IMPLEMENTACIÓN EFICIENTE DE ALGORITMOS CRIPTOGRÁFICOS USANDO CURVAS DE KOBLITZ

ALONSO DE JESÚS GARCÍA HERRERA
CARLOS MARIO PENAGOS HOLLMANN

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
BARRANQUILLA
2008

IMPLEMENTACIÓN EFICIENTE DE ALGORITMOS CRIPTOGRÁFICOS USANDO CURVAS DE KOBLITZ

ALONSO DE JESÚS GARCÍA HERRERA
CARLOS MARIO PENAGOS HOLLMANN

Monografía para optar al título de Ingeniero de Sistemas

Director:
Ismael Segundo Gutierrez García

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
BARRANQUILLA
2008

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Dr. rer. nat. Ismael Segundo Gutiérrez García
Director del proyecto

_____
Ing. José Rafael Capacho Portilla
Coord. Programa de Ing. Sistemas

_____
Corrector

_____
Jurado

_____
Jurado

INTRODUCCIÓN

En este tiempo moderno el uso de las redes de comunicación esta cada vez al alcance de más personas, su uso va desde operaciones militares hasta juegos online domésticos, es por eso que cada usuario y organización preocupada por su confidencialidad en una red insegura ,como la Internet, se halla en la necesidad de proteger la integridad de sus datos y la confidencialidad de sus operaciones, la criptografía de clave publica nace de estos requerimientos Universales, basada en sólidas teorías matemáticas en las que su seguridad son los problemas matemáticos intratables para las maquinas actuales, como lo son el calculo de los factores primos de un numero grande y el calculo del logaritmo discreto, este ultimo problema es en el que se basa la criptografía de curva elíptica propuesto por Miller[1] en el año 1985. Es una sólida posibilidad para proteger la información confidencial de cada ente en una red insegura, luego fue en el año en el que Neals Koblitz propuso el uso de dos curvas E_a y E_b, estas curvas presentan unas propiedades especiales matemáticas que hacen que estas curvas logren una gran eficiencia a la hora de una implementación, se presenta en esta monografía para el titulo de ingeniero de sistema esas propiedades y los algoritmos utilizados para poder lograr una implementación eficiente de algoritmos criptográficos utilizando curvas de koblitz en el lenguaje de programación java.

[1]MILLER V., Use of elliptic curves in cryptography, CRYPTO 85, 1985.

Índice general

Índice de figuras

Lista de Algoritmos

Capítulo 1

GENERALIDADES SOBRE GRUPOS FINITOS

1.1. Definiciones básicas

Definición. 1.1.1 *Sea G un conjunto no vacío y $*$ una operación binaria definida sobre G, diremos que el par $(G, *)$ es un grupo si se satisfacen las siguientes propiedades:*

1. $\forall\, x, y, z \in G,\ \ x * (y * z) = (x * y) * z$. *(Asociatividad).*
2. $\exists\, e \in G$ *tal que* $\forall\, x \in G,\ \ e * x = x * e = x$. *(Identidad).*
3. $\forall\, x \in G\ \exists\, y \in G$ *tal que* $x * y = y * x = e$. *(Inverso).*
   Si además se verifica:
4. $\forall\, x, y \in G,\ \ x * y = y * x$. *(Conmutatividad).*
   Se dice que el grupo es abeliano.

Los grupos abelianos son grupos especiales que, como se mostrará mas adelante, tienen importantes aplicaciones para la criptografía, pero en general no todo grupo es abeliano. A lo largo de esta monografia se referira a los grupos en general, a menos que se especifique que es abeliano.

Ejemplo. 1.1.2 *El conjunto de los números reales sin el cero y $\cdot$, producto usual de los reales, es un grupo. Esté será denotado como* $\left(\mathbb{R}^{\mathrm{x}}, \cdot\right)$.

Ejemplo. 1.1.3 *El conjunto de los enteros $\mathbb{Z}$ junto con la suma forman un grupo abeliano.*

Teorema. 1.1.4 *Sea G un grupo. Se cumple:*

1. *Existe un solo módulo $e \in G$.*
2. *Para todo $x \in G$ existe un elemento único $y \in G$, tal que y es el inverso de x, el cual se notará como x^{-1}.*

3. $\forall x \in G$, *se verifica* $(x^{-1})^{-1} = x$.

4. $\forall x, y \in G$ *se tiene* $(xy)^{-1} = y^{-1}x^{-1}$.

5. $\forall x, y, z \in G$ *se cumple,* $xy = xz \Rightarrow y = z$.

Demostración.

1. Sean e, e' módulos en G, entonces $e = e'e = e'$.

2. Sea $x \in G$, y supongamos $y, z \in G$ inversos de x, entonces

$$z = ze = z(xy) = (zx)y = ey = y.$$

3. Se sigue de la definición de inverso.

4. Sean $x, y \in G$, $(xy)(y^{-1}x^{-1}) = x(y^{-1}y)x^{-1} = xx^{-1} = e$. Luego entonces

$$(xy)^{-1} = y^{-1}x^{-1}.$$

5. Se tiene $xy = xz$, entonces $x^{-1}xy = x^{-1}xz \Rightarrow y = z$.

Definición. 1.1.5 *Sea G un grupo, se dice orden del grupo al cardinal de G, en caso de de ser finito el grupo también lo es. Se notará con $|G|$. Otra notación usual encontrada en la literatura es $o(G)$.*

1.1.1. Subgrupos

Definición. 1.1.6 *Sea G un grupo y $H \neq \emptyset$ un subconjunto de G. Se dice que H es un subgrupo de G si la operacion de G restringida a H hace de este un grupo. Se notara con $H < G$. En caso de $H \subseteq G$ como $H \leq G$.*

Teorema. 1.1.7 *Sea G un grupo y $H < G$, se cumple entonces que para todo $x, y \in H$, $xy^{-1} \in H$.*

Demostración.

1. Sea $x \in H$, entonces $xx^{-1} \in H$ lo cual implica $e \in H$.

2. $x^{-1} \in H$ (consecuencia de 1.).

3. Sean $x, y \in H$ se verifica que $xy = x(y^{-1})^{-1} \in H$, luego la cerradura en H se cumple.

Algunos ejemplos de subgrupos son:

Ejemplo. 1.1.8 *Los enteros con la suma es un subgrupo de $(\mathbb{R}, +)$.*

Ejemplo. 1.1.9 *Sea $(\mathbb{Z}, +)$, se define $H = \{nx \mid x \in \mathbb{Z}\}$. Entonces $H < G$.*

Ejemplo. 1.1.10 *Sea G un grupo abeliano y $n \in \mathbb{Z}$. Entonces $nG = \{nx \mid x \in G\}$ es un subgrupo de G.*

Lema. 1.1.11 *Sea G un grupo y $U, V, U_j \leq G$, con $j \in J$.*

1. *$\bigcap_{j\in J} U_j \leq G$.*
2. *$U \cap V \leq G$ si y solo si $U \subseteq V$ o $V \subseteq U$.*

Demostración.

1. Es claro que la intersección no es vacía, dado que $e \in U_j$. Sean $u, v \in \bigcap_{j\in J} U_j$. Entonces $u, v \in U_j$ para todo $j \in J$. Por consiguiente $uv^{-1} \in U_j$, para todo $j \in J$, por lo cual se cumple la afirmación.
2. Si $U \subseteq V$ o $V \subseteq U$, es claro entonces $U \cup V \leq G$. Por otro lado, Supóngase que $U \cup V \leq G$, pero $U \nsubseteq V$ y $V \nsubseteq U$. Considerese ahora $u \in U\backslash V$ y $v \in V\backslash U$. Entonces $uv \in U \cup V$. Podemos suponer que $uv \in U$, entonces $v \in U$ lo cual es una contradicción.

En general, este lema se refiere a que la intersección de subgrupos también es un subgrupo del mismo grupo, pero no se puede decir lo mismo para la union.

Definición. 1.1.12 *Sean H, U subconjuntos no vacíos de un grupo G. Se define*

$$HU := \{hu \mid h \in H,\, u \in U\} \quad y \quad H^{-1} := \{h^{-1} \mid h \in H\}.$$

Lema. 1.1.13 *Sean H, U, V subconjuntos no vacíos de un grupo G. Entonces*

1. *$H(UV) = (HU)V$*
2. *Si $H \subseteq U$, entonces $HV \subseteq UV$ y $VH \subseteq VU$*
3. *Si G es abeliano, entonces $HU = UH$, lo cual no necesariamente sigue a $hu = uh$ para todo $h \in H$ y $u \in U$.*
4. *Si $\emptyset \neq X \subseteq H \leq G$, entonces se cumple que $XH = HX = H$*
5. *$(H^{-1})^{-1} = H$*
6. *Si $H \leq G$, entonces $H^{-1} = H$*
7. *$(HU)^{-1} = H^{-1}U^{-1}$*

Teorema. 1.1.14 *Sea G un grupo y $H, U \leq G$.*

1. *$HU \leq G$ si y solo si $HU = UH$*
2. *Si $HU = UH$, entonces $HU = \langle H \cup U \rangle$*

Demostración.

1. Si $HU \leq G$, entonces del lema anterior se tiene que $HU = (HU)^{-1} = H^{-1}U^{-1} = UH$. Repricamente, para la via contraria, suponemos que $HU = UH$, por el lema anterior se tiene que $(HU)(HU)^{-1} = (HU)(H^{-1}U^{-1}) = (UH)(HU) = HUH = HHU = HU$, es decir $HU \leq G$.

2. Es facil ver que $HU \leq \langle H \cup U \rangle$. Por otra parte, si $H \cup U \subseteq HU$ y $HU \leq G$, se tiene que $\langle H \cup U \rangle \leq HU$.

Definición. 1.1.15 *Sea G un grupo y $H < G$. Una clase lateral izquierda de H en G es un conjunto de la forma gH, $g \in G$, donde:*

$$gH = \{gh \mid h \in H\}.$$

Se puede decir entonces que estas clases inducen una partición en G, esto es:

$$G = \bigcup_{g \in G} gH \quad \text{y} \quad gH \cap xH = \begin{cases} \emptyset & \text{si } x \notin gH \\ gH & \text{si } x \in gH \end{cases}$$

Ahora se define entonces un conjunto T llamado transversal izquierdo, el cual contiene representantes tales que las particiones de G sean disjuntas, esto es:

$$G = \dot{\bigcup_{t \in T}} tH$$

Definición. 1.1.16 *Si T es finito, se llama a $|T|$, como indice de H en G y se notara con $|G : H|$.*

Lema. 1.1.17 *Sea G un grupo y $H \leq G$. Entonces para todo $g \in G$ se cumple que $|gH| = |G|$.*

Lema. 1.1.18 *Sea G un grupo y $H \leq G$, y g, $u \in G$. Entonces*[2]

1. *Si $gH \subseteq uH$, entonces $gH = uH$*

2. *Si $gH \cap uH \neq \emptyset$, entonces $gH = uH$*

3. *$gH = uH$ si y solo si $gu^{-1} \in H$*

Demostración.

1. Como $H \leq G$ y g, $u \in G$, entonces

$$g = ge \in gH \subseteq uH,$$

es decir que existe $w \in H$ tal que $g = wu$, es decir $u = w^{-1}g \in gH$. Ahora si $v \in H$, $vu = vw^{-1}g \in gH$, entonces $uH \subseteq gH$, es decir $gH \subseteq uH$.

[2]ANDERSON, M., FEIL, T. A First Course in Abstract Algebra., p. 401, 30 de agosto de 2008.

2. Supongamos que $gH \cap uH \neq \emptyset$ y sea $v \in gH \cap uH$. Entonces $v \in gH$ y $vH \subseteq gH$. Pero por la parte 1., $vH = gH$, de forma similar $vH = uH$, entonces $gH = uH$.

3. Si $gH = uH$, entonces $g = ge \in gH = uH$, es decir existe un $v \in H$ tal que $g = vu$, es decir $gu^{-1} = v \; inH$. Reciprocamente si $u^{-1}g = v \; inH$, entonces $uu^{-1}g = v \; inuH$, pero $g \in uH \subseteq gH$, entonces por 2., $gH = uH$.

Teorema. 1.1.19 (Lagrange) *Supóngase que G es un grupo y $H \leq G$, entonces*

$$|G| = |G : H| \times |H|$$

Demostración.

$$|G| = \sum_{t \in T} |tH| = \sum_{t \in T} |H| = |T||H| = |G : H||H|.^{3}$$

1.2. Subgrupos normales y homomorfismos de grupos

Definición. 1.2.1 *Sean G y H grupos. Una función $\varphi : G \to H$ es un homomorfismo si para todo x, y en G se cumple $\varphi(xy) = \varphi(x)\varphi(y)$.*

Note que el producto de la parte izquierda de la igualdad toma lugar en G y el de la parte derecha en H.

Definición. 1.2.2 *Sea $\varphi : G \to H$ un homorfismo.*

1. *Si φ es inyectiva entonces se denomina monomorfismo.*

2. *Si φ es sobreyectiva, entonces se llama epimorfismo.*

3. *Si φ es biyectiva, entonces se denomina isomorfismo. Este hecho se notara como $G \cong H$, es decir G y H son isomorfos.*

Se define además dos conjuntos, el kernel y la imagen de φ:

1. $ker(\varphi) = \{g \in G \mid \varphi(g) = e\}$

2. $img(\varphi) = \{\varphi(g) \mid g \in G\}$

Ejemplo. 1.2.3 *La función logaritmo es un homomorfismo de $(\mathbb{R}^{\times}, \cdot)$ a $(\mathbb{R}, +)$.*

Ejemplo. 1.2.4 *Sea $g \in G$ un elemento fijo, entonces la función $\varphi : \mathbb{Z} \to G$, definida por $\varphi(n) = g^n$ es un homomorfismo de $\mathbb{Z}$ a G.*

El siguiente teorema muestra algunas de las consecuencias inmediatas mas importantes de la definición de homomorfismos.

[3]GUTIERREZ, I. Notas de Clase - Electiva-Criptografía. 2008, p. 49, 5 de septiembre de 2008.

Teorema. 1.2.5 *Sean G y H dos grupos, con modulos e y e' respectivamente, y sea φ un homomorfismo de G a H. Entonces:*

1. *$\varphi(e) = e'$.*
2. *$\varphi(g^{-1}) = \varphi(g)^{-1}$, para todo $g \in G$.*
3. *$\varphi(g^n) = \varphi(g)^n$, para todo $n \in \mathbb{Z}$ y $g \in G$.*
4. *$ker(\varphi) \leq G$, ademas se verifica que $gxg^{-1} \in ker(\varphi)$, para todo $g \in G$ y $x \in ker(\varphi)$.*
5. *Si $U \leq G$, entonces $\varphi(U) \leq H$.*
6. *Si $V \leq H$, entonces $\varphi^{-1}(V) \leq G$.*

Demostración.

1. $e'\varphi(e) = \varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$. Entonces $\varphi(e) = e'$.
2. $e' = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, luego entonces $\varphi(g^{-1})$ es el inverso de $\varphi(g)$.
3. Haciendo inducción sobre n:
   a) Si $n = 1$ se cumple.
   b) Supóngase que $\varphi(g^k) = \varphi(g)^k$ para todo $g \in G$ y para todo $k \in \mathbb{N}$. Entonces:
   $$\varphi(g^{k+1}) = \varphi(g^k g) = \varphi(g^k)\varphi(g) = \varphi(g)^k\varphi(g) = \varphi(g)^{k+1}.$$
   c) Sea $n < 0$. De $g^n g^{-n} = e$ se sigue que
   $$\varphi(g^n g^{-n}) = \varphi(g^n)\varphi(g^{-1}) = e'.$$
   Entonces
   $$\varphi(g^n) = \varphi(g^{-n})^{-1} = (\varphi(g)^{-n})^{-1} = \varphi(g)^n.$$
4. Si $\varphi(g) = e'$ y $\varphi(h) = e'$, entonces $\varphi(gh) = \varphi(g)\varphi(h) = e' \cdot e' = e'$, y $\varphi(g^{-1}) = \varphi(g)^{-1} = -e' = e'$. Esto demuestra $ker(\varphi) \leq G$. Para lo segundo, sean $g \in G$, $x \in ker(\varphi)$, entonces
   $$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e'.$$
   Esto demuestra la segunda parte.
5. Sean $\varphi(g)$, $\varphi(h) \in \varphi(U)$. Entonces $\varphi(g)\varphi(h)^{-1} = \varphi(g)\varphi(h^{-1}) = \varphi(gh^{-1}) \in \varphi(U)$.
6. Sean u, $v \in \varphi^{-1}(V)$. Entonces $\varphi(uv^{-1}) = \varphi(u)\varphi(v^{-1}) = \varphi(u)\varphi(v)^{-1} \in V$.

Lema. 1.2.6 *Sean G y H dos grupos, y φ un homomorfismo de G a H. Entonces:*

1. *φ es un monomorfismo si y solo si $ker(\varphi) = \{e\}$.*

2. *φ es un epimorfismo si y solo si $img(\varphi) = H$.*

3. *φ es un isomorfismo si y solo si $ker(\varphi) = \{e\}$ y $img(\varphi) = H$.*

DEMOSTRACIÓN.

1. Supóngase que φ es inyectiva y sea $g \in ker(\varphi)$. Del teorema anterior se tiene que $e \in ker(\varphi)$. Por otra parte, $\varphi(g) = e' = \varphi(e)$, es decir $g = e$. Con esto se demuestra que $ker(\varphi) = \{e\}$.

2. Se sigue de la definición de epimorfismo.

3. Consecuencia de 1. y 2.

Teorema. 1.2.7 *Si $\varphi : G \to H$ y $\psi : H \to U$ son homomorfismos de grupos entonces también los es su composición $\varphi \circ \psi : G \to U$.*

DEMOSTRACIÓN. Para g, $h \in G$, se tiene que $\psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h))$.

Definición. 1.2.8 *Sea G un grupo y $N \leq G$. Se dice que N es un subgrupo normal de G si para algún $g \in G$, $gN = Ng$ o equivalentemente $g^{-1}Ng = N$. Se notará como $N \trianglelefteq G$. Si se quiere enfatizar que $N < G$ entonces se escribirá $N \lhd G$.*

Dado que $g \in G$, y $N \trianglelefteq G$, se sabe que $gN = Ng$. Es igual a decir que las clases laterales son iguales

$$\{gn \mid n \in N\} = \{ng \mid n \in N\},$$

pero no necesariamente significa que $gn = ng$ para todo $n \in N$. El hecho que $gN = Ng$ significa que g se conmuta con N como conjunto, pero esto no forza a que g se conmute con cada elemento individual de N. Sin embargo, si $H \leq G$ y cada elemento de H conmuta con cada elemento de G, entonces $N \trianglelefteq G$.[4]

Lema. 1.2.9 *Sea $N \leq G$, $N \trianglelefteq G$ si y solo si $g^{-1}ng \in N$ para todo $n \in N$ y $g \in G$*

DEMOSTRACIÓN. Si $N \trianglelefteq G$, entonces $gN = Ng$ para todo $g \in G$. Como $N = g^{-1}Ng$ entonces $g^{-1}ng \in N$ para todo $n \in N$ y $g \in G$. Para la ir en la otra vía, Supóngase que $g^{-1}ng \in N$ para todo $n \in N$ y $g \in G$. Por lo tanto $g^{-1}Ng \subseteq N$. Reemplazando g por g^{-1} se tiene $gNg^{-1} \subseteq N$ por lo tanto $N = g^{-1}gNg^{-1}g \subseteq g^{-1}Ng$. Con ambas inclusiones se llega a $N = g^{-1}Ng$ para todo $g \in G$ entonces $N \trianglelefteq G$.[5]

Ejemplo. 1.2.10 *En un grupo abeliano todos los subgrupos son normales.*

Lema. 1.2.11 *Sea G un grupo y $N < G$ tal que $|G : H| = 2$. Entonces $N \lhd G$.*[6]

DEMOSTRACIÓN. Se tiene que $|G : H| = 2$, por lo cual se sigue $G = N \cup gN = N \cup Ng$, con $g \notin N$. Por consiguiente $gN = \complement N = Ng$, entonces por definición se tiene que $N \lhd G$.

[4]SMITH, G., TABACHNIKOVA, O. Topics in Group Theory., p. 48, 6 de septiembre de 2008.
[5]Ibid.
[6]GUTIERREZ, I. Notas de Clase - Electiva-Criptografía. 2008, p. 56, 6 de septiembre de 2008.

Teorema. 1.2.12 *Sea G un grupo, N, N_1, $N_2 \trianglelefteq G$ y $H \leq G$. Entonces*[7]

1. $(H \cap N) \trianglelefteq H$
2. $HN = NH \leq G$
3. $N_1 N_2 \trianglelefteq G$
4. $N_1 \cap N_2 \trianglelefteq G$
5. *Si* $N_1 \cap N_2 = \{e\}$, *entonces* $n_1 n_2 = n_2 n_1$ *para todo* $n_1 \in N_1$, $n_2 \in N_2$

Demostración.

1. Sean $h \in H$ y $n \in (H \cap N)$, dado entonces que $N \trianglelefteq G$, se tiene entonces $nhn^{-1} \in N$. Se verifica además la cerradura en H, es decir $nhn^{-1} \in H$. Por consiguiente $nhn^{-1} \in (H \cap N)$.
2. De la definición se sigue que $HN = NH$ y del teorema 1.1.12 se sigue $NH \leq G$.
3. Sean $g \in G$, $n_1 \in N_1$ y $n_2 \in N_2$. Entonces $gn_1n_2g^{-1} = (gn_1g^{-1})(gn_2g^{-1}) \in N_1N_2$.
4. Sea $g \in G$ y $n \in (N_1 \cap N_2)$. Dado que $N_1, N_2 \trianglelefteq G$, se tiene que $gng^{-1} \in N_1$ y $gng^{-1} \in N_2$. Por consiguiente $gng^{-1} \in (N_1 \cap N_2)$.
5. Sean $n_1 \in N_1$ y $n_2 \in N_2$. Entonces $n_1n_2n_1^{-1}n_2^{-1} = n_1(n_2n_1^{-1}n_2^{-1}) \in N_1$ y $n_1n_2n_1^{-1}n_2^{-1} = (n_1n_2n_1^{-1})n_2^{-1}) \in N_2$, lo que es igual $n_1n_2n_1^{-1}n_2^{-1} \in (N_1 \cap N_2)$. Se tiene entonces $n_1^{-1}n_2^{-1}n_1n_2 = 1$ se sigue entonces que $n_1n_2 = n_2n_1$.

Teorema. 1.2.13 *Sea G un grupo y $N \trianglelefteq G$. Entonces el conjunto G/N de las clases laterales izquierdas, $G/N := \{gN \mid g \in G\}$, es un grupo bajo la operación*

$$(gN)(hN) = ghN, \quad \forall g, h \in G.$$

Este grupo se llamara como grupo factor o grupo cociente de G módulo N. Si $|G : N|$ es finito, entonces $|G/N| = |G : N|$.

Demostración. Primero cabe demostrar que la operación esta bien definida, es decir que sea independiente de los representantes de la clase lateral.

Supóngase que $gN = uN$ y $hN = vN$. Decimos entonces que $ghN = uvN$ y por el lema 1.1.17 esto se resume a $gh(uv)^{-1} \in N$. Como $hN = vN$ se sabe que $hv^{-1} \in N$ y $gN = Ng$. Es decir $g(hv^{-1}) = ng$ para algun $n \in N$, entonces $gh(uv)^{-1} = ghv^{-1}u^{-1} = ngu^{-1}$. Como $gN = uN$ implica que $gu^{-1} \in N$, por lo tanto $ngu^{-1} \in N$. Esto prueba que la operación esta bien definida.

La asociatividad de en G/N es consecuencia de la asociatividad en G.

Sea $g \in G$, entonces $N(gN) = (eN)(gN) = (eg)N = gN$. Es decir que N es el módulo de G/N. Por otro lado $g^{-1}NgN = g^{-1}gN = N$, entonces un elemento gN tiene un inverso $g^{-1}N$.

[7] Ibid.

Si $N \trianglelefteq G$, entonces es usual el siguiente diagrama para visualizar G y G/N [8]

$$\begin{array}{c} G \\ \Big\| \Big\}_{G/N} \\ N \\ | \\ \{e\} \end{array}$$

Ejemplo. 1.2.14 *Sea $G = (\mathbb{Z}, +)$ y $N = n\mathbb{Z}$, con $n \in \mathbb{Z}$. Se sabe que G es un grupo abeliano, entonces se tiene $N \trianglelefteq G$. Podemos formar un grupo cociente $G/N = \mathbb{Z}/n\mathbb{Z}$, usualmente notado como $\mathbb{Z}_n$. Es decir que se tiene*

$$\mathbb{Z}_n = \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\}.$$

Note que cada elemento de $\mathbb{Z}_n$ coincide con una clase de equivalencia de la relación de congruencia módulo n. Se tiene entonces

$$\begin{aligned} i + n\mathbb{Z} = j + n\mathbb{Z} &\Leftrightarrow (i - j) + n\mathbb{Z} = n\mathbb{Z} \\ &\Leftrightarrow (i - j) \in n\mathbb{Z} \\ &\Leftrightarrow n \mid (i - j) \end{aligned}$$

Entonces el conjunto $T := \{0, 1, \ldots, n-1\}$ es un transversal de N en G. Es equivalente a decir,

$$\mathbb{Z}_n = \{i + n\mathbb{Z} \mid i = 0, 1, \ldots, n-1\}$$

y se tiene que $|G/N| = n$. Además,

$$(i + n\mathbb{Z}) + (j + n\mathbb{Z}) = \begin{cases} (i + j) + n\mathbb{Z} & si\ i + j < n \\ (i + j - n) + n\mathbb{Z} & si\ i + j \geq n \end{cases}$$

Teorema. 1.2.15 (Teorema de Isomorfía I) .

1. *Sean G y H grupos, y $\alpha : G \to H$. Entonces la función ρ definida por $\rho(gker(\alpha)) = \alpha(g)$ es un isomorfismo de $G/ker(\alpha)$ en $img(\alpha)$. Es decir*[9]*,*

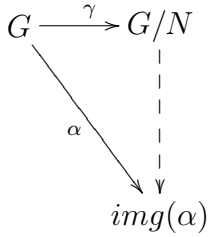
$$G/ker(\alpha) \cong img(\alpha)$$

2. *Reciprocamente, si G es un grupo y $N \trianglelefteq G$, entonces la función*

$$G \ni g \xrightarrow{\gamma} gN \in G/N,$$

[8] Ibid., p. 57.
[9] Ibid., p. 58.

es un epimorfismo y $ker(\gamma) = N$. Esta función γ se llamará epimorfismo canónico. Este teorema suele ilustrarse como se muestra



Demostración.

1. Del teorema 1.2.5(4) se tiene que $ker(\alpha) \trianglelefteq G$.

   a) ρ está bien definida: Sean $x, y \in G$.

$$\begin{aligned} x\mathbf{ker}(\alpha) = y\mathbf{ker}(\alpha) &\Leftrightarrow y^{-1}x \in \mathbf{ker}(\alpha) \\ &\Leftrightarrow \alpha(y^{-1}x) = 1 \\ &\Leftrightarrow \alpha(x) = \alpha(y) \\ &\Leftrightarrow \rho(x\mathbf{ker}(\alpha)) = \rho(y\mathbf{ker}(\alpha)) \end{aligned}$$

   b) Es claro que ρ es un epimorfismo.

   c) ρ es un monomorfiso: Sea $x \in G$.

$$\begin{aligned} x\mathbf{ker}(\alpha) \in \mathbf{ker}(\rho) &\Leftrightarrow \alpha(x) = 1 \\ &\Leftrightarrow x \in \mathbf{ker}(\alpha) \\ &\Leftrightarrow x\mathbf{ker}(\alpha) = \mathbf{ker}(\alpha) \end{aligned}$$

   Esto demuestra que $ker(\rho) = ker(\alpha) = \{e\}$.

2. Considerese ahora la función γ:

   a) γ es un homomorfismo: Sean $x, y \in G$. Entonces

$$\gamma(xy) = xyN = (xN)(yN) = \gamma(x)\gamma(y).$$

   b) Es claro que γ es un epimorfismo.

   c) γ es un monomorfismo: Sea $x \in G$.

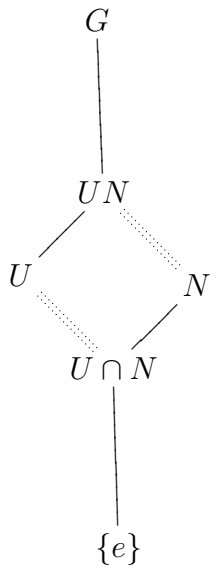
$$\begin{aligned} x \in ker(\gamma) &\Leftrightarrow \gamma(x) = 1 \\ &\Leftrightarrow xN = N \\ &\Leftrightarrow x \in N. \end{aligned}$$

   Entonces $ker(\gamma) = N$.

Teorema. 1.2.16 (Teorema de Isomorfía II) *Sea G un grupo y $N \trianglelefteq G, U \leq G$. Entonces*

$$UN/N \cong U(U \cap N).$$

Este teorema se ilustra de la siguiente forma:



Demostración. Del teorema 1.2.12 se tiene que $UN \trianglelefteq G$ y $(U \cap N) \trianglelefteq U$. Considerese la función φ definida de la siguiente manera:

$$U \ni u \xrightarrow{\varphi} uN \in UN/N.$$

1. La función φ esta bien definida, es decir, sean $u, v \in U$. Si $u = v$, entonces $v^{-1}u = 1 \in N$. Por lo tanto, $v^{-1}uN = N$. Entonces $vN = uN$.

2. Es claro que φ es un epimorfismo.

3. Sea $u \in U$. Entonces

$$\begin{aligned} u \in ker(\varphi) &\Leftrightarrow uN = N \\ &\Leftrightarrow uN = N \\ &\Leftrightarrow u \in N \\ &\Leftrightarrow u \in (U \cap N) \end{aligned}$$

   Esto demuestra que $ker(\varphi) = (U \cap N)$. A partir del primer teorema de isomorfía se tiene que

$$U/(U \cap N) = U/\mathbf{ker}(\varphi) \cong \mathbf{img}(\varphi) = UN/N.$$

1.3. Grupos Cíclicos

Definición. 1.3.1 *Sea $M \neq \emptyset$ un subconjunto de un grupo G. Se define $\langle M \rangle$, el subgrupo generado de M en G, como la intersección de todos los subgrupos de G que contienen*

a M. Es decir

$$\langle M\rangle = \bigcap_{M\subseteq U\leq G} U$$

Teorema. 1.3.2 *Sea G un grupo y $M \subseteq G$.*[10]

1. *Si $M \neq \emptyset$, entonces*

$$\langle M\rangle = \{x_1^{n_1}\cdots x_k^{n_k} \mid k \in \mathbb{N},\, x_i \in M,\, n_i \in \mathbb{Z},\, 1 \leq i \leq k\}.$$

   En otros palabras, $\langle M\rangle$ es el conjunto de todos los productos finitos de potencias que se pueden formar con elementos de M.

2. *Si G es abeliano y M es finito, Supóngase $M = x_1, \ldots, x_m$, entonces $\langle M\rangle$ es un grupo abeliano y*

$$\langle M\rangle = \{x_1^{n_1}\cdots x_m^{n_m} \mid n_1 \in \mathbb{Z},\, 1 \leq i \leq m\}.$$

   En particular, si $g \in G$ y $\langle M\rangle = \{g\}$, entonces $\langle M\rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Demostración.

1. Se define

$$U := \{x_1^{n_1}\cdots x_k^{n_k} \mid k \in \mathbb{N},\, x_i \in M,\, n_i \in \mathbb{Z},\, 1 \leq i \leq k\}.$$

   Primero se muestra que $M \subseteq U \leq G$, es decir, sea $x_1 \in M$, entonces $x_1 = x_1^1 \in U$. Esto demuestra $M \subseteq U$. Dado que U no es vacío, sean $x, y \in U$ y Supóngase $x = x_1^{n_1}\cdots x_r^{n_r}$ y $y = y_1^{n_1}\cdots y_s^{n_s}$. Entonces,

$$xy^{-1} = x = x_1^{n_1}\cdots x_r^{n_r} y = y_1^{-n_1}\cdots y_s^{-n_s} \in U,$$

   por lo tanto se demuestra que $U \leq G$, luego $\langle M\rangle \leq U$ se sigue por definición.

2. Se sigue de 1.

Definición. 1.3.3 *Un grupo se dice finitamente generedo, si $M \subseteq G$ finito, tal que $G = \langle M\rangle$. Si esto se cumple, entonces se llamará a M un sistema de generadores para G. Si $|G| = 1$ entonces G se denomina cíclico. Para simplificar la notación se escribirá como $G = \langle g\rangle$.*

Ejemplo. 1.3.4 *Un ejemplo de un grupo cíclico infinito es $(\mathbb{Z}, +)$. Con elementos generadores 1 o -1.*

Ejemplo. 1.3.5 *El grupo factor $\mathbb{Z}_n$ es generado por $1+n\mathbb{Z}$. Sin embargo los elementos de la forma $r + n\mathbb{Z}$, con $mcd(r, n) = 1$ es generardor de $\mathbb{Z}_n$.*

Lema. 1.3.6 *Sean G un grupo, $g \in G$ y $n \in \mathbb{N}$. Entonces*

[10] Ibid, p. 46.

1. *$o(g) = \infty$, si y solo si todas las potencias de g son distintas.*

2. *Si $o(g) = n$, entonces $g^m = e$ si y solo si $n \mid m$. Además $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$.*

3. *Si $o(g) = n$, entonces $o(g^k) = \frac{n}{mcd(n,k)}$.*[11]

Demostración.

1. Si todas las potencias de g son distintas, entonces $o(g) = |\langle g \rangle| = \infty$. Supóngase que no todas las potencias de g son distintas, entonces existen enteros positivos r y s tales que $g^r = g^s$. Podria asumirse que $r < s$. Ahora multiplicamos ambos lados de la ecuación anterior por $(g^{-1})^r$:

$$e = (g^{-1})^r(g^r) = g^{-1})^r(g^s) = g^{s-r}.$$

   Esto implica que existe un n, en este caso $s - r$ tal que $g^n = e$. Por el principio de buen ordenamiento, se escoje el menor n. Entonces se dice que

$$g, g^2, \ldots, g^n = e,$$

   son todos elementos distintos. Sino $g^r = g^s$, donde $e \leq r < s \leq n$, por el mismo argumento anterior $g^{s-1} = e$, pero esto es imposile puesto que $s - r < n$ porque n es mínimo.

2. Sea $g \in G$ y $o(g) = n$. Supóngase que $g^m = e$. Sea n un entero mínimo tal que $g^n = e$. Puesto que $n \leq m$, por el algoritmo de la división, se tiene que $m = qn+r$, donde $g \in \mathbb{N}$ y $0 \leq r \leq n$, entonces

$$e = g^m = g^{qn+r} = (g^n)^q g^r = g^r.$$

   Debido a que n se escojio como minimo, entonces $r = 0$, es decir $n|m$.

3. Claramente n divide a $\frac{nk}{mcd(n,k)}$. Entonces

$$e = g^{\frac{nk}{mcd(n,k)}} = (g^k)^{\frac{n}{mcd(n,k)}}.$$

   De 2. se sigue que $o(g^k)$ divide a $\frac{n}{mcd(n,k)}$. Si se define $t := o(g^k)$, entonces $(g^k)^t = e$. Esto es, $n|kt$ y es obvio que $\frac{n}{mcd(n,k)}$ divide a $\frac{kn}{mcd(n,k)}$. Entonces $\frac{n}{mcd(n,k)}$ divide a t. En conclusión $t = o(g^k) = \frac{n}{mcd(n,k)}$.

Teorema. 1.3.7 *Sea G un grupo cíclico.*

1. *Si $|G| = \infty$, entonces $G \cong \mathbb{Z}$.*

2. *Si $|G| = n$, entonces $G \cong \mathbb{Z}_n$.*

Demostración. Sea $G = \langle g \rangle$. Considerese la función $\varphi : \mathbb{Z} \to G$, definida como $\varphi(i) = g^i$, es claro que φ es un homomorfismo y además se verifica que es un epimorfismo.

[11] Ibid., p. 64.

1. Sea $|G| = \infty$. Si $i \in ker(\varphi)$, entonces $g^i = e$. Lo cual es solo valido para $i = 0$. Es claro entonces que $ker(\varphi) = e$, por lo tanto es inyectiva. En conclusión, φ es un isomorfismo.

2. Sea $|G| = n$. Entonces

$$\begin{aligned} i \in ker(\varphi) &\Leftrightarrow g^i = e \\ &\Leftrightarrow n|i \\ &\Leftrightarrow i \in n\mathbb{Z} \end{aligned}$$

   Por medio del primer teorema de isomorfía, se tiene que:

$$\mathbb{Z}_n = \mathbb{Z}/ker(\varphi) \cong img(\varphi) = G.$$

Capítulo 2

FUNDAMENTOS SOBRE CUERPOS FINITOS

2.1. Estructura del anillo conmutativo

Definición. 2.1.1 *Un anillo es un conjunto R no vacio con dos operaciones binarias, $+$ (adición) y $\cdot$ (multiplicación), notado como $(R, +, \cdot)$, con las siguientes propiedades. (Por simplificación el $\cdot$ para la multiplicación se omite.)*

1. *El conjunto R bajo la operación $+$ forma un grupo abeliano con 0 como elemento identidad.*

2. *La multiplicación es asociativa, esto es, para todo $a, b, c \in R$,*

$$(ab)c = a(bc).$$

3. *Ley distributiva, esto es, para todo $a, b, c \in R$,*

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc.$$

Los anillos conmutativos, que son el caso de interes para este documento, tienen la siguiente extra propiedad.

4. *La multiplicación es conmutativa, esto es, para todo $a, b \in R$,*

$$ab = bc;$$

Un anillo con unidad R tiene las propiedades 1-3, junto con la siguiente propiedad.

5. *Existe una identidad multiplicativa, esto es, existe un elemento $1 \in R$ tal que para todo $a \in R$,*

$$1a = a1;$$

Un anillo conmutativo con unidad, es decir que cumple las propiedades 1-5 de la definicón anterior se llama un dominio integral si satisface la siguiente propiedad.

6. *Cancelación, esto es, para todo* $a, b, c \in R$, *con* $c \neq 0$,

$$ca = cb \Rightarrow a = b.$$

Definición. 2.1.2 *Un anillo conmutativo con unidad, es decir que cumple las propiedades 1-5, se llama un dominio integral si satisface la siguiente propiedad.*

Ejemplo. 2.1.3 *El conjunto* $\mathbb{Z}$ *bajo las operaciones de adición y multiplicación usuales forma un anillo.*

2.1.1. El anillo $\mathbb{Z}_n$

Al definir sobre $\mathbb{Z}$ la relación

$$x \equiv y \text{ mód } n \quad n \in \mathbb{N}$$

se tiene una relación de equivalencia. El conjunto de todas las clases de equivalencia, notado por $\mathbb{Z}_n$, está dado por

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Note que

$$[k] = \{\ldots, k-2m, k-m, k, k+m, k+2m, \ldots\} \quad 0 \leq k \leq n$$

Definición. 2.1.4 *Se definen las siguientes operaciones sobre* $\mathbb{Z}_n$*:*

1. $[x] + [y] = [x + y]$
2. $[x][y] = [xy]$

Las operaciones anteriores estan bien definidas: supóngase $[x] = [x']$ y $[y] = [y']$, entonces $x \equiv x'$ mód n y $y \equiv y'$ mód n. Por lo tanto

$$x + y \equiv x' + y' \text{ mód } n.$$

Lo que significa que $[x + y] = [x' + y']$.

Por otro lado, $x \equiv x'$ mód n, si y solo si $x - x' = kn$, para algún $k \in \mathbb{Z}$ y $y \cong y'$ mód n, si y solo si $y - y' = sn$, para algún $s \in \mathbb{Z}$. Entonces $x = x' + kn$ y $y = y' + sn$. Por consiguiente $xy = x'y' + x'sn + y'kn + ksnn$. Lo cual demuestra que

$$xy \equiv x'y' \text{ mód } n$$

. Esto es $[xy] = [x'y']$.

Definición. 2.1.5 *Sea* $\mathbb{Z}_n$ *el conjunto de todas las clases de equivalencia módulo* n*, entonces* $(\mathbb{Z}_n, +, \cdot)$ *es un anillo conmutativo con unidad. Se tiene entonces,*

1. $[x] + [y] = [y] + [x]$

2. $([x]+[y])+[z]=[x]+([y]+[z])$

3. $[x]+[0]=[x]$ *(Existencia del módulo aditivo).*

4. $[x]-[y]=[0]$ *(Existencia de inversos aditivos).*

5. $[x][y]=[y][x]$

6. $([x][y])[z]=[x]([y][z])$

7. $[x]([y]+[z])=[x][y]+[x][z]$

8. $[x][1]=[x]$ *(Identidad multiplicativa).*

Todas estas propiedades se siguen de sus correspondientes en los enteros, además de que las operaciones estan bien definidas.

Lema. 2.1.6 *Sea p un número primo. Entonces todo elemento no nulo $[x]\in\mathbb{Z}_p$ es invertible, es decir, existe $[y]\in\mathbb{Z}_p$ tal que*

$$[x][y]=[1] \quad (xy\equiv 1 \text{ mód } p).$$

Demostración. Sea $[x]\in\mathbb{Z}_p$, $[x]\neq[0]$, entonces $mcd(x,p)=1$. Entonces existen $a,b\in\mathbb{Z}$ tal que $ax+bp=1$, por lo tanto

$$\begin{aligned}[a][x]+[b][p]&=[1]\\ [a][x]+[b][0]&=[1]\\ [a][x]&=[1]\end{aligned}$$

Definición. 2.1.7 *Sea K un anillo conmutativo con unidad. K se llama cuerpo si $K^\times=K\backslash\{0\}$, entonces $(K^\times,\cdot)$ es un grupo abeliano.*

Es claro que la definición anterior implica la existencia de inversos multiplicativos, esto es, para todo $0\neq a\in K$ existe $a^{-1}\in K$ tal que $aa^{-1}=1$. Es facil ver además que la propiedad 6. de la definición de anillo se sigue de la existencia de inversos pero no lo contrario.

Ejemplo. 2.1.8 *En conjunto de los números reales bajo la operación usual de adición y multiplicación es un cuerpo.*

Teorema. 2.1.9 *Sea n un entero positivo. El anillo $\mathbb{Z}_n$ es un cuerpo si y solo si n es primo.*

Demostración. supóngase que n no es primo. Entonces $n=rs$, donde $1<r<n$ y $1<s<n$. En $\mathbb{Z}_n$ se tiene $[r][s]=[0]$, entonces por definición, $\mathbb{Z}_n$ no puede ser un cuerpo. De la misma manera, supóngase ahora que n es primo, entonces se necesita establecer la existencia de inversos, lo cual se se sigue del lema 2.1.6

Este cuerpo se notará con $\mathbb{F}_p$. Otra notacion usual es $GF(p)$, Galois Field.

Definición. 2.1.10 *La característica de un cuerpo K se define como el entero más pequeño $n > 0$ tal que,*

$$n \cdot 1 = \overbrace{1 + 1 + \cdots + 1}^{n \text{ veces}} = 0,$$

si tal número no existe entonces es la característica es 0*.*

Teorema. 2.1.11 *La característica de un cuerpo es* 0 *o un número primo. La característica de un cuerpo finito es siempre un número primo.*

Demostración. supóngase que n no es un número primo y $char(K) = n$, digamos que $n = rs$, donde $r > 1$, $s > 1$. Aplicando la ley distributiva repetidas veces, se tiene

$$(r \cdot 1)(s \cdot 1) = \overbrace{(1 + 1 + \cdots + 1)}^{\text{r veces}}\overbrace{(1 + 1 + \cdots + 1)}^{\text{s veces}} = n \cdot 1 = 0.$$

Como K es un cuerpo se sigue que $r \cdot 1 = 0$ o $s \cdot 1 = 0$ (no hay divisores de cero). Lo cual contradice la minimalidad de n.

Ahora supóngase que K es finito. Entonces la suscesión

$$0, 1, 1 + 1, 1 + 1 + 1, \ldots$$

llegará a un punto en que se repita. Es decir

$$r \cdot 1 = s \cdot 1, \quad r < s.$$

Entonces, $(r \cdot s) \cdot 1 = 0$ y así se demuestra que K tiene característica finita.

Definición. 2.1.12 *Sea K un cuerpo y $F \subseteq K$. Se dice que F es un subcuerpo de K si y solo si:*

1. $0, 1 \in F$.
2. *Para todo $x, y \in F$ se tiene que $x + y$, $x - y$, $xy^{-1} (y \neq 0) \in F$*

Este hecho se notará como $F \leq K$.

Teorema. 2.1.13 *Sea K un cuerpo. Entonces K contiene un subcuerpo que está contenido en todo subcuerpo de K.*

Demostración. Si F_1, F_2 son subcuerpos de K, entonces $F_1 \cap F_2$ es un subcuerpo de K y esta contenido en F_1 y F_2. Entonces

$$P := \bigcap_{F \leq K} F$$

es un subcuerpo y está contenido en cualquier subcuerpo de K.

Definición. 2.1.14 *P es llamado el subcuerpo primo de K.*

Teorema. 2.1.15 *Si K en cuerpo y $char(K) = p$, entonces su subcuerpo primo $P \subset K$ es isomorfo a $\mathbb{Z}_p$. Es decir*

$$char(K) = p \quad \Rightarrow \quad P \cong \mathbb{Z}_p.$$

DEMOSTRACIÓN. Supongamos que $char(K) = p$ y se define la función

$$\varphi : \mathbb{Z}_p \to K.$$

φ es un homorfismo de cuerpos:

1. $\varphi([x] + [y]) = \varphi([x + y]) = (x + y) \cdot 1 = x \cdot 1 + y \cdot 1 = \varphi([x]) + \varphi([y])$.
2. $\varphi([x] \cdot [y]) = \varphi([xy]) = (xy) \cdot 1 = (x \cdot 1)(y \cdot 1) = \varphi([x])\varphi([y])$.
3. $\varphi([1]) = 1 \cdot 1 = 1$.

Supongamos que $\varphi([x]) = \varphi([y])$. Entonces

$$\begin{aligned} &\varphi([x]) - \varphi([y]) = 0 \\ \Leftrightarrow\ &\varphi([x - y]) = 0 \\ \Leftrightarrow\ &(x - y) \cdot 1 = 0 \end{aligned}$$

Dado que $0 \leq x - y < p$, se tiene que $x - y = 0 \Rightarrow x = y$ por lo tanto $[x] = [y]$. Entonces φ es un homomorfismo entre $\mathbb{Z}_p$ y $img(\varphi)$.

Pero cada subcuerpo de K contiene al elemento 1 y por lo tanto contiene a $r \cdot 1 = 1 + 1 + \cdots + 1$. Es decir, cada subcuerpo de K contiene a $img(\varphi) = \{r \cdot 1 \mid [r] \in \mathbb{Z}_p\}$. Entonces $P = img(\varphi) \cong \mathbb{Z}_p$. Finalmente, el isomorfismo φ es único, dado que

$$\begin{aligned} \varphi([1]) = 1 \Rightarrow \varphi([x]) &= \varphi([1] + \cdots + [1])) \\ &= \varphi([1]) + \cdots + \varphi([x]) \cdots + [1])) \\ &= 1 + \cdots + 1 \\ &= x \cdot 1 \end{aligned}$$

Corolario. 2.1.16 *$\mathbb{Z}_p$ es el único cuerpo con p elementos.*

2.2. Estructura de espacios vectoriales

Supóngase que K es un cuerpo finito con caracterícа p con un subcuerpo primo $P \cong \mathbb{Z}_p$. Entonces podemos dotar a K de la estructura de espacio vectorial sobre P.

Teorema. 2.2.1 *Sea K un cuerpo con $char(K) = p$. Entonces K tiene p^n elementos, para algún $n \in \mathbb{N}$. Es decir $|K| = p^n$.*[12]

[12]MURPHY, T. TRINITY COLLEGE Course 373 Finite Fields. `http://www.maths.tcd.ie/pub/Maths/Courseware/373-2000/FiniteFields.pdf`, p. 8, 30 de septiembre de 2008.

DEMOSTRACIÓN. supóngase que $dim_p K = n$. Entonces se puede encontrar una base $B = (e_1, \dots, e_n)$ de K sobre P. Todo elemento de K puede expresarse de una única manera, de la forma

$$x = \sum_{j=1}^{n} \lambda_j e_j, \quad \lambda_j \in P.$$

Para cada coordenada λ_j existen p posibilidades. Por lo tanto el número de elementos de K es

$$p \cdot p \cdots p = p^n.$$

Esto demuestra que todo cuerpo finito tiene como orden potencia de un primo.

Teorema. 2.2.2 *Sea K un cuerpo con $q = p^n$ elementos y sea $\mathbb{F}$ un subcuerpo de K. Entonces $\mathbb{F}$ tiene p^m elementos y se verifica además que $m \mid n$.*

DEMOSTRACIÓN. Considerese K como espacio vectorial sobre $\mathbb{F}$. Por medio del argumento del teorema anterior se tiene que

$$|K| = |\mathbb{F}|^d.$$

Si $|K| = p^n$, entonces se sigue que $|\mathbb{F}| = p^m$, con $n = md$.

2.3. Anillo de polinomios sobre un cuerpo finito

Sea K un cuerpo y se define

$$P(K) := \{(a_0, a_1, \dots) \mid a_j \in K,\ a_j \neq 0 \quad \text{para algún j finito}\}.$$

Sobre $P(K)$ se definen las siguientes operaciones:

1. Suma: $(a_0, a_1, \dots) + (b_0, b_1, \dots) := (a_0 + b_0, a_1 + b_1, \dots)$
2. Multiplicación por un escalar: $\lambda(a_0, a_1, \dots) := (\lambda a_0, \lambda a_1, \dots)$.

De esta forma $P(K)$ adquiere la estructura de espacio vectorial. Se define también una multiplicación sobre $P(K)$ de la siguiente forma:

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) := (c_0, c_1, \dots), \textit{ donde}$$

$$c_k = \sum_{i+j=k} a_i b_j = \sum_{j=0}^{k} a_j b_{k-j}, \quad a_j = 0,\ \forall j > m, \quad b_j = 0,\ \forall j > n.$$

Esta multiplicación es cerrada, esto es, si $k > m + n$, entonces $c_k = 0$.

1. $i > m$. Entonces $a_i = 0$, por lo tanto $a_i b_{k-i} = 0$.
2. $i \leq m$. Entonces $k - i > m + n - i \geq n$. Por lo tanto $b_{k-i} = 0$.

Dotada de esta multiplicación, se tiene que $P(K)$ adquiere la estructura de anillo conmutativo con elemento identidad $i = (1, 0, \dots, 0)$ y además

$$\lambda(fg) = (\lambda f)g = f(\lambda g) \quad f, g \in P(K), \lambda \in K.$$

Se define ahora $x = (0, 1, \dots)$ y $x^n = xx^{n-1}$ para $n \in \mathbb{N}$. Entonces

$$x^n = (0, \dots, 0, \overset{\downarrow}{1}, \dots)$$

Por inducción sobre n se tiene: $n = 0$, $X^0 = (1, 0, \dots)$ $n = 1$, $X^1 = (\delta_{01}, \delta_{11}, \delta_{21}, \dots) = (0, 1, \dots)$

supóngase que se cumple para

$$X^{n-1} = (\delta_{0,n-1}, \delta_{1,n-1}, \dots)$$

Entonces:

$$X^n = XX^{n-1} = (a_0, a_1, \dots) \text{ con}$$

$$a_k = \sum_{j=0}^{k} a_j c_{k-j}, \text{ donde } b_j = \delta_{j1} \text{ y } c_{k-j} = \delta_{k-j,n-1}$$

$$= \sum_{j=0}^{k} \delta_{j1}\delta_{k-j,n-1} = \delta_{11}\delta_{k-1,n-1} = \begin{cases} 1 & \text{si } k-1 = n-1 \\ 0 & \text{en otro caso} \end{cases}$$

Se tiene que

$$X^n = (0, \dots, 0, \overset{\downarrow}{1}, 0, \dots).$$

Con esta notación la suma y la multiplicación pueden escribirse de la siguiente manera:

$$\text{Suma: } \sum_{i=0}^{m} a_i X^i + \sum_{j=0}^{n} b_j X^j = \sum_{k=0}^{r} (a_k + b_k) X^k, \text{ donde } r = max\{m, n\}.$$

$$\text{Multiplicación: } \left(\sum_{i=0}^{m} a_i X^i\right)\left(\sum_{j=0}^{n} b_j X^j\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k.$$

Definición. 2.3.1 *$P(K) = K[X]$ se llamará el anillo de los polinomios en la indeterminada X. Los elementos de $K[X]$ se llamaran polinomios en X sobre K.*

Definición. 2.3.2 *Sea $f \in K[X]$, $f = \sum_{j=0}^{n} a_j X^j$. Si $a_n \neq 0$, entonces se define el grado de f, notado $grad(f)$, como el número n. Los elementos de K son polinomios constantes y serán de grado 0. Además se define el $grad(0) = -\infty$.*

Teorema. 2.3.3 *Sean $f, g \in K[X]$*

1. *$grad(f + g) \leq max\{graf(f), grad(g)\}$.*
2. *Si $grad(f) \neq grad(g)$, entonces $grad(f + g) = max\{graf(f), grad(g)\}$.*

3. $grad(fg) = grad(f) + grad(g)$.

DEMOSTRACIÓN. Sean $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j$, $grad(f) = m$, $grad(g) = n$.

1. $f + g = \sum_{k=0}^{r} (a_k + b_k) X^k$, con $r = max\{m, n\}$. Es claro que algunos de los a_k o b_k seran nulos. Se tiene entonces

$$grad(f + g) \leq r = max\{graf(f), grad(g)\}.$$

2. Si los grados de los polinomios son distintos entonces alguno es mayor que el otro, supóngase que $m > n$. Entonces

$$grad(f + g) = m = max\{graf(f), grad(g)\}.$$

3. supóngase $m, n \geq 0$. Entonces

$$fg = \sum_{k=0}^{m+n} c_k X^k, \text{ donde}$$

$$c_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i}.$$

Si $i < m$, entonces $b_{m+n-i} = 0$. Si $i > m$, entonces $a_i = 0$. Por lo tanto $c_{m+n} = a_m b_n$. Entonces $grad(fg) = m + n$.

Teorema. 2.3.4 (División con residuo) *Sean $f, g \in K[X]$, $g \neq 0$. Entonces existen polinomios únicos $q, r \in K[X]$ tal que $f = gq + r$ con $grad(r) < grad(g)$.*

DEMOSTRACIÓN.

1. Existencia: Si $f = 0$ el resultado es trivial, es decir $f = 0g + 0$. supóngase que $f \neq 0$. Si $grad(f) < grad(g)$, entonces tómese $q = 0$ y $r = f$. supóngase entonces que $grad(f) \geq grad(q)$ y sean

$$f = \sum_{i=0}^{m} a_i X^i, \quad g = \sum_{j=0}^{n} b_j X^j, \quad a_m, b_n \neq 0, \, m \geq n.$$

La prueba será por inducción sobre $grad(f) = m$. Si $m = 0$, entonces $f = a_0$, $g = b_0 \neq 0$ y

$$a_0 = \underbrace{(a_0 b_0^{-1})}_{=: \text{ q}} b_0 + \underbrace{0}_{=: \text{ r}}.$$

supóngase que el teorema se cumple para cualquier polinomio $h \in K[X]$ con $grad(h) < m$. Se define $h := f - a_m b_n^{-1} X^{m-n} g$. Es claro que $grad(h) < m$. Por la hipótesis de inducción se tiene que existen $q_1, r \in K[X]$ tal que

$$h = gq_1 + r \text{ y } grad(r) < grad(g).$$

Entonces

$$\begin{aligned} f &= h + a_m b_n^{-1} X^{m-n} g \\ &= gq_1 + r + a_m b_n^{-1} X^{m-n} g \\ &= g \underbrace{(q_1 + a_m b_n^{-1} X^{m-n})}_{=:\, q} + r \end{aligned}$$

2. Unicidad: supóngase que

$$f = gq + r = gq' + r', \text{ con } grad(r), grad(r') < grad(g).$$

Entonces $r - r' = (q' - q)g$, por lo tanto $grad((q' - q)g) = grad(r - r') < grad(g)$. Por el teorema 2.3.3 $grad(r - r') = max\{grad(r), grad(r')\} < grad(g)$, lo cual no puede suceder a menos que $q - q' = 0$. Entonces $q = q'$, como consecuencia $r = r'$.

Definición. 2.3.5 *Sea R un anillo conmutativo con unidad.*

1. *Sean $f, g \in R$, g se llama un divisor de f si existe $n \in R$ tal que $f = gh$. Se notara como $g|f$.*

2. *$f \in R$ se llama unidad, si $f|1$. Es decir, existe $e \in R$ tal que $fg = 1$.*

3. *$f \neq 0$ se denomina irreducible, si f no es una unidad y de $f = gh$ se sigue que g o h es una unidad. Si f no es irreducible entonces se llama reducible.*

Ejemplo. 2.3.6 *Sea $R = \mathbb{Z}$. Entonces $\{1, -1\}$ es el conjunto de las unidades y para $n \in \mathbb{Z}$, n es irreducible si y solo si n es un número primo.*

Ejemplo. 2.3.7 *Sea $R = K[X]$, las unidades de $K[X]$ son los polinomios constantes no nulos.*

Ejemplo. 2.3.8 *Sea $f = X^2 + 1 \in \mathbb{C}$. Entonces $f = (X - i)(X + i)$, por lo tanto es reducible.*

Ejemplo. 2.3.9 *Sea $f = X^2 + 1 \in \mathbb{R}[X]$. Entonces f es irreducible.*

Definición. 2.3.10 *Sea R un anillo conmutativo con unidad.*

1. *$\emptyset \neq I \subseteq R$ se llama un ideal de R si y solo si*

   a) *$x, y \in I$ entonces $x \pm y \in I$*

   b) *$x \in I$, $r \in R$ entonces $rx \in I$*

2. *I es un ideal de R si existe $r \in R$ tal que*

$$I = rR = \{x \in R\},$$

entonces I se denomina un ideal principal.

Si todos los ideales de R son principales, entonces R se llama un anillo de ideales principales.

Ejemplo. 2.3.11 *Sea $R = \mathbb{Z}$, entonces $I = nR$ es un ideal para $n \in \mathbb{N}$.*

Teorema. 2.3.12 *Si K es un cuerpo entonces $K[X]$ es anillo de ideales principales.*

DEMOSTRACIÓN. Sea I un ideal de $K[X]$.

1. Si $I = \{0\}$, entonces $I = 0K[X]$
2. Sea $I \neq \{0\}$ Se define $M := \{grad(f) | 0 \neq f \in I\}$. Es claro que $M \subseteq \mathbb{N}$ y además $M \neq \emptyset$. Por el principio de buen orden, M tiene un elemento mínimo n. Sea $g \in I$ con $grad(g) = n$ y sea $f \in I$ cualquiera. Entonces por el teorema de división con residuo se tiene que existen $q, r \in K[X]$ tal que

   $$f = gq + r, \text{ con } 0 \leq grad(r) < grad(g).$$

   Entonces

   $$r = f - gq \in I.$$

   De la elección de g se sigue que $r = 0$. Es decir $f = gq$ y así se demuestra que $f \in gK[X]$. Es decir $I \subseteq gK[X]$. Dado que $g \in I$, se sigue que $gK[X] \subseteq I$.

Lema. 2.3.13 *Sean $f, g \in K[X]$. Entonces son equivalentes*

1. *$f|g$*
2. *$gK[X] \subseteq fK[X]$*

DEMOSTRACIÓN.

1. Dado que $f|g$, entonces $\exists h \in K[X]$ tal que $g = fh$. Entonces

   $$gK[X] = fhK[X] \subseteq fK[X]$$

2. Teniendo como base la suposición $gK[X] \subseteq fK[X]$. Entonces

   $$g = g \cdot 1 \in gK[X] \subseteq fK[X].$$

   Es decir $g = fh$, para algún $h \in K[X]$.

Corolario. 2.3.14 *Se tiene que $f|g \wedge g|f$ si y solo si $fK[X] = gK[X]$, esto es $f = ag$ con $0 \neq a \in K$.*

DEMOSTRACIÓN.

1. Sea $f = ag$, con $0 \neq a \in K$. Entonces $g = a^{-1}f$.

2. Sea $fK[X] = gK[X]$. Entonces $g = fh \vee f = gk$ con $h, k \in K[X]$. Por lo tanto

$$\begin{aligned} g &= fh = gkh \\ &\Rightarrow g(1 - kh) = 0 \\ &\Rightarrow g = 0 \vee kh = 1. \end{aligned}$$

Si $g = 0$, entonces $f = 0$ y $f = ag \ \forall a \in K$.
Si $hk = 1$, entoncesg h y k son unidades, por lo tanto $f = gk$.

Definición. 2.3.15 *Sean $f_1, \ldots, f_n \in K[X]$, $d \in K[X]$ se denomina máximo común divisor de $f_1, \ldots, f_n$, notado como $mcd(f_1, \ldots, f_n)$, si y solo si*

1. *$d|f_j$ para todo $j = 1, \ldots, n$*
2. *Si $h \in K[X]$ y $h|f_j$, para todo $j = 1, \ldots, n$, entonces $h|d$.*

Teorema. 2.3.16 *Sean $f_1, \ldots, f_n \in K[X]$. Entonces*

1. *$d = mcd(f_1, \ldots, f_n)$ si y solo si $dK[X] = f$*
2. *Si d_1 y d_2 son mcd de $f_1, \ldots, f_n$, entonces $d_1 = ad_2$, con $a \in K$.*

Demostración.

1. *a)* Supongamos que $dK[X] = f_1K[X] + \cdots + f_nK[X]$. Es facil ver que para todo $j = 1, \ldots, n$ se verifica que $f_jK[X] \subseteq d$. Por el lema 2.3.13 se sigue

$$d|f_j \quad \forall j = 1, \ldots, n.$$

Sea $h \in K[X]$ tal que $h|f_j$ para todo $j = 1, \ldots, n$. Entonces

$$dK[X] = f_1K[X] + \cdots + f_nK[X] \subseteq hK[X].$$

Usando el lema 2.3.13 nuevamente se tiene que $h|d$, lo cual demuestra que $d = mcd(f_1, \ldots, f_n)$.

b) Sea $f = mcd(f_1, \ldots, f_n)$. Entonces $f|f_j$ para todo $j = 1, \ldots, n$, además se tiene que $f_jK[X] \subseteq fK[X] \ \forall j = 1, \ldots, n$. Entonces

$$\underbrace{f_1K[X] + \cdots + f_nK[X]}_{=:dK[X]} \subseteq fK[X].$$

Por la parte (a) se tiene

$$\left.\begin{array}{l} d = mcd(f_1, \ldots, f_n) \\ f = mcd(f_1, \ldots, f_n) \end{array}\right\} \Rightarrow f|d \wedge d|f.$$

2. Sean d_1, d_2 dos *mcd* de $f_1, \ldots, f_n$. Entonces $d_1 \mid d_2 \wedge d_2 \mid d_1$. Es decir $d_1K[X] = d_2K[X]$. El resto de la prueba se sigue del corooario 2.3.14.

Definición. 2.3.17 *Sean $f_1, \ldots, f_n \in K[X]$. Si $mcd(f_1, \ldots, f_n) = 1$, entonces se dice que $f_1, \ldots, f_n$ son primos relativos.*

2.4. Grupo multiplicativo de un cuerpo finito

Sea K un cuerpo. Se definio anteriormente el conjuno $K^\times$, el cual tiene orden $q-1$, si K tiene q elementos. Entonces del teorema de Lagrange se sigue que

$$a^{q-1} = 1 \quad \forall a \in K^{\mathrm{x}}.$$

Definición. 2.4.1 *Sea G un grupo. El exponente de G se define de la siguiente manera:*

$$e := Exp(G) := m.c.m\{o(g) \mid g \in G\}.$$

En palabras, el mínimo común multiplo de los órdenes de los elementos de G. Es decir, $Exp(G)$ es el número natural mas pequeño con la propiedad

$$x^e = 1 \quad \forall x \in G.$$

Lema. 2.4.2 *Sea $\mathbb{A}$ un grupo abeliano finito y sean $a, b \in \mathbb{A}$ tales que $o(a) = m$, $o(b) = n$ y $m.c.d(m,n) = 1$. Entonces $o(ab) = mn$.*

Demostración. supóngase que $o(ab) = d$. Dado que

$$(ab)^{mn} = (a^m)^n (b^n)^m = 1$$

se tiene que $d|mn$. Por otro lado, de $(ab)^{dn} = 1$, se sigue que $a^{nd} = 1$, pero $o(a) = m$, por lo tanto $m|nd$. Por hipótesis $m.c.d(m,n) = 1$, entonces $m|d$. De la misma manera se demuestra que $n|d$, entonces se sigue que $mn|d$. Es decit $mn = d = o(ab)$.

Lema. 2.4.3 *Sea $\mathbb{A}$ un grupo abeliano finito con exponente $Exp(\mathbb{A})$. Entonces existe $a \in \mathbb{A}$ tal que $o(a) = Exp(\mathbb{A})$.*

Demostración. supóngase que la descomposición en factores primos de $Exp(\mathbb{A})$ está dad por

$$Exp(\mathbb{A}) = p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r}.$$

De la definición de exponente se sigue que para cada $j = 1, \ldots, r$ existe $a_j \in \mathbb{A}$ tal que

$$p_j^{\varepsilon_j} \mid o(a_j)$$

ya que de lo contrario p_j apareceria como una potencia mucho menor en $Exp(\mathbb{A})$. Entonces $g_j := a_j^m$ tiene orden $p_j^{\varepsilon_j}$. Del lema anterior se tiene que

$$a := g_1 g_2 \cdots g_r$$

tiene orden $Exp(\mathbb{A})$.

Teorema. 2.4.4 *Sea K un cuerpo finito. Entonces el grupo multiplicativo $K^\times$ es cíclico.*

DEMOSTRACIÓN. supóngase que $Exp(K^\times) = m$ y $|K| = q$. Entonces cada uno de los elementos de $K^\times$ son ceros del polinomio

$$f(x) = X^m - 1$$

por lo tanto $q - 1 \leq m$, debido a que el número de raices de un polinomio es menor igual al grado. Dado que $m|q-1$, se concluye que $m = q - 1$. Entonces existe $\alpha \in K^\times$ cuyo orden es m. Este α genera a $K^\times$.

Definición. 2.4.5 *Sea K un cuerpo finito. Un generador de $K^\times$ se llama un elemento primitivo ó raiz primitiva de K.*[13]

Lema. 2.4.6 *1. Sea G un grupo, $g \in G$ y $o(g) = n$. Entonces*

$$o(g^k) = \frac{n}{mcd(n,k)}.$$

2. Sea $G = \langle g \rangle$ un grupo cíclico con $|G| = n$. Entonces los generadores de G son elementos de la forma g^k con $mcd(n,k) = 1$. Es decir, el número de generadores de un grupo cíclico de orden n es $\phi(n)$. En particular el número de raices primitivas de un cuerpo K, con orden q, es $\phi(q-1)$.

DEMOSTRACIÓN.

1. Es claro que $n \mid \frac{nk}{mcd(n,k)}$. Entonces

$$e = g^{\frac{nk}{mcd(n,k)}} = \left(g^k\right)^{\frac{n}{mcd(n,k)}}.$$

Es decir $o(g^k) \mid \frac{n}{mcd(n,k)}$. Se define $d := o(g^k)$. Entonces $(g^k)^d = e$, es decir $n|kd$ y es claro que $\frac{n}{mcd(n,k)} \mid \frac{kd}{mcd(n,k)}$. Como consecuencia de esto se tiene que $\frac{n}{mcd(n,k)} \mid d$, ya que

$$mcd\left(\frac{n}{mcd(n,k)}, \frac{k}{mcd(n,k)}\right) = 1.$$

Esto demuestra que $o(g^k) = d = \frac{n}{mcd(n,k)}$.

2.

$$\begin{aligned} G = \left\langle g^k \right\rangle &\Leftrightarrow o(g^k) = n \\ &\Leftrightarrow \frac{n}{mcd(n,k)} = n \\ &\Leftrightarrow mcd(n,k) = 1 \end{aligned}$$

Teorema. 2.4.7 .

1. Si $mcd(m,n) = 1$, entonces $\phi(mn) = \phi(m)\phi(n)$.

[13]Ibid., p. 18.

2. *Si p es un número primo, entonces $\phi(p^n) = p^{n-1}(p-1)$, $n \in \mathbb{N}$.*

3. *Si $n = p_1^{\varepsilon_1} \cdots p_t^{\varepsilon_t}$, entonces*

$$\phi(n) = \prod_{i=1}^{t} p_i^{\varepsilon_i - 1}(p_i - 1).$$

DEMOSTRACIÓN.

1. El teorema del residuo chino muestra que para $m, n \in \mathbb{N}$ con $mcd(m,n) = 1$, $\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$. En particular $\phi(mn) = |\mathbb{Z}_{mn}^{\times}| = |\mathbb{Z}_m^{\times}||\mathbb{Z}_n^{\times}| = \phi(m)\phi(n)$.

2. En el conjunto $\{k | 1 \leq k \leq p^n\}$ los números divisibles por p son de la forma lp con $l = 1, 2, \ldots, p^{n-1}$ por lo tanto $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

3. Se sigue de 2.

Teorema. 2.4.8 (Teorema de Euler) *Sea $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ con $mcd(n,a) = 1$. Entonces $a^{\phi(n)} \equiv 1$ mód n.*

DEMOSTRACIÓN. Es claro que para $n = 1$ se cumple. Supongamos entonces que $n > 1$. Dado que $mcd(n,a) = 1$ se tiene que $[a] \in \mathbb{Z}_n^{\times}$. Por otra parte $[1] = [a]^{|\mathbb{Z}_n^{\times}|} = [a]^{\phi(n)} = \left[a^{\phi(n)}\right]$. Esto demuestra que $a^{\phi(n)} \equiv 1$ mód n.

Teorema. 2.4.9 (Pequeño teorema de Fermat) *Sea p un número primo, $a \in \mathbb{Z}$ tal que $p \nmid a$. Entonces $a^{p-1} \equiv 1$ mód p.*

DEMOSTRACIÓN. Se sigue del Teorema de Euler.

Ejemplo. 2.4.10 *En este ejemplo se mostrará como determinar el número de raices primitiva en un cuerpo.*

Si $K = \mathbb{F}_{2^4}$, entonces el número de raices primitivas en K es $\phi(2^4 - 1) = \phi(15) = 8$, mientras que $\mathbb{F}_{2^5}$ tiene $\phi(31) = 30$. Si K es un cuerpo finito y $a \in K^{\times}$ es una raiz primitiva, entonces resulta facil obtener las otras ya que estas son potencias de

$$a^k \text{ con } mcd(k, q-1) = 1.$$

Considere el cuerpo $\mathbb{F}_7$. Se tiene que $2^3 = 8 \equiv 1$ mód 7, es decir que 2 tiene orden 3 y no es primitivo. Por otro lado 3 tiene orden $6 = q - 1$, por lo tanto es un elemento primitivo. Existen $\phi(6) = 2$ elementos primitivos los cuales son 3^k con $0 \leq k < 6$ y $mcd(k,6) = 1$. Por lo anterior se tiene que $k = 1, 5$, entonces los elementos primitivos son 3 y $3^5 = 5$.

2.5. Extensiones finitas de cuerpos

Definición. 2.5.1 *Sean K y L cuerpos. Se dice que L es una extensión de cuerpo, o simplemente extensión, de K si existe un homomorfismo de K a L. Tal extensión se notará con L/K, o en algunos casos como $L : K$.*[14]

L puede ser visto como un espacio vectorial sobre K, ya que los axiomas de los espacios vectoriales son consecuencia de los axiomas de cuerpo para L. Por lo tanto existe una base de L sobre K.

Ejemplo. 2.5.2 *Sea $\mathbb{R}$ el cuerpo de los numeros reales con las operaciones usuales. Es claro que $\mathbb{R}$ es una extensión de $\mathbb{Q}$. Se considera ahora $\sqrt{2} \in \mathbb{R}$ y un subconjunto de $\mathbb{R}$ con los elementos de la forma $a + \sqrt{2}b$ con $a, b \in \mathbb{Q}$. Si se toma $a + \sqrt{2}b$ y $a' + \sqrt{2}b'$*

$$(a + \sqrt{2}b) + (a' + \sqrt{2}b') = a + a' + \sqrt{2}(b + b')$$

y

$$(a + \sqrt{2}b) \times (a' + \sqrt{2}b') = aa' + 2bb' + \sqrt{2}(ab' + a'b),$$

es facil ver que se obtiene un cuerpo notado por $\mathbb{Q}(\sqrt{2})$, el cual es una extensión de $\mathbb{Q}$.

Definición. 2.5.3 *Sean L y L' dos extensiones de K y $\varphi : L \to L'$ un isomorfismo de cuerpos. Se dice que φ es un $K - isomorfismo$ si $\varphi(x) = x$ para todo $x \in K$.*

Definición. 2.5.4 *Si se considera a L como un $K-$espacio vectorial, se define la dimensión de L/K como el grado de L/K notado por $[L : K]$ o $grad(L/K)$. Si el grado de L/K es finito se dice que la extensión es finita.*

Teorema. 2.5.5 *Sean L/K, M/L extensiones de cuerpo. Entonces*

$$[M : L][L : K] = [M : K].$$[15]

Demostración. Sea $\{a_1, a_2, \ldots, a_r\}$ un subconjunto linealmente independiente de M/L, y sea $\{b_1, b_2, \ldots, b_s\}$ un subconjunto linealmente independiente de L/K. Se puede ver que

$$\{a_i b_j : i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, s\}$$

es un subconjunto linealmente independiente de M/K y además es una base. Entonces $[M : K] = rs = [M : L][L : K]$.

Definición. 2.5.6 *Si L es una extensión de K, entonces un elemento de L que sea raiz de un polinomio no nulo de K se dice algebraico sobre K.*

Definición. 2.5.7 *Si cada elemento de L es algebraico sobre K, se dice que L es una extensión algebraica de K.*

[14] AVANZI, R., COHEN, H., DOCHE, C., FREY, G., LANGE, T., NGUYEN, K., VERCAUTEREN, F. Handbook of Elliptic and Hyperelliptic Curve Cryptography, p. 25, 5 de Octubre de 2008.

[15] HOWIE, J. Fields and Galois Theory, p. 53, 5 de octubre de 2008.

Capítulo 3

CURVAS ELÍPTICAS

3.1. Curvas elípticas sobre cuerpos finitos

Una curva elíptica E sobre un cuerpo K se define con la ecuación de Weierstrass[16]

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1}$$

donde $a_1, a_2, a_3, a_4, a_6 \in K$ y $\triangle \neq 0$ donde $\triangle$ es el discriminante de E y se define como[17]

$$\begin{cases} \triangle = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 = a_1^2 + 4a_2 \\ d_4 = 2a_4 + a_1a_3 \\ d_6 = a_3^2 + 4a_6d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{cases}$$

Se exige que $\triangle \neq 0$ para garantizar la "suavidad" de la curva, esto es, garantizar la existencia de una sola tangente para cada punto sobre la curva. Sea L una extensión del cuerpo K, la curva E/K también se considera definida sobre L. El conjunto de puntos $L-$racionales de E son aquellos que satisfacen

$$E(L) = \{(x, y) \in L \times L | y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$$

donde ∞ es llamado el punto al infinito y se considera que satisface la ecuación de Weierstrass. ∞ se considera un punto $L-$racional para cualquier extensión L de K.[18]

Las curvas de interés para esta monografía son aquellas definidas sobre cuerpos de característica 2. Las curvas definidas sobre cuerpos binarios se clasifican como[19]

1. **No-Supersingulares:** La curva se define como

$$y^2 + xy = x^3 + ax^2 + b.$$

[16]WASHINGTON, L. Elliptic Curves: Number Theory and Cryptography, p. 10, 30 de octubre de 2008.

[17]HANKERSON, D, MENEZES, A, VANSTONE, S. Guide to Elliptic Curve Cryptography, p. 76, 8 de noviembre de 2008.

[18]CRUZ, J. Multiplicación Escalar en Curvas de Koblitz: Arquitectura en Hardware Reconfigurable. `http://delta.cs.cinvestav.mx/~francisco/tesis_JMCA.pdf`, p. 23, 10 de noviembre de 2008.

[19]Ibid., p. 24.

El discriminante $\triangle = b$.

2. **Supersingulares:** La curva se define como

$$y^2 + cy = x^3 + ax + b.$$

El discriminante $\triangle = c^4$.

3.2. Estructura de grupos

Definición. 3.2.1 *Sea $E(K)$ los puntos de una curva no-supersingular definidas sobre un cuerpo K. El número de puntos en la curva es llamado el orden del grupo y se notará como $\#E(K)$.*

Es posible construir un grupo abeliano a partir del conjunto de puntos y la definición de una operación de adición entre puntos. Dicha operación debe cumplir las leyes de conmutación, asociatividad, inverso aditivo, elemento identidad y cerradura.

La operación de adición se puede definir de una manera sencilla por medio de la geométria, en un principio sobre los números reales. Sean $P = (x_1, y_)), Q = (x_2, y_2) \in E$ con $P \neq Q$. Se define el punto R correspondiente a la suma entre P y Q como sigue, primero se dibuja una recta secante s a la curva E que interseca a P y Q. La recta s corta a la curva en un tercer punto, el cúal es notado como $-R$. Se obtiene el reflejo de $-R$ sobre el eje x y este cuarto punto se define como R, es decir, $R = P + Q$. Dicho proceso se muestra en figura 3.1.

El doblado de un punto se puede ver como la adición de un punto P consigo mismo, es decir $2P = R$. Al ser $Q = P$, la recta secante s se convierte en tangente a la curva sobre el punto P. La recta tangente corta la curva en un segundo punto $-R$. El reflejo de $-R$ sobre el eje x dará como resultado R.

El grupo abeliano del conjunto de puntos de una curva elíptica no-supersingular, con ecuación

$$y^2 + xy = x^3 + ax^2 + b$$

definida sobre $\mathbb{F}_{2^m}$ se define como sigue[21]

Definición. 3.2.2 .

1. ***Identidad:*** *$P + \infty = \infty + P = P$ para toda $P \in E(\mathbb{F}_{2^m})$.*

2. ***Inverso Aditivo:*** *Sea $P = (x, y) \in E(\mathbb{F}_{2^m})$, entonces $-P = (x, x + y)$ es el inverso de P.*

[20]HANKERSON, D, MENEZES, A, VANSTONE, S. Guide to Elliptic Curve Cryptography, p. 77, 12 de noviembre de 2008.

[21]CRUZ, J. Multiplicación Escalar en Curvas de Koblitz: Arquitectura en Hardware Reconfigurable. `http://delta.cs.cinvestav.mx/~francisco/tesis_JMCA.pdf`, p. 24, 12 de noviembre de 2008.

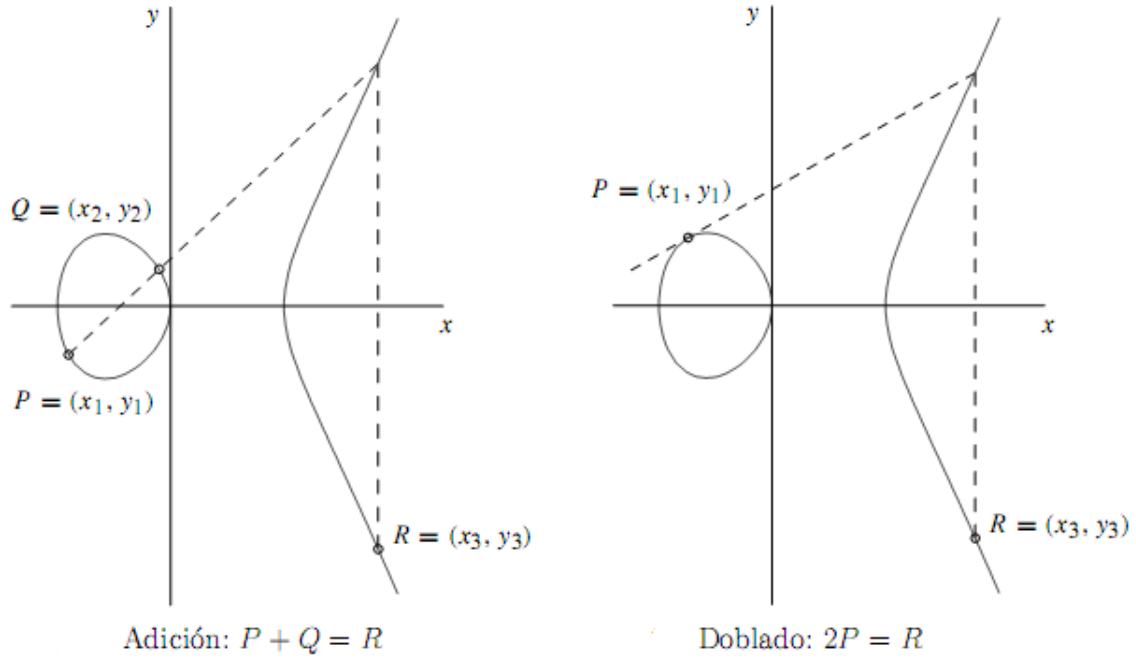


Figura 3.1: Suma y doble de un punto[20]

3. ***Adición entre puntos:*** *Sea* $P = (x_1, y_1) \in E(\mathbb{F}_{2^m}$ *y* $Q = (x_2, y_2) \in E(\mathbb{F}_{2^m}$, *donde* $P \neq \pm Q$. *Entonces* $P + Q = (x_3, y_3)$ *se define como*

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \tag{3.2}$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \tag{3.3}$$

donde $\lambda = \frac{y_1+y_2}{x_1+x_2}$.

4. ***Doblado de un punto:*** *Sea* $P = (x_1, y_1) \in E(\mathbb{F}_{2^m}$, *donde* $P \neq -P$. *Se define* $P + P = 2P = (x_3, y_3)$*como:*

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2} \tag{3.4}$$
$$y_3 = x_1^2 + x_3(\lambda + 1) \tag{3.5}$$

donde $\lambda = x_1 + \frac{y_1}{x_1}$

3.3. Endomorfismo de Frobenius

Una función que manda un elemento $x \in \mathbb{Z}$ y a su cuadrado $x^2 \in \mathbb{Z}$ es llamado endomorfismo de Frobenius y puede ser aplicado de forma directa a un punto elíptico.[22]

[22]CRUZ, J. Multiplicación Escalar en Curvas de Koblitz: Arquitectura en Hardware Reconfigurable. `http://delta.cs.cinvestav.mx/~francisco/tesis_JMCA.pdf`, p. 32, 10 de noviembre de 2008.

El endomorfismo de Frobenius se notará como ϕ_2, esto es

$$\phi_2(x, y) = (x^2, y^2).$$

Como se vera en el Capítulo 5, esta función es la base para que las curvas de Koblitz tengan una mayor eficiencia. Esta curvas satisfacen

$$(x^4, y^4) + 2(x, y) = \mu(x^2, y^2).$$

Donde $\mu = (-1)^{1-a}$. Esto se analizará con detalle en capítulos posteriores.

Capítulo 4

ARITMÉTICA DE CURVAS ELÍPTICAS SOBRE $\mathbb{F}_{2^m}$

La ecuación de una curva elíptica sobre un cuerpo binario $\mathbb{F}_{2^m}$ es $y^2 + xy = x^3 + ax^2 + b$, donde $b \neq 0$. Aquí los elementos del cuerpo finito son enteros con longitud a lo sumo de m bits. Estos números pueden ser considerados como un polinomio binario de grado $m - 1$. Los coeficientes de un polinomio binario pueden ser solamente 0 y 1. Todas las operaciones como la multiplicación, la suma, la resta y la división involucran polinomios de grado $m - 1$ o menos. El m es seleccionado de forma que genere una gran cantidad finita de puntos sobre la curva, con esto se logra un criptosistema seguro. SEC[23] especifica curvas con m entre $113 - 571$ bits.

4.1. Algoritmos para la suma y doble de un punto

4.1.1. Suma de puntos

Considírese dos puntos distintos J y K tales que $J = (x_J, y_J)$ y $K = (x_K, y_K)$. Sea $L = J + K$ donde $L = (x_L, y_L)$, estas son coordernadas afines, entonces

$$\begin{aligned} x_L &= \lambda^2 + s + x_J + x_K + a \\ y_L &= \lambda(x_J + x_L) + x_L + y_J \\ \lambda &= (y_J + y_K)/(x_J + x_K) \end{aligned}$$

λ es la pendiente de la línea que pasa por J y K. Si $K = -J$, por ejemplo $K = (x_J, x_J + y_J)$ entonces $J + K = \infty$. Donde ∞ es el punto al infinito. Si $K = J$ entonces $J + K = 2J$ para $2J$ se usa el doblado de punto. Note que $J + K = K + J$.

4.1.2. Resta de puntos

Considírese dos puntos distintos J y K tales que $J = (x_J, y_J)$ y $K = (x_K, y_K)$ entonces $J - K = J + (-K)$ donde $-K = (x_K, x_K + y_K)$. La resta de puntos se utiliza

[23]STANDARDS FOR EFFICIENT CRYPTOGRAPHY, para mayor información consultar `http://www.secg.org/collateral/sec1_final.pdf`

en algunas implementaciones de multiplicación de puntos como en τNAF.

4.1.3. Doblado de punto

Considírese el punto J tal que $J = (x_J, y_J)$ con $x_J \neq 0$. Sea $L = 2J$ donde $L = (x_L, y_L)$, entonces

$$\begin{aligned} x_L &= \lambda^2 + \lambda + a \\ y_L &= x_J^2 + (\lambda + 1)x_L \\ \lambda &= x_J + y_J/x_J \end{aligned}$$

donde λ es la tangente al punto J y a es un parámetro de la curva. Si $x_J = 0$ entonces $2J = \infty$, donde ∞ es el punto al infinito.

4.2. Parámetros de dominio

Además de los parámetros a y b de la curva, existen otros parámetros que deben ser convenidos por las entidades involucradas en un sistema seguro de comunicación usando la CCE. Estos son los parámetros de dominio.

4.2.1. Parámetros de dominio para curvas elípticas sobre $\mathbb{F}_{2^m}$

Los parámetros de dominio para las curvas elípticas definidas sobre $\mathbb{F}_{2^m}$ son m, $f(z)$, a, b, G, n y h.

Donde m es un entero definido para el cuerpo $\mathbb{F}_{2^m}$; los elementos del cuerpo $\mathbb{F}_{2^m}$ son eneros de longitud m bits. $f(z)$ es el polinomio irreducible de grado m usado para las operaciones de curva elíptica como se vera en capitulos posteriores, a y b son los parámetros que definen la curva $y^2+xy = x^3+ax^2+b$. G es el punto generador (x_G, y_G), un punto sobre la curva elíptica seleccionado para operaciones criptográficas. Para la multiplicación escalar kP se selecciona k entre 0 y $n-1$, donde n es el orden de la curva. Por ultimo h es el cofactor, donde $\#E(\mathbb{F}_{2^m}) = hn$ y $\#E(\mathbb{F}_{2^m})$ es el número de puntos sobre la curva elíptica.

4.3. Coordenadas

En esta sección se presentan otras coordenadas en las que es posible representar un punto en $\mathbb{F}_{2^m}$).

4.3.1. Coordenadas projectivas

Con coordenadas proyectivas la curva se parametriza con la ecuación[24]

$$Y^2 + XYZ = X^3 + aX^2Z + bZ^3.$$

[24] AVANZI, R., COHEN, H., DOCHE, C., FREY, G., LANGE, T., NGUYEN, K., VERCAUTEREN, F. Handbook of Elliptic and Hyperelliptic Curve Cryptography, p. 292, 30 de Octubre de 2008.

Donde $(X_1 : Y_1 : Z_1)$ representan el punto $(X_1/Z_1, Y_1/Z_1)$ con $Z_1 \neq 0$ y $\infty = (0 : 1 : 0)$. El opuesto a $(X_1 : Y_1 : Z_1)$ es $(X_1 : X_1 + Y_1 : Z_1)$.

Adición

Sea $P = (X_1 : Y_1 : Z_1), Q = (X_2 : Y_2 : Z_2)$ tal que $P \neq \pm Q$ entonces $P + Q = (X_3 : Y_3 : Z_3)$ esta dado por

$$\begin{array}{lll} A = Y_1Z_2 + Z_1Y_2, & B = X_1Z_2 + Z_1X_2, & C = B^2, \\ D = C^2, & E = (B^2 + BC + aD), & \\ X_3 = BE, & Y_3 = C(AX_1 + Y_1B)Z_2 + (A + B)E, & Z_3 = B^3D \end{array}$$

Doblar

Si $P = (X_1 : Y_1 : Z_1)$ entonces $2P = (X_3 : Y_3 : Z_3)$ esta dado por

$$\begin{array}{lll} A = X_1^2, & B = A + Y_1Z_1, & C = X_1Z_1, \\ D = C^2, & E = (B^2 + BC + aD), & \\ X_3 = CE, & Y_3 = (B + C)E + A^2C, & Z_3 = CD. \end{array}$$

4.3.2. Coordenadas jacobianas

En coordenadas jacobianas la curva esta dada por la ecuación[25]

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6.$$

Donde $(X_1 : Y_1 : Z_1)$ representan el punto $(X_1/Z_1^2, Y_1/Z_1^3)$ con $Z_1 \neq 0$ y $\infty = (1 : 1 : 0)$. El opuesto a $(X_1 : Y_1 : Z_1)$ es $(X_1 : X_1Z_1 + Y_1 : Z_1)$.

Adición

Sea $P = (X_1 : Y_1 : Z_1), Q = (X_2 : Y_2 : Z_2)$ tal que $P \neq \pm Q$ entonces $P + Q = (X_3 : Y_3 : Z_3)$ esta dado por

$$\begin{array}{lll} A = X_1Z_2^2, & B = X_2Z_1^2, & C = Y_1Z_2^3, \\ D = Y_2Z_1^3, & E = A + B, & F = C + D, \\ G = EZ_1, & H = FX_2 + GY_2, & Z_3 = GZ_2, \\ I = F + Z_3, & X_3 = aZ_3^2 + FI + E^3, & Y_3 = IX_3 + G^2H. \end{array}$$

Doblar

Si $P = (X_1 : Y_1 : Z_1)$ entonces $2P = (X_3 : Y_3 : Z_3)$ esta dado por

$$\begin{array}{lll} A = X_1^2, & B = A^2, & C = Z_1^2, \\ X_3 = B + bC^4, & Z_3 = X_1C, & Y_3 = BZ_3 + (A + Y_1Z_1 + Z_3)X_3. \end{array}$$

[25]Ibid.

4.3.3. Coordenadas López-Dahab

Estas coordenadas fueron introducidas por Julio López y Ricardo Dahab, en donde la curva esta dada por la ecuación[26]

$$Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4.$$

Donde $(X_1 : Y_1 : Z_1)$ representan el punto $(X_1/Z_1, Y_1/Z_1^2)$ con $Z_1 \neq 0$ y $\infty = (1 : 0 : 0)$. El opuesto a $(X_1 : Y_1 : Z_1)$ es $(X_1 : X_1Z_1 + Y_1 : Z_1)$

Adición

Sea $P = (X_1 : Y_1 : Z_1), Q = (X_2 : Y_2 : Z_2)$ tal que $P \neq \pm Q$ entonces $P + Q = (X_3 : Y_3 : Z_3)$ esta dado por

$$\begin{array}{lll} A = X_1Z_2, & B = X_2Z_1, & C = A^2, \\ D = B^2, & E = A + B, & F = C + D, \\ G = Y_1Z_2^2, & H = Y_2Z_1^2, & I = G + H, \\ J = IE, & & \\ Z_3 = FZ_1Z_2, & X_3 = A(H + D) + B(C + G), & Y^3 = (AJ + FG)F + (J + Z_3)X_3. \end{array}$$

Adición mixta

Si Q esta en coordenadas afines es posible lograr reducir el costo de esta operación, esta dada por

$$\begin{array}{lll} A = Y_1 + Y_2Z_1^2, & B = X_1 + X_2Z_1, & C = BZ_1, \\ Z_3 = C^2, & D = X_2Z_3, & X_3 = A^2 + C(A + B^2 + aC), \\ Y_3 = (D + X_3)(AC + Z_3) + (Y_2 + X_2)Z_3^2. & & \end{array}$$

Doblar

Si $P = (X_1 : Y_1 : Z_1)$ entonces $2P = (X_3 : Y_3 : Z_3)$

$$\begin{array}{lll} A = Z_1^2, & B = bA^2, & C = X_1^2, \\ Z_3 = AC, & X_3 = C^2 + B, & Y_3 = (Y_1^2 + aZ_3 + B)X_3 + Z_3B. \end{array}$$

Para un a y b dados es posible usar menos adiciones si $\sqrt{b}$ es precomputado y en la practica a se puede tomar en $\mathbb{F}_2$. Supóngase $a = 1$, se tiene

$$\begin{array}{lll} A = X_1^2, & B = \sqrt{b}Z_1^2, & C = X_1Z_1, \\ Z_3 = C^2, & X_3 = (A + B)^2, & Y_3 = (AC + (Y_1 + B)(A + B))^2. \end{array}$$

Ahora para $a = 0$, X_3 y Z_3 se definen igual pero $Y_3 = (BC + (Y_1 + B)(A + B))^2$

[26] Ibid., p. 293.

4.4. Compresión de puntos

Para algunas aplicaciones e ocaciones se desea transmitir la menor cantidad de bits posibles y aún así mantener la misma cantidad de información. La compresión de puntos es una técnica que reduce el espacio requerido para almacenar un punto de una curva elíptica.

Para una curva elíptica $E : y^2 + xy = x^3 + ax^2 + b$ existen a lo sumo dos puntos con la misma coordenada x, sean $P = (x_1, y_1)$ y $-P = (x_1, -y_1)$, los cuales son iguales si y solo si $y_1 = 0$. Para identificar el punto de una manera única se guarda x_1 y un bit $b(y_1)$.[27]

Compresión

Se escoje $b(y_1)$ como el bit menos significativo de y_1/x_1.

Decompresión

Sea $P = (x_1, b(y_1))$, entonces la ecuación cuadratica $y^2 + x_1 y = x_1^3 + ax_1^2 + b$ tiene dos soluciones. La solución existe si $Y^2 + Y + x_1 + a + \left(\frac{b}{x_1^2}\right)$ tiene solución, es decir

$$Tr\left(x_1 + a + \left(\frac{b}{x_1^2}\right)\right) = 0.$$

Se tiene que si y' es solución entonces $y' + 1$ también lo es. El bit $b(y_1)$ permite distinguir entre las soluciones. Una vez se tiene la solución, entonces $y_1 = y' x_1$.

[27] Ibid., p. 289.

Capítulo 5

ARITMÉTICA DE CURVAS ESPECIALES

5.1. Curvas de Koblitz binarias

Las curvas de Koblitz, también conocidas como curvas anomalas binarias, son curvas elípticas definidas sobre $\mathbb{F}_2$ y consideradas sobre la extension de campo $\mathbb{F}_{2^m}$. La ventaja de estas curvas consiste en que la multiplicación escalar se logra sin usar doblado de puntos.

Definición. 5.1.1 *Una curva de Koblitz esta dada por la ecuación*

$$E_a : y^2 + xy = x^3 + ax^2 + 1, \ \textit{con } a = 0 \, o \, 1. \tag{5.1}$$

Definición. 5.1.2 *Una curva de Koblitz E_a tiene un grupo de orden casi primo sobre $\mathbb{F}_{2^m}$ si $\#E_a(\mathbb{F}_{2^m}) = hn$ donde n es primo y*

$$h = \begin{cases} 4 & si \ a = 0 \\ 2 & si \ a = 1. \end{cases}$$

h es llamado cofactor.[28]

5.2. El anillo $\mathbb{Z}_{[\tau]}$

Dada una curva de Koblitz, el polinomio característica del endomorfismo de Frobenius es

$$\chi_a(T) = T^2 - \mu T + 2 \tag{5.2}$$

donde $\mu = (-1)^{1-a}$. Se sigue entonces que doblar un punto puede reemplzarse por computaciones que involucran el endomorfismo de Frobenius

$$\tau(\tau P) + 2P = \mu \tau P, \text{ para todo } P \in E_a. \tag{5.3}$$

[28]HANKERSON, D, MENEZES, A, VANSTONE, S. Guide to Elliptic Curve Cryptography, p. 114, 18 de noviembre de 2008.

Es decir que elevar al cuadrado puede verse como una multiplicación por el número complejo τ que satisfaga (5.3). Explicitamente se tiene que tal número es $\tau = \frac{\mu+\sqrt{-7}}{2}$.

Sea $\mathbb{Z}_{[\tau]}$ el anillo de polinomios en τ con coeficientes enteros. Al combinar el endomorfismo de frobenius con la multiplicación escalar, se pueden multiplicar puntos sobre E_a con un elemento del anillo $\mathbb{Z}_{[\tau]}$. Si $u_{l-1}\tau^{l-1}+\cdots+u_1\tau+u_0 \in \mathbb{Z}_{[\tau]}$ y $P \in E_a$, entonces

$$(u_{l-1}\tau^{l-1} + \cdots + u_1\tau + u_0)P = u_{l-1}\tau^{l-1}(P) + \cdots + u_1\tau(P) + u_0P.^{29} \tag{5.4}$$

La estrategia general para desarrollar un multiplicación escalar eficiente consiste en encontrar una expresión reducida de la forma $k = \sum_{i=0}^{l-1} u_i\tau^i$.

Definición. 5.2.1 *Todo elemento $\alpha \in \mathbb{Z}_{[\tau]}$ puede expresarse de forma canonica como $\alpha = a_0 + a_1\tau$ con $a_0, a_1 \in \mathbb{Z}_{[\tau]}$.*

Definición. 5.2.2 *Todo elemento $\alpha = a_0 + a_1 \in \mathbb{Z}_{[\tau]}$ se puede asociar con la norma de α, que es el producto de α con su conjugada compleja. Esto es*

$$N(a_0 + a_1\tau) = a_0^2 + \mu a_0 a_1 + 2a_1^2.$$

Teorema. 5.2.3 *Sean $\alpha, \beta \in \mathbb{Z}_{[\tau]}$. Las propiedades de la función norma son*[30]*:*

1. *$N(\alpha) \geq 0$ y la igualdad se cumple si y solo si $\alpha = 0$.*
2. *1 y -1 son los únicos elementos de $\mathbb{Z}_{[\tau]}$ que poseen norma 1.*
3. *$N(\tau) = 2$ y $N(\tau - 1) = h$.*
4. *$N(\tau^m - 1) = \#E_a(\mathbb{Z}_{2^m})$ y $N((\tau^m - 1)/(\tau - 1)) = n$.*
5. *La norma es una funcion multiplicativa, esto es $N(\alpha\beta) = N(\alpha)N(\beta)$.*
6. *$\mathbb{Z}_{[\tau]}$ es un dominio Euclidiano con respecto a la norma. Esto es, existen $\kappa, \rho \in \mathbb{Z}_{[\tau]}$ tal que $\alpha = \kappa\beta + \rho$ y $N(\rho) < N(\beta)$.*

Definición. 5.2.4 *La secuencia de Lucas es una secuencia de números asociada a un polinomio cuadratico usando la relación de recurrencia dada por*

$$L_{k+1} = \mu L_k - 2L_{k-1}, \quad k \geq 1. \tag{5.5}$$

Existen dos secuencias de Lucas que difieren de la inicialización de los dos primeros terminos de la secuencia usando la misma relación de recurrencia dada en (5.5). Se define

$$U_k, \text{ con } U_0 = 0, U_1 = 1 \tag{5.6}$$

y

$$V_k, \text{ con } V_0 = 2, V_1 = \mu. \tag{5.7}$$

[29]Ibid., p. 116.
[30]Ibid.

Al usar (5.5) se ve inmediatamente que[31]

$$\tau^k = -2U_{k-1} + U_k\tau \tag{5.8}$$

y

$$\tau^k + \bar{\tau}^k = -2V_{k-1} + V_k\tau. \tag{5.9}$$

La segunda secuencia permite computar la cardinaliad de $E_a(\mathbb{F}_{2^m})$ por medio de[32]

$$\begin{aligned} \#E_a(\mathbb{F}_{2^m}) &= (1-\tau^m)(1-\bar{\tau}^m) \\ &= 2^m + 1 - (\tau^m - \bar{\tau}^m) \\ &= 2^m + 1 + V_m. \end{aligned} \tag{5.10}$$

5.2.1. Expansión τ-adica

Por medio de (5.3) se tiene la relación $2 = \mu\tau - \tau^2$, es decir que se podrian encontrar expansiones similares para cada entero.

Definición. 5.2.5 *Al igual que las expansiones binarias, se define la expansión τ-adica no adjacente o τNAF para todo elemento distinto de* 0 $\alpha \in \mathbb{Z}_{[\tau]}$ *como*

$$\alpha = \sum_{i=0}^{l-1} u_i\tau^i$$

donde $u_i \in \{0, \pm 1\}$ y $u_i u_{i+1} = 0$ para todo i. Esta expansión se notará como $(u_{l-1} \dots u_0)_{\tau NAF}$ donde l es la longitud del τNAF.

Asi como cada número entero tiene una expansión binaria única así también poseen una única expansión τ-adica.

Lema. 5.2.6 *Sea $\alpha = a_0 + a_1\tau, \delta = d_0 + d_1\tau \in \mathbb{Z}_{[\tau]}$.*

1. *α es divisible por τ si y solo si r_0 es par.*
2. *α es divisible por τ^2 si y solo si $a_0 \equiv 2a_1$* mód 4.

Demostración.

1. De (5.3) se tiene que un múltiplo de τ tiene la forma

$$\beta\tau = (b_0 - b_1\tau)\tau = -2b_1 + (b_0 + \mu b_1)\tau.$$

Se sigue que si τ divide α entonces a_0 es par. Como consecuencia, si a_0 es par, entonces

$$\alpha/\tau = \frac{a_1 + \mu a_0}{2} - \frac{a_0}{2}\tau$$

es un elemento de $\mathbb{Z}_{[\tau]}$.

[31] AVANZI, R., COHEN, H., DOCHE, C., FREY, G., LANGE, T., NGUYEN, K., VERCAUTEREN, F. Handbook of Elliptic and Hyperelliptic Curve Cryptography, p. 357, 19 de noviembre de 2008.

[32] Ibid.

2. Considerese la identidad

$$\tau^2 = \mu\tau - 2.$$

Se sigue que cada múltiplo de τ^2 tiene la forma

$$\beta(\mu\tau - 2) = (b_0 + b_1\tau)(\mu\tau - 2) = -2(b_0 + \mu b_1) + (\mu b_0 - b_1)\tau.$$

Se verifica facilmente que los valores

$$\begin{aligned} a_0 &= -2(b_0 + \mu b_1) \\ a_1 &= \mu b_0 - b_1 \end{aligned}$$

satisfacen $a_0 \equiv 2a_1$ mód 4.

En base al lema anterior se presenta el algoritmo para calcular la expansión τ-adica de un elemento.[33]

Algoritmo 5.1 Representación τNAF

INPUT: $\alpha = a_0 + a_1\tau \in \mathbb{Z}_{[\tau]}$
OUTPUT: $\tau NAF(\alpha)$

```
1: S ← ()
2: while a_0 ≠ 0 o a_1 ≠ 0 do
3:    if a_0 ≡ 1 mód 2 then
4:       u ← 2 − ((a_0 − 2a_1) mód 4)
5:       a_0 = a_0 − u
6:    else
7:       u ← 0
8:    S ← u || S
9:    t ← a_0, a_0 ← a_1 + μa_0/2, a_1 ← −t/2
10: return S
```

La longuitud l del τNAF de $n \in \mathbb{Z}$ es aproximadamente $2\log n$.

Ejemplo. 5.2.7 *Sea $\mu = 1$ y $n = 409$. Usando el algoritmo 5.2.1 se obtiene*

$$409 = (\bar{1}00\bar{1}000010\bar{1}01001001)_{\tau NAF}.$$

Por medio del τNAF es posible construir un algoritmo de multiplicación escalar donde doblar un punto se reemplaza por una accion de frobenius.
Lo siguiente consiste en reducir la longitud del τNAF.

Lema. 5.2.8 *Sea $P \in E_a(\mathbb{F}_{2^m})$. Si*

$$\delta \equiv \rho \text{ mód } (\tau^m - 1)$$

entonces $\delta P = \rho P$, con $\delta, \rho \in \mathbb{Z}_{[\tau]}$.

[33]SOLINAS, J. Efficient Arithmetic on Koblitz Curves. Designs, Codes and Cryptography, 19,195-249 (2000), p. 208, 19 de noviembre de 2008.

Demostración. Se tiene que

$$(\tau^m - 1)(P) = \tau^m(P) - P = P - P = \infty.$$

supóngase ahora que $\delta \equiv \rho$ mód $(\tau^m - 1)$ entonces $\delta = \rho + \kappa(\tau^m - 1)$ para algún $\kappa \in \mathbb{Z}_{[\tau]}$, por lo tanto

$$\begin{aligned} \delta P &= \rho + \kappa(\tau^m - 1)P \\ &= \rho P + \kappa\infty \\ &= \rho P + \infty \\ &= \rho P \end{aligned}$$

De la definición 5.1.1 se sabe que $\#E_a(\mathbb{F}_{2^m}) = hn$ y por la propiedad 4 de la norma se tiene que el elemento $\delta = (\tau^m - 1)/(\tau - 1)$ tiene norma n.

Lema. 5.2.9 *Sea $P \in E_a(\mathbb{F}_{2^m})$ y $\delta = (\tau^m - 1)/(\tau - 1)$ entonces $\delta P = \infty$.*

Demostración. Existe un punto Q tal que $P = hQ$, lo cual se sigue de las propiedades de los grupos cíclicos finitos. Del lema 5.2.8 se sabe que $(\tau^m - 1)Q = \infty$, entonces

$$\begin{aligned} \infty &= \delta(\tau - 1)Q \\ &= \delta(\tau - 1)\overline{(\tau - 1)}Q \\ &= \delta N(\tau - 1)Q \\ &= \delta hQ \\ &= \delta P \end{aligned}$$

Teorema. 5.2.10 *Sea $P \in E_a(\mathbb{F}_{2^m})$ y $\delta = (\tau^m - 1)/(\tau - 1)$. Si $\gamma, \rho \in \mathbb{Z}_{[\tau]}$ y $\gamma \equiv \rho$ mód δ entonces*[34]

$$\gamma P = \rho P.$$

Demostración. Se sigue del lema 5.2.9 y se procede igual que en el lema 5.2.8.

Para poder lograr esta reducción el primer paso es encontrar δ. Sea $\delta = d_0 + d_1\tau$ entonces

$$\begin{aligned} d_1 &= -s_0 \\ d_0 &= s_0 - \mu d_1. \end{aligned}$$

Donde los enteros s_i se pueden identificar en terminos de la secuencia de Lucas U_k[35]

$$s_i = \frac{(-1)^i}{h}(1 - \mu U_{m+2-a-i}), \text{ con } i = 0, 1. \tag{5.11}$$

Del teorema 5.2.10 se tiene que $\gamma = \kappa\delta + \rho$ para algún $\kappa \in \mathbb{Z}_{[\tau]}$. Lo cual implica que para computar esta division con residuo se necesita la noción de redondeo.

[34] Ibid., p. 223.
[35] Ibid., p. 225.

Definición. 5.2.11 *Se define* $\lfloor\lambda\rceil = \lfloor\lambda +^1 /_2\rfloor$ *para algún* $\lambda \in \mathbb{Q}$.

De forma similar para $\lambda \in \mathbb{Q}(\tau)$, se necesita encontrar su vecino mas cercano en $\mathbb{Z}_{[\tau]}$. Se muestra el algoritmo para redondear un elemento $\lambda \in \mathbb{Q}(\tau)$.[36]

Algoritmo 5.2 Redondeo

INPUT: λ_0 y λ_1 determinando $\lambda = \lambda_0 + \lambda_1\tau \in \mathbb{Q}(\tau)$
OUTPUT: Enteros q_0 y q_1 tal que $q_0 + q_1\tau = \lfloor\lambda\rceil_\tau \in \mathbb{Z}_{[\tau]}$

$f_0 \leftarrow \lfloor\lambda_0\rceil$
$f_1 \leftarrow \lfloor\lambda_1\rceil$
$\eta_0 \leftarrow \lambda_0 - f_0$
$\eta_1 \leftarrow \lambda_1 - f_1$
$h_0 \leftarrow 0$
$h_1 \leftarrow 0$
$\eta \leftarrow 2\eta_0 + \mu\eta_1$
if $\eta \geq 1$ **then**
    if $\eta_0 - 3\mu\eta_1 < -1$ **then**
        $h_1 \leftarrow \mu$
    else
        $h_0 \leftarrow 1$
else
    if $\eta_0 + 4\mu\eta_1 \geq 2$ **then**
        $h_1 \leftarrow \mu$
if $\eta < -1$ **then**
    if $\eta_0 - 3\mu\eta_1 \geq 1$ **then**
        $h_1 \leftarrow -\mu$
    else
        $h_0 \leftarrow -1$
else
    if $\eta_0 + 4\mu\eta_1 < -2$ **then**
        $h_1 \leftarrow -\mu$
$q_0 \leftarrow f_0 + h_0$
$q_1 \leftarrow f_1 + h_1$
return (q_0, q_1)

Ejemplo. 5.2.12 *Sea* $\lambda = -18{,}5\overline{909} + 9{,}29\overline{54}\tau$ *entonces* $\lfloor\lambda\rceil_\tau = -19 + 9\tau$.

Al tener el algoritmo 5.2.1 se presenta el algoritmo para la reducción módulo δ según el teorema 5.2.10 y $\delta = (\tau^m - 1)/(\tau - 1) = d_0 + d_1\tau$ determinada por los parámetros dados en 5.11.[37]

[36] Ibid., p. 219.
[37] Ibid., p. 225.

Algoritmo 5.3 Reducción módulo $(\tau^m - 1)/(\tau - 1)$

INPUT: Entero $k \in [1, n-1]$ donde $n = N((\tau^m - 1)/(\tau - 1))$
OUTPUT: El elemento $\rho = r_0 + r_1\tau \equiv \text{mód}\delta$

1: $d_0 \leftarrow s_0 + \mu s_1$
2: $\lambda_0 \leftarrow s_0 k/n$
3: $\lambda_1 \leftarrow s_1 k/n$
4: $(q_0, q_1) \leftarrow \lfloor \lambda_0 + \lambda_1 \tau \rceil_\tau$
5: $r_0 \leftarrow k - d_0 q_0 - 2 s_1 q_1$
6: $r_1 \leftarrow s_1 q_0 - s_0 q_1$
7: $\eta \leftarrow 2\eta_0 + \mu\eta_1$
8: **return** $r_0 + r_1\tau$

5.3. Multiplicación escalar utilizando endomorfismos

Con las ideas de las secciones anteriores es posible construir un metodo eficiente para la multiplicación de puntos.[38]

Algoritmo 5.4 Multiplicación escalar con τNAF

INPUT: Entero k, $P \in E_a(\mathbb{F}_{2^m})$
OUTPUT: $Q = kP$

1: $r_0 + r_1\tau = \rho \leftarrow k \bmod \delta$
2: $Q \leftarrow \infty$, $R \leftarrow P$
3: **while** $r_0 \neq 0$ o $r_1 \neq 0$ **do**
4: **if** $r_0 \equiv 1 \bmod 2$ **then**
5: $u \leftarrow 2 - ((r_0 - 2r_1) \bmod 4)$
6: **else**
7: $u \leftarrow 0$
8: $r_0 \leftarrow r_0 - u$
9: **if** $u = 1$ **then**
10: $Q \leftarrow Q + R$
11: **if** $u = -1$ **then**
12: $Q \leftarrow Q - R$
13: $R \leftarrow \tau R$
14: $t \leftarrow r_0$, $r_0 \leftarrow r_1 + \mu r_0/2$, $r_1 \leftarrow -t/2$
15: **return** Q

5.4. Reducción a la mitad (Point Halving)

Sea $E(\mathbb{F}_{2^m})$ una curva elíptica definida por la ecuación

$$E : y^2 + xy = x^3 + ax^2 + b, \text{ con } a, b \in \mathbb{F}_{2^m}.$$

[38] Ibid., p. 227.

Sea $P = (x, y) \in E$ con $P \neq -P$. Las coordenadas afines de $Q = 2P = (u, v)$ se pueden computar como sigue

$$\lambda = x + x/y \tag{5.12}$$
$$u = \lambda^2 + \lambda + a \tag{5.13}$$
$$v = x^2 + u(\lambda + 1) \tag{5.14}$$

Reducir un punto a la mitad significa, dado P encontrar un punto Q tal que $Q = 2P$. Esta operación es la inversa a doblar un punto, la idea básica esta en resolver 5.12 para λ, luego 5.13 y 5.14 para x e y.[39] Sea G un subgrupo de orden impar n en E, entonces las funciones de doblar un punto y reducirlo a la mitad son automorfismos de G.

Definición. 5.4.1 *La función Traza sobre $\mathbb{F}_{2^m}$ está definida por $Tr(c) = c + c^2 + c^{2^2} + \cdots + c^{2^{m-1}}$.*

Lema. 5.4.2 *Sean $c, d \in \mathbb{F}_{2^m}$.*[40]

1. *$Tr(c) = Tr(c^2) = Tr(c)^2$, en particular, $Tr(c) \in \{0, 1\}$.*
2. *$Tr(c + d) = Tr(c) + Tr(d)$.*

El primer paso en la reducción a la mitad consiste en encontrar $\lambda = x + y/x$ al resolver 5.13.

Teorema. 5.4.3 *Sea $P = (x, y), Q = (u, v) \in G$ tal que $Q = 2P$ y sea $\lambda = x + x/y$. Sea γ una solución de $\gamma^2 + \gamma = u + a$, y $t = v + u\gamma$. supóngase que $Tr(a) = 1$. Entonces $\gamma = \lambda$ si y solo si $Tr(t) = 0$.*[41]

Demostración. De 5.14 se tiene que $x^2 = v + u(\lambda + 1)$. Del lema 5.4.2 se sigue que $Tr(x) = Tr(a)$ con $P = (x, y) \in G$. Entonces

$$Tr(v + u(\lambda + 1)) = Tr(x^2) = Tr(x) = Tr(a) = 1.$$

Se tiene que si $\gamma = \lambda + 1$, entonces $Tr(t) = Tr(v + u(\lambda + 1)) = 1$. De otra forma se debe tener $\gamma = \lambda$, lo cual lleva a $Tr(t) = Tr(v + u\lambda) = Tr(v + u((\lambda + 1) + 1))$. Como la función traza es lineal,

$$Tr(v + u((\lambda + 1) + 1)) = Tr(v + u(\lambda + 1)) + Tr(u) = 1 + Tr(u) = 0.$$

Esto concluye que $\gamma = \lambda$ si y solo si $Tr(t) = 0$.
En base a estas observaciones se presenta el algoritmo de reducción a la mitad.[42]

[39] HANKERSON, D, MENEZES, A, VANSTONE, S. Guide to Elliptic Curve Cryptography, p. 130, 20 de noviembre de 2008.
[40] Ibid.
[41] Ibid., p. 131.
[42] Ibid.

Algoritmo 5.5 Reducción a la mitad (Point halving)

INPUT: $Q = (u, v) \in G$ en coordenadas afin.
OUTPUT: Representación (x, λ_P) de $P = (x, y) \in G$, donde $Q = 2P$

1: Encontrar la solución γ de $\gamma^2 + \gamma = u + a$
2: $t \leftarrow v + u\gamma$
3: **if** $Tr(t) = 0$ **then**
4: $\quad x = \sqrt{t + u}$, $\lambda_P = \gamma$
5: **else**
6: $\quad \lambda_P \leftarrow \gamma + 1$, $x \leftarrow \sqrt{t}$
7: **return** (x, λ_P)

Se presentara ahora un algoritmo para resolver la equación cuadartica del algoritmo anterior en la linea 1.

Definición. 5.4.4 *Sea m un entero impar. Se define la función media-traza $H : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$, como*

$$H(c) = \sum_{i=0}^{(m-1)/2} c^{2^{2i}}.$$

Lema. 5.4.5 *Sean $c, d \in \mathbb{F}_{2^m}$.*

1. *$H(c + d) = H(c) + H(d)$.*
2. *$H(c)$ es una solución de la ecuación $x^2 + x = c + Tr(c)$.*
3. *$H(c) = H(c^2) + c + Tr(c)$.*

Sea $f(z)$ el polinomio irreducible de un cuerpo dado, entonces note que para i par,

$$H(z^i) = H(z^{i/2}) + z^{i/2} + Tr(z^i).$$

En base a esta observación se muestra el algoritmo para resolver la ecuación cuadratica en 5.4.

Algoritmo 5.6 Resolver $x^2 + x = c$

INPUT: $c = \sum_{i=0}^{m-1} c_i z_i \in \mathbb{F}_{2^m}$, con $c_i \in \{0, 1\}$, donde m es impar y $Tr(c) = 0$.
OUTPUT: Una solución s de la ecuación $x^2 + x = c$.

1: Precomputar $H(z^i)$ para i impar, $1 \leq i \leq m - 2$.
2: $s \leftarrow 0$
3: **for** $i = (m - 1)/2$ downto 1 **do**
4: $\quad$ **if** $c_{2i} = 1$ **then**
5: $\quad\quad c \leftarrow c + z^i$
6: $\quad\quad s \leftarrow s + z^i$
7: $s \leftarrow s + \sum_{i=1}^{(m-1)/2} c_{2i-1} H(z^{2i-1})$
8: **return** s

Es posible mejorar el algoritmo anterior usando el lema 5.4.5 junto con el polinomio de reducción $f(z)$. Sea i impar, se define j y s como

$$m \leq 2_i^j = m + s < 2m.$$

La idea es aplicar el lema 5.4.5 j veces, se obtiene[43]

$$H(z^i) = H(z^{2_i^j}) + z^{2^{j-1}{}_i} + \cdots + z^{4i} + z^{2i} + z^i + jTr(z^i).$$

Sea $f(z) = z^m + r(z)$, donde $r(z) = z^{b_l} + \cdots + z^{b_1} + 1$ y $0 < b_1 < \cdots < b_l < m$. Entonces

$$H(z^{2_i^j}) = H(z^s r(z)) = H(z^{s+b_l}) + H(z^{s+b_{l-1}}) + \cdots + H(z^{s+b_1}) + H(z^s).$$

Algoritmo 5.7 Resolver $x^2 + x = c$

INPUT: $c = \sum_{i=0}^{m-1} c_i z_i \in \mathbb{F}_{2^m}$, con $c_i \in \{0, 1\}$, donde m es impar y $Tr(c) = 0$, y polinomio de reducción $f(z) = z^m + r(z)$.

OUTPUT: Una solución s de la ecuación $x^2 + x = c$.

1: Precomputar $H(z^i)$ para $i \in I_0 \cup I_1$, donde son los números impares en $[1, (m-1/2)]$ y $[m - grad(r), m - 2]$ respectivamente.
2: $s \leftarrow 0$
3: **for all** i impar $\in ((m-1)/2, m - grad(r))$ en orden decresiente **do**
4: **if** $c_i = 1$ **then**
5: $c \leftarrow c + z^{2i-m+b_l} + \cdots + z^{2i-m}$
6: $s \leftarrow s + z^i$
7: **for** $i = (m-1)/2$ downto 1 **do**
8: **if** $c_{2i} = 1$ **then**
9: $c \leftarrow c + z^i$
10: $s \leftarrow s + z^i$
11: $s \leftarrow s + \sum_{i \in I_0 \cup I_1} c_i H(z^i)$
12: **return** s

5.4.1. Multiplicación de puntos usando reducción a la mitad

Sea $P = (x, y) \in G$ de orden n, k un entero tal que $0 \leq k < n$ y $t = \lceil \log_2 n \rceil$. Dependiendo de la aplicación, puede ser necesario convertir k para usarlo en los metodos de reducción a la mitad. Sea k' como sigue

$$k \equiv k'_{t-1}/2^{t-1} + \cdots + k'_2/2^2 + k'_1/2 + k'_0 \text{ mód } n \tag{5.15}$$

entonces $kP = \sum_{i=0}^{t-1} k'_i/2^i P$, esto es, $(k'_{t-1}, \ldots, k'_0)$ se usa en los metodos basados en reducción a la mitad. Al igual que el τNAF, existen representaciones no adjacentes de k, es decir $NAF(k) = \sum_{i=0}^{l-1} k_i 2^i$ [44] con $k_i \in \{0, \pm 1\}$, con la propiedad de que dos

[43] Ibid., p. 133.
[44] Ibid., p. 137.

coeficientes k_i son distintos de cero. La forma con ventana $wNAF$ es una generalización, donde cada coeficiente k_i distinto de cero es impar, es decir $|k_i| < 2^{w-1}$ y a lo sumo uno de los w digitos consecutivos es distinto de cero. La representación NAF tiene las siguiente propiedades[45]

1. La representación $wNAF(k)$ es única.
2. $NAF_2(k) = NAF(k)$
3. La longitud de $wNAF(k)$ es a lo sumo uno mas que la longitud de la representación binaria de k.

Lema. 5.4.6 *Sea* $\sum_{i=0}^{t} k_i' 2^i$ *con* $t = \lceil \log_2 n \rceil$, *la representación* $wNAF$ *de* $2^{t-1}k$ mód n. *Entonces*

$$k \equiv \sum_{i=0}^{t-1} \frac{k'_{t-1-i}}{2^i} + 2k'_t \text{ mód } n.$$

Donde n *es como en 5.15.*

Demostración. Se tiene que $2^{t-1}k \equiv \sum_{i=0}^{t} k_i' 2^i$ mód n. Dado que n es primo la congruencia se puede dividir por 2^{t-1} para obtener

$$k \equiv \sum_{i=0}^{t} \frac{k'_i}{2^{t-1-i}} \equiv \sum_{i=0}^{t-1} \frac{k'_{t-1-i}}{2^i} + 2k'_t \text{ mód } n.$$

Se presenta el algoritmo para la multiplicación de puntos usando reducción a la mitad con parametro de entrada $wNAF(2^{t-1}k \text{ mód } n)$.[46]

Algoritmo 5.8 Multiplicación escalar con reducción a la mitad

INPUT: Tamaño de la ventana w, $wNAF(2^{t-1}k \text{ mód } n) = \sum_{i=0}^{t} k_i' 2^i$, $P \in G$.
OUTPUT: kP (Nota: $k = k_0'/2^{t-1} + \cdots + k'_{t-2}/2 + k'_{t-1} + 2k'_t$ mód n)

1: $Q \leftarrow \infty$ para $i \in I = \{1, 3, \ldots, 2^{w-1} - 1\}$
2: **if** $k'_t = 1$ **then**
3: $\quad Q_1 = 2P$
4: **for** $i = t - 1$ donwto 0 **do**
5: $\quad$ **if** $k'_i > 0$ **then**
6: $\quad\quad Q_{k'_i} \leftarrow Q_{k'_i} + P$
7: $\quad$ **if** $k'_i < 0$ **then**
8: $\quad\quad Q_{-k'_i} \leftarrow Q_{-k'_i} - P$
9: $\quad P \leftarrow Pfrm{-}e$
10: $Q \leftarrow \sum_{i \in I} iQ_i$
11: **return** Q

[45]FONG, K., HANKERSON, D., LÓPEZ, J., MENEZES, A. Field Inversion and Point Halving Revisited. Technical Report CORR 2003 - 18, p. 13, 22 de noviembre de 2008.

[46]HANKERSON, D, MENEZES, A, VANSTONE, S. Guide to Elliptic Curve Cryptography, p. 138, 22 de noviembre de 2008.

Capítulo 6

CRIPTOGRAFÍA DE CURVAS ELÍPTICAS

6.1. Fundamentos de criptografía de clave publica

La criptografía de clave publica también conocida como criptografía asimétrica surge como una solución al problema del intercambio de claves privadas sobre un canal inseguro, sin duda este es un problema de especial relevancia para los sistemas criptográficos en una red, ya que toda la seguridad de dicho sistema depende de la clave la cual se utiliza tanto para cifrar como para descifrar. El tamaño de las redes modernas presenta un problema insuperable a la hora de mantener las llaves privadas se requieren $n(n-1)/2$ claves distintas, donde n es el número de usuarios en una red, así cada mensaje requiere un nuevo intercambio de clave, lo que genera un retraso.

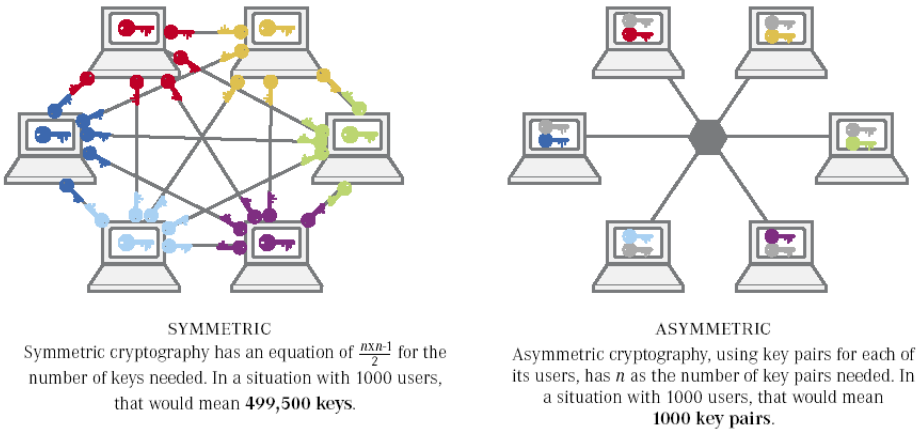


Figura 6.1: Criptografía asimétrica vs Criptografía de llave publica.[47]

Fue en 1976 cuando William Diffie y Martin Hellman propusieron un novedoso sistema de encriptación en el que se empleaban diferentes claves para el cifrado y el descifra-

[47]Tomado de `http://www.deviceforge.com/files/misc/symmetric_vs_asymmetric_crypto.gif`, 29 de noviembre de 2008.

do[48] evitando por completo el intercambio de claves, a su vez estas claves se encuentran relacionadas mediante un determinado algoritmo o función matemática unidireccional.

Cada usuario de una red de comunicación suministra su clave pública B y la correspondiente función de cifrado e_B a su vez cada función de descifrado d_B se conserva secreta y, además, esta no puede ser calculada a partir de e_B por otra persona, en un tiempo computacionalmente razonable.

Alice y Bob son dos usuarios de una red, utlizando criptografía de llave pública Alice desea enviar un mensaje x a Bob, ella utiliza la función de cifrado e_B de Bob y envía $e_B(x)$. Bob que posee d_B puede luego calcular $d_B(e_B(x)) = x$.

Formalmente hablando un sistema criptográfico de llave pública es:

Definición. 6.1.1 *Sean X y Y conjuntos. Una función inyectiva $f : X \to Y$ se denomina una función de una vía (one way function), si f es fácil de calcular, pero su función inversa $f^{-1} : Img(f) \to X$, sin información adicional, no puede calcularse en un tiempo justificable.*

Una función de una vía se llama una trampa (trap door) si $f^{-1} : Img(f) \to X$ puede ser calculada eficientemente conociendo alguna información adicional.

El concepto de función de una vía puede formalizarse de manera exacta utilizando teoría de la complejidad y máquinas de Turing.[49]

Definición. 6.1.2 *Un criptosistema K se denomina un criptosistema de clave pública, si todas las funciones de cifrado e_K son funciones trampas.*

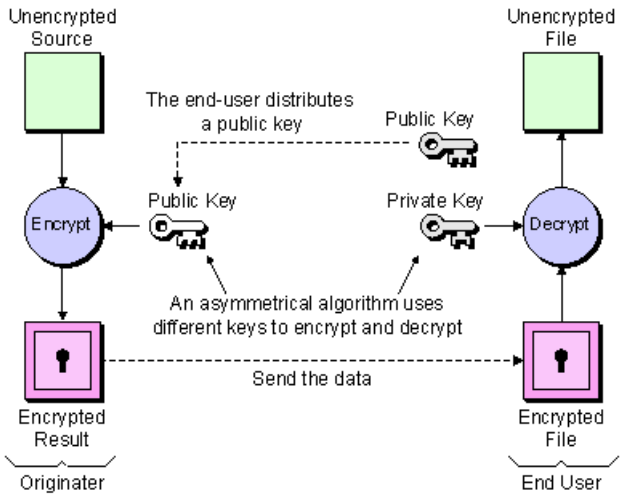


Figura 6.2: Criptografía de llave pública.[50]

Los pasos fundamentales de la criptografía de clave pública son:

[48]DIFFIE, W., HELLMAN., M.E. New directions in cryptography. IEEE Transactions on Information Theory, vol. IT-22. 1976, pp:644-654, 29 de noviembre de 2008.

[49]WILLEMS, W., GUTIERREZ, I. Introducción a la Criptografía de Clave Pública. 30 de noviembre de 2008.

[50]Tomado de `http://www.chipdesignmag.com/images/idesign/misc/chips040207_figure2.gif`, 30 de noviembre de 2008.

1. Cada usuario genera una pareja de claves para el cifrado y para el descifrado de mensajes.

2. Cada usuario localiza una de las dos claves en un servidor público. Esta es la clave pública. La otra clave no se revela, de igual manera cada usuario, mantiene un grupo de claves públicas que ha obtenido de otros.

3. Si Bob quiere enviar un mensaje M privado a Alice, cifra el mensaje usando la clave publica de Alice.

4. Cuando Alice recibe el mensaje cifrado C, lo descifra usando su calve privada.

Ningún otro receptor puede descifrar el mensaje porque sólo Alice conoce su clave privada.

Para un usuario que utiliza un criptosistema de clave pública se deben cumplir las siguientes condiciones desde un punto de vista computacional:

1. Es fácil para un usuario generar una pareja de claves (clave publica y clave privada).

2. Para un emisor A que conozca la clave publica, y el mensaje x que ha de cifrarse, es fácil general el texto cifrado correspondiente, esto es

$$e_B(M) = C.$$

3. Para un receptor es fácil descifrar el texto cifrado resultante usando la clave privada para recuperar el mensaje original, es decir

$$d_B(e_B(M)) = M.$$

4. Es infactible que un oponente, conociendo la clave publica, pueda llegar a determinar la clave privada.

5. Es infactible que un oponente, conociendo la clave publica, y un texto cifrado, pueda llegar a recuperar un texto original.

Dependiendo de la aplicación el emisor usa su clave privada o la clave publica del receptor, o las dos, estos procedimientos clasifican a los criptosistemas de clave publica en tres categorías:

- **Cifrado/Descifrado:** el emisor cifra un mensaje con la clave publica del receptor.

- **Firma Digital:** El usuario Bob quiere enviar un mensaje a Alice y, aunque no es necesario que el mensaje se mantenga en secreto, quiere que Alice se asegure que el mensaje, efectivamente proviene de él. En este caso Bob utiliza su propia clave privada para cifrar el mensaje. Cuando Alice recibe el texto cifrado, se encuentra con que puede descifrarlo con la clave publica de Bob, demostrando así que el mensaje ha debido de ser cifrado por él. Nadie más tiene la clave privada de Bob

y, por tanto, nadie mas ha podido crear un texto cifrado que pueda ser descifrado con su clave publica. Por consiguiente el mensaje sirve como firma digital. Además es imposible alterar el mensaje sin acceso a la clave de Bob, así que el mensaje queda autentificado tanto en lo que respecta a la fuente como a la integridad de los datos.

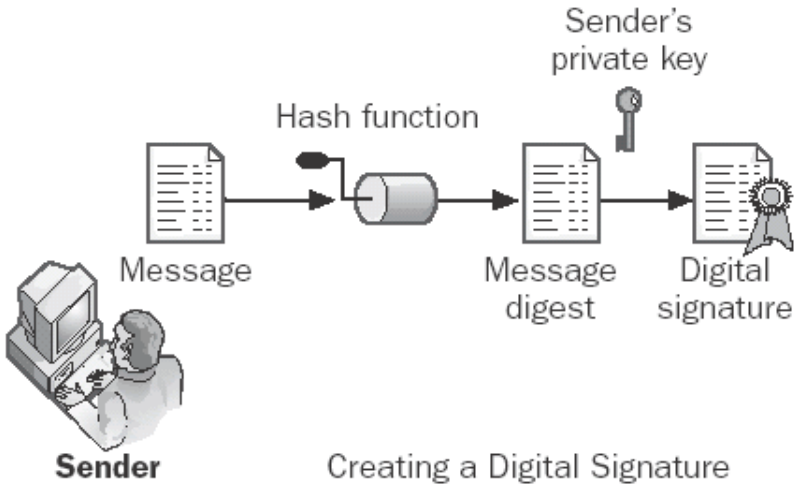


Figura 6.3: Firma digital.[51]

- **Intercambio de claves:** Dos partes cooperan para intercambiar una clave de sesión. Hay distintas posibilidades que implican la clave privada de una o de las dos partes.[52]

6.2. Algoritmos criptografícos

Los algoritmos utilizados en criptosistemas de clave publica basan su seguridad esencialmente en problemas matemáticos computacionalmente intratables como lo son el calculo del logaritmo discreto y la factorización de números primos grandes.

6.2.1. Factorización

Sea $n \geq 2$ un entero y $n = pq$, factorización consiste en hallar los factores p y q de n. Para números grandes, en general, no es posible calcular en un tiempo justificable su descomposición en factores primos.

[51]Tomado de `http://www.microsoft.com/mspress/books/sampchap/6429/0-7356-1877-3.gif`, 30 de noviembre de 2008.

[52]Diffie W. and Hellman M.E: New directions in cryptography. IEE Trans. Inform. Theory, 1976.

6.2.2. Logaritmo discreto

Sea $(G, \cdot)$ un grupo multiplicativo, $\alpha \in G$ un elemento de orden n y $\beta \in \langle\alpha\rangle$. El logaritmo discreto consiste en hallar un único entero ρ, $0 \leq \rho \leq n-1$, tal que:

$$\alpha^{\rho} = \beta.$$

Se tiene que $\rho = \log_{\alpha} \beta$ es llamado el logaritmo discreto.

6.3. Procedimiento RSA

Fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Len Adleman, en MIT[53] y se basa en la factorización de números grandes, para algún texto claro M y un texto cifrado C, el cifrado y el descifrado son de la siguiente forma:

Algoritmo 6.1 Generación claves para RSA

1: Seleccionar números primos p, q, $p \neq q$
2: $n = pq$
3: $\phi(n) \leftarrow (p-1)(q-1)$
4: Seleccionar e tal que $mcd(\phi(n), e) = 1$, con $1 < e < \phi(n)$
5: $d \leftarrow e^{-1}$ mód $\phi(n)$
6: La clave publica es (e, n)
7: La clave privada es (d, n)

Algoritmo 6.2 Cifrado RSA

INPUT: Texto plano M con longitud menor n
OUTPUT: Texto cifrado C
1: $C = M^e$ mód n
2: **return** C

Algoritmo 6.3 Descifrado RSA

INPUT: Texto cifrado C
OUTPUT: Texto descifrado M
1: $M = C^d$ mód n
2: **return** M

Tanto el emisor como el receptor deben conocer los valores de n y e. Solo el receptor conoce el valor de d, para que este algoritmo sea satisfactorio se deben cumplir con los siguientes requisitos:

[53] RIVEST, R., SHAMIR, A., ADLEMAN, L. A Method for Obtaining Digital Signatures and Public Key Cryptosistems. Communications of the ACM 21, 1978, 120-126, 29 de noviembre de 2008.

1. Que sea posible encontrar valores de e, d y n tal que $M^{ed} = M$ mód n para todo $M < n$.

2. Que sea relativamente fácil calcular M^e y C^d para todos los valores de $M < n$.

3. Que sea imposible determinar d dados e y n.

Los dos primeros requisitos se cumplen fácilmente. El tercero se puede cumplir para valores grandes de e y n.

Ejemplo. 6.3.1 .

1. *Seleccionar dos números primos* $p = 17$ *y* $q = 11$.

2. $n = 17 \times 11$.

3. $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.

4. *Seleccionar* e *tal que sea primo relativo de* $\phi(n)$ *y menor que* $\phi(n)$, *se elige* $e = 7$.

5. *Determinar* d *tal que de* mód $160 = 1$ *y* $d < 160$. *El valor correcto es* $d = 23$, *por que* $23 \times 7 = 161$.

Las claves resultantes son: Clave privada $(7, 187)$. *Clave publica* $(23, 187)$. *Para un texto claro* $M = 88$, *el texto es cifrado teniendo en cuenta las propiedades de la aritmética modular de la siguiente manera:*

$$\begin{aligned}
88^7 \text{ mód } 187 &= [(88^4 \text{ mód } 187)(88^2 \text{ mód } 187)(88 \text{ mód } 187)] \text{ mód } 187 \\
88 \text{ mód } 187 &= 88 \\
88^2 \text{ mód } 187 &= 7744 \text{ mód } 187 = 77 \\
88^4 \text{ mód } 187 &= 59969536 \text{ mód } 187 = 132 \\
88^7 \text{ mód } 187 &= 88 \times 77 \times 132 \text{ mód } 187 = 11
\end{aligned}$$

Se tiene entonces que $C = 11$. *Para descifrar* $C = 11$ *se calcula* $M = 11^83$ mód 187.

$$\begin{aligned}
11^23 \text{ mód } 187 &= [(11 \text{ mód } 187)(11^2 \text{ mód } 187)(11^4 \text{ mód } 187)(11^8 \text{ mód } 187)(11^8 \text{ mód } 187)] \text{ mód } 187 \\
11 \text{ mód } 187 &= 11 \\
11^2 \text{ mód } 187 &= 121 \\
11^4 \text{ mód } 187 &= 14641 \text{ mód } 187 = 55 \\
11^8 \text{ mód } 187 &= 214358881 \text{ mód } 187 = 33 \\
11^23 \text{ mód } 187 &= (11 \times 121 \times 55 \times 33 \times 33) \text{ mód } 187 = 88
\end{aligned}$$

6.4. Procedimiento ElGamal

Creado por Taher Elgamal en 1984 con licencia GNU, lo que lo hace de uso libre, utilizado en GNU privacy guard, en versiones recientes de PGP, y otros sistemas criptográficos. Este algoritmo esta basado en el problema del Logaritmo Discreto en $(\mathbb{Z}_p, \cdot)$.

Sea p un número primo tal que el problema del Logaritmo Discreto en $(\mathbb{Z}_p^*, \cdot)$ sea intratable. Sea K el conjunto de posibles claves, y sea $\alpha \in mathbbZ_p^*$ un elemento primitivo. Se define:

$$K = \{(p, \alpha, a, \beta) | \beta \equiv \alpha^a \text{ mód } p.\}$$

Los valores p, α y β, son la clave pública y a es la clave privada.

Para un $k \in K$ y un número aleatorio secreto $n \in \mathbb{Z}_{p-1}$, se define

$$e_B(y_1, y_2)$$

donde

$$y_1 = \alpha^n \text{ mód } p$$

y

$$y_2 = x\beta^n \text{ mód } p.$$

La función de descifrado esta dada por

$$d_B(y_1, y_2) = y_2(y_1^a)^{-1} \text{ mód } p.$$

Ejemplo. 6.4.1 *Dados $p = 2579$, $\alpha = 2$, $a = 765$, entonces $\beta = 2^{765}$ mód $2579 = 949$*

Ahora Alice desea enviar el mensaje $x = 1299$ a Bob. Sea $n = 853$ el entero aleatorio seleccionado por Alice, entonces ella debe computar:

$$\begin{aligned} y_1 &= 2^{853} \text{ mód } 2579 \\ &= 453 \end{aligned}$$

y

$$\begin{aligned} y_2 &= 1299 \times 949^{853} \text{ mód } 2579 \\ &= 2396. \end{aligned}$$

Cuando Bob reciba el texto cifrado $y = (435, 2396)$, el debe computar:

$$\begin{aligned} x &= 2396(435^{765})^{-1} \text{ mód } 2579 \\ &= 1299 \end{aligned}$$

Claramente se pude observar que el ciptosistema ElGamal seria inseguro si un enemigo pudiera calcular el valor $a = \log_\alpha \beta$.

6.5. Ataques al logaritmo discreto

En esta sección se asume que G es un grupo multiplicativo y $\alpha \in G$ tiene orden n. Por lo tanto el problema del Logaritmo Discreto se puede expresar de la siguiente manera, dado $\beta \in \langle\alpha\rangle$, encontrar el único exponente a, $0 \leq a \leq n-1$, tal que $\alpha^a = \beta$.

Algoritmo de Shanks

Este algoritmo realiza una búsqueda exhaustiva de $a = \log_\alpha \beta$ mód n. Para cualquier $\beta \in \langle\alpha\rangle$, se tiene que a, $0 \leq \log_\alpha \beta \leq n-1$, luego, los pasos 2 y 3 se pueden precalcular. Obsérvese que si $(j, y) \in L_1$ y $(j, y) \in L_2$ entonces $\alpha^{mj} = y = \beta\alpha^{-i}$, es decir $\alpha^{mj+i} = \beta$. Dividiendo $\log_\alpha \beta$ por un entero m se tiene que

$$\alpha^{mj+i} = \beta = mj + i, \text{ donde } 0 \leq i, j \leq m-1$$

debido a que $\log_\alpha \beta leqn - 1 \leq m^2 - 1 = m(m-1) + m - 1$.

Por lo tanto la búsqueda en el paso 6 es acertada, si esto no sucede se debe a $\beta \notin \langle\alpha\rangle$.

Ejemplo. 6.5.1 *Encontrar* $\log_3 525$ *en* $\mathbb{Z}_{809}$*, note que* 809 *es primo y que* 3 *es un elemento primitivo en* $\mathbb{Z}_{809}$*, con* $\alpha = 3$*,* $n = 808$*,* $\beta = 525$ *y* $m = \mid \sqrt{808} \mid = 29$*, entonces*

$$\alpha^2 9 \text{ mód } 809 = 99.$$

Primero se computan los pares ordenados $(j, 99^j \text{ mód } 809) = 99$ *para* $0 \leq j \leq 28$ *obteniendo la siguiente lista:*

$$(0,1)(1,99)(2,93)(3,308)(4,559)$$
$$(5,329)(6,211)(7,664)(8,207)(9,268)$$
$$(10,644)(11,654)(12,26)(13,147)(14,800)$$
$$(15,727)(16,781)(17,464)(18,632)(19,275)$$
$$(20,528)(21,496)(22,564)(23,15)(24,676)$$
$$(25,586)(26,575)(27,295)(28,81).$$

La segunda lista contiene los pares ordenados $(i, 525(3^i)^{-1} \text{ mód } 809)$.

$$(0,525)(1,175)(2,328)(3,379)(4,396)$$
$$(5,132)(6,44)(7,554)(8,724)(9,511)$$
$$(10,440)(11,686)(12,768)(13,256)(14,355)$$
$$(15,388)(16,399)(17,133)(18,314)(19,644)$$
$$(20,754)(21,521)(22,713)(23,777)(24,259)$$
$$(25,356)(26,658)(27,489)(28,163)$$

Nótese que $(10,644)$ *esta en* L_1 *y* $(19,644)$ *esta en* L_2*, entonces por el paso 6 se puede computar:*

$$\log_3(525) = (29 \times 10 + 19) \text{ mód } 808 = 309$$

Side channel attack

Este ataque toma ventaja del hecho, de que el dispositivo criptográfico presenta escapes de información física durante el proceso de un algoritmo criptográfico. Estos escapes (disipación de energía, información del tiempo de un algoritmo, emanación electromagnética, y ruido) pueden ser capturados exteriormente y utilizados para comprometer claves secretas de algoritmos criptográficos con la ayuda de herramientas estadísticas. Generalmente todos los algoritmos criptográficos son vulnerables al Side Channel Attack si no se tienen consideraciones especiales a la hora de la implementación. Casos generales de Side channel attack incluyen:

- **Timing attack:** ataques basados en el tiempo de ejecución del algoritmo criptográfico, calcula el tiempo que se demora la CPU en transferir las claves, con esto se podría calcular la longitud de las claves.
- **Power monitoring attack:** ataque basado en el análisis de de energía consumido por el hardware mientras se ejecuta un procedimiento criptográfico.
- **TEMPEST (radiation monitoring):** ataque basado en el escape de radiación electromagnética del hardware.
- **Acoustic cryptanalysis:** ataque basado en la emanación de sonido mientras se ejecuta un procedimiento criptográfico, se podría analizar acústicamente el sonido generado electrónicamente al digitar una tecla, logrando saber que tecla fue utilizada.

Contramedidas
Debido a que el Side Channel Attack se basa esencialmente en los escapes de información física, es notorio que para mejorar la seguridad de una implementación criptográfica se deben utilizar materiales de alta calidad y con protección electromagnética. Otra contramedida es llenar el canal con ruido, sea señal sonora o electromagnética y por supuesto la seguridad física, así se evitan la instalación de micrófonos y censores de radiación.

6.6. Criptografía de curva elíptica

La criptografía de curva elíptica (CCE) es de cierta forma criptografía de clave publica. En la criptografía de clave publica cada usuario o el dispositivo criptográfico generalmente posee un par de claves, una clave publica y una clave privada, y un conjunto de operaciones relacionadas con las claves para realizar procedimientos criptográficos. Cada usuario en particular conoce su clave privada mientras que la clave publica se distribuye a todos los usuarios que tendrán parte en la comunicación, algunos algoritmos de clave publica podrían requerir un conjunto predefinido de constantes conocidas por todos los dispositivos que tendrán parte en la comunicación. En la CCE los parámetros de dominio son un ejemplo de estas constantes. Las operaciones matemáticas de la CCE se definen sobre la curva $y^2 = x^3 + ax + b$, donde $4a3 + 27b2 \neq 0$. Cada valor de a y b generan una curva elíptica. Todos los puntos (x,y) que satisfagan la condición anterior, mas el punto al infinito pertenecen a la curva elíptica. La clave publica es un punto sobre la curva y la clave privada es un número aleatorio. La clave publica es obtenida de multiplicar la clave privada con el punto generador G de la curva, los parámetros de la curva a y b, junto con otras constantes constituyen los parámetros de dominio de la CCE. Como se puede observar en la imagen, una de las ventajas de CCE es el uso de

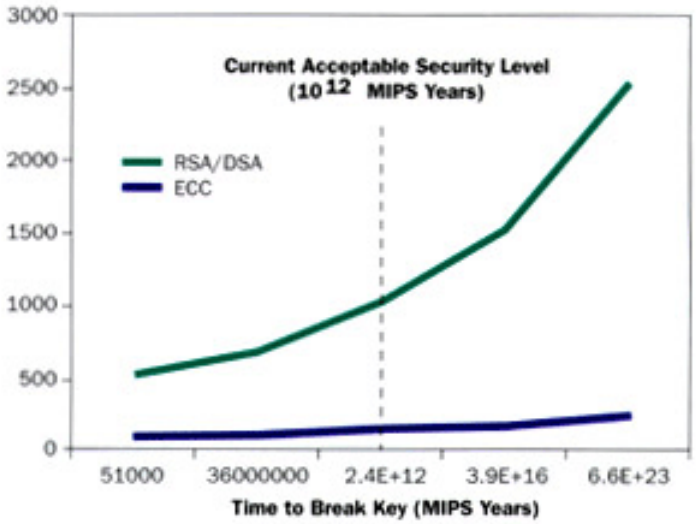


Figura 6.4: RSA vs ECC.[54]

claves pequeñas, una clave de 160 bits en la CCE se considera tan segura como una de 1024 bits en RSA.

La seguridad de la CCE depende de la dificultad del problema del logaritmo discreto sobre curva elíptica. Sea P y Q dos puntos sobre una curva elíptica, tales que $kp = Q$, donde k es un escalar. Dados P y Q, es computacionalmente intratable en un tiempo razonable hallar el valor de k, si k es lo suficientemente grande, entonces, k es el logaritmo discreto de Q a la base P. Por esta razón la operación mas importante de la CCE es la multiplicación de un punto por un escalar.

[54]Tomado de `http://www.codeproject.com/KB/security/ECIESProductKey/image003.gif`, 28 de noviembre de 2008.

Capítulo 7

CONCLUSIONES

La operación mas importante de la criptografía de curvas elípticas es la multiplicación escalar o de puntos. Esta operación consiste en sumar k veces un punto P de la curva. Para lograr una mayor seguridad la curva debe ser de mas bits pero esto implica que el tiempo necesario para realizar las operaciones se incremente, por lo cual es de suma importancia realizar métodos mas eficientes que mantengan el mismo nivel de seguridad sin disminuir el desempeño, o por lo menos que el cambio no sea tan notorio para un usuario final.

Dentro de las curvas elípticas binarias existen dos curvas especiales, llamadas curvas de Koblitz, con la particularidad de poder realizar métodos eficientes para realizar las operaciones necesarias dentro de la criptografía de curva elíptica.

Para poder lograr realizar métodos mas eficientes es importante tener bases claras, es decir todo el fundamento teórico que implica la criptografía de curvas elípticas, porque es ahí donde nacen los métodos que aprovechan las facultades de las curvas, como es el caso de la multiplicación escalar por medio del endomorfismo de Frobenius.

Además de lo anterior, también es necesario implementar cada detalle de manera eficiente, esto incluye la aritmética de los cuerpos finitos, el uso de coordenadas con métodos eficientes para las operaciones de puntos, precomputaciones, etc. Cada paso juega un papel importante al momento de desarrollar métodos eficientes, que no se podrían optimizar al no tener como base la teoría matemática que implica la criptografía y las curvas elípticas.

Bibliografía

[1] ANDERSON, M., FEIL, T. A First Course in Abstract Algebra. Chapman & Hall/CRC, 2005, 2ed., 673p.

[2] AVANZI, R., CIET, M. Faster Scalar Multiplication on Koblitz Curves combining Point Halving with the Frobenius Endomorphism. `http://caccioppoli.mac.rub.de/website/papers/taumachin.pdf`, 14p, Diciembre 8 de 2008.

[3] AVANZI, R., COHEN, H., DOCHE, C., FREY, G., LANGE, T., NGUYEN, K., VERCAUTEREN, F. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2005, 848p.

[4] AVANZI, R., HEUBERGER, C., PRODINGER, H. Minimality of the Hamming Weight of the τNAF for Koblitz Curves and Improved Combination with Point Halving. `http://eprint.iacr.org/2005/225.pdf`, 15p, Diciembre 8 de 2008.

[5] CAICEDO, J. Teoría de Grupos. Universidad Nacional de Colombia, 2004, 169p.

[6] CRUZ, J. Multiplicación Escalar en Curvas de Koblitz: Arquitectura en Hardware Reconfigurable. `http://delta.cs.cinvestav.mx/~francisco/tesis_JMCA.pdf`, 143p, Diciembre 8 de 2008.

[7] DAHAB, R., LÓPEZ, J. An Overview of Elliptic Curve Cryptography, Technical Report IC - 00 - 10. Relatório Técnico, 2000.

[8] FONG, K., HANKERSON, D., LÓPEZ, J., MENEZES, A. Field Inversion and Point Halving Revisited. Technical Report CORR 2003 - 18. Department of Combinatorics and Optimization, Canada: 2003.

[9] GUTIERREZ, I. Notas de Clase - Electiva-Criptografía (Pre-impresión). 2008.

[10] HANKERSON, D, MENEZES, A, VANSTONE, S. Guide to Elliptic Curve Cryptography. Springer - Verlag, 2004, 1ed., 311p.

[11] HOWIE, J. Fields and Galois Theory. Springer, 2006, p227.

[12] HUNGERFORD, T. Algebra. Springer Verlag, 2003 (Quinta Impresión), 1ed., 528p.

[13] HUSEMÖLLER, D. Elliptic Curves. Springer - Verlag, 2003, 2ed., 487p.

[14] KOBLITZ, N. A Course in Number Theory and Cryptography. Springer - Verlag, 2001, 2ed., 235p.

[15] KOBLITZ, N. Algebraic Aspects of Cryptography. Springer - Verlag, 2004, 206p.

[16] KRAMER, D., WELSCHENBACH, M. Cryptography in C and C++. Apress, 2001, 432p.

[17] KNUDSEN, E. Elliptic Scalar Multiplication using Point Halving. Advances in Cryptology - ASIACRYPT, 1999 (LNCS 1716). Berlín: Springer - Verlag, 1999, 135 - 149.

[18] MENEZES, A., VAN OORSCHOT, P., VANSTONE, S. Handbook of Applied Cryptography. CRC Press, 1996, 1ed., 816p.

[19] MURPHY, T. TRINITY COLLEGE Course 373 Finite Fields. `http://www.maths.tcd.ie/pub/Maths/Courseware/373-2000/FiniteFields.pdf`, 79p, Noviembre 15 de 2008.

[20] SHOUP, V. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005, 534p.

[21] SILVERMAN, J., TATE, J. Rational Points on Elliptic Curves. Springer, 2000, 281p.

[22] SMITH, G., TABACHNIKOVA, O. Topics in Group Theory. Springer, 2000, 255p.

[23] SOLINAS, J. Efficient Arithmetic on Koblitz Curves. Designs, Codes and Cryptography, 19,195-249 (2000). Kluwer Academic Publishers, 2000, 195 - 249.

[24] TRAPPE, W., WASHINGTON, L. Introduction to Cryptography with Coding Theory. Prentice Hall, 2005, 2ed., 592p.

[25] WASHINGTON, L. Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC, 2008, 2ed., 513p.

[26] WILLEMS, W., GUTIERREZ, I. Introducción a la Criptografía de Clave Pública. Ediciones Uninorte, 2008, 83p.