MA-53G Intr. a la Criptografía **Semestre Otoño, 1998**

Cátedra No. 13 : 4 de Mayo

Transcriptor: Manuel Reyes[1]

Teorema: Sea K un cuerpo finito y f un polinomio irreductible de grado $n > 1$ en $K[x]$. Entonces $K[x]|_{(f)}$ es un cuerpo finito de $|K|^n$ elementos.

Lema: Para todo enterno $n \geq 1$ y p primo, existe un polinomio irrductible de grado n en $Z_p[x]$.

Teorema: Para todo entero $n \geq 1$ y p primo existe un cuerpo finito con p^n elementos.

Cabe destacar que, salvo isomorfismos, existe un 'unico cuerpo finito con q elementos (donde $q = p^k$, p primo y $k \in N,\ k \geq 1$).

De lo anterior sigue que mientras estemos interesados en la estructura algebraica del cuerpo con q elementos, podemos denotarlo sin ambiguedades por F_q.

Sin embargo, es posible que estemos interesados en distintas implementaciones de F_q, por razones computacionales. A las implementaciones F's las vamos a llamar modelos de F_q.

Formalmente, un modelo de F_{p^n} (con p primo) consiste en un primo p y una base de F_{p^n} como espacio vectorial de $F_p \cong Z_p$, y una tabla de multiplicar (que consiste en $O(n^2 n)$ elementos en F_p, i.e. $O(n^3 \log p)$ bits), es decir, dados

$$x = \sum_{i=1}^{n} \alpha_i e_i; \quad y = \sum_{j=1}^{n} \beta_j e_j$$

definimos el producto $z = xy$ por

$$z = \sum_{i,j=1}^{n} \alpha_i \beta_j e_i e_j$$

En la pr'actica, se necesita menos informaci'on para especificar un producto de F_{p^n}. Por ejemplo (p, f), donde p es un primo y f es un polinomio irreductible de $F_p[x]$ se determina un modelo de $F_{p^n} \cong F_p[x]|_{(f)}$ cuya base es $\{1, x, x^2, ..., x^{n-1}\}$ y cuya tabla de multiplicaci'on es

$$x^{i+j} \pmod f$$

para todos $i, j \in \{0, ..., n-1\}$, en este modelo cada elemento de F_{p^n} puede representarse como

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 \in Z_p[x]$$

Se suman dos elementos de F_{p^n} sumando los polinomios correspondientes y se multiplica reduciendo. Por ejemplo

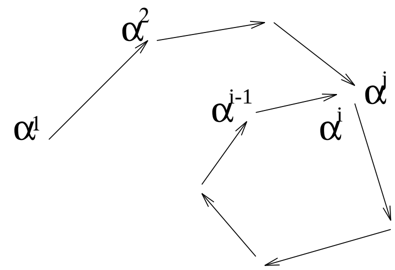
$$x^n = -c_{n-1}x^{n-1} - c_{n-1}x^{n-1} - ... - c_0$$

si $f(x) = x^n + c_{n-1}x^{n-1} + c_{n-1}x^{n-1} + ... + c_0$. Ref: BACH.

[1] La primera parte modificando a Marcos Kiwi.

Sea F un cuerpo finito, denotamos por F^* al conjunto $F^* = F - \{0\}$

Definici'on: Sea $\alpha \in F^*$. Al menor entero positivo k tal que $\alpha^k = 1$ (neutro multiplicativo) se le denomina el *orden de* α.



Como $a^i = \alpha^j$ tendremos que $\alpha^{i-j} = 1$.

Observaci'on: Como F es cuerpo, F^* ser'a un grupo abeliano de orden $|F| - 1$.

Teorema (Lagrange): Todo $\alpha \in F_q^*$ tiene orden que divide a $q - 1$.

Demostraci'on: Primero veamos que $\alpha^{q-1} = 1$.

Observemos que $f : F_q^* \to F_q^*$ tal que $f(x) = \alpha x$ es biyecci'on (ya que es invertible). Luego

$$\Pi_x \in F_q^* x = \Pi_x \in F_q^* f(x) = \Pi_x \in F_q^* \alpha x = \alpha^{q-1} \Pi_x \in F_q^* x$$

de donde $\alpha^{q-1} = 1$.

Sea $d = ord(\alpha)$, y supongamos que d no divide a $q-1$. Notar que $d \geq q-1$ (asi que existe), entonces existe $t \in Z$ tal que $q - 1 = td + r$, donde $0 < r < \alpha$, luego

$$1 = \alpha^{q-1} = (\alpha^d)^t \alpha^r,$$

pero como d es el orden de α, se tiene $\alpha^d = 1$, luego $\alpha^r = 1$, lo que contradice la minimalidad de d.

Dedinici'on: Un grupo G se dice *c'iclico* si existe $g \in G$ tal que $G = \{g^i / i \in Z\}$. A tal g se le llama *generador*.

Z_p^* c'iclico si p primo, implica que existe g tal que para todo $b \in Z_p^*$ existe un 'unico a tal que $g^a = b$. Esto sugiere definir $\log_g b = a$.

Luego, un generador de F_q^* tiene orden $q - 1$.

Lema: Si F_q es un cuerpo finito, entonces F_q^* es c'iclico. Si g es un generador de F_q^*, entonces g^j es un generador de F_q^* ssi $(i, q-1) = 1$. En particular hay $\phi(q-1)$ generadores de F_q^*.

Dem: Sea d el orden de α en F_q^*, i.e. $\alpha^d = 1$ y α, $\alpha^2, ..., \alpha^d$ son soluciones de la ecuaci'on $x^d = 1$ tiene d soluciones (Teorema Fundamental del Algebra) en F_q^*.

Es f'acil ver que $\{1, \alpha, ..., \alpha^{d-1}\}$ son todas las soluciones distintas de $x^d = 1$. Luego todos los elemtos β de orden d son tales que $\beta \in \{\alpha, ..., \alpha^d\}$.

Veamos que α^j es de orden d ssi $(j,d)=1$.

$(\Rightarrow)$ Supongamos que $d'=(j,d)>1$, entonces $\alpha^{jd/d'}=(\alpha^j)^{d/d'}=1$, lo que es una contradicci'on (pues $d/d'<d$ y d es el orden de α^j).

$(\Leftarrow)$ Si $(j,d)=1$, entonces existe $u,v\in Z$ tal que $ju+vd=1$. Luego, si α^p, tiene orden $d'<d$, sigue que $\alpha^{d'}=\alpha^{jud'+vdd'}=(\alpha^j)^{d'u}\cdot(\alpha^d)^{vd'}=1\cdot 1=1$, lo que es una contradicci'on pues α tiene orden d.

Entonces si existe un elemento de orden d hay $\phi(\alpha)$ elementos de orden d.

Luego o hay $\phi(\alpha)$ elementos de orden d o hay 0.

$$\begin{aligned} q-1 &= \sum_{d|q-1} |\{\alpha : \mathrm{ord}(\alpha)=\alpha\}| \\ &\leq \sum_{d|q-1} \phi(\alpha) \\ &= q-1 \end{aligned}$$

Asi que

$$\sum_{d|q-1} (\phi(\alpha) - |\{\alpha : \mathrm{ord}(\alpha)=\alpha\}|) = 0$$

de donde $|\{\alpha : \mathrm{ord}(\alpha)=\alpha\}| = \phi(\alpha)$ si $d|q-1$.