver que f y g tienen un factor común de grado mayor o igual que 1 en $A[X]$ es equivalente a ver que $\exists\ h, g \in A[X]$ no ambos nulos y con $\deg(h) < \deg(g)$ y $\deg(k) < \deg(f)$, de forma que $hf = kg$.

La existencia de estos polinomios h y k está ligada a la existencia de una solución no trivial del sistema homogéneo mencionado más arriba cuya matriz de coeficientes es $S_{n,m}(f,g)$. Por hipótesis, $R_{n,m}(f,g) = \det(S_{n,m}(f,g)) = 0$ lo que nos asegura la existencia de una solución no trivial, como queríamos ver.

$\boxed{2 \Rightarrow 1}$
Si $a_0 = b_0 = 0$ entonces $S_{n,m}(f,g)$ tiene una columna de ceros y por lo tanto $R_{n,m} = 0$.
Ahora supongamos que no ocurre que $a_0 = b_0 = 0$ pero que $f(x)$ y $g(x)$ tienen algún factor común de grado mayor o igual que uno en $A[X]$. Sin pérdida de generalidad, sea $a_0 = 0$, entonces $\deg(f) = n$ y $f \neq 0$. Como f y g no están ambos en A, por el Teorema 10.2.1 el sistema homogéneo tiene una solución no trivial, lo que da lugar a que $R_{n,m}(f,g) = 0$.

$\boxed{2 \Leftrightarrow 3}$
Es evidente por la equivalencia del Teorema 10.2.1. □

10.3 Propiedades de $R_{n,m}(f,g)$

1. Si a la última columna de la matriz $S_{n,m}(f,g)$ le sumamos la columna i-ésima multiplicada por x^{n+m-i} el determinante no cambia y por lo tanto tenemos que,

$$R_{n,m}(f,g) = \begin{vmatrix} a_0 & \dots & a_n & 0 & \dots & \dots & 0 & x^{m-1}f \\ 0 & a_0 & \dots & a_n & 0 & \dots & 0 & x^{m-2}f \\ & & \ddots & & \ddots & & & \\ 0 & \dots & \dots & 0 & a_0 & \dots & a_1 & f \\ b_0 & \dots & \dots & b_m & 0 & \dots & 0 & x^{n-1}g \\ & \ddots & & & \ddots & & & \\ 0 & \dots & 0 & b_0 & \dots & \dots & b_1 & g \end{vmatrix}$$

   y ahora, desarrollando el determinante por la última columna comprobamos que,

$$R_{n,m}(f,g) = f\cdot(\text{polinomio de grado} < m) + g\cdot(\text{polinomio de grado} < n).$$

2. Si suponemos que $a_0 = \cdots = a_{k-1} = 0$ entonces, desarrollando el determinante de $S_{n,m}(f,g)$ por la primera columna y repitiendo el proceso k veces llegamos a que,

$$R_{n,m}(f,g) = b_0^k(-1)^{mk}R_{n-k,m}(f,g)$$

   Se deduce una propiedad análoga si se parte de $b_0 = \cdots = b_{k-1} = 0$.

3. Si $j \leq n-m$ entonces, $\forall \lambda \in A$ se verifica que $R_{n,m}(f - \lambda x^j g, g) = R_{n,m}(f,g)$.
   Para verlo basta observar que el determinante no varía pues lo que estamos haciendo es sumarle a cada fila i-ésima $(0 \leq i \leq m-1)$ la fila $(m+n-j)$-ésima multiplicada por un escalar.

4. Si realizamos la división euclídea entre f y g tenemos que $f = qg + r$ donde $r = 0$ o $\deg(r) < m$. Es fácil comprobar que si $r = 0$ entonces $R_{n,m}(f,g) = 0$ y que si $r \neq 0$, se tiene que

$$R_{n,m}(f,g) = (-1)^{nm}b_0^{n-k}R_{n,m}(g,r).$$

5. Supongamos ahora que f desompone en factores lineales, es decir,

$$f = a_0\prod_{j=1}^{m}(x - \alpha_j)$$

   en ese caso, se verifica que

$$Res_{n,m}(f,g) = a_0^m\prod_{j=1}^{m}g(\alpha_i).$$

   Existe un resultado análogo si es g quien se puede descomponer en factores lineales,

$$g = b_0\prod_{j=1}^{n}(x - \beta_j)$$

   entonces,

$$Res_{n,m}(f,g) = (-1)^{nm}b_0^n\prod_{j=1}^{m}f(\beta_j).$$

Observación 10.3.1 Sea K cuerpo y sean

$$f = a_0(t_1, \ldots, t_r)x^n + \cdots + a_n(t_1, \ldots, t_r) \qquad g = b_0(t_1, \ldots, t_r)x^m + \cdots + b_m(t_1, \ldots, t_r)$$

polinomios con coeficientes en $A = K[t_1, \ldots, t_r]$.
$Res(f, g) = R(t_1, \ldots, t_r)$. Ahora, dado $t^0 = (t_1^0, \ldots, t_r^0)$ son equivalentes,

- $R(t^0) = 0$
- $a_0(t^0) = b_0(t^0) = 0 \quad \vee \quad Res(f(t^0, x), g(t^0, x)) = 0.$

Ejercicio: Supongamos que tenemos $f(x) \in \mathbb{Q}[X]$ que se anula en $\alpha \in \mathbb{Q}$ y $g(x) \in \mathbb{Q}[X]$ que se anula en $\beta \in \mathbb{Q}$.
Calcular un polinomio $h(x) \in \mathbb{Q}[X]$ que se anule en $\alpha + \beta$.

Podemos considerar que los polinomios f y g tienen coeficientes en $A = \mathbb{Q}[T]$. Entonces,

$$Res_{A=\mathbb{Q}[T]}(f(T - x), g(x)) = P(T) \in \mathbb{Q}[T].$$

Observemos que si, fijado t, $f(t - x)$ y $g(x)$ comparten una raíz en $\mathbb{Q}[X]$ entonces $P(t) = 0$ ya que $Res(f(t - x), g(x)) = 0$.
Como $f(\alpha + \beta - x)$ y $g(x)$ comparten la raíz β tenemos que $P(\alpha + \beta)$ es cero, como queríamos.

Como ejemplo vamos a calcular un polinomio con coeficientes en $\mathbb{Q}$ que se anule en $\sqrt{2} + \sqrt{3}$.
Sea $f(x) = x^2 - 2$ y sea $g(x) = x^2 - 3$. Claramente f se anula en $\sqrt{2}$ y g se anula en $\sqrt{3}$.
Sabemos que el polinomio $P(T) = Res(f(T - x), g(x))$ se anula en $\sqrt{2} + \sqrt{3}$, así que calculémoslo:

Tenemos que $f(T - x) = (T - x)^2 - 2 = x^2 - 2Tx + T^2 - 2$ y entonces,

$$P(t) = \begin{vmatrix} 1 & -2T & T^2-2 & 0 \\ 0 & 1 & -2T & T^2-2 \\ 1 & 0 & -3 & 0 \\ 0 & 1 & 0 & -3 \end{vmatrix} = \begin{vmatrix} 1 & -2T & T^2-2 \\ 0 & -3 & 0 \\ 1 & 0 & -3 \end{vmatrix} + \begin{vmatrix} -2T & T^2-2 & 0 \\ 1 & -2T & T^2-2 \\ 1 & 0 & -3 \end{vmatrix}$$

es decir,

$$P(T) = 9 + 3(T^2 - 2) - 12T^2 + (T^2 - 2)^2 + 3(T^2 - 2) = \boxed{T^4 - 10T^2 + 1}$$

Polinomio con coeficientes en $\mathbb{Q}$ que se anula en $\sqrt{2} + \sqrt{3}$.

10.4 Discriminante

Definición 10.4.1 Sea K cuerpo y $f \in K[X]$ tal que $f = a_0 \prod_{j=1}^{n}(x - \alpha_j) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ entonces llamamos discriminante de f a

$$\Delta(f) = a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Proposición 10.4.1 El discriminante de f verifica,

$$a_0\Delta(f) = (-1)^{\frac{n(n-1)}{2}} Res(f, f')$$

Demostración:
Tenemos que, como $f = a_0 \prod_{j=1} n(x - \alpha_j)$,

$$f' = a_0 \left(\sum_{k=1}^{n} \left(\prod_{j \neq k} (x - \alpha_j \right) \right) \qquad f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j)$$

Por otra parte, utilizando la quita propiedad de $R_{n,m}(f, g)$ tenemos que,

$$R(f, f') = a_0^{n-1} a_0^n \prod_{i=1}^{n} \left(\prod_{j \neq i} (\alpha_i - \alpha_j) \right) = a^{2n-1} (-1)^{\binom{n}{2}} \prod_{k \neq l} (\alpha_k - \alpha_l)^2$$

es decir,

$$R(f, f') = a_0^{2n-1} (-1)^{\frac{n(n-1)}{2}} \prod_{k<l} (\alpha_k - \alpha_l)^2$$

por lo tanto,

$$(-1)^{\frac{n(n-1)}{2}} Res(f, f') = a_0 \left(a^{2n-2} \prod_{k<l} (\alpha_k - \alpha_l)^2 \right) = a_0 \Delta(f). \ \square$$

Ejercicio: Dar condiciones sobre p y q para que el polinomio $f(x) = x^3 + px + q$ tenga alguna raíz múltiple.
Es lo mismo que dar condiciones para que se anulen simultáneamente $f(x)$ y $f'(x) = 3x^2 + p$. Calculemos $Res(f, f')$, para ello observemos que el resto de dividir f entre f' es $\frac{2p}{3}x + q$ y entonces,

$$Res(f, f') = (-1)^{3 \cdot 2} 3^{3-1} Res(3x^2 + p, \frac{2p}{3}x + q)$$

$$Res(3x^2 + p, \frac{2p}{3}x + q) = \begin{vmatrix} 3 & 0 & p \\ \frac{2p}{3} & q & 0 \\ 0 & \frac{2p}{3} & q \end{vmatrix} = 3q^2 + \frac{4p^3}{9}.$$

Por lo tanto, $Res(f, f') = 4p^3 + 27q^2$.
Hemos llegado a que si p y q son tales que $4p^3 + 27q^2 = 0$ entonces f y f' tienen una raíz común y por lo tanto f tiene una raíz múltiple.

Proposición 10.4.2 Sean $f(x) = a_0 x^n + \cdots + a_n$ y $g = b_0 x^m + \cdots + b_m$ con $\deg(f) = n$, $\deg(g) = m$ y $f, g \in A[X]$ siendo A *DFU*. Si además f y g son no ambos constantes, entonces son equivalentes,

- $\deg(mcd(f, g)) \geq d$.
- $\operatorname{rg}(S_{n,m}(f, g)) \leq n + m - d$

y si en una se da la igualdad, en la otra también.

11 Examen de febrero 2012

Para terminar estas notas incluyo el examen que tuvimos en la convocatoria de febrero:

1. Catalogar los problemas numerados abajo en los tres apartados:

   a) No se conoce un algoritmo determinista polinomial en el número de bits de n para encontrar la solución.

   b) Sí se conoce un algoritmo determinista polinomial en el número de bits de n para encontrar la solución.

   c) Sí se conoce un algoritmo probabilístico polinomial en el número de bits de n para encontrar, con alta probabilidad, una solución.

   • Dado un entero $n \in \mathbb{Z}^+$, averiguar si es un cuadrado perfecto y, en caso afirmativo, calcular su raíz cuadrada.

   • Dado un entero $n \in \mathbb{Z}^+$, averiguar si es primo o compuesto.

   • Dado un entero $n \in \mathbb{Z}^+$ del que se sabe que es compuesto, calcular un factor primo.

   • Dado un número primo p y un $b \in \mathbb{Z}^+$, averiguar si existe solución de la ecuación $x^2 \equiv b \pmod{p}$.

   • Dado un número primo p, calcular un $n \in \mathbb{Z}^+$ que no sea resíduo cuadrático módulo p.

   • Dado un entero $n \in \mathbb{Z}^+$, averiguar si es una potencia pura, es decir, si existen $r, k \in \mathbb{Z}$ tales que $n = r^k$ y calcularlos.

   • Dado un primo p y $g, b \in \mathbb{Z}^+$ enteros menores que p, tales que $b \in \{g^k \pmod{p} : k = 1, \ldots, p-1\}$, encontrar un k_0 tal que $b \equiv g^{k_0} \pmod{p}$.

   • Dado un entero impar $n \in \mathbb{Z}^+$ del que se sabe que es producto de dos números primos, ambos congruentes con 3 (mód 4), pero no se conocen dichos factores, calcular todas las soluciones de la ecuación $x^2 = 1$ distintas de la solución $x = 1$ y $x = -1$.

2. Enunciar el problema del logaritmo discreto y explicar el sistema criptográfico de clave pública ElGamal. Discutir la firma digital en este sistema.

3. Considérese el polinomio $f(x) = x^6 + x^5 + x^4 + x^2 + 1 \in \mathbb{F}_2[X]$. Se pide:

   a) Probar que f es irreducible. ¿Es primitivo?

   b) Sea $\mathbb{F}_{2^6}$ el cuerpo $\frac{\mathbb{F}_2[X]}{<f(x)>}$ y $\alpha = x \pmod{f}$. Calcular el orden de α^3, expresar α^3 en función de la base $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^5\}$ (pregunta absurda) y calcular su polinomio mínimo sobre $\mathbb{F}_2$.

   c) Demostrar que $\mathbb{F}_{2^6}$ contiene las raíces primitivas cúbicas de 1, expresarlas en la base $\mathcal{B}$ y encontrar su polinomio mínimo sobre $\mathbb{F}_2$.

   d) Sea un $LFSR$ con polinomio característico $f(x)$. Calcular el período de una secuencia producida por f para el valor inicial $s_0 = 1$, $s_1 = 1$, $s_2 = 1$, $s_3 = 0$, $s_4 = 1$, $s_5 = 1$. Escribir la serie generatriz de la secuencia $(s_i)_{i \geq 0}$ en la forma de $\frac{u(x)}{f^*(x)}$ con $\deg(u(x)) \leq \deg(f(x)) - 1$ y f^* el recíproco de f.

4. Sean F y G polinomios en $A[X]$ donde A es un DFU.

   a) Definir resultante de Sylvester de F y G.

   b) En el caso de que A sea un cuerpo, enunciar la relación que hay entre la resultante de F y G y la de G y H, donde H es el resto de dividir F entre G.

   c) Sean
   $$F(x,y,a) = x^2y + x - a \qquad G(x,y,a) = x^2y + x + y^2 - 4a$$
   polinomios con coeficientes en el cuerpo $\mathbb{C}$. Sea $R(y,a)$ la resultante de F y G como polinomios en x con coeficientes en el anillo $A = \mathbb{C}[y,a]$. ¿Para qué valores de $y, a \in \mathbb{C}$ es $R(y,a)$ la resultante de los polinomios $F(x,y,a)$ y $G(x,y,a)$? Estudiar según los valores de $a \in \mathbb{C}$ cuántos puntos distintos $(x,y) \in \mathbb{C}^2$ son solución del sistema
   $$F(x,y,a) = 0,\ G(x,y,a) = 0.$$

5. Sea p un número primo $p - 1 = 2^s t$, con t impar. Se pide:

   a) Demostrar que en $\mathbb{F}_p$ existen raíces primitivas $2^{s'}$-ésimas de la unidad, para $s' \leq s$. Sea η una raíz primitiva 2^s-ésima de la unidad, escribir las raíces primitivas $2^{s'}$-ésimas de la unidad en función de η.

   b) Sea $n < p$ un no resíduo cuadrático módulo p, es decir, $\left(\frac{n}{p}\right) = -1$ y $b = n^t \pmod p$. Demostrar que $b \in \mathbb{F}_p^*$ es una raíz primitiva 2^s-éstima de la unidad.

   c) Sea $p = 2^{2^k} + 1$ con $k \geq 1$ un primo de Fermat. Demostrar que 7 es generador de $\mathbb{F}_p^*$.

   d) Explicar razonadamente si sería buena la idea de utilizar los grupos $\mathbb{F}_p^*$ para p primo de Fermat en un sistema criptográfico de tipo DLP.